

Inhaltsverzeichnis

Seitenkanalattacken	02
Dezentrale Autonome Organisation (DAO)	04
NFTs: Eine Revolution in der digitalen Kunst?	08
Palantir in deutschen Polizeibehörden	11
Predator	12
Was sind Kryptowährungen?	15
Zahlungsdienstleister	20
Was ist ein Token?	23
Open-Source-Datenbanken	28
Datenbanken – Was ist ACID?	31
Border Gateway Protocol (BGP)	34
Quishing – Betrug mit dem QR-Code.....	36
Starlink - Internet aus dem Weltall	39
Shadow Banning bei TikTok & Co.	44
Rechenzentren - Konzeption, Aufbau und Security	47
Rechenzentren – Tier-Standards und Datensicherheit	82
Exploit - EternalBlue	91
Spracheingabe unter Windows	94
Was sind Lootboxen?	97
Was ist eine Spine-Leaf-Architektur?	99
Was ist eine Hub-and-Spoke-Architektur?	104
Was ist ein Metaversum?	107
Virtuelle Grundstücke im Metaverse	109
Telegram- Privatsphäre und Sicherheit	112
Suchmaschine für Geräte und Maschinen	115
Was sind NoSQL-Datenbanken?	118
Grundlagen zur Normalisierung von Datenbanken	125
Bildersuche mittels einer Suchmaschine	135
Spionage durch Smart-TV's?	139
Darknet-Suchmaschine Memex	146
Arbeitsgruppe Kritische Infrastrukturen (AG KRITIS)	150
Was ist Cybergrooming?	151
Saugroboter und Co.	155

UNDER CONSTRUCTION

Staatstrojaner – Einsatz und Erkennung	xx
Was ist über die verwendeten Algorithmen einiger	
Suchmaschinen bekannt?	xx
Online-Partnervermittlungen und ihre Algorithmen	xx
Datenschutz beim Video-Chat (Zoom, Skype)	xx
Datensicherheit im DarkNet (Onion)	xx
Streamingwebseiten - Odyssee, Peertube, Youtube	xx
Cell Broadcast: Warnstufe 1 bis 5	xx
Netzwerk-Kollisionen: Was sind die Unterschiede bei	
Kabel und WLAN?	xx
Künstliche Intelligenz und Chat GPT	xx
Gibt es sichere Smartphone's (Bittium Corporation)?	xx
Datensicherheit: Solarparks und Windkraftanlagen (kritische	
Infrastruktur)	xx
Fake Shop Finder	xx
Übersetzungsprogramm DeepL App	xx
Gesetze zur künstlichen Intelligenz (KI, AI)	xx
HAMNET - Funknetz in Deutschland	xx
CyberAttacken – Software der Firma NTC Vulkan (HTC	
ВУПКАН)	xx
Deep Fake - Anzeichen für Fälschungen	xx
Polizei-Software Autopsy	xx
Satelliten - Aufnahme in die kritische Infrastruktur	xx
Datensicherheit - Smarthome Computer, Saugroboter,	
Protokoll-Familie für Bluetooth	xx

Seitenkanalattacken 1/2

Allgemeines

Der Begriff Seitenkanalattacke (Side-channel attack; korrekter übersetzt, aber unüblich: Nebenkanal-Angriff) bezeichnet eine kryptoanalytische Angriffs- oder Hacking-Methode, bei der die zu schützenden Algorithmen, technischen Systeme oder Daten indirekt angegriffen werden. Die Angriffsmethode nutzt physische oder logische Nebeneffekte der Systeme und versucht durch deren Beobachtung und Analyse Informationen über das tatsächliche Angriffsziel zu erhalten. Geprägt hat den Begriff Side-Channel Attack der amerikanische Kryptologe Paul C. Kocher im Jahr 1996.

Seitenkanalangriffe können passiv oder aktiv erfolgen. Typische Methoden der Angriffe sind Messungen physikalischer Größen beispielsweise des Stromverbrauchs, der elektromagnetischen Abstrahlung oder der Wärme. So lässt der Stromverbrauch Rückschlüsse auf die aktuelle Rechenleistung und die durchgeführten Operationen eines Prozessors zu. Weitere Methoden messen die Zeit, die ein System für die Ausführung einer bestimmten Aktion benötigt oder sie analysieren die Speichernutzung einzelner Prozesse. Seitenkanalangriffe sind oft komplex und aufwendig. Sie benötigen meist viele Einzeldurchläufe, um verwertbare Informationen zu gewinnen.

Die in der Vergangenheit veröffentlichten Hardware-Sicherheitslücken von Mikroprozessoren basierten auf Nebenkanalangriffen und nutzen Timing-Methoden, um unautorisierten Zugriff auf Speicher fremder Prozesse zu erhalten. Seitenkanalattacken sind schwer zu verhindern und Gegenmaßnahmen können aufwendig sein.

Besonders kritisch zu sehen sind Informationslecks, wenn Verschlüsselungssoftware angegriffen wird und die geheimen oder privaten Schlüssel entwendet werden können.

Die verschiedenen Methoden der Seitenkanalattacken

Grundsätzlich lässt sich zwischen aktiven und passiven Seitenkanalattacken unterscheiden. Passive Methoden versuchen durch reine Beobachtung der Nebeneffekte, Zugriff auf schützenswerte Informationen oder Objekte zu erhalten.

- Ein Beispiel einer passiven Methode ist die Analyse einer Tastatur mit einer Wärmebildkamera, um durch die von den Fingern auf die Tastatur abgestrahlte Wärme, auf die eingegebenen Passwörter oder PINs zu schließen.
- Aktive Angriffsmethoden greifen in den Ablauf oder die Funktion eines Geräts ein, indem sie beispielsweise eine Fehleingabe machen oder das System zur Ausführung einer bestimmten Funktion auffordern.



Seitenkanalattacken 2/2

- Durch Beobachtung und Analyse der Reaktion des Geräts oder des Systems wie das Messen der Zeit bis zur Ausgabe einer Meldung sind Rückschlüsse auf die Funktionsweise und den verwendeten Algorithmus möglich.

Typische aktive und passive Methoden für Seitenkanalattacken sind:

- Timing-Angriff: Messung der Rechenzeit bei der Ausführung bestimmter Funktionen; Systeme benötigen leicht unterschiedliche Ausführungszeiten, um unterschiedliche Eingaben zu verarbeiten; durch Laufzeitanalysen können Informationen nach und nach rekonstruiert werden; Timing Attacks sind sowohl gegen Chipkarten als auch gegen Software-Implementierungen bereits veröffentlicht worden (Rechenzeitangriff oder auch Timing-Attack)
- Erfassung und Analyse der Wärmeabstrahlung
- Erfassung und Analyse der Schallabstrahlung; eine Analyse der Betriebsgeräusche eines Computers, mithilfe von Mikrofone, kann zur Extraktion von Informationen und Daten verwendet werden
- Messung und Analyse des Energieverbrauchs von Prozessoren; der Stromverbrauch liefert Hinweise auf die aktuelle Rechenleistung und die durchgeführten Operationen eines Prozessors (SPA oder Simple Power Analysis, DPA oder Differential Power Analysis)
- Messung und Analyse der elektromagnetischen Abstrahlung; die von einem Rechner oder Gerät bei Berechnungen erzeugten elektromagnetischen Felder lassen sich oft noch in einiger Entfernung messen und erlauben ebenfalls Rückschlüsse auf die durchgeführten Operationen (tempest, wörtlich übersetzt: Gewitter, heftiger Sturm)

- Beobachtung und Analyse der Reaktion auf Falscheingaben; Implementierungen reagieren auf falsche Eingaben unterschiedlich, abhängig davon, an welcher Stelle der Verarbeitung ein Fehler auftritt (DFA oder Differential Fault Analysis, Glitch-Attack); eine Glitch-Attack (Störimpuls-Angriff) ist eine Methode, um einen Kryptoprozessor zu kompromittieren, indem man die Ausführung von Maschinenbefehlen unterbricht
- die Ausnutzung fehlerhaft implementierter Funktionen (Bug-Attack)
- Auswertung der Speichernutzung; wenn sich Prozesse auf einem Rechner Speicherbereiche teilen, kann man aus der Nutzung des Speichers durch einen anderen Prozess auf die durchgeführten Operationen schließen

Schutzmaßnahmen gegen Seitenkanalattacken

Der Schutz vor Seitenkanalattacken ist aufwendig und schwierig. Gegenmaßnahmen wirken in der Regel nur gegen eine Angriffsmethode. Die Attacken basieren aber häufig auf der Beobachtung und Analyse mehrerer Kanäle. Typische Maßnahmen gegen Seitenkanalangriffe sind:

- elektromagnetische Abschirmung der Geräte (z.B. Bildschirme)
- physikalische Maßnahmen gegen Schall- und Wärmeabstrahlung
- Angleichung von Laufzeiten unterschiedlicher Prozesse durch Einfügen von Redundanzen
- Erzeugen von Laufzeiten, die von Zufallsfunktionen abhängig sind
- Einfügen von physikalischen und logischen Rauschfunktionen
- eingabeunabhängige Ausführung von Programmcode
- identische Reaktionen auf fehlerhafte Eingaben

Hinweis: Einige Forschergruppen entwickeln bereits Schutzverfahren und Werkzeuge für den Nachweis von Seitenkanalattacken.

Dezentrale Autonome Organisation (DAO) 1/4

Was sind DAOs?

Eine DAO (Decentralized Autonomous Organization) ist eine kollektiv geführte und durch die Blockchain verwaltete Organisation, die auf eine gemeinsame Mission hinarbeitet. DAOs sind dadurch vor allem bei jungen Unternehmen (Startups) beliebt. Das Management wird zwar nicht vollständig überflüssig, da die Kontrolle über das DAO-Unternehmen weitestgehend von den in den Programmcode eingebauten Regeln und von der Gesamtheit der Anteilseigner übernommen wird.

DAOs ermöglichen es, mit Gleichgesinnten rund um den Globus zusammenzuarbeiten, ohne das Vertrauen in das Wohlwollen einer Führungskraft setzen zu müssen, die die Fonds oder Operationen verwaltet. Es gibt keinen Geschäftsführer, der Geld nach Lust und Laune ausgeben kann, und keinen Finanzchef, der die Buchhaltung manipulieren kann. Stattdessen bestimmen in den Code eingebaute Blockchain-basierte Regeln (Quellcode-Implementierung: Prozesse, Belohnungen und Regeln), wie die Organisation arbeitet und wie die Mittel ausgegeben werden. Die Finanzverwaltung ist integriert und niemand kann ohne die Zustimmung der Gruppe darauf zugreifen.

Entscheidungen werden durch Vorschläge und Abstimmungen geregelt, um sicherzustellen, dass jeder in der Organisation ein Mitspracherecht hat, und dies alles geschieht autonom entsprechend der Blockchain-basierten Regeln transparent.

Warum brauchen wir DAOs?

Ein Unternehmen gemeinsam mit anderen Personen zu gründen und dafür Gelder und Finanzierungsmöglichkeiten bereitzustellen, benötigt viel Vertrauen in die Menschen, mit denen man arbeiten möchte. Doch es ist alles andere als leicht, jemandem zu vertrauen, den man nur über das Internet kennt. *Mit DAOs muss man anderen in der Gruppe nicht vertrauen, sondern nur dem quelloffenen DAO-Code, der vollständig transparent und für jeden einsehbar ist*



(deutliche Programmier-Kenntnisse vorausgesetzt). Das eröffnet viele neue Möglichkeiten für die globale Zusammenarbeit und Koordination.

DAO - ein herkömmliches Unternehmen?

Die DAO ist kein herkömmliches Unternehmen. Es hat sogar keinen realen Firmensitz und es existiert nur virtuell auf vielen Rechnern, welche als Nodes (Knoten, Rechner) in der Blockchain eingebunden sind. Technisch betrachtet ist eine DAO eine Sammlung an implementierten Smart Contracts in der Blockchain. Smart Contracts sind quelloffene Programmcodes, in dem die Vertragsbedingungen hinterlegt sind. Anhand dieser werden Verträge völlig automatisiert durchgeführt bzw. überwacht. Diese Verträge (Smart Contracts) in der Blockchain übernehmen Funktionen, welche sonst den Managern zustanden. Der Smart Contract ist damit das Rückgrat einer DAO. DAOs werden im Allgemeinen als Smart Contracts der komplexesten Form bezeichnet.

Damit zeichnen sich zwei Entscheidungsformate in der DAO ab: Zum

Dezentrale Autonome Organisation (DAO) 2/4

einen die hart-programmierten Regeln der Smart Contracts zum Beispiel für die Höhe der Ausschüttungen und zum anderen die Abstimmungen der Anteilseigner über die Projekte.

- DAOs besitzen in der Regel flache Strukturen und sind vollständig demokratisiert (Voraussetzung: hohe Wahlbeteiligung bei allen Abstimmungen)
- in DAOs ist die Abstimmung durch die Gruppe erforderlich, um Veränderungen zu implementieren
- Veränderungen können je nach Struktur durch einzelne Parteien verlangt oder durch offene Abstimmungen beschlossen werden
- alle Aktivitäten sind transparent und vollständig öffentlich für die Mitglieder
- Aktivitäten sind normalerweise unternehmensintern, mit einer begrenzten Einsicht für die Öffentlichkeit
- angebotene Dienste werden automatisch auf dezentrale Weise abgewickelt

Beispiele für DAOs:

- Wohltätigkeitsorganisation - DAOs können von jedem auf der Welt Spenden annehmen und darüber abstimmen, welche Zwecke damit finanziert werden sollen.
- Kollektives Eigentum - DAOs können physische oder digitale Vermögenswerte erwerben und die Mitglieder können über deren Verwendung abstimmen.
- Unternehmen und Zuschüsse: DAOs können Risikofonds gründen, der Investitionskapital bündelt und über die zu unterstützenden Unternehmen abstimmen. Das zurückgezahlte Geld kann später unter den DAO-Mitgliedern neu verteilt werden.

Wie funktionieren DAOs?

Das Fundament einer DAO ist ihr Smart Contract, der das Regelwerk der Organisation festhält und die Schatzkammer verwaltet. Sobald ein Smart Contract auf Ethereum (Kryptowährung) aktiv ist, können die Regeln ausschließlich per Abstimmung geändert werden. Vorgänge,

die nicht durch die Regeln und Logik des Codes (der Code ist »Gesetz«) abgedeckt sind, schlagen fehl. Da auch die Finanzverwaltung durch den Smart Contract definiert ist, kann niemand das Geld ohne die Zustimmung der Gruppe ausgeben. Daher benötigen DAOs keine zentrale Instanz. Stattdessen trifft die Gruppe gemeinsam Entscheidungen, wobei Zahlungen bei positiver Abstimmung automatisch genehmigt werden. Möglich wird dies durch die Manipulationssicherheit veröffentlichter Smart Contracts.

Da alle Vorgänge für die Mitglieder öffentlich sind, sind unbemerkte Änderungen am Code (also den Regeln der DAO) unmöglich.

Ethereum (ETH) eine brauchbare Plattform für DAOs

- Der Ethereum-eigene Konsens ist so weit verbreitet und etabliert, dass Unternehmen dem Netzwerk vertrauen können.
- Der Code eines Smart Contracts kann nach seiner Veröffentlichung nicht mehr geändert werden, auch nicht von seinen Eigentümern. Damit kann die DAO nach den Regeln arbeiten, mit denen sie programmiert wurde.
- Smart Contracts können Geldmittel senden und empfangen. Andernfalls wäre für die Verwaltung der Geldmittel der Gruppe ein vertrauenswürdiger Vermittler erforderlich.
- Die Ethereum-Community ist bekannt dafür, dass es um Zusammenarbeit und nicht um Wettbewerb geht. Daher können sich bewährte Verfahren und Unterstützungssysteme schnell herausbilden.

DAO-Mitgliedschaft

Für die Mitgliedschaft in einer DAO gibt es verschiedene Modelle. Über die Mitgliedschaft wird festgelegt, wie Abstimmungen und andere wesentliche Bereiche der DAO funktionieren.

Token-basierte Mitgliedschaft: In der Regel völlig frei von Berechtigungen, je nach verwendeten Token.

Dezentrale Autonome Organisation (DAO) 3/4

Meistens können diese Governance-Token (Kontroll-Token) an einer dezentralen Börse berechtigungsfrei gehandelt werden. Andere müssen erworben werden, durch die Bereitstellung liquider Mittel oder eine andere Form des »Arbeitsnachweises«. In jedem Fall gewährt der Besitz des Tokens Zugang zur Abstimmung.

Anteilsbasierte Mitgliedschaft: Anteilsbasierte DAOs sind stärker reglementiert, aber immer noch recht offen. Alle potenziellen Mitglieder können Anträge stellen, um der DAO beizutreten. Dafür wird meist eine Gegenleistung in Form von Tokens (Kryptowährung) oder geleisteter Arbeit angeboten. Anteile stehen für direkte Stimmrechte und Eigentum. Mitglieder können jeder Zeit aussteigen und erhalten einen proportionalen Anteil an der Schatzkammer. Findet in der Regel Anwendung für kleinere, auf den Menschen ausgerichtete Organisationen wie Wohltätigkeitsorganisationen, Gewerkschaften und Investmentclubs. Sie können auch Protokolle und Token regeln.

MolochDAO: MolochDAO ist auf die Finanzierung von Ethereum-Projekten ausgerichtet. Gefordert wird ein Antrag auf Mitgliedschaft, damit die Gruppe beurteilen kann, ob Interessenten über das nötige Fachwissen und Kapital verfügen, um fundierte Entscheidungen über potenzielle Zuschussempfänger zu treffen. Es ist nicht möglich, den Zugang zur DAO einfach auf dem freien Markt zu kaufen.

Reputationsbasierte Mitgliedschaft: Reputation ist ein Nachweis der Teilnahme und gewährt Stimmrechte im DAO. Im Gegensatz zur token- oder anteilsbasierten Mitgliedschaft übertragen reputationsbasierte DAOs keine Vermögenswerte an Mitwirkende. Reputation kann weder gekauft, übertragen noch delegiert werden. DAO-Mitglieder können Reputation nur durch Teilnahme erwerben. On-Chain-Abstimmungen sind frei zugänglich. Jedes potenzielle Mitglied kann einen Antrag auf Beitritt zur DAO und Vergütung seiner Mitwirkung in Form von Reputation und Token stellen. Typischerweise

für die dezentrale Entwicklung und Steuerung von Protokollen und dApps (dezentralisierte Anwendungen) verwendet, aber auch gut geeignet für eine Vielzahl von Organisationen wie Wohltätigkeits-Organisationen, Arbeitskollektive, Investmentclubs usw.

DXdao: DXdao ist ein globales und souveränes Kollektiv, das seit 2019 dezentralisierte Protokolle und Anwendungen entwickelt und administriert. Zur Koordinierung und Verwaltung der Geldmittel wird auf eine reputationsbasierte Administration gesetzt und ein holografischer Konsens verwendet. Somit ist es nicht möglich, sich die Entscheidungsmacht über die Organisation zu erkaufen.

DAO und Wertschöpfung

Die DAO selbst kann keine eigenen Produkte herstellen oder Dienstleistungen erbringen. Dafür benötigt die DAO ausführende Kräfte, Anbieter oder externe Lieferanten. Die implementierten Smart Contracts stellen die Basis der Zusammenarbeit mit den externen Lieferanten dar.

Der Prozess der Zusammenarbeit und die Entscheidungsfindung in der DAO läuft folgendermaßen ab:

- **Vorschlag:** Jemand bereitet einen Vorschlag, welches Produkt/Dienstleistungen von welchem Anbieter für wie viel Kryptogeld (Ethereum) geliefert wird
- **Abstimmung:** Die Anteilseigner diskutieren und entscheiden in einer gemeinsamen Abstimmung über den erbrachten Vorschlag
- **Lieferung:** Der Anbieter stellt das Produkt her oder ist bereit dazu, die Dienstleistung zu erbringen
- **Vertrieb:** Kunden können dieses Produkt erwerben oder die Dienstleistung in Anspruch nehmen.
- **Verwendung der Einnahmen:** Die Einnahmen aus dem Geschäft kann die DAO entweder reinvestieren in das Unternehmenswachstum oder an die Anteilseigner ausschütten.

Dezentrale Autonome Organisation (DAO) 4/4

Bekannte Probleme mit DAO

Ein bekanntes Beispiel für die Finanzierung von Risikokapital war die DAO »The DAO«, das im Juni 2016 mit Crowdfunding in Höhe von 150 Millionen US-Dollar startete und sofort um 50 Millionen US-Dollar an Kryptowährung bestohlen wurde (ermöglicht durch einen »kleinen« Softwarefehler, einer einzigen unnötigen Programmzeile).

Dieser Hack wurde in den folgenden Wochen rückgängig gemacht und das Kryptogeld über einen hard fork (»Notoperation«) der Ethereum-Blockchain wiederhergestellt.

Die dezentrale Rettung wurde durch eine Mehrheitswahl der Ethereum-Gemeinschaft ermöglicht, um den ursprünglichen Vertrag zu retten.

Sicherheit einer DAO

Der Code einer bestimmten DAO wird schwer zu ändern sein, sobald das System in Betrieb ist. Korrekturen für eine DAO würden die Erstellung eines neuen Codes und die Zustimmung zur Migration aller Teilnehmer einer DAO erfordern. Obwohl der Code für alle sichtbar ist, ist er schwer zu reparieren und lässt somit bekannte Sicherheitslücken offen für die Ausbeutung durch Angreifer zu, es sei denn, ein Moratorium wird aufgerufen, um Fehlerbehebungen zu ermöglichen.

DAO - offene Fragen

- Der genaue rechtliche Status einer DAO ist nicht geklärt.
- Wie steht es um die Haftung, wenn die DAO Schaden verursacht?
- Wie sehen Steuerzahlungen aus für den erwirtschafteten Gewinn, wenn das Unternehmen keinen klaren Firmensitz hat?
- Durch die offenen Fragen kann es für eine DAO schwierig sein, einen Anwalt zu engagieren oder einen schriftlichen Vertrag abzuschließen.

Obwohl unklar, kann eine DAO funktionell eine Körperschaft ohne rechtlichen Status sein: also eine allgemeine Partnerschaft. Dies bedeutet eine potenziell unbeschränkte Haftung für die Teilnehmer, selbst wenn der Smart-Contract-Code oder die Förderer der DAO etwas anderes sagen.

Darüber hinaus sind DAOs zumeist unreguliert und neigen dazu, sich über viele Gerichtsbarkeiten zu verteilen, was die Lösung potenzieller rechtlicher Probleme bestenfalls extrem kompliziert oder sogar völlig unmöglich macht.

Auch wenn nicht alles geklärt ist, ist das Konzept der dezentralen autonomen Organisationen sehr spannend.

Fazit

Eine DAO ist also ein Unternehmen, das in der Lage ist, seine Kosten auf ein Minimum zu reduzieren. Dies geschieht durch eine schnelle und einfache Entscheidungsfindung. Somit benötigen DAOs keine Mitarbeiter, die Verwaltungsaufgaben erfüllen. Dies reduziert die Komplexität erheblich. Somit braucht man auch kein Büro mehr. Man kann von überall auf der Welt arbeiten und sein volles Potenzial ausschöpfen.

NFTs: Eine Revolution in der digitalen Kunst? 1/3

Spätestens seit der Versteigerung einer digitalen Collage des Künstlers Mike »Beeple« Winkelmann im Jahr 2021 für 69 Millionen US-Dollar bei Christie's sind Non Fungible Tokens (NFTs) in der Kunst zum absoluten Hype-Thema geworden (erste Versteigerung von NFTs 2018). Und wenn ein traditionelles Auktionshaus wie Christie's anfängt, sich für digitale Kunst zu interessieren, heißt das: NFTs sind kein schneller Trend, sondern ein ernst zu nehmender Kunstmarkt.

Was sind NFTs?

NFT steht für Non-Fungible Token (nicht austauschbare oder nicht veränderbare Merkmale eines Objektes). Durch NFTs, wird aus einer normalen Datei ein Original, das gehandelt werden kann. Das heißt, ein NFT-Token ist ein einzigartiges digitales Kennzeichen das nicht ersetzbar oder kopierbar ist. NFTs werden am besten als Dateien in Kombination mit Eigentums- und Echtheitsnachweisen verstanden, etwa wie eine Urkunde.

Die Technologie, mit der man über die Blockchain die Besitzrechte für solche digitalen Kunstwerke verkaufen kann, ist die so genannte NFT-Technologie. Es ist also ein nicht austauschbares Objekt, eine Bezeichnung für ein einzigartiges digitales Kennzeichen, welches nicht ersetzbar oder kopierbar ist. Das Verkaufen von Kunst wird sehr viel einfacher und Künstler erhalten so gleichzeitig eine ganz neue Form der Vermarktung.

Es ist zwar möglich, kryptografische Kunst zu kopieren und zu vervielfältigen, indem man sie einfach herunterlädt oder einen Screenshot macht, aber dabei wird das wichtigste Merkmal der Kunst entfernt: ihre Metadaten.

Bevor das digitalen Kunstwerk als NFT bezeichnet werden kann, mit einen bestimmten Geldwert, muss das Werk mit einer eindeutigen ID versehen werden. Die eindeutige ID der NFTs



NFT-Artwork von Satoshi Nakamoto

bestätigt somit die Legitimität des Wertes und des Eigentums an der Kunst. Je nach Dienstleister und Blockchain-Host können die Kosten für die Prägung einer NFT 1 bis 3-stellige Werte erreichen.

Durch die zugrundeliegende Blockchain-Technologie kann der Besitz jedes Tokens eindeutig und jederzeit transparent nachgewiesen und übertragen werden. Im Wesen sind NFTs also digital einzigartige Kunst- und Wirtschaftsgüter, deren Echtheit und Einzigartigkeit durch das Speichern auf der Blockchain fälschungssicher dokumentiert werden kann. Wenn Kryptokunst verkauft oder übertragen wird, werden die Metadaten in der Blockchain mit einem Zeitstempel versehen.

Die Möglichkeiten der NFTs stellen die klassische Kunsthändler vor einigen neuen Herausforderungen. Durch das digitale Metaverse oder Metaversum (Metaversum: kann digitale Kunst und andere Objekte in einer virtuellen Welt darstellen) kann ja jeder selbst zum Kurator werden, was den Einfluss von traditionellen Galerien, Museen und Ausstellungen vermutlich verringert.

NFTs: Eine Revolution in der digitalen Kunst? 2/3

Wie macht man aus digitaler Kunst ein NFT?

Nachdem ein digitales Kunstwerk geschaffen wurde, wird dieses Objekt durch einen Kryptowährungsdienst in dessen Blockchain geprägt (geminted) und gespeichert, es wird zu einem Token.

1. Wählen oder erstellen von Kunst

Der erste Schritt ist das Erstellen oder Finden eines Kunstwerkes. Man sollte daran denken, dass es nur sehr wenige Regeln gibt, was man als NFT verkaufen könnte. Solange der Originalinhalt (Kunstwerke, Songs oder sogar Rezepte) einem selbst gehört, kann man es auch auf einem NFT-Marktplatz verkaufen.

2. Ein Ethereum-Wallet einrichten

Der NFT-Markt konzentriert sich auf Kryptowährungen wie Ethereum. Wenn man daran interessiert ist, NFTs zu verkaufen, muss man eine eigene digitale Brieftasche (Wallet) einrichten. Auf diese Weise kann man nicht nur die Gebühren zahlen, die mit dem Hosting von NFTs auf einem Marktplatz verbunden sind, sondern wenn jemand ein NFT-Objekt kauft, wird man automatisch auch in Kryptowährung bezahlt. **Hinweis:** Es gibt noch einige andere Plattformen auf denen digitale Geldbörsen erstellt werden können.

3. Kryptowährung für das Wallet (ETH) kaufen

Nachdem eine digitale Brieftasche eingerichtet wurde, kann man im nächsten Schritt eine kleine Menge Ethereum (ETH) für die eigene Brieftasche kaufen. Dies mag zwar seltsam erscheinen, da man nicht derjenige ist, der NFTs kauft, aber es gibt einen guten Grund, dies zu tun. Die meisten Marktplätze haben eine Art von Gebühren im Zusammenhang mit dem Verkauf von NFTs auf ihren NFT-Plattformen, daher benötigt man ein wenig ETH für den Verkauf.

Hinweis: Der Preis von ETH kann von Tag zu Tag schwanken, aber sobald man einen Dollarbetrag ausgewählt hat, den man investieren möchte, muss man nur noch die Kryptowährung kaufen. Die gute Nachricht ist, dass man wahrscheinlich keine separate

Austauschplattform verwenden muss, um ETH zu erhalten. Die meisten Wallets, einschließlich MetaMask und Rainbow, ermöglicht es, ETH direkt zu kaufen, sodass keine separate Überweisung vorgenommen werden muss.

Wenn die gewählte Brieftasche den direkten Kauf von Ethereum nicht zulässt, kann man natürlich immer noch von anderen Plattformen ETH kaufen, mit denen man bereits vertraut ist (Venmo oder Paypal).

4. Finden eines NFT-Marktplatzes

Der nächste Schritt besteht darin, einen Marktplatz zu finden, auf dem man NFTs verkaufen kann. Wie beim Erstellen einer digitalen Brieftasche gibt es mehr als eine Plattform zur Auswahl. Einige der bestehenden Plattformen auf dem Markt sind die folgenden: Rarible, OpenSea, SuperRare ... **Hinweis:** Die Anmeldeprozeduren der Plattformen können mitunter ein wenig kompliziert sein.

5. Verbinden des Wallet mit dem Marktplatz

Wenn man sich auf einen Marktplatz anmeldet, bietet die gewählte Plattform wahrscheinlich die Möglichkeit an, die Brieftasche mit dem Marktplatz zu verbinden. Dies ist ein Schritt, den man nicht verpassen sollte, insbesondere wenn man sofort mit dem Hochladen und Prägen von NFTs beginnen möchte.

6. Hochladen und prägen einer digitalen Datei

Sobald man bereit ist, kann man mit dem Hochladen einer Datei beginnen. Vorher sollte man sich informieren, welche Dateitypen vom aktuellen Marktplatz unterstützt werden. In nächsten Schritt kann man wählen, ob die NFTs als Einzelstücke oder als umfangreiche Sammlung von Dateien geprägt werden sollen. Bevor die Prägung abgeschlossen wird, muss man die Gebühr für die Prägung der NFT (Gas-Gebühren) normalerweise erst bezahlen.

NFTs: Eine Revolution in der digitalen Kunst? 3/3

Nach dem Hochladen und Prägen eines Kunstwerks, wird vom Kunstwerk ein einzigartiger Hash erzeugt. Das Verändern auch nur eines Pixels eines Bildes führte sofort zu einem völlig anderen Hash-Code. Daher kann dieser Hash zur eindeutigen Identifizierung des Originalwerkes dienen.

Beispiel:

256-Bit-Hexadezimal-Hashwert für ein Kunstwerk von Beeple
6314b55cc6ff34f67a18e1ccc977234b803f7a5497b94f1f994ac9d1b896a017

Ist dieser Hashwert erzeugt, wird eine begleitende Metadaten-Datei für das Kunstwerk erstellt. Diese Datei im JSON-Format (JSON ... JavaScript Object Notation) enthält Metadaten zum Kunstwerk, wie z.B. Namen und Titel des Kunstwerks, den Namen des Künstlers, eine Beschreibung des Werkes und andere Informationen. In diesem Zusammenhang besonders relevant ist jedoch, dass die Metadaten-Datei auch den Hash der Kunstwerk-Datei und einen exakten Hyperlink zu dem Hosting-Bereich enthält, auf dem die Kunstwerk-Datei gehostet wird.

7. Erstellen eines Titels und Beschreibung

Während einige Künstler diesen Teil vielleicht beschönigen möchten, sind der Titel eines Stücks und seine Beschreibung oft das, was die Leute dazu verleitet, sich ein NFT etwas genauer anzusehen. In der Beschreibung sollte man vielleicht über das Thema des Stücks, das Konzept und die Bedeutung dahinter sprechen.

8. Wählen eines Preises für ein NFT

Dies kann zwar je nach Plattform variieren, aber auf den meisten NFT-Marktplätzen kann man NFTs auf zwei Arten verkaufen - entweder zu einem Festpreis oder als Auktionsmodell.

9. Werben für neue NFTs

Sobald ein NFT erstellt wurde und nun als Token verfügbar ist, kann

man sich nicht immer darauf verlassen, dass die neuen NFTs auch gefunden werden. Während einige Plattformen besser darin sind, neue Kunstwerke zu veröffentlichen als andere, schadet es auch nie, ein wenig selbst Werbung zu machen. Falls Künstler eine feste bestehende Fangemeinde in den sozialen Medien haben, können die Follower ja auch jederzeit über ein neues verkaufswürdiges NFT informiert werden.

10. Benachrichtigung über die Kaufangebote

Nicht alle Plattformen benachrichtigen den Eigentümer eines NFTs, wenn jemand ein Gebot abgegeben hat. Deshalb ist es immer eine gute Idee, sich regelmäßig über die aktuellen Angebote zu informieren. Der Künstler oder der Eigentümer eines NFTs haben dann die Möglichkeit die Gebote anzunehmen oder auch nicht. Wenn man sich für einen Festpreis entschieden hat, wird man möglicherweise nur benachrichtigt, dass jemand das NFT gekauft hat.

Der Vorteil der Verwendung eines NFT-Marktplatzes besteht darin, dass man nach dem Auflisten eines Tokens nicht mehr viel Arbeit damit hat, außer nach den aktuellen Geboten zu schauen. Sobald jemand ein NFT gekauft hat, kümmert sich die Plattform um den Rest und das vereinbarte Kryptogeld gelangt automatisch in die digitale Brieftasche.

Fazit

Die Menschen die an NFTs glauben und die zunehmende gesellschaftliche Akzeptanz werden die Zukunft der Kryptokunst beeinflussen. Während das Potenzial von Kryptokunst, noch nicht vollständig erforscht ist, hat die aufkommende Technologie bereits unsere Wahrnehmung von wertvollen Sammlerstücken und Kunst verändert. In Zukunft könnte Krypto-Kunst dazu genutzt werden, jeden Aspekt unseres Lebens virtuell abzubilden.

Palantir in deutschen Polizeibehörden

Die umstrittene Fahndungssoftware Palantir des gleichnamigen US-amerikanischen Herstellers Palantir ist bereits seit dem Jahr 2017 (soweit öffentlich bekannt) in deutschen Polizeibehörden im Einsatz.

Mit Palantir ist eine datenbankübergreifende automatisierte Analyse, Recherche und Datenauswertung - auch über die Grenzen einer Polizeibehörde - möglich (z.B. Daten aus den sozialen Medien).

In Hamburg gibt es - im Vergleich zu anderen Bundesländern eine Besonderheit: Ein eigenes »Gesetz über die Datenverarbeitung der Polizei« (PoIDVG) vom 12.12.2019. Die Befugnisse und Grenzen der polizeilichen Datenverarbeitung sind in vielen anderen Polizeibehörden der Bundesländer in den entsprechenden Polizei-Gesetzen geregelt. Der Paragraph 49 im Hamburgischen PoIDVG regelt, was in begründeten Einzelfällen in polizeilichen Dateisystemen an gespeicherten personenbezogenen Daten - mittels einer automatisierten Anwendung - zur Datenauswertung verarbeitet werden darf.

Mit »unverbindlichen Markterkundungsverfahren« interessierten sich einige staatliche Behörden für am Markt befindliche Unternehmen, die die Entwicklung, Herstellung oder den Vertrieb von verfahrensübergreifenden Recherche- und Analyseplattformen (VeRA) für staatliche Behörden zur Durchführung von polizeilichen Analysen anbieten.

Gegen die »unverbindlichen Markterkundungsverfahren« und den Einsatz von Fahndungssoftware ist nichts einzuwenden, solange die europäische Datenschutzgrundverordnung (DSGVO) strikt eingehalten wird.

Es ist aber zu bezweifeln das die Hersteller von Software aus einem Nicht-EU-Land die Datenschutzgrundverordnung in den Quellcode auch nur Ansatzweise eingearbeitet haben.



Auch einige Oppositionspolitiker stellen sich die Frage, ob man eine Firma, die so tief mit dem militärisch-digitalen Komplex der USA verwachsen ist, in die Nähe von Daten der deutschen Polizei lassen sollte.

Hinweis: Palantir wurde auch in Afghanistan und im Irak von der US-Armee eingesetzt. Siehe auch: Internet → Key-Words: → Cambridge Analytica oder Preisentwicklung von Palantir

Predator 1/3

Predator (Hersteller: Konsortium von Spähsoftware-Anbietern namens Intellexa, Tochterunternehmen: Cytrox) kann wie Pegasus (Hersteller: nsogroup) Informationen aus mobilen Geräten und damit verbundenen Cloud-Diensten, Dateien, Fotos, Internetverläufe, Kontakte und Passwörter abgreifen und an ihre Auftraggeber weiterleiten. Beide laufen sowohl auf Android als auch auf iOS Mobilgeräten.

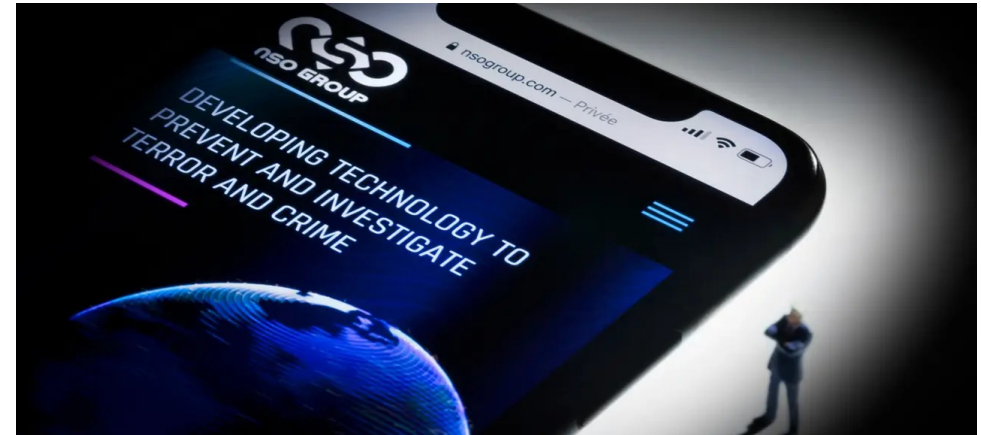
»Intellexa« wurde 2019 von Tal Dilian in Zypern gegründet. Dilian hatte zuvor mehrere einflussreiche Posten im israelischen Sicherheits- und Geheimdienstapparat. Auf ihrer Webseite beschreibt sich die Intellexa Alliance als ein in der EU ansässiges und von der EU reguliertes Unternehmen zum Zwecke der Entwicklung und Integration von Technologien zur Stärkung der Geheimdienste.

Hersteller von Predator ist die von israelischen und ungarischen Staatsangehörigen als Aktiengesellschaft in Skopje (Nordmazedonien) gegründete Firma Cytrox. Sie soll in beiden Ländern Büros zur Herstellung der Cyberwaffen unterhalten. Cytrox gehört inzwischen zu einer Gesellschaft in Ungarn, als Eigentümer gilt der Luftwaffenveteran Meir Shamir aus Israel.

Hinweis: Mindestens eine deutsche Bundesbehörde interessierte sich für Spionagesoftware des umstrittenen Konsortiums »Intellexa«. Die meisten Fragen der interessierten Parlamentarier an die Regierung zu diesem Thema blieben unter Verweis auf das Staatswohl unbeantwortet. Auch die Europäische Union befasste sich auf mehreren Ebenen mit dem Einsatz von staatlichen Spionageprogrammen gegen Oppositionelle und Medienschaffende.

Cyber-Stalking - ein gut dokumentierter Fall

Eine ehemalige Angestellte des Facebook-Konzerns Meta wurde in Griechenland mit der Spionagesoftware Predator ausgespäht. Das



haben Sicherheitsforscher vom Citizen Lab an der Universität Toronto (Kanada) nachgewiesen. Artemis Seaford besitzt sowohl die US-amerikanische als auch die griechische Staatsbürgerschaft.

Von 2020 bis 2022 arbeitete sie teils von Griechenland aus als Managerin im »Trust and Safety Team« von Meta. Dort habe sie sich unter anderem mit politischen Fragen im Zusammenhang mit IT-Sicherheit auseinandergesetzt und auch mit griechischen und europäischen Beamten zusammengearbeitet.

Dem Bericht der New York Times zufolge hatte Seaford ihren Namen auf einer Liste von Personen entdeckt, die vermutlich mit der Spähsoftware Predator angegriffen wurde. Daraufhin hatte sie ihr Smartphone für eine forensische Analyse an das Citizen Lab der Universität Toronto (Kanada) übergeben.

Die Sicherheitsforscher konnten nachweisen, dass Seafords Telefon im September 2021 mit Predator angegriffen und mindestens zwei Monate lang ausgespäht wurde.

Predator 2/3

Predator kann ein Smartphone komplett übernehmen und die darauf gespeicherten Informationen auslesen. Angreifer können auch die Kamera und das Mikrofon unbemerkt einschalten.

Laut dem Bericht hatte Seaford im September 2021 einen Termin für eine Corona-Auffrischungsimpfung über das offizielle Portal der Regierung gebucht, der anschließend per SMS bestätigt wurde.

Wenige Stunden später erhielt sie eine weitere Textnachricht mit den Details ihres Termins, in der sie aufgefordert wurde, diesen durch Klick auf einen Link zu bestätigen. Wie später die Untersuchungen der Sicherheitsforscher ergeben hatten, wurde so die Predator-Infektion ausgelöst.

Wer hinter der Spionageaktion steht ist unklar. Es gibt nur unbestätigte Informationen, Seaford sei zwischen August 2021 und Anfang 2022 vom griechischen Geheimdienst EYP abgehört worden.

Unklar bleibt darüber hinaus, warum Seaford überwacht worden sein könnte. Seaford hat in dem Fall Anzeige in Griechenland erstattet. Außerdem hat sie Auskunft darüber verlangt, ob sie vom Geheimdienst abgehört wurde.

Anzeichen für eine Späh-App

Textnachrichten mitlesen, Standortdaten abgreifen, die Kamera einschalten. Spähsoftware auf dem Smartphone kann ein mächtiges Werkzeug sein, um einen Menschen auszuspionieren. Und offenbar nimmt die Nutzung solcher Programme weltweit zu - auch in Deutschland.

Tipps, wie man sich vor einer Ausspäh-App schützt

- **Gute Passwörter und physischer Schutz:** Mobile Geräte sollten über PIN-Codes, Biometrie oder sichere Muster gesperrt sein,

außerdem sollte man Geräte und Online-Konten jeweils mit einem starken Passwort schützen, das nicht an Dritte weitergegeben wird, auch nicht an Vertrauenspersonen. Wo möglich, sollte eine Zwei-Faktor-Authentifizierung eingerichtet werden.

- **Updates machen:** Betriebssystem und Apps sollten immer auf dem neuesten Stand sein.
- **Die richtigen Einstellungen:** Auf dem Smartphone lässt sich in den Einstellungen die Installation von Programmen aus unbekannten Quellen blockieren.
- **Vorsicht bei Anhängen:** Unbekannte Dateien, die etwa unaufgefordert geschickt werden, sollten auf persönlichen Endgeräten nicht geöffnet oder gar gespeichert werden. Im Zweifel lieber noch einmal telefonisch beim Absender nachfragen.
- **Einen Schlusstrich ziehen - auch digital:** Wenn eine Beziehung zu Ende gegangen ist, sollten die Sicherheitseinstellungen auf allen Geräten geändert werden.
- **Den Überblick behalten:** Nutzer sollten regelmäßig prüfen, welche Apps auf dem Smartphone installiert und in Benutzung sind. Nicht benötigte Apps sollten gelöscht oder deaktiviert werden.

Warnzeichen die auf Stalkerware hindeuten

- **Der Datenverbrauch ist gestiegen:** Steigt plötzlich der Datenverbrauch deutlich, könnte das an einer unerwünschten App liegen, die im Hintergrund Daten überträgt.
- **Das Smartphone läuft langsamer:** Wird ein Gerät plötzlich auffallend langsam oder der Akku muss neuerdings häufiger aufgeladen werden, so könnte dies auf Stalkerware hindeuten.
- **Unbekannte Apps auf dem Smartphone:** Wer den Verdacht hat, eine Stalkerware auf dem Smartphone zu haben, sollte alle Apps auf dem Smartphone überprüfen. Dieses betrifft in der

Predator 3/3

- Regel nicht die sichtbaren Icons auf dem Bildschirm, sondern die gelisteten Apps in den Einstellungen.
- **Veränderungen am Browser:** Das Erscheinen einer plötzlichen neuen Startseite oder merkwürdige Werbefenster, ist ein weiteres Symptom für Schadsoftware.
 - **Aufbau einer Internetverbindung:** Ein selbständiger Verbindungsaufbau mit dem Internet oder eine dauerhafte Warnung der Firewall ist ebenfalls typisch für Schadcode.
 - **Hintergrundgeräusche beim Telefonieren:** Mehrfach auftretende Stör- und Hintergrundgeräusche bei Telefonaten, die sich die Gesprächspartner nicht erklären können, deuten eventuell auf ein Abhören oder Aufzeichnen von Telefonaten hin.
 - **Jemand weiß zu viel:** Während ein guter Cyberangriff technisch oft unentdeckt bleibt, verraten sich Menschen schon eher und man sollte sich folgende Frage stellen. Kommt es häufiger vor, dass Bekannte, Freunde oder andere Menschen mehr wissen, als sie eigentlich sollten? Dann könnte jemand eine digitale Wanze im Smartphone installiert haben.
 - **Menschen ins Vertrauen ziehen:** Wer sich beobachtet und gestalkt fühlt, sollte mit vertrauten Menschen darüber reden, um Schutz und Unterstützung zu erhalten.
 - **Hilfe holen:** Neben der Polizei gibt es verschiedene Stellen, die als erste Anlaufstellen Informationen bereithalten.
 - **Schutz aufbauen:** Wer selbst gegen eine Stalkerware auf seinen Geräten vorgehen möchte, hat verschiedene Möglichkeiten: Das Zurücksetzen aller Geräte auf die Werkseinstellungen kann ratsam sein, ebenso das Ändern der Passwörter und das Einrichten von Zwei-Faktor-Authentifizierung. Weiterhin ist es ratsam eine neue E-Mail-Adresse einzurichten und die wichtigsten Konten und Dienste damit zu verknüpfen. Auch die Berechtigung für einen Zugriff auf die Kamera sollte für alle Anwendungen ausgeschaltet werden, die keinen Zugriff auf die Webcam benötigen.

Ferner gibt es noch ein paar Möglichkeiten, die vor allem mit dem eigenen Verhalten im Umgang mit dem Internet und fremden Programmen zu tun haben. Man sollte zum Beispiel keine Programme installieren und auch keine Links anklicken, denen man nicht vertraut.

Was man bei einem Verdacht tun kann

Wer eine verdächtige App gefunden hat oder aufgrund anderer Indizien glaubt, per Späh-Programm gestalkt zu werden, sollte zunächst in Ruhe abwägen, was zu tun ist.

- **Nicht löschen - sondern Beweise sichern:** Wird die Stalkerware entdeckt und entfernt, so bekommt auch der Täter dies mit und ist vorgewarnt. Zur Beweissicherung ist es hilfreich Screenshots zu erstellen und das führen eines Tagebuchs über die Verdachtsmomente.
- **Einen zweiten Kanal suchen:** Sollte eine Späh-Software auf dem Smartphone installiert sein, ist dieses Gerät ungeeignet für vertrauliche Telefongespräche. Wer irgendwie die Möglichkeit hat, sollte sich vorübergehend ein zweites Smartphone besorgen, um wieder einen eigenen Kommunikationskanal zu haben.

Was sind Kryptowährungen? 1/5

Kryptowährungen sind im Grunde genommen dezentral verwaltetes digitales Geld, das extra für die Verwendung im Internet geschaffen wurde. Die Grundprinzipien hinter Bitcoin sowie der Bitcoin-Blockchain wurden erstmals in einem Ende 2008 veröffentlichten Whitepaper einer Person oder Gruppe mit dem Namen Satoshi Nakamoto veröffentlicht. Die erste Kryptowährung, Bitcoin ist nach wie vor die bei weitem größte, einflussreichste und bekannteste Kryptowährung. In den vergangenen Jahren haben sich noch andere Kryptowährungen wie Ethereum zu digitalen Alternativen weiterentwickelt.

Kryptowährungen werden in der Regel nicht von Regierungen oder anderen Zentralbehörden herausgegeben oder kontrolliert. Sie werden von Peer-to-Peer-Computernetzwerken verwaltet, in denen Open-Source-Software zum Einsatz kommt. Es handelt sich um frei zugängliche Systeme und die Kernsoftware ist und sie sollte für die Zukunft auch immer quelloffen bleiben.

Mit Kryptowährungen können Vermögenswerte übertragen werden, ohne dabei auf eine Vermittlungsinstanz wie eine Bank oder ein Zahlungssystem zurückzugreifen. So lassen sich Vermögenswerte weltweit, praktisch in Echtzeit, rund um die Uhr und zu geringen Gebühren übertragen. Kryptowährungen sind relativ sicher, weil sämtliche Transaktionen der meisten Kryptowährungen mithilfe einer Technologie namens Blockchain unter Einsatz einer enormen Rechenleistung laufend überprüft und verifiziert werden.

Grundsätzlich ist eine Blockchain »nur« eine Liste von Transaktionen, die jeder einsehen und überprüfen kann.

Die Blockchain einer Kryptowährung kann man auch mit dem Kontobuch (Ledger) einer Bank vergleichen. Jede Währung hat ihre eigene Blockchain. Es handelt sich dabei um ein fortlaufendes, ständig neu überprüftes Register, das jede einzelne Transaktion, die



mit der digitalen Währung durchgeführt wurde, aufzeichnet. Im Gegensatz zum Kontobuch einer Bank ist die Blockchain von Kryptowährungen auf alle Teilnehmer im Netzwerk der digitalen Währung verteilt.

Kein Unternehmen, Land oder Drittanbieter hat die Kontrolle über dieses Netzwerk und jeder kann Teil davon werden. Am wichtigsten ist, dass die Menschen mithilfe von Kryptowährungen die volle Kontrolle über ihr digitales Vermögen erlangen können.

Durch kryptografische Verfahren können Transaktionen in digitaler Währung ohne Angabe von Klarnamen, sicher und vertrauensvoll abgewickelt werden.

Wenn man mit Kryptowährungen bezahlt, muss man dem Händler gegenüber keine überflüssigen personenbezogenen Daten preisgeben. Damit ist sichergestellt, dass die Finanzdaten nicht an Drittparteien wie Banken, Zahlungsanbieter, Werbetreibende und Kreditauskunfteien

Was sind Kryptowährungen? 2/5

weitergegeben werden. Und da keine sensiblen Daten über das Internet verschickt werden müssen, ist das Risiko äußerst gering, dass die Finanzdaten in falsche Hände geraten oder die Identität gestohlen wird.

Jede Transaktion in den Netzwerken kann ausnahmslos öffentlich eingesehen werden. Das bedeutet, dass weder die Transaktionen noch die Geldmenge noch das Reglement nachträglich geändert werden können. Anders als bei Kreditkartenzahlungen können Zahlungen per Kryptowährung nicht rückgängig gemacht werden. Dies senkt das Betrugsrisiko für Händler enorm.

Die Grundkonzepte aller Kryptowährungen setzen auf ein asymmetrisches Verschlüsselungsverfahren, das öffentliche und private Schlüssel zur Übertragung des Eigentumsrechts an digitaler Werte innerhalb eines sicheren und verteilten Ledgers (Kontobuch) verwendet. Ein privater Schlüssel ist ein extrem sicheres Passwort. Er darf niemals mit anderen geteilt werden. Mit diesem Schlüssel kann man im Netzwerk Vermögenswerte übertragen. Ein dazu passender öffentlicher Schlüssel kann anderen Personen problemlos mitgeteilt werden, um Vermögenswerte im Netzwerk zu erhalten. Anhand des öffentlichen Schlüssels kann niemand Rückschlüsse auf Ihren privaten Schlüssel ziehen.

Hinweis: Das Netzwerk, das Bitcoin zugrunde liegt, wurde noch nie gehackt.

Was bedeutet Mining von Kryptowährungen?

Die Einheiten der meisten Kryptowährungen werden über ein dezentrales (auch als Peer-to-Peer bekanntes) Computernetzwerk im Rahmen eines Vorgangs erzeugt, der »Mining« genannt wird. Aber Mining erzeugt nicht einfach nur weitere Bitcoin- oder Ethereum-Einheiten. Es handelt sich dabei auch um einen Mechanismus, der das Netzwerk mittels der Mining-Anlagen auf den neuesten Stand bringt

und absichert, indem er den öffentlichen Blockchain-Ledger laufend überprüft und um neue Transaktionen ergänzt.

Mining Rigs (Mining-Anlagen) führen kurz gesagt Gleichungen aus, die zum Verifizieren und Aufzeichnen einer neuen Transaktion erforderlich sind.

Im Prinzip kann jeder mit einem Computer und einer Internetverbindung sich als Miner betätigen. Aber man darf sich nicht zu früh freuen - es darf dabei nicht vergessen werden, dass Mining nicht immer lukrativ ist. Je nachdem, welche Kryptowährung man per Mining erzeugt, wie schnell der Computer ist und wie viel der Strom in der Region kostet, können die Ausgaben für das Mining unterm Strich die Einnahmen durch Kryptowährungen übersteigen.

Aus diesem Grund wird das Mining von Kryptowährungen heutzutage größtenteils von Spezialunternehmen durchgeführt oder von Einzelpersonen, die ihre Rechenleistung in großen Gruppen erbringen.

Wie motiviert das Netzwerk Miner, sich an der Pflege der Blockchain zu beteiligen?

Bei Bitcoin zum Beispiel verwendet das Netzwerk ein Losverfahren, in dessen Rahmen alle Mining-Anlagen (Mining Rigs) weltweit miteinander konkurrieren.

Hier wird versucht als Erstes ein mathematisches Problem zu lösen, das gleichzeitig die Blockchain überprüft und ihr neue Transaktionen hinzufügt. Jeder Gewinner erhält neue Bitcoins, die dann ihren Weg in den breiter gefassten Markt finden.

Was bestimmt den Wert einer Kryptowährung?

Der wirtschaftliche Wert von Kryptowährungen wird, wie bei allen anderen Waren und Dienstleistungen auch, von Angebot und

Was sind Kryptowährungen? 3/5

Nachfrage bestimmt.

Das Angebot bezieht sich auf die verfügbare Menge - beispielsweise wie viele Bitcoin zu einem bestimmten Zeitpunkt zum Kauf zur Verfügung stehen. Die Nachfrage bezieht auf den Besitzwunsch, d.h. wie viele Personen Bitcoin kaufen möchten und wie stark ihr Wunsch danach ist. Der Wert einer Kryptowährung wird immer durch das Verhältnis dieser beiden Faktoren bestimmt.

Auch die aktuelle Verwendung und Akzeptanz einer Kryptowährung - Kauf von Waren und Dienstleistungen - kann den Wert mehr oder weniger beeinflussen.

Bei Bitcoin wird der Wert auch durch die Begrenzung auf etwa 21 Millionen (hat mathematische Gründe, bedingt durch die Konzeption der Technologie) möglichen Bitcoins beeinflusst. Diese Knappheit ist ein wertbestimmender Faktor.

Wie kann man Kryptogeld erwerben?

Am einfachsten lassen sich Kryptowährungen über eine vertrauenswürdige Online-Börse erwerben. Auf Coinbase kann man die bekanntesten Kryptowährungen kaufen, darunter Bitcoin (BTC), Litecoin (LTC), Ethereum (ETH), Bitcoin Cash (BCH) und Ethereum Classic (ETC).

Vor dem Kauf stellt man sich am besten die Frage, was man mit einer Kryptowährung anfangen möchte, und wählt dann die Währung aus, mit der man seine Ziele am besten erreichen kann. Wenn man beispielsweise einen Rechner mit einer Kryptowährung kaufen möchten, wäre Bitcoin wahrscheinlich eine gute Wahl, da es sich um die Kryptowährung mit der größten Akzeptanz handelt. Wenn man jedoch ein digitales Kartenspiel spielen möchten, bietet sich dafür eher Ethereum an.

Hinweis: Man muss kein ganzes digitales Geldstück kaufen. Auf den

Börsen können auch Teile von digitalen Geldstücken - in festgelegten Abstufungen - erworben werden.

Wie werden Kryptowährungen aufbewahrt?

Die Aufbewahrung von Kryptowährungen ist vergleichbar mit der Aufbewahrung von Geld, was bedeutet, man muss sie auch vor Diebstahl und Verlust schützen.

Es gibt viele Möglichkeiten, Kryptowährungen sowohl online als auch offline aufzubewahren, aber die einfachste Lösung ist eine vertrauenswürdige, sichere Börse. Kunden von Coinbase können Kryptowährungen sicher aufbewahren, senden, erhalten und umtauschen, indem sie sich per Computer, Tablet oder Telefon an ihrem Konto anmelden (**Hinweis:** Stiftung Warentest rät zur Aufbewahrung der Kryptowährung ein eigenes Wallet zu benutzen).

Möchte man Geld aus dem Wallet auf ein Bankkonto übertragen, so ist dieser Vorgang mit einer speziellen App so einfach wie das Überweisen von Geld von einer Bank zu einer anderen. Ähnlich wie bei herkömmlichen Banküberweisungen oder Abhebungen an Geldautomaten legen Börsen ein Tageslimit fest. **Hinweis:** Es kann zwischen einigen Tagen und einer Woche dauern, bis die Transaktion vollständig abgeschlossen ist.

Was kann man mit Kryptowährungen anfangen?

- Es gibt eine breite Palette an Anwendungen für Kryptowährungen und im Laufe der Zeit kommen immer neue hinzu.
- Es gibt weltweit bereits mehrere tausend Händler die Kryptowährungen akzeptieren.
- Autoren, Musiker und andere Verfasser von Online-Inhalten hinterlassen manchmal ihre Bitcoin-Adresse oder einen QR-Code am Ende ihrer Artikel. Wenn deren Inhalte einen bleibenden Eindruck hinterlassen haben, kann man sich mit einem kleinen Krypto-Betrag dafür bedanken.

Was sind Kryptowährungen? 4/5

- Da Kryptowährungen nicht an ein bestimmtes Land gebunden sind, kann das Reisen mit Kryptowährungen die mit Geldwechsellvorgängen verbundenen Kosten senken. Es gibt bereits eine kleine, aber stetig wachsende Community von selbsternannten »Krypto-Nomaden«, die auf Reisen in erster Linie oder in manchen Fällen ausschließlich mit Kryptowährungen bezahlen.
- Mittels einer Kryptowährung kann man virtuelle Besitztümer in einer virtuellen Spielewelt erwerben. Nutzer können dort virtuelle Grundstücke, Kleidung für Avatare und verschiedene andere Gegenstände kaufen und verkaufen, in virtuellen Nachtclubs feiern oder sich in virtuellen Kunstgalerien unter die Leute mischen.
- Eine breite Palette an neuen Unternehmen verfolgt das Ziel, das gesamte weltweite Finanzsystem nachzubilden, angefangen von Investitionen in Strukturen, die Anlagefonds ähneln, bis hin zu Mechanismen für die Kreditausgabe/-aufnahme und weit darüber hinaus, ohne jegliche Zentralinstanzen.

Was ist Ethereum 2.0?

Ethereum 2.0 (ETH2, Dezember 2020 Upgrade auf Ethereum 2.0) stellt eine wesentliche Verbesserung des Ethereum-Netzwerks dar, durch die Erhöhung der möglichen Transaktionen in einer Zeiteinheit. Dem Konzept nach soll es dem Ethereum-Netzwerk weiteres Wachstum ermöglichen, während gleichzeitig die Sicherheit, Geschwindigkeit und Effizienz erhöht werden.

Das Proof-of-Work-Verfahren (Ausführungsnachweis), dass bis dahin verwendet wurde, erfordert einen hohen Bearbeitungsaufwand, der hauptsächlich durch die Miner getragen wird, die weltweit miteinander konkurrieren, um ein zeitaufwändiges mathematisches Puzzle zu lösen.

Der Gewinner darf die Blockchain mit den letzten verifizierten Transaktionen aktualisieren und wird mit einem vorher festgelegten ETH-Betrag belohnt.

Dieser Prozess findet alle 30 Sekunden statt (im Gegensatz zum 10-Minuten-Takt bei Bitcoin). Da der Verkehr im Netzwerk gestiegen ist, sind die Beschränkungen des Proof-of-Work-Verfahrens in Form von Staus offensichtlich geworden, wobei die Gebühren während dieser Staus unvorhersehbar ansteigen.

Ethereum 2.0 verwendet ein Konsensverfahren, genannt Proof of Stake, das schneller, weniger ressourcenintensiv und zumindest theoretisch sicherer ist. Das Endergebnis ähnelt dem Proof-of-Work-Verfahren darin, dass ein Netzwerkteilnehmer ausgewählt wird, die letzten Transaktionen zu verifizieren, die Blockchain zu aktualisieren und einige ETH zu verdienen.

Das Proof-of-Stake-Verfahren erfordert jedoch kein Netzwerk von miteinander konkurrierenden Minern, um möglichst schnell ein Puzzle zu lösen, sondern ein robustes Netzwerk von Teilnehmern, die tatsächlich in den Erfolg des Unternehmens investieren.

Diese Stakeholder (Anspruchsberechtigte, Interessengruppe) werden Validatoren genannt. Statt, wie es die Miner tun, zur Verarbeitungsleistung beizutragen, steuern Validatoren ETH zu einem Staking Pool bei.

Dieser Vorgang, bei dem ETH zum Pool beigesteuert werden, wird Staking genannt. Sollte man sich dafür entscheiden, einige ETH zu staken, dann erhält man ein Reward (Belohnung, Prämie), die im Umfang dem Stake entspricht.

Das Netzwerk wählt einen Gewinner auf Basis des ETH-Betrags aus, den jeder Validator im Pool hat, sowie abhängig von der Zeit, die dieser ETH-

Was sind Kryptowährungen? 5/5

Betrag sich im Pool befindet - es werden also die am meisten investierenden Teilnehmer belohnt.

Sobald der Gewinner den letzten Transaktionsblock validiert hat, können andere Validatoren die Richtigkeit des Blocks bestätigen. Wenn die Anzahl dieser Bestätigungen einen Schwellenwert erreicht, aktualisiert das Netzwerk die Blockchain. Und alle teilnehmenden Validatoren erhalten einen Reward bzw. eine Reward in ETH, die vom Netzwerk im Verhältnis zum Stake jedes einzelnen Validators vergeben wird.

Steuern auf Kryptowährungen

Fallen beim Verkauf von Kryptowährungen Gewinne an, so ist es ein guter Gedanke die Geschäfte mit Kryptowährungen auch in der Steuererklärung mit anzugeben.

Wann fallen Steuern auf Kryptowährungen an?

Die kurze Antwort: Bei privatem Handel nur sehr selten. Die lange Antwort: Es gibt zwei Faktoren, die darüber bestimmen, ob für das Tauschen oder Verkaufen von Kryptowährungen Steuern anfallen. Das eine ist die sogenannte Haltedauer der Kryptowährungen. Also der Zeitraum, über den die Kryptowährung im Besitz war. Das andere ist die Höhe des Gewinns beim Handel.

Zur Haltedauer: Behält man eine Kryptowährung länger als 12 Monate, sind die Gewinne aus dem Verkauf oder Tausch steuerfrei und der Handel muss nicht in die Steuererklärung. Klingt erstmal einfach. Es kann aber kompliziert werden, wenn man öfter mit einer bestimmten Kryptowährung handelt. Dann sind mal mehr und mal weniger Coins (Münzen) im Depot. Wie also soll man die Haltedauer für genau die Coins ermitteln, die man zu einem bestimmten Zeitpunkt verkauft hat? In der Regel nutzt man dafür die Fifo-Methode: Die Abkürzung bedeutet »First in, first out«. Dabei geht das Finanzamt davon aus, dass man die zuerst

angeschafften Coins auch als Erstes wieder verkauft hat. Bei jedem Verkauf gibt man also die Coins ab, die am längsten im Depot lagen. Am besten fragt man im vorab beim Finanzamt nach, ob man diese Methode auch verwenden kann.

Zur Höhe des Gewinns: Ist die Haltedauer kürzer als ein Jahr, zahlt man bei Gewinnen über 600 Euro Steuern auf den gesamten Betrag. Hat man im selben Jahr auch Verluste mit dem Krypto-Handel gemacht, zieht man diese einfach von den Gewinnen ab. Macht man schließlich unterm Strich beispielsweise 601 Euro Gewinn, muss man auch die vollen 601 Euro versteuern. Die Freigrenze fällt dann komplett weg.

Der Haken dabei: Nicht nur der Handel mit Kryptowährungen ist für die 600-Euro-Grenze relevant. Auch Einnahmen aus anderen sogenannten privaten Veräußerungen werden hier mit eingerechnet. Dazu zählt zum Beispiel, wenn man innerhalb eines Jahres ein Schmuckstück, ein Auto oder eine Münzsammlung kauft und mit Gewinn wieder verkauft.

Hinweis: Wer seine Gewinne aus privaten Veräußerungen nicht oder in zu geringer Höhe angibt, kann sich unter Umständen der Steuerhinterziehung schuldig machen. Dafür droht im schlimmsten Fall sogar eine Freiheitsstrafe.

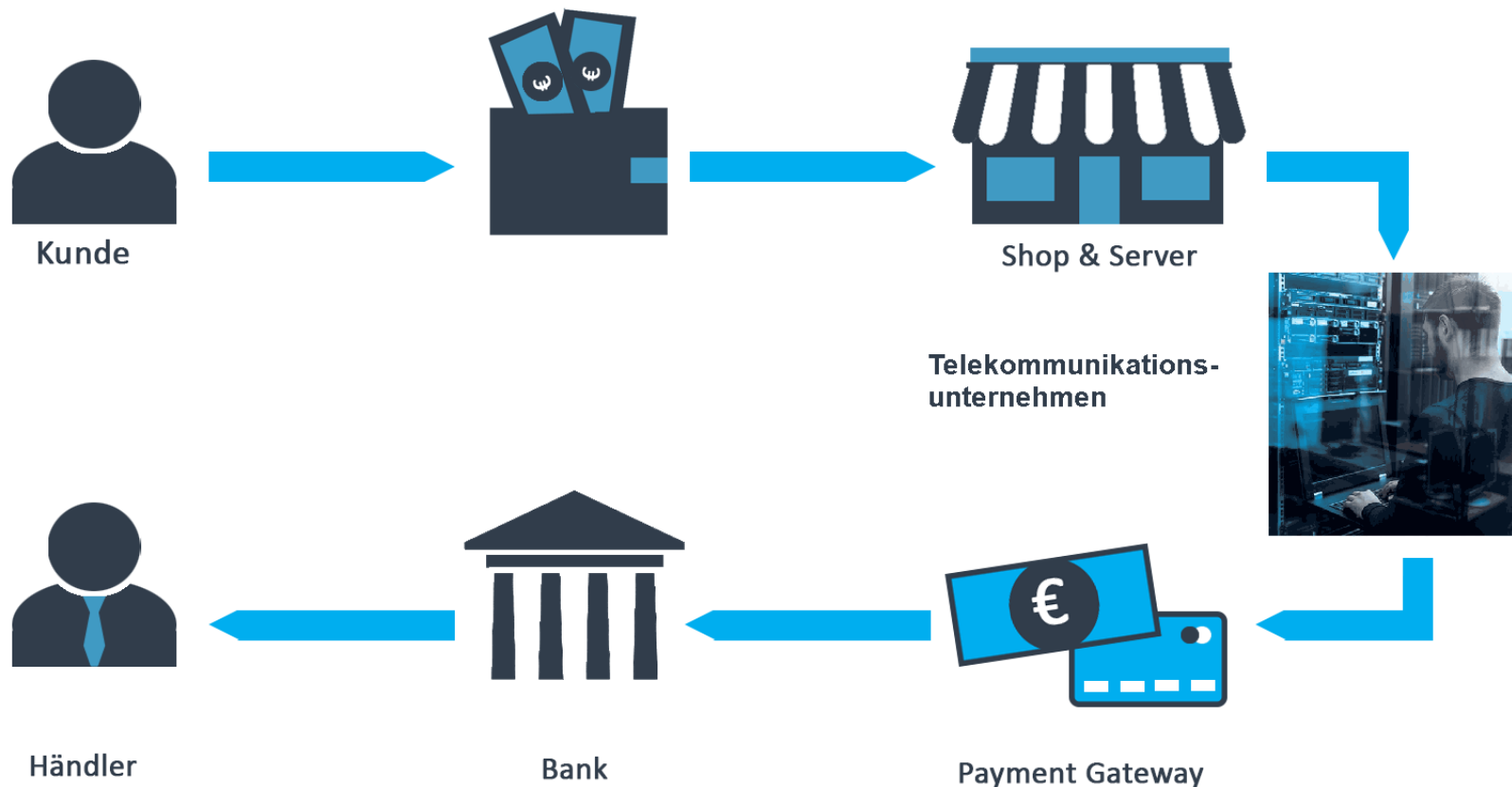
Kritik an den Kryptowährungen

- Die meisten Kryptowährungen erlauben nur eine begrenzte gleichzeitige Abwicklung von Finanztransfers.
- Durch die starken Wertschwankungen der Kryptowährungen am Markt, kann die digitale Währung niemals den Rang einer stabilen alltagstauglichen Währung erlangen. Investitionen in Kryptowährungen sind damit hoch riskant.
- Der hohe Energie- und Stromverbrauch (ökologische Fußabdruck). Im Oktober 2019 benötigte es 12 Billionen Mal mehr Rechenleistung, um einen Bitcoin zu minen, als dies der Fall war, als Satoshi Nakamoto im Januar 2009 die ersten Blöcke durch Mining gewonnen hat.

Zahlungsdienstleister 1/3

Zahlungsdienstleister sind allgegenwärtig und werden allgemein doch kaum wahrgenommen. Zahlungsdienstleister - auch Payment Service Provider oder Zahlungs-Provider genannt - agieren meist unbemerkt im Hintergrund. Payment-Service-Provider stellen die technische Anbindung und einen Teil des Weges von elektronischen Bezahlmethoden bereit. Die elektronischen Bezahlmethoden sind Online-Banking, Wallets (PayPal, Apple Pay, ...), Rechnung, Bank- und Kreditkarten, aber auch Lastschrift und Nachnahme.

Den wenigsten ist vertraut, welche zentrale Rolle die Zahlungsdienstleister im Zahlungsalltag tatsächlich einnehmen. Immer wenn Konsumenten eine Ware oder Dienstleistung bargeldlos zahlen, erhalten Zahlungsdienstleister den Auftrag, die Zahlung abzuwickeln. Das gilt bei Zahlungen per Kartenlesegerät der Verkaufsstelle eines Händlers (POS oder Point of Sale) oder Dienstleister (z.B. Friseur, Gastronomie-Unternehmen) ebenso wie bei Zahlungen in Online-Shops.



Zahlungsdienstleister 2/3

Wissenswertes zum Zahlungsverkehr

Um zu verstehen, was ein Zahlungsdienstleister eigentlich macht, hilft es, den Weg zu verfolgen, den ein Zahlungsbetrag nimmt, wenn ein Kunde bei einem Händler ein Produkt erwirbt oder eine Dienstleistung in Anspruch nimmt. Grundsätzlich muss der Zahlungsbetrag vom Bankkonto des Kunden abgebucht und dem Bankkonto des Händlers oder Dienstleisters gutgeschrieben werden.

Barzahlung

Im Fall der Barzahlung ist der Vorgang sehr einfach: Der Kunde hebt bei seiner Bank Bargeld ab und überreicht es im Geschäft dem Händler oder zahlt im Restaurant seine Rechnung und erhält seine Ware oder z.B. Speisen. Rechtlich gesehen, schließen beide Parteien mündliche Verträge entsprechend den Regelungen des Bürgerlichen Gesetzbuches (BGB) ab. Der Händler oder Gastronom nimmt dann das erhaltene Bargeld und zahlt es auf seiner Bank auf sein Konto ein. Diese Transaktion erfordert keinen Zahlungsdienstleister.

Bargeldlos ist etwas komplizierter

Für den bargeldlosen Verkehr werden Technik, sowie Verträge zur Absicherung aller Beteiligten benötigt. Möchte der Kunde bargeldlos z.B. mit der Bankkarte seiner Bank zahlen, ist der Vorgang schon nicht mehr so einfach. Eine Grundlage für bargeldloses Zahlen ist ein Vertrag zwischen Kundenbank und Händler. Dieser Vertrag verpflichtet die Kundenbank, dem Händler den Zahlungsbetrag auf das Händlerkonto zu überweisen, wenn der Kunde eine Ware erwirbt. Den Erwerb der Ware muss der Händler gegenüber der Kundenbank nachweisen. Als Nachweis gilt, dass der Kunde der Zahlung zustimmt. Im Fachbegriff heißt das »die Zahlung autorisieren«. Den Zahlungsbetrag belastet die Kundenbank außerdem dem Kundenkonto.

Die Zahlungsautorisierung an die Bank erfolgt elektronisch über ein Kartenlesegerät. Außer dem vorgenanntem Vertrag benötigt der

Händler also auch noch Hard- und Software. Das sind das Kartenlesegerät selbst sowie die Programme, welche die Kommunikation zwischen dem Kartenlesegerät und den Zahlungssystemen der Kundenbank erlauben. Hat der Händler nun den Vertrag mit der Kundenbank und das Kartenlesegerät am POS (Point of Sale oder Kartenlesegerät), kann er ausschließlich mit dieser einen Bank bargeldlose Zahlungen abwickeln.

Damit der Händler für bargeldlose Zahlungen mit den Kundenbanken seiner weiteren Kunden zusammenarbeiten kann, müsste er mit allen Kundenbanken Verträge abschließen und jeweils die zugehörige Zahlungstechnik anschaffen. Diese vertragliche und technische Anbindung an viele Banken ist zwar möglich, aber offensichtlich keine praktikable Lösung. Darüber hinaus bleibt es nicht nur bei einer Bankkarte und einer Vielzahl weiterer Möglichkeiten für den bargeldlosen Zahlungsverkehr.

Ein Zahlungsdienstleister schafft nun die Möglichkeit, dass alle Händler und Banken, Kreditkartenunternehmen, PayPal & Co. miteinander Zahlungen mit vertretbarem Aufwand und zu niedrigen Kosten abwickeln können. Der Zahlungsdienstleister tritt als Vermittler zwischen Banken, Zahlungssystemen und Händlern auf. Das gilt nicht nur an den POS (Point of Sale), sondern auch bei Online-Shops, die meist über noch eine viel größere Zahl an Kunden verfügen. Bei Online-Shops entfällt das Kartenlesegerät natürlich, die technische Anbindung von Online-Shops an die Zahlungssysteme ist aber erforderlich. Diese technisch durchaus komplexe Anbindung leisten die Zahlungsdienstleister.

Fazit

Die Zahlungsdienstleister oder Payment-Service-Provider vollziehen also die Annahme, Authentifizierung sowie die Abwicklung von Zahlungen. Für ihre Dienstleistung erheben die verschiedenen Zahlungsdienstleister unterschiedlich hohe Gebühren.

Zahlungsdienstleister 3/3

Einige Gedanken zum bargeldlosen Zahlungsverkehr

- Am bargeldlosen Zahlungsverkehr sind mindesten 4 bis 5 Unternehmen beteiligt und alle Beteiligten müssen einen zuverlässigen Zahlungsverkehr jederzeit garantieren.
- Weiterhin gibt es staatliche Aufsichtsinstanzen, die für ihre Prüfung Zugang zu der technischen und verwaltungstechnischen Abwicklung des gesamten Zahlungsverkehr benötigen.
- Bei Verstößen gegen das geltende Recht, bekommen die ermittelnden Polizeibehörden per Gerichtsbeschluss einen ausreichenden Zugang zum interessierenden Zahlungsverkehr.
- Im bargeldlosen Zahlungsverkehr verschwindet schon seit Jahren sehr viel mehr Geld, als beim Zahlungsverkehr mittels Papiergeld bekannt geworden ist. Und das sind nur die Informationen die durch die Banken weltweit »freiwillig« öffentlich bekannt gegeben werden.
- Weiterhin ist es durchaus möglich, dass nicht autorisierte Personen mit Insider-Kenntnisse über die Schwächen des Zahlungsverkehres zu deutlich informiert sind und bei ausreichender krimineller Energie versucht sind diese Kenntnisse auch anzuwenden oder diese Informationen an Interessierte Personenkreise weitergeben oder verkaufen.
- Die Kartenlesegeräte strahlen während der Zahlungsabwicklung einige Informationen in die nähere Umgebung ab, die durch Fachleute oder andere gut informierte Personen mit der entsprechenden technischen Ausrüstung gelesen werden können.

In Deutschland ist ein Fall bekannt geworden, wo zertifizierte Kartenlesegeräte während der Hauptgeschäftszeit, von scheinbar berechtigten Personen gegen manipulierte Kartenlesegeräte ausgetauscht wurden. Mit den Informationen von den manipulierten Kartenlesegeräte können z.B. gefälschte Bank- und Kreditkarten erstellt werden.

Bei wachsamem Karteninhabern können diese gefälschten Bank- und Kreditkarten, möglicherweise nur 3 bis 4 Tage genutzt werden.



Was ist ein Token? 1/5

Die Verwendung und Deutung des Begriffes »**Token**« (englisch: Zeichen, Marke, Münze), kann schon etwas sehr verwirrend sein.

- Ein Token kann ein Vermögenswert, Vermögensgegenstand oder ein Wirtschaftsgut repräsentieren. Im Gegensatz zu Münzen (Coins) haben Token keine eigene Blockchain. Sie können jedoch mit relativ wenig Aufwand auf existierenden Blockchains erzeugt werden. Token werden häufig wie Aktien oder Anteilscheine an einem Projekt benutzt. Daher können sie einerseits als **Treibstoff für das Netzwerk**, andererseits als **Unternehmensanteile** oder **Stimmrechte** im Blockchain-Projekt dienen.

Token sind also grundlegende Bausteine für Operationen mit Kryptowerten. Sie dienen als Hilfsmittel zur Identifizierung und Authentifizierung von Usern eines Computer-Netzwerks. Nur wer ein gültiges Token besitzt, ist dazu berechtigt, eine Transaktion auf der zugehörigen Blockchain auszuführen. Zahlungen im Internet lassen sich so sehr einfach, schnell und kostengünstig durchführen.

- In der Datenverarbeitung wird die Methode der tokenbasierten Kompression (englisch: token-based compression) angewendet, um Speicherplatz zu sparen. Dabei werden die Seiten eines Dokuments als eine Ansammlung aus im Dokument vorkommenden Symbolen (Tokens) repräsentiert. Positionsinformationen geben an, wo die Symbole erscheinen sollen. Jedes Symbol ist hierbei eine Abbildung eines Teils des Dokuments, etwa ein Buchstabe, ein Wort oder eine Grafik. Häufig wiederkehrende Schlüsselwörter werden durch Abkürzungen, Tokens, ersetzt.

Beispiel:

Ausgangstext: Print "Hallo"; Print "Hier"
kodierter Text: 3F "Hallo"; 3F "Hier"



- Ein Token ist aber auch ein Hilfsmittel zur Synchronisation paralleler Prozesse - wer ein Token besitzt, darf auf die Ressource (zum Beispiel einen Speicherbereich oder eine Schnittstelle) zugreifen. Wenn der Besitzer den Token wieder freigegeben hat, darf ein Konkurrent als neuer Besitzer des Tokens die Ressource benutzen, bis er den Token ebenfalls wieder freigibt.

Das Token-Verfahren wird in einem Rechnernetz eingesetzt, um Kollisionen beim Zugriff auf Ressourcen zu verhindern und sicherzustellen, dass alle angeschlossenen Rechner Gelegenheit zum Zugriff und Nutzung von Ressourcen bekommen.

Die Token fungieren in geschlossenen Computer-Netzwerken also als eine Art des Identifizierungs-Zugangs.

Was ist ein Token? 2/5

Arten von Token im Finanzwesen und Informatik

- **Utility Token:** Diese Tokens dienen als Tausch- oder Betriebsmittel, das bestimmte Funktionalitäten, Abstimmungsrechte oder Zugänge gewährleistet. Startups nutzen Utility Tokens beispielsweise zur Kapitalbeschaffung. Sie dürfen Anleger und Anlegerinnen Zugang zu Produkten oder Dienstleistungen, jedoch keinen finanziellen Anreiz bieten.
- **Equity Token:** Unternehmensanteile, die man als Investor erwerben kann. Sie sind insbesondere für junge Unternehmer eine Alternative zur Börse, um sich zu finanzieren. Diese Form ist derzeit auf Krypto-Börsen nicht handelbar.
- **Security Token:** Spezielle Hardwarekomponente zur Identifizierung und Authentifizierung von Benutzern. Um die Authentifizierung zusätzlich abzusichern, werden beispielsweise eine PIN oder ein Passwort eingesetzt. Security Token dürfen nicht auf Krypto-Börsen gehandelt werden.
- **Asset Token:** Realwirtschaftliche Güter, die als Absicherung dienen. Ihr Wert ist fest mit realen Gütern verknüpft, wie beispielsweise Immobilien, Edelmetalle und andere Kapitalanlagen.
- **Payment/Currency Token:** Währungstoken, die speziell für finanzielle Transaktionen genutzt werden. Sie stellen die Währungseinheit einer eigenständigen Kryptowährung wie Bitcoin, Ripple, Ether & Co. dar.
- **Governance Token:** Ein Governance Token verleiht seinen Besitzern die Möglichkeit, über Entscheidungen, wie beispielsweise über das Protokoll oder Funktionen des Netzwerkes, mitzubestimmen.
- **Non-fungible Token:** Ein Non-fungible Token (NFT) ist eine nicht austauschbare digitale Marke, die den Besitz an bestimmten Vermögenswerten protokolliert. NTFs sind einzigartig und daher nicht austauschbar. Am häufigsten werden sie im Zusammenhang mit Kunstwerken verwendet.

Token sind im Kontext von Kryptowerten gesonderte Einheiten, die ihre Inhabern zu einer Handlung auf eine digitalen Ressource, zumeist einer Blockchain, berechtigen.

Der Unterschied zu Coins ist, dass ein Token immer in einem geschlossenen System bleiben muss und außerhalb dieses Netzwerks keine Anwendung findet.

Hinweis: Alle Token haben eine unterschiedlich lange Gültigkeit. Bis zum Ablauf des festgelegten Zeitrahmens bleibt der Token gültig.

Bauformen und Technologien

Der technische Überbegriff Token bezeichnet alle eingesetzten Technologien gleichermaßen und hängt nicht von einer bestimmten Erscheinungsform der Hardware ab. Dazu gehören alle Gegenstände, die Informationen zum Zweck der Identifikation und Authentifizierung speichern und übertragen können.

Passive Medien

Bei Smartcards handelt es sich ebenfalls um Token. USB-Token, welche an einem USB-Port angeschlossen werden, weisen die Vorteile einer Smartcard auf, ohne dabei ein Kartenlesegerät zu benötigen.

Es kommen auch kontaktlose Token zum Einsatz. Diese sogenannten RFID-Transponder (RFID ... Radio Frequency Identification) können in Schlüsselanhänger, Chipkarten und jedes andere Produkt integriert sein, solange dessen Eigenschaften die Funktion nicht stören. Somit wird das jeweilige Produkt selbst zum Token. Die Gegenstation muss den Token aktivieren und auch lesen können.

Übliche Verwendungen:

- Fahrzeug- und Gebäudeschlüssel
- Kleidung, Armbanduhren und Schmuck
- Implantate in Tieren (Chipping)

Was ist ein Token? 3/5

Es gibt auch Tokengeneratoren, welche eine stetig wechselnde und zeitlich begrenzt gültige Zahlenkombination als Sicherheitstoken nach dem Einmal-Passwort-Verfahren (One-Time Password- (OTP-)) anzeigen. Generator und Server errechnen diese pseudozufällige Zahl gleichzeitig. Somit ist eine eindeutige Authentifizierung möglich. Diese Zahl wird gegebenenfalls auch mit einer Smartcard in einem tragbaren Lesegerät erzeugt. Als zusätzliche Sicherheitsmerkmale muss häufig eine PIN und/oder ein Anforderungscode in das Gerät eingegeben werden. Beispiel hierfür ist das Smart-TAN-Verfahren.

Trusted Platform Modules (TPM) sind Chips, die ähnlich einer Smartcard geheime Schlüssel speichern. Der Chip ist in diesem Fall aber fest in ein Gerät eingebaut (z.B. auf ein Computer-Mainboard). Es besteht nun die Möglichkeit, ein über das TPM eindeutig identifizierbares Gerät einem Benutzer zuzuordnen. Das TPM bietet gleichzeitig die Möglichkeit der Zugangssicherung zum Gerät (Pre-Boot Authentication). Somit kann (indirekt) eine Authentifikation des Benutzers vorgenommen werden.

Aktive Medien

Es gibt auch handelsübliche Geräte, welche als Token arbeiten und einen Authentifikationsfaktor übertragen. Dazu muss für die Authentifizierung eine sichere Kommunikation zwischen dem Gerät und dem Prüfgerät oder Arbeitsplatz gewährleistet sein.

Bekannte Beispiele sind:

- Mobiltelefone oder Smartphones
- USB-, NFC- und Bluetooth-Token
- aktive RFID-Transponder
- herkömmliche Chip-Karten
- RFID NFC (RFID ... Radio Frequency Identification, NFC ... Near Field Communication) mittels Smartphones

Einsatzzwecke

Security-Token kommen meist als Benutzer-Ausweise zur Absicherung von Transaktionen zum Einsatz:

- zur Anmeldung an Arbeitsplatzrechner, (Firmen- oder Behörden-)Netzwerke, z.B. eine Netzwerk-Domäne
- zur Nutzung von Internetdiensten, insbesondere als HBCI-Karte beim Onlinebanking
- als Schlüsselcontainer für Daten- und E-Mail-Verschlüsselung sowie digitale Signaturen
- als Zugangsberechtigung und Ausweis (z. B. Firmenausweis, E-Pass, Autoschlüssel)
- zur Personalzeiterfassung
- als SIM-Karte in Mobiltelefonen (subscriber identity module)
- als Zahlungsmittel und/oder Kundenkarte an Automaten und Kundenterminals (z. B. Telefonzelle)
- als Zugangskarte zu Pay-TV Angeboten
- als Bankkarte, meist in Einheit mit der Geldkarte, zur Nutzung von Geldautomaten und Bezahlterminals
- als Krankenversicherungskarte; auch die (zukünftige); Die elektronische Gesundheitskarte wird als Token für den Zugang zu einem Datennetz eingesetzt.
- als Fahrkarten und Eintrittskarten
- als Sicherheitsmodul zur eindeutigen Identifikation z. B. Trusted Platform Module
- beim Digital Rights Management; hier wird das Nutzungsrecht an Daten (Software, Musik, E-Books, ...) eventuell an die Hardware gebunden

Allgemein werden dezentrale Systeme, in denen Daten auf dem Token selbst gespeichert waren, immer häufiger durch vernetzte Systeme ersetzt, in denen der Token nur noch als Ausweis dient.

Durch die Herausgeber der Token werden bevorzugt mehrere

Was ist ein Token? 4/5

Funktionen in einen Token integriert um einen »Mehrwert« durch die Benutzung des Tokens zu erreichen und **umfassende Nutzungs- und Bewegungsprofile** zu erstellen.

Ablauf einer Authentifizierung mit einem Security-Token

1. Der Nutzer leitet den Datenaustausch zwischen Token und Prüfsystem ein, indem er z. B. das Token vor ein Lesegerät hält.
2. Das Lesegerät identifiziert das Token über dessen eindeutige Identifikationsnummer(n), wie dessen Typennummer, eine Medien-Seriennummer, eine Träger-Registriernummer und/oder eine Benutzer-Klassennummer.
3. Der vom Token gelesene Datensatz wird vom Prüfsystem mit entsprechenden lokalen Referenzdaten nach einem wohl definierten Prüfverfahren verglichen: Die Authentifizierung des Tokens erfolgt mittels Challenge-Response-Authentifizierung (Überprüfung der Identität durch Aufforderung, die zu einer entsprechenden Antwort führt), eventuell werden hierfür weitere Prüfdaten als zusätzliche Sicherheitsmerkmale, etwa eine PIN vom Träger des Tokens abgefragt.
4. Zur Sicherheit werden die lokalen Referenzdaten mit weiteren Referenzdaten aus einer Datenbank von einem entfernten Server verglichen.
5. Bei ungültigem Token oder ungültigen weiteren Referenzdaten weist das Prüfsystem weitere Zugriffe ab.
6. Zur Rückverfolgung der Authentifizierung werden Ereignisdaten des Prüfungsvorgangs an den Server zurück übermittelt.
7. Das Prüfsystem gibt die für den Träger des Tokens zulässige Benutzung, wie Funktionen und/oder Daten frei.

Hinweis: Für sicherheitskritische Anwendungen muss ein Security-Token ein einmaliger Gegenstand sein, der gegen Manipulation und Vervielfältigung bzw. Fälschung besonders gesichert ist.

Vorteile und Nachteile

Vorteile:

Der Einsatz von Token bietet eine maximale Sicherheit gegen unberechtigte Nutzung unter folgenden Bedingungen:

- mindestens ein weiteres Authentifizierungsmerkmal wird eingesetzt, z.B. PIN.
- das Token ist tatsächlich einmalig und kann nicht vervielfältigt oder manipuliert werden, siehe Skimming bei EC-Karten und Kreditkarten (skimming ... kriminelles Auslesen von Daten auf Zahlkarten)
- das Token kann im Falle eines Diebstahls oder Verlustes im System gesperrt werden, um unberechtigte Benutzung auszuschließen
- Token können mit Funkverfahren verdeckt eingesetzt werden

Nachteile:

- Ein Token als alleiniges Authentifizierungsmerkmal ohne zweites unabhängiges Authentifizierungsmerkmal bietet keinen zuverlässigen Schutz gegen Manipulation, Verlust oder Attacken;
- der Einsatz von Token verursacht wie jede technische Lösung Kosten für die Herstellung, die Registrierung und/oder Personalisierung, die Verteilung und die Bereitstellung von Infrastruktur in Form von Prüf- oder Lesegeräten und Software;
- das Token kann zerstört oder verloren werden und den Benutzer dann zeitweise von wichtigen Funktionen des täglichen Lebens oder beruflicher Tätigkeit ausschließen;
- das Token, und damit dessen Nutzer, ist immer eindeutig identifizierbar: eine Freigabe von Zugriffen für anonyme Nutzer ist wegen mangelnder Sicherheit nicht vorgesehen.

Was ist ein Token? 5/5

Software-Token

Neben den Hardware-Token gibt es auch Software- oder Soft-Token. Software-Token sind auf elektronischen Geräten gespeichert und können dupliziert werden. Bei Hardware Tokens können die Berechtigungsnachweise im Gegensatz dazu - nicht dupliziert werden, es sei denn, man dringt physisch in das Gerät ein.

Da es sich bei Software-Tokens um etwas handelt, das man nicht physisch besitzt, sind sie besonderen Bedrohungen ausgesetzt, die auf der Vervielfältigung des zugrunde liegenden kryptografischen Materials beruhen (z.B. durch Malware). Sowohl Hardware- als auch Software-Tokens sind anfällig für Bot-basierte Man-in-the-Middle-Angriffe oder für einfache Phishing-Angriffe, bei denen das vom Token bereitgestellte Einmalpasswort erfragt und dann rechtzeitig an die echte Webseite übermittelt wird. Software-Token haben Vorteile: Man muss keinen physischen Token mit sich führen, sie enthalten keine Batterien, die irgendwann leer werden, und sie sind billiger als Hardware-Token.

Einige neuere Software-Tokens basieren auf der Public-Key-Kryptographie oder asymmetrischer Kryptographie. Diese Architektur beseitigt einige der traditionellen Schwächen von Software-Tokens, aber nicht ihre Hauptschwäche - die Möglichkeit der Duplizierung. Eine PIN kann auf einem entfernten Authentifizierungsserver statt auf dem Token-Client gespeichert werden, so dass ein gestohlener Software-Token nur dann verwendet werden kann, wenn auch die PIN bekannt ist.

Im Falle von Malware-Angriffen kann das kryptografische Material jedoch dupliziert und die PIN bei der nächsten Authentifizierung des Benutzers über Keylogging oder ähnliche Verfahren abgefangen werden. Wenn Versuche unternommen werden, die PIN zu erraten, kann dies erkannt und auf dem Authentifizierungsserver

protokolliert werden, wodurch das Token deaktiviert werden kann. Die Verwendung asymmetrischer Kryptographie vereinfacht auch die Implementierung, da der Token-Client sein eigenes Schlüsselpaar erzeugen und öffentliche Schlüssel mit dem Server austauschen kann.

Open-Source-Datenbanken 1/3

Für einen reibungslosen Ablauf, für eine sorgfältige und strukturierte Speicherung und Lagerung sämtlicher Daten sowie für die Vergabe und Kontrolle der Zugriffsrechte ist eine gute Datenbank für die meisten Unternehmen unerlässlich. Das ist zwar schon seit langer Zeit so, ebenso lange war der Unterhalt einer solchen Datenbank aber mit hohen Kosten verbunden. Mittlerweile gibt es immer mehr Open-Source Datenbanken, die sehr verlässlich funktionieren.

Bei der Entscheidung, welche Open-Source Database die richtige Datenbank ist, spielen viele Faktoren eine Rolle. Neben der Geschwindigkeit bei der Verarbeitung vieler kleiner oder großer Datensätze, sind auch die Möglichkeiten des Austausches mit einer Community zu beachten. Durch den offenen Quellcode der Open Source Datenbanken, ist ein uneingeschränktes Vertrauen in die Software überhaupt erst möglich.

Fehler und Sicherheitslücken werden bei Open Source Projekten in der Regel schnell aufgedeckt und transparent behoben. Diese Argumente sind einzeln oder zusammen genommen für viele Unternehmen ausschlaggebend, um auf die offene Variante umzusteigen. Dabei gilt aber natürlich nicht automatisch, dass kostenlos zwangsläufig auch besser ist. Ein Vergleich der freien Datenbanken lohnt sich immer.

Es gibt eine riesige Anzahl unterschiedlicher Open Source Datenbanken im Vergleich zu den wenigen großen Anbietern, die den Markt lange unter sich aufgeteilt haben. Zum einen gibt es Zusammenschlüsse motivierter Entwickler, die innovative und zuverlässige Lösungen suchen und so neue Optionen für Unternehmen schaffen. Zum anderen gibt es aber auch jene Anbieter, die durchaus einen kommerziellen Ansatz verfolgen, dabei aber auf den Input einer interessierten Community gerne zurückgreifen.



PostgreSQL

Die **SQL-Datenbank** PostgreSQL ist hinlänglich bekannt auf dem Feld der Open-Source-Datenbanken. Schließlich gehen die Ursprünge des objektrelationalen Datenbankmanagementsystems bis in die 1980er Jahre zurück. Die Software konnte unter der BSD-Lizenz (BSD ... Berkeley Software Distribution) über die Jahre stetig wachsen und verbessert werden und ist größtenteils mit dem SQL-Standard (SQL ... Structured Query Language) kompatibel. Die Open-Source-Datenbank ist plattformunabhängig nutzbar, wobei Client und Server auf verschiedenen Systemen laufen können. PostgreSQL kann einfach und unproblematisch erweitert und angepasst werden, weshalb auch zahlreiche große Unternehmen auf diese Datenbank setzen.

Hinweis: Relationalen Datenbanksystemen speichern und verwalten die Informationen in Tabellen. Das hört sich einfach an, ist jedoch mit komplexen Konzepten wie den 5 Normalformen, Schlüsselbeziehungen und JOINS (Datenbank-Tabellen mittels Abfragen verbinden) verbunden.

Open-Source-Datenbanken 2/3

Vorteile: hohe Kompatibilität mit SQL-Standards, Plattformunabhängig nutzbar, zahlreiche Features, viele Anpassungen und Erweiterungen möglich, unterstützt JSON (JavaScript Object Notation, das Datenformat kann von jeder Programmiersprache gelesen werden), kann komplexe Datentypen verarbeiten, hat eine große Community und daher ein gutes Monitoring

Nachteile: Administration ist vergleichsweise fordernd, geringere Lesegeschwindigkeit im Vergleich zu anderen Open-Source Datenbanken, schwierige Anbindung an einige Frameworks

Apache Cassandra

Gerade bei besonders großen Datenmengen können Open-Source-Datenbanken an ihre Grenzen stoßen. Eine ausdrückliche Ausnahme ist Apache Cassandra. Das Datenbankmanagementsystem basiert auf Java und überzeugt durch seine Nulltoleranz für Ausfallzeiten. 2008 wurde das System von Facebook veröffentlicht, heute verfügt es über eine eigene Abfragesprache. Apache Cassandra ist eine spaltenorientierte **NoSQL-Datenbank** und verteilt die gewaltigen Datenmengen auf verschiedene Cluster. Auch im Bereich der Analyse und Protokollierung punktet Apache Cassandra im Vergleich mit anderen Open-Source Datenbanken.

Vorteile: Ideal für große Datenmengen, hohe Fehlertoleranz, gute Ergebnisse bei Analyse und Protokollierung, starke Performance, hohe Skalierbarkeit

Nachteile: geringere Lesegenauigkeit, keine ACID-Eigenschaften

Hinweis: Der Begriff ACID (Atomicity, Consistency, Isolation, Durability) beschreibt Regeln und Eigenschaften zur Durchführung von Transaktionen in Datenbankmanagementsystemen (DBMS). Hält die Transaktion das ACID-Prinzip ein, gelten die Informationen in den Datenbanksystemen als verlässlich und konsistent.

MongoDB

MongoDB ist eine **NoSQL-Datenbank**. Sie überzeugt unter anderem im Umgang mit mobilen Apps, Produktkatalogen und Content Management. Die dokumentbasierte Datenbank läuft auf verschiedenen Betriebssystemen, wobei die Daten bei MongoDB im BSON-Format in sogenannten Collections gespeichert werden. Weil diese auf verschiedene Server verteilt werden, erhöht sich die Verfügbarkeit und die Datenlast wird von mehreren Servern getragen. Seit der Erstveröffentlichung 2009 wurde MongoDB stetig weiterentwickelt und gehört heute zu den beliebtesten und meistgenutzten NoSQL-Datenbanksystemen weltweit. Neben der kostenlosen Open-Source-Variante gibt es auch eine kommerzielle Version mit zusätzlichen Features für Unternehmen.

Vorteile: einfache Änderung der Datenstruktur, hohe Skalierbarkeit, hohe Flexibilität und einfache Verwaltung großer unstrukturierter Datenmengen, gut nutzbar im Umgang mit mobilen Apps

Nachteile: keine Unterstützung für JOINS (Datenbank-Tabellen mittels Abfragen verbinden), höhere Speicheranforderungen

Hinweis: BSON (Binary JSON) ist die binäre Codierung von JSON-ähnlichen Dokumenten, die MongoDB beim Speichern von Dokumenten in Sammlungen verwendet. Es bietet Unterstützung für Datentypen wie Datum und Binär, die in JSON nicht unterstützt werden.

MySQL und MariaDB

Soll es allerdings doch eine **SQL-Datenbank** werden, schwören viele Firmen auf MySQL. Das Datenbankmanagementsystem, das bereits seit 1995 erhältlich ist, überzeugt durch eine sehr einfache und intuitive Administration und eine schnelle Installation auf verschiedenen Betriebssystemen. Auch die Pflege des Systems ist leicht durchzuführen. Leider sind viele zusätzliche Features, die zum

Open-Source-Datenbanken 3/3

Teil für eine ideale Nutzung auf höchstem Niveau unabdingbar sind, nur in der kostenpflichtigen Version erhältlich. Gerade in den Bereichen Datensicherheit und Monitoring offenbart die kostenlose Datenbank Schwächen.

Der Datenbankserver MariaDB stammt von denselben Entwicklern wie MySQL und enthält auch sämtliche Sicherheitspatches der älteren Datenbank. MariaDB funktioniert ebenfalls in der Nutzung ähnlich und kann die Funktionen von MySQL auch anbieten. Die erwähnten kostenpflichtigen Features finden sich hier nach wie vor zur freien Verwendung. Durch die große Community im Hintergrund schreitet MariaDB stetig voran und wartet so mit neuen Funktionen auf. Eine Engine für verteilte Transaktionen, eine höhere Geschwindigkeit im Vergleich zu MySQL, dynamische Spalten und einiges mehr sorgen dafür, dass sich die Datenbank im Vergleich zu anderen Datenbanksystemen nicht verstecken muss.

Vorteile: Standard für viele Unternehmen, intuitive Administration, kompatibel mit vielen Betriebssystemen, hohes Speichervolumen, einfacher Wechsel von MySQL auf MariaDB

Nachteile: viele Features kostenpflichtig (MySQL), keine Migration von MariaDB auf MySQL möglich

Redis (Remote Dictionary Server)

Die In-Memory-Datenbank Redis arbeitet ebenfalls nicht relational und gehört somit zur **NoSQL-Familie**. Die Database überzeugt vor allem durch ihr Tempo (mit Reaktionszeiten unter einer Millisekunde) und die besonders einfache Nutzung. Gerade im Bereich des Caching schwören viele Unternehmen auf Redis. Abzüge gibt es dagegen beim Umgang mit komplexeren Datenstrukturen. Da die Daten bei In-Memory-Datenbanken direkt im Arbeitsspeicher abgelegt werden, benötigt der Remote Dictionary Server deutlich mehr Arbeitsspeicher im Vergleich zu anderen Datenbanken.

Vorteile: extrem schnelle Reaktionszeiten, intuitive Nutzung, gute horizontale und vertikale Skalierung, Clients für fast jede Programmiersprache, Verteilung auf verschiedene Server

Nachteile: hoher Speicherbedarf, noch ausbaufähig im Umgang mit komplexen Datenstrukturen

Open-Source-Datenbanken und die Cloud

Statt stationäre Datenbanken zu unterhalten, weichen immer mehr Unternehmen auf Cloud-Lösungen aus. Die Vorteile liegen auf der Hand: statt eines kostenintensiven und stromfressenden Servers vor Ort werden die eigenen Daten ausgelagert.

Neben der kompletten Verlagerung in die Private- oder Public-Cloud, gibt es auch Hybrid-Modelle, die neben der Cloud auch ein Teil der Daten im eigenen Haus belassen. Gerade bei besonders großen Datensätzen kann das ein kluger Ansatz sein. Die entstehenden Kosten lassen sich in der Regel gut abschätzen und sie sind keinen starken Schwankungen unterworfen. Teure Hard- oder Software muss bei Cloud-Lösungen nicht angeschafft oder auf den neuesten Stand gebracht werden. Auch die Verknüpfung verschiedener Standorte ist mit einem Cloud-Modell einfacher.

Alle hier vorgestellten Open-Source-Datenbanken eignen sich auch für den vollständigen oder hybriden Einsatz in einer Cloud. Wenn man sich für eine Cloud-Lösung entscheidet, ist man vermutlich auch an hochskalierbaren Datenbanken interessiert. Gleichzeitig wünscht man sich auch schnelle Reaktionszeiten, da durch die Verbindung zur Cloud ohnehin schon leichte Latenzen auftreten können. Hier spielen vor allem Apache Cassandra und Redis ihre Stärken aus, da diese beiden Datenbanksysteme sowohl hochskalierbar sind als auch mit guter Performance beeindrucken.

Der Begriff ACID (Atomicity, Consistency, Isolation, Durability) beschreibt Regeln und Eigenschaften zur Durchführung von Transaktionen in Datenbankmanagementsystemen (DBMS). Hält die Transaktion das ACID-Prinzip ein, gelten die Informationen in den Datenbanksystemen als verlässlich und konsistent.

ACID steht für die vier englischen Einzelbegriffe Atomicity, Consistency, Isolation und Durability und ist eine gängige Abkürzung in der Informationstechnik. Im Deutschen lauten die vier Begriffe Atomarität, Konsistenz, Isolation und Dauerhaftigkeit. Oft wird im deutschsprachigen Raum das Akronym AKID verwendet. Das ACID-Prinzip stellt Regeln auf, wie mit Transaktionen in Datenbankmanagementsystemen zu verfahren ist, um für verlässliche, konsistente Daten und Systeme zu sorgen. Eine Transaktion besteht aus einer Folge verschiedener Vorgänge, die diese ACID-Regeln einzuhalten haben.

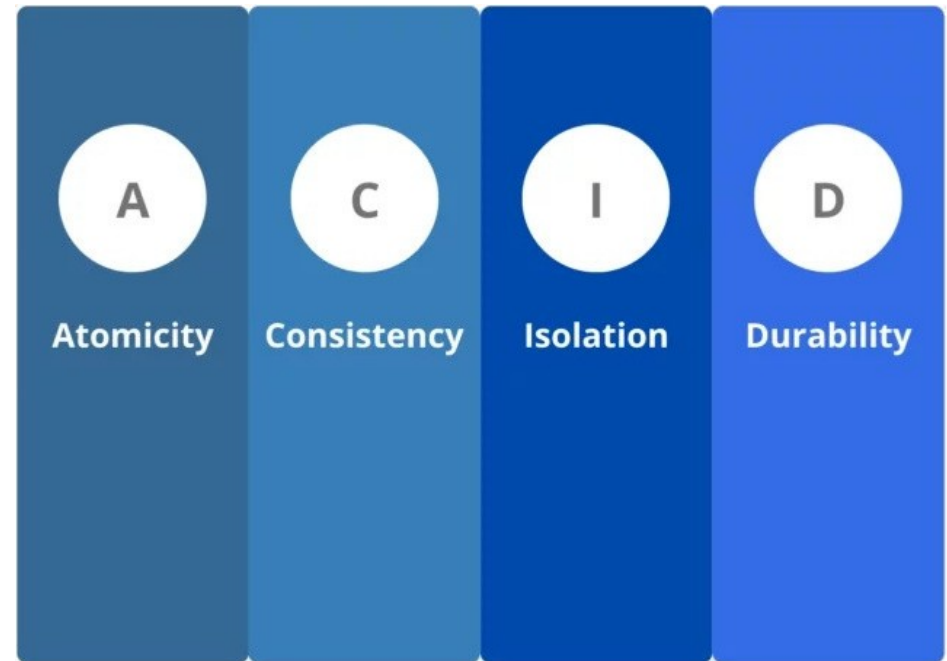
Die vier ACID-Grundprinzipien

Das ACID-Konzept besteht aus vier einzelnen Grundprinzipien. Diese Grundprinzipien lauten:

- Atomicity (Atomarität): Ausführung aller oder keiner Informationsteile einer Transaktion
- Consistency (Konsistenz): Transaktionen erzeugen einen gültigen Zustand oder fallen in den alten Zustand zurück
- Isolation (Abgrenzung): Transaktionen verschiedener Anwender oder Prozesse bleiben voneinander isoliert
- Durability (Dauerhaftigkeit): Nach einer erfolgreichen Transaktion bleiben die Daten dauerhaft gespeichert

Atomicity oder Atomarität: Eine Transaktion besteht aus einer Sequenz einzelner Aktionen. Diese Sequenz muss so ablaufen, dass entweder alle Einzelschritte komplett oder gar nicht ausgeführt werden. Treten während einer Sequenz Fehler auf, hat das System

dafür zu sorgen, dass sämtliche bereits durch die Transaktion erfolgten Änderungen zurückgenommen werden. Alle Informationen einer unterbrochenen Transaktion sind ohne Spuren aus der Datenbank zu entfernen. Die einzelnen Datenbank-Operationen einer Transaktion sind erst gültig, wenn sie alle abgeschlossen sind. Datenbanksysteme realisieren die Atomarität durch ausführliches Logging aller durchgeführten Aktionen.



Consistency oder Konsistenz: Ist eine Transaktion erfolgreich abgeschlossen, muss sie in der zuvor konsistenten Datenbank einen wieder konsistenten Zustand hinterlassen. Es sind vor dem Abschluss der Transaktion die in einer Datenbank definierten Bedingungen für die Integrität und logische Konsistenz der Daten zu prüfen. Solche Bedingungen können die Einhaltung bestimmter Wertebereiche, das Vorhandensein von Schlüsseigenschaften oder

Datenbanken – Was ist ACID? 2/3

die Eindeutigkeit von Beziehungen sein. Führt eine Transaktion zur Verletzung der Konsistenzbedingungen, wird sie zurückgewiesen und sämtliche Daten werden auf den Zustand vor der Transaktion zurückgesetzt. Die Konsistenz ist vor und nach einer Transaktion sicherzustellen. Während der Transaktion dürfen durchaus inkonsistente Zustände auftreten.

Isolation oder Abgrenzung: Mit einer Datenbank arbeiten mehrere Benutzer oder Prozesse gleichzeitig. Sie lesen oder schreiben parallel Daten. Die Isolation (Abgrenzung) stellt sicher, dass die Nutzung der Datenbank durch mehrere Anwender keine negativen Auswirkungen nach sich zieht. Ereignisse wie das gegenseitige Überschreiben oder Löschen einzelner Datensätze ist unter allen Umständen zu verhindern. Für jeden Benutzer erscheint das Datenbankmanagementsystem wie ein exklusiv genutztes System, in dem sich die Transaktionen gegenseitig nicht beeinflussen und parallele Zugriffe unsichtbar bleiben. Man spricht auch von der Integrität des Ablaufs. Datenbanksysteme realisieren die Isolation mithilfe von Sperrverfahren.

Durability oder Dauerhaftigkeit: Ist eine Transaktion ausgeführt und konsistent, sind ihre Informationen dauerhaft in der Datenbank gespeichert. Zukünftige Fehler, Speicherausfälle oder Systemabstürze dürfen nicht dazu führen, dass Daten gelöscht und nicht mehr hergestellt werden können. Die Dauerhaftigkeit lässt sich in einem Datenbankmanagementsystem ähnlich wie die Atomarität durch Logging-Maßnahmen realisieren. Mit einem Transaktionslog sind die Informationen nach einem Systemausfall durch Ausführung der protokollierten Schreib-Operationen reproduzierbar.

Vorteile durch die Einhaltung der ACID-Prinzipien

Durch die Einhaltung der ACID-Prinzipien entstehen bei der Arbeit mit Datenbanken zahlreiche Vorteile. Sowohl Anwender als auch Entwickler können von einer fehlerfreien Umgebung und konsistenten Daten ausgehen. Ist eine Transaktion vollständig ausgeführt, ist die

Verfügbarkeit und Dauerhaftigkeit der Daten sichergestellt. Fehler während Transaktionen führen nicht zu fehlerhaften oder inkonsistenten Informationen in der Datenbank. Aufwendige manuelle Recherche- und Änderungsarbeiten zur Bereinigung von Fehlern sind nicht notwendig. In Mehrbenutzersystemen verhindert das ACID-Prinzip die gegenseitige Beeinflussung der Anwender. Eine nachgelagerte Überwachung der Integrität der Daten in den weiterverarbeitenden Anwendungen ist meist überflüssig.

ACID in verteilten Systemen

In verteilt arbeitenden Datenbankmanagementsystemen kann die Einhaltung des ACID-Prinzips zu einem erhöhten Aufwand führen. Insbesondere die parallele Arbeitsweise und die Datenhaltung an verschiedenen Orten der verteilten Systeme kann für ACID kritisch sein.

Die Grundprinzipien von ACID am Beispiel

Das gängigste Beispiel, um die Komponenten von ACID zu veranschaulichen sind Banküberweisungen, bei denen Geld von einem Konto zum anderen transferiert wird. Das Ziel ist es natürlich, dass alle Überweisungen korrekt ablaufen und alle Kunden den Geldbetrag auf dem Konto haben, der ihnen zusteht.

Angenommen es findet eine Überweisung von Konto A auf Konto B statt. Die Atomarität beschreibt, dass Transaktionen entweder komplett ausgeführt werden oder komplett fehlschlagen. Für unser Beispiel bedeutet das, dass wenn Konto A mit dem Geldbetrag belastet wird und es dann zu einem Systemfehler kommt, das Geld dem Konto A einfach wieder gutgeschrieben wird. Würde das nicht passieren, hätten wir Geld vernichtet und das System wäre in einem falschen Zustand.

Der Konsistenz zur Folge muss nach jeder Transaktion festgestellt werden, dass die Datenbank weiterhin in einem konsistenten Zustand ist, also beispielsweise keine widersprüchlichen Daten enthält.

Datenbanken – Was ist ACID? 3/3

Angenommen unsere Beispielbank führt eine Tabelle mit allen Konten und den aktuellen Guthabenbeträgen. In dieser Tabelle ist die Kontonummer ein Primärschlüssel, sodass jede Kontonummer nur einmal in der Datenbank vorkommen darf. Wenn nach einer fehlerhaften Datenbanktransaktion möglicherweise zwei Datensätze zu einer Kontonummer vorliegen, so liegt eine Inkonsistenz vor und die Transaktion muss rückgängig gemacht werden.

Die Isolation besagt, dass mehrere parallel laufende Transaktionen nicht zu anderen Ergebnissen führen darf, als wenn die Transaktionen einzeln und hintereinander stattfinden würden. Wenn also eine Bank während eines oder mehrerer Peaks (Spitzenbelastung) 100 Überweisungen gleichzeitig verarbeiten muss, dann muss sichergestellt sein, dass die Guthaben der betroffenen Konten genauso hoch sind, als wenn die Überweisungen nacheinander stattgefunden hätten.

Abschließend muss die Bank für die Dauerhaftigkeit der Daten gewährleisten können, dass der konsistente Datenbestand nicht durch äußere Einflüsse beeinträchtigt wird. Dazu gehören beispielsweise Stromausfälle, Systemabstürze oder Softwareupdates.

Border Gateway Protocol (BGP) 1/2

Das Border Gateway Protocol (BGP) ist das im Internet eingesetzte Routingprotokoll und verbindet autonome Systeme (AS) miteinander. Diese autonomen Systeme werden in der Regel von Internetdiensteanbietern gebildet.

Das Border Gateway Protocol ist nicht auf das Routing von IPv4 oder IPv6 beschränkt, sondern kann auch für andere Protokolle oder MPLS-Label (MPLS ... Multiprotocol Label Switching) verwendet werden. BGP ist optimiert für eine maximale Skalierbarkeit und hohe Zuverlässigkeit.

Arten von BGP-Nachrichten

BGP verwendet vier verschiedene Arten von Nachrichten im Protokoll:

OPEN - Wird nur zu Beginn einer Verbindung gesendet und muss mit einer KEEPALIVE-Nachricht beantwortet werden. Bei der OPEN-Nachricht werden die Parameter BGP-Version, AS-Nummer, Hold Timer, BGP Identifier sowie optionale Parameter mitgeschickt. Danach werden die Routeninformationen zwischen den Routern ausgetauscht.

UPDATE - Teilt eine Pfadänderung mit. Es können pro UPDATE-Nachricht gleichzeitig mehrere Pfade hinzugefügt und mehrere entfernt werden. UPDATE-Nachrichten sind das Kernstück von BGP.

NOTIFICATION - Beendet eine Verbindung und gibt Fehler- bzw. Statuscodes an. Alle Pfade, die über diese beendete Verbindung empfangen wurden, müssen nun gelöscht werden. Über ein BGP-Update würde dann verbreitet werden, dass diese Route nicht mehr verfügbar ist.

KEEPALIVE - Bestätigt die OPEN-Anfrage. Zur regelmäßigen Überprüfung, ob der verbundene Router noch online ist oder ob die Verbindung unterbrochen ist und die Pfade über den verbundenen Router somit ungültig geworden sind. Die Router, welche gerade eine BGP-Session aufgebaut haben, senden sich gegenseitig in regelmäßigen Abständen eine KEEPALIVE-Nachricht. Diese besteht nur aus dem Message Header. Im Attribut Hold Time einer OPEN-Nachricht wird die maximale Zeit angegeben, in der ein BGP-Router eine KEEPALIVE-Nachricht vom BGP-Partner der Session erwartet. Kommt innerhalb der Hold Time keine KEEPALIVE-Nachricht an, wird die BGP-Session mit einer NOTIFICATION beendet.

Kernstück von BGP ist die UPDATE-Nachricht, über welche sich BGP-Router die Existenz neuer Routen (Announcement ... Ankündigung, Anmeldung) oder den Wegfall bestehender Routen (Withdrawal ... Austritt, Rückzug) mitteilen. Der Empfänger einer UPDATE-Nachricht entscheidet anhand seiner Routing-Richtlinien (policies), ob er sein Routing umstellt und daraufhin selbst UPDATE-Nachrichten versenden muss oder ob die Nachricht einfach nur weiterleitet oder schlichtweg ignoriert werden soll.

BGP weist prinzipbedingt eine Reihe von Schwächen auf, die in einer Minimalkonfiguration entstehen können. Die Schwächen werden jedoch in der Regel dadurch kompensiert, da die Priorisierung von Pfaden Routing-Policies unterliegen, die der jeweilige Netzbetreiber steuern kann.

Besondere Ereignisse

YouTube-Blockade: Im Februar 2008 wurde Pakistan Telecom durch einen Gerichtsbeschluss dazu gezwungen, YouTube-Verkehr in Pakistan zu blockieren. Technisch wurde dies umgesetzt, indem eine falsche Route zum Netzwerk von YouTube eingespeist wurde. Durch einen Konfigurationsfehler wurde diese falsche Route jedoch

Border Gateway Protocol (BGP) 2/2

nicht nur in Pakistan verwendet, sondern irrtümlich auch an andere Internetanbieter verteilt, was insbesondere in Asien zu mehrstündigen Blockaden von YouTube führte.

Fehlkonfigurierter BGP-Router: Im Februar 2009 wurden über einen tschechischen BGP-Router zu lange AS-Pfade an öffentliche BGP-Router weitergeleitet. Einige BGP-Router hatten Probleme in der Verarbeitung dieser langen AS-Pfade, so dass es zu Beeinträchtigungen des Internetverkehrs kam. Administratoren können durch eine Konfiguration, in welche die maximale Länge des akzeptierten AS-Pfads beschränkt wird, einem solchen Problem entgegenwirken.

Revolution in Ägypten 2011: Während der Revolution in Ägypten wurden im Januar 2011 via BGP in wenigen Minuten ca. 3.500 Routen aller ägyptischer Internetanbieter zurückgezogen, wodurch fast ganz Ägypten vom Internet getrennt war. Auch Mobilfunkdienste und soziale Netze waren nicht mehr erreichbar. Dieses scheint der erste Fall in der Geschichte des Internets zu sein, in welchem aus politischen Gründen ein gesamtes Land vom Internet abgeschottet wurde.

Softwarefehler: Das BGP Path Attribute kann den Wert 255 annehmen. Dieses steht für Entwicklungen (RFC 2042) zur Verfügung. Bereits im Jahr 2010 führte ein Experiment mit diesem Flag zu Abstürzen in einigen Routern. Bei einem neuerlichen Versuch Ende 2018 wurden wieder fehlerhaft implementierte Router gefunden.

RFC ... Request for comments, Internet Standard oder Diskussionsschrift

Facebook, Instagram und Whatsapp: Am 4. Oktober 2021 waren für ca. 6 Stunden weltweit alle Dienste von Facebook, Instagram und Whatsapp nicht erreichbar. Dies ging auf eine fehlerhafte Konfiguration von Facebooks selbst gehosteten BGP-Routern zurück.

Quishing - Betrug mit dem QR-Code 1/3

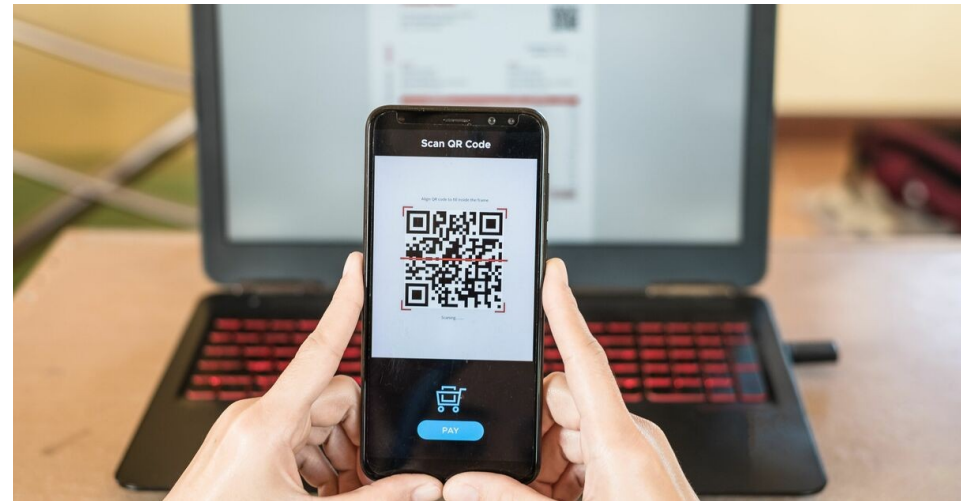
Was ist Quishing?

Das Wort Quishing setzt sich aus den beiden Begriffen »QR« (Quick Response) und »Phishing« zusammen. Es handelt sich dabei um einen Phishing-Angriff, bei dem man direkt oder indirekt aufgefordert wird, einen QR-Code mit dem Smartphone zu scannen. Kommt man dieser Aufforderung nach, wird man zu einer entsprechend vorbereiteten Webseite (beim Quishing meist mit betrügerischen Absichten) weitergeleitet.

Eine Quishing-E-Mail weist zahlreiche Merkmale auf, die auch von Phishing-Attacken bekannt sind (Nutzer zu verleiten einen Link anzuklicken oder anders ausgedrückt »den angebotenen Angelhaken mit dem Leckerbissen« mit all seinen Konsequenzen anzunehmen). So geben Cyberkriminelle beispielsweise vor, dass aufgrund eines Sicherheitsproblems sofortiger Handlungsbedarf bestehe. In der Nachricht drohen sie zudem mit negativen Konsequenzen, die eintreten würden, falls man nicht umgehend aktiv wird. Auf der Zielseite wiederum soll man seine Zugangsdaten eingeben, die dann direkt in die Hände der Betrüger wandern, oder Dokumente herunterladen, die das eigene Smartphone mit Malware kompromittieren.

Während eine herkömmliche Phishing-E-Mail den ahnungslosen Nutzer über einen Link auf die gefälschte Seite lockt, geschieht dies beim Quishing über einen als Bild eingebundenen QR-Code. Und genau das macht diese Methode so gefährlich: die meisten Sicherheitsprogramme können nämlich nur verdächtige Anhänge und URLs als mögliche Bedrohungen identifizieren, nicht jedoch Bilder. Folglich stufen Virens Scanner Quishing-E-Mails häufig als harmlos ein und verschieben sie nicht in den Spam-Ordner.

Hinweis: Die Phishing-Nachrichten mit QR-Codes laufen »unter dem Sicherheitsradar« der Anti-Viren-Programme und gelangen



unbeanstandet in die E-Mail-Postfächer der Nutzer.

Gleichzeitig ist die Wahrscheinlichkeit, dass ein Nutzer einen betrügerischen QR-Code tatsächlich scannt, relativ hoch. Der QR-Code ist in unserer digitalen Welt weit verbreitet und gilt als praktische Lösung, um Informationen aus dem Internet unkompliziert mit dem Smartphone aufzurufen. Darüber hinaus stellt er eine smarte Möglichkeit dar, um Sicherheitsabfragen geräteübergreifend durchzuführen. So setzen etwa manche Banken QR-Codes ein, um die Freigabe für eine Überweisung per Smartphone einzuholen. Wir alle sind es also bereits gewohnt, QR-Codes am Bildschirm (Computer-Monitor, TV-Gerät, ...) zu scannen, und sehen sie als vertrauenswürdig an.

Quishing in der Praxis: Daten die für Betrüger besonders interessant sind

Hacker haben das Vertrauen in QR-Codes in jüngster

Quishing - Betrug mit dem QR-Code 2/3

Vergangenheit bereits mehrfach für ihre kriminellen Aktivitäten ausgenutzt. Das Vorgehen der Cyberkriminellen ähnelt dabei in vielen Punkten dem herkömmlichen Phishing. In der Betreffzeile der Quishing-E-Mails wird auf ein Sicherheitsproblem hingewiesen, bei dem die Nutzer aktiv werden müssten. Manchmal wird den Nutzern auch vorgespielt, sie benötigten ein Dokument, an das sie durch das Einscannen des QR-Codes auf ihrem Smartphone gelangen könnten. Auf jeden Fall ist meist von einem akuten Handlungsbedarf die Rede. Das Ziel der Betrüger ist es, dass die Nutzer den QR-Code auf ihrem Smartphone einscannen. Dies leitet die Nutzer nun auf eine gefälschte Webseite weiter. Die Smartphones erkennen in der Regel nicht, dass die angesteuerte Webseite gefälscht ist und lassen diese Weiterleitung zu. Auf der gefälschten und vorbereiteten Webseite können unterschiedliche Dinge passieren. Entweder laden Nutzer Dokumente herunter, die mit Malware verseucht sind oder sie geben Login-Daten ein, die direkt an die Betrüger weitergeleitet werden.

Besonders beliebt sind dabei Betrugsmaschinen, die auf Zugangsdaten von Microsoft-Office-365-Konten abzielen. Mit diesen lassen sich nämlich häufig auch andere Konten desselben Nutzers attackieren. So haben Betrüger beispielsweise Quishing-E-Mails im Namen eines Unternehmens verschickt. Diese enthalten die Nachricht, dass eine Zahlung erfolgt sei, sowie einen PDF-Anhang. Wer die PDF-Datei öffnet, bekommt eine verschwommene Rechnung angezeigt, über der ein QR-Code liegt. Nach dem Scannen gelangt der Nutzer zu einer manipulierten, täuschend echt wirkenden Login-Seite von Microsoft Office 365, auf der er seine Nutzerdaten eingeben soll, damit die Rechnung sichtbar wird.

Mögliche Inhalte der Betreffzeile von Quishing-E-Mails:

- Ihr Zugang zum Bankkonto ist gesperrt!
- Wichtige Information zu Ihrer Kreditkarte!

- Verbraucherzentrale - Vorsicht, Falle!
- Bundesamt für Verbraucherschutz
- Sparkassen Secure +
- Ihr Google-Speicher ist voll!
- Termin für Glasfaser-Internetanschluss
- Kontolöschung bei XXX und vieles mehr

Wie kann man sich vor Quishing schützen?

Auch wenn E-Mail Spam- und Virenschutz Quishing-E-Mails nicht aussortieren, so ist man den Cyberkriminellen dennoch nicht hilflos ausgeliefert. Bei der Befolgung einiger Handlungsempfehlungen, sollte sich der Schutz vor Quishing-Angriffen deutlich verbessern:

1. Plausibilitätscheck durchführen

Noch bevor man eine E-Mail öffnet, sollten man immer kritisch hinterfragen, ob es sich um eine Phishing-Nachricht handeln könnte. Vorsicht ist auch immer geboten, wenn der Absender der E-Mail unbekannt ist und der Betreff unüblich ist oder keinen Sinn ergibt oder der Betreff den Empfänger unter Druck setzt. Ist dann auch noch eine Datei angehängt, so sollte man die E-Mail sofort löschen und zwar ohne sich die Nachricht genauer anzusehen. Schon das Öffnen einer entsprechend vorbereiteten E-Mail kann im Hintergrund einige unerwünschte Aktionen auslösen.

2. Betriebssystem und Virenschutz auf den aktuellen Stand bringen

Sicherheitsupdates sind das A und O für einen wirksamen Schutz vor Cyberangriffen. Das Betriebssystem als auch sämtliche Anwendungen sollten immer zeitnah auf den aktuellen Stand gebracht werden. Man kann auch automatische Update-Services und Webseiten von vertrauenswürdigen Softwareherstellern nutzen, um kein Sicherheitsupdate zu verpassen.

Quishing - Betrug mit dem QR-Code 3/3

3. Multifaktor-Authentifizierung einrichten und nutzen

Falls man doch einmal auf eine Quishing-Mail hereingefallen ist und die Zugangsdaten an Betrügern übermittelt wurden, dann ist das nur halb so schlimm, wenn das Nutzerkonto zuvor über eine Multifaktor-Authentifizierung (MFA) geschützt wurde. Denn die MFA erfordert für einen erfolgreichen Login zwei oder mehrere Berechtigungsnachweise. Meist handelt es sich dabei um die Kombination aus einem Passwort und einem weiteren Anmeldefaktor, der auf einer Sicherheitsfrage, biometrischen Merkmalen oder einem physischen Objekt - etwa einem Smartphone - basiert. Ohne diese zusätzliche Authentifizierung ist das Passwort für die Betrüger nutzlos.

4. Sicherheitsrichtlinie in den Unternehmen anpassen

Die Sicherheitsrichtlinie eines Unternehmens sollte zwingend auch Smartphones einschließen. Oftmals existieren für Rechner und Notebooks recht strenge Sicherheitsvorkehrungen, aber kaum für Firmentelefone. Hier muss umgedacht werden.

5. Weiterbildung der Mitarbeiter eines Unternehmens

Der beste Schutz vor Quishing ist die Weiterbildung aller Beschäftigten. Denn nur wenn Gefahren bekannt sind und erkannt werden, können Mitarbeiter entsprechend handeln.

Der Vorsatz, niemals wieder einen QR-Code zu scannen ist verständlich, aber unrealistisch. Stattdessen sollte man sich an die bekannten Regeln erinnern und sie auch anwenden.

Hinweis an die Mitarbeiter: Vorgänge immer abbrechen, wenn direkt nach dem Scannen eines QR-Codes sensible Daten abgefragt werden.

6. Angreiferfrüherkennung

Einige Unternehmen haben sich auf die kostenpflichtige

Früherkennung von Angriffen auf IT-Systeme spezialisiert. Die IT-Systeme werden von diesen spezialisierten Unternehmen in der Regel rund um die Uhr überwacht.

Für Personen die sich diesen kostenpflichtigen Service nicht leisten können, bleibt nur der vorsichtige Umgang mit den modernen Kommunikationsmöglichkeiten und ein Plausibilitätscheck aller eingehenden Nachrichten.

Hinweis: Angriffe auf IT-Systeme sind weitgehend chancenlos, wenn der Nutzer die Verseuchung nicht selbst einleitet, indem er auf etwas klickt, worauf er nicht klicken sollte.

ERST NACHDENKEN, DANN KLICKEN.





Starlink: Schnelles Satelliten-Internet aus dem All

Das private Raumfahrtunternehmen SpaceX will die Erde mit Internet aus dem Weltraum versorgen. Dafür schickt SpaceX tausende Starlink-Satelliten ins All. Die ersten Satelliten wurden von SpaceX im Jahr 2018 ins All befördert. Besonders in den Tagen nach ihrer Eingliederung in einer vorläufigen Erdumlaufbahn erscheinen sie als helle Lichterkette am Himmel.

Internet per Satellit ist nichts Neues. Schon in den frühen 2000er-Jahren gab es Internet-Satelliten-Anbieter. Doch sie hatten eine gänzlich andere Funktionsweise als Starlink. Bis zum Jahr 2027 sollen allein für diesen Dienst 12.000 neue Satelliten im All sein. Sie befinden sich nicht - wie bei den anderen Anbietern (z.B. Eutelsat) - in 36.000 Kilometern Höhe, sondern in nur etwa 500 Kilometern. Das hat für die Nutzer einen unschätzbaren Vorteil: Die Signallaufzeit (Latenz) ist viel geringer. Denn statt 72.000 Kilometer vom Nutzer zum Satelliten und zurück muss das Datensignal nur 1.000 Kilometer bis zur Bodenstation zurücklegen.

Hinweis: Für die Anforderung eines Datenpaketes legt das Signal 1.000 Kilometer und für den Empfang nochmals 1.000 Kilometer zurück. Das heißt, bis das angeforderte Datenpaket den Nutzer erreicht, wurde eine Signalstrecke von 2.000 Kilometer zurückgelegt. Für geostationäre Satelliten beträgt der vollständige Signalweg 144.000 Kilometer. Die Reaktionszeiten, etwa beim Aufbau von Internetseiten, sind bei Starlink-Verbindungen deutlich besser (**durchschnittliche** Latenzzeiten im Jahr 2023: Starlink - 47 Millisekunden, Festnetz - 14 Millisekunden, 5G-Mobilfunk unter 5 Millisekunden).

Starlink - Internet aus dem Weltall 2/5

Ein freier Himmel reicht - schon online

Der Vorteil von Internet per Satellit, liegt in der Flexibilität. Ein freier Blick zum Himmel reicht - schon kann man online gehen. Man stellt dazu eine vergleichsweise kleine Satellitenschüssel auf - etwa auf dem Balkon, auf dem Dach oder im Garten -, die sich selbständig optimal ausrichtet. Schon nach wenigen Minuten steht die Verbindung und es können Daten fließen.

Allerdings ist Surfen per Satellit kein günstiges Vergnügen. Den Onlinedienst kann man für unter 100 Euro im Monat bekommen. Dafür gibt es ein Datentempo, das durchaus bei 300 MBit/Sekunde im Downstream und bis zu 30 MBit/Sekunde im Upstream liegen **kann** (plus unbegrenztes Datenvolumen). Ein Tempo, das so mancher anderer Anbieter nicht leisten kann oder will. Schon gar nicht auf dem flachen Land.

Starlink peilt in Zukunft Übertragungsraten im Downstream von bis zu 10 Gbit/s an, das ist deutlich schneller als die aktuellen Glasfaserverbindungen.

Für Menschen, die weder eine schnelle DSL-Leitung (DSL .. digital subscriber line) bekommen, noch in einem 5G-Ausbaubereich wohnen, können Lösungen wie Starlink durchaus interessant sein.

Wie werden die Satelliten ins All gebracht?

Die Starlink-Satelliten sind anders als andere künstliche Trabanten flach, ähnlich wie eine Tischplatte. Jedes Exemplar wiegt etwa 250 Kilogramm.

Die SpaceX Falcon 9-Rakete transportiert jeweils Dutzende gleichzeitig und lädt sie im All ab. Das dauert vom Start bis zur Stationierung nur knapp 65 Minuten. Die Himmelskörper breiten dann ihre Solarpaneele aus und fliegen allein. Das Schauspiel nach

dem Start (Launch) sieht ziemlich spektakulär aus: Die Himmelskörper ziehen anfangs wie auf einer Kette aufgereiht über den Himmel. Das kann man abends und morgens beobachten, wenn sie das Licht der Sonne reflektieren.

Nach der Eingliederung werden die meisten Trabanten in einer ungefähren Höhe von 550 Kilometern fliegen. Einige werden den Plänen zufolge aber höher und niedriger unterwegs sein: Sie kreisen dann in rund 340 und 1.200 Kilometern über der Erdoberfläche.

Wo ist Starlink verfügbar?

Im Sommer 2023 sind etwa 3.880 der geplanten 12.000 Satelliten aktiv. In Deutschland stehen nach unbestätigten Informationen immerhin zwei dieser Bodenstationen - eine in Usingen bei Frankfurt und eine in Aerzen bei Hameln.

Verfügbar ist Starlink aktuell in Europa neben Deutschland z.B. in Großbritannien, Polen, Frankreich, Benelux und der Schweiz, nicht aber in Norwegen, Nordschweden oder auf den Kanaren. Starlink wird künftig einen neuen Satellitentyp einsetzen, der nicht mehr in jeder Region der Welt Bodenstationen benötigt. Die Daten verteilen die Satelliten dann untereinander per Laser im All.

Hardware für den Starlink-Dienst

Die Preise für die Hardware sind inzwischen gesunken. Auch die Miete der Schüssel ist inzwischen möglich. Die Benutzung setzt voraus, dass man einen freien Blick zum Himmel hat. Bei TV-Satelliten-Antennen muss man einen freien Blick zum südlichen Horizont haben, bei Starlink soll es ein Rundum-Blick sein. Idealerweise sollte die Schüssel im Garten oder auf dem Dach stehen. Der Balkon kann als Aufstellungsort problematisch sein.

Starlink - Internet aus dem Weltall 3/5

Die Standard-Starlink-Schüssel ist mit 23 Meter Kabel ausgestattet, das man nicht von der Schüssel abtrennen kann. Das schützt zwar vor dem Eindringen von Wasser, kann aber beim Verlegen problematisch sein. Das Kabel ist ein Power-over-Ethernet-Kabel (PoE), es überträgt gleichzeitig die Daten und den Strom zur Antenne. Im Gebäude schließt man einen mitgelieferten PoE-Adapter an das Stromnetz sowie ein Netzkabel zum mitgelieferten Router an. Bei der neuen eckigen Starlink-Schüssel (High Performance Antenne) ist das Kabel abtrennbar.

Hat man die Schüssel aufgestellt und die Kabel verlegt, kann man die Ersteinrichtung in wenigen Minuten durchführen (Starlink App). Man muss sich dazu nur mit dem neuen WLAN von Starlink verbinden, ein paar Daten für das neue WLAN festlegen und schon ist die Starlink-Schüssel online. Doch Achtung: Die volle Leistungsfähigkeit entfaltet Starlink erst nach einigen Stunden. Nutzen kann man den neuen Internetanschluss aber sofort.

Alternativ zur Standardschüssel gibt es auch noch eine High-Performance-Schüssel und eine Schüssel für Wohnmobile.

Starlink bietet zudem die Möglichkeit, den Standort (der Portability-Modus verursacht zusätzliche Kosten) zu verändern. Starlink-Nutzer müssen aber jeden neuen Standort erneut extra freischalten, um das Satelliten-Internet zu empfangen. Damit ist eine Standortveränderung nur für längere Aufenthalte auf einem Campingplatz oder in einem einsamen Sommerhaus lohnenswert. Denn die mobile Nutzung in einem bewegten Vehikel ist seit Mai 2022 in den Geschäftsbedingungen verboten worden. Jedoch arbeitet Starlink laut eigener Aussage daran, das Satelliten-Internet wieder in mobilen Fahrzeugen anzubieten.

Hinweis: Gelegentliche Verbindungsabbrüche können bei den Starlink-Verbindungen noch vorkommen.



Die Standardausrüstung für den Aufbau einer Starlink-Verbindung.



High Performance Satellitenantenne

Starlink - Internet aus dem Weltall 4/5

Europäisches Breitband aus dem All

Eine Studie der Berliner Stiftung Wissenschaft und Politik empfiehlt der Bundesregierung, sich für ein Internet-Satellitennetz der EU einzusetzen. Sonst droht die Gefahr von den internationalen Konzernen abhängig zu werden.

Durch die Abhängigkeit von internationalen Konzernen droht möglicherweise eine Konzentration von wirtschaftlicher Macht und damit auch ein bisher unbekanntes Maß an politischer Kontrolle über die globalen Kommunikationsnetze.

Die Europäische Kommission untersucht mit Hilfe mehrere beauftragter Unternehmen, ein Konzept für ein europäisches Hochgeschwindigkeitsinternet per Satellit.

Drei kommerzielle Unternehmen planen oder bieten bereits Breitband-Internet aus dem All an: Starlink von Space-X, ein gemeinsames Netz von Amazon und Oneweb, sowie eine chinesisch-russische Breitbandnetz-Partnerschaft.

Der Service - Internet aus dem All - wird schon jetzt von einigen Menschen in ländlichen Regionen genutzt. In den Ballungsräumen dominiert weiterhin die Versorgung über Glasfasernetze.

Kritik an Starlink

Besonders in den ersten Tagen vor ihrer endgültigen Eingliederung erscheinen die Satelliten als helle Lichterkette am Nachthimmel.

Nach einigen Tagen, nachdem die Phase der Umlaufbahnanhebung und die Eingliederung abgeschlossen ist, werden sie dann nicht mehr zu erkennen sein.

Im August 2020 war dies für manche Astronomie-Freunde ein

bitterer Beigeschmack. Viele wollten sich die Sternschnuppen der Perseiden anschauen. Eine Lichterkette an weißen Punkten war für manche dann eine Überraschung (Gerüchte über UFOs verbreiteten sich).

Nach dem Erreichen der gewünschten Betriebshöhe, richten sich die künstlichen Objekte neu aus. Die Helligkeit nimmt ab und die Lichterketten verschwinden.

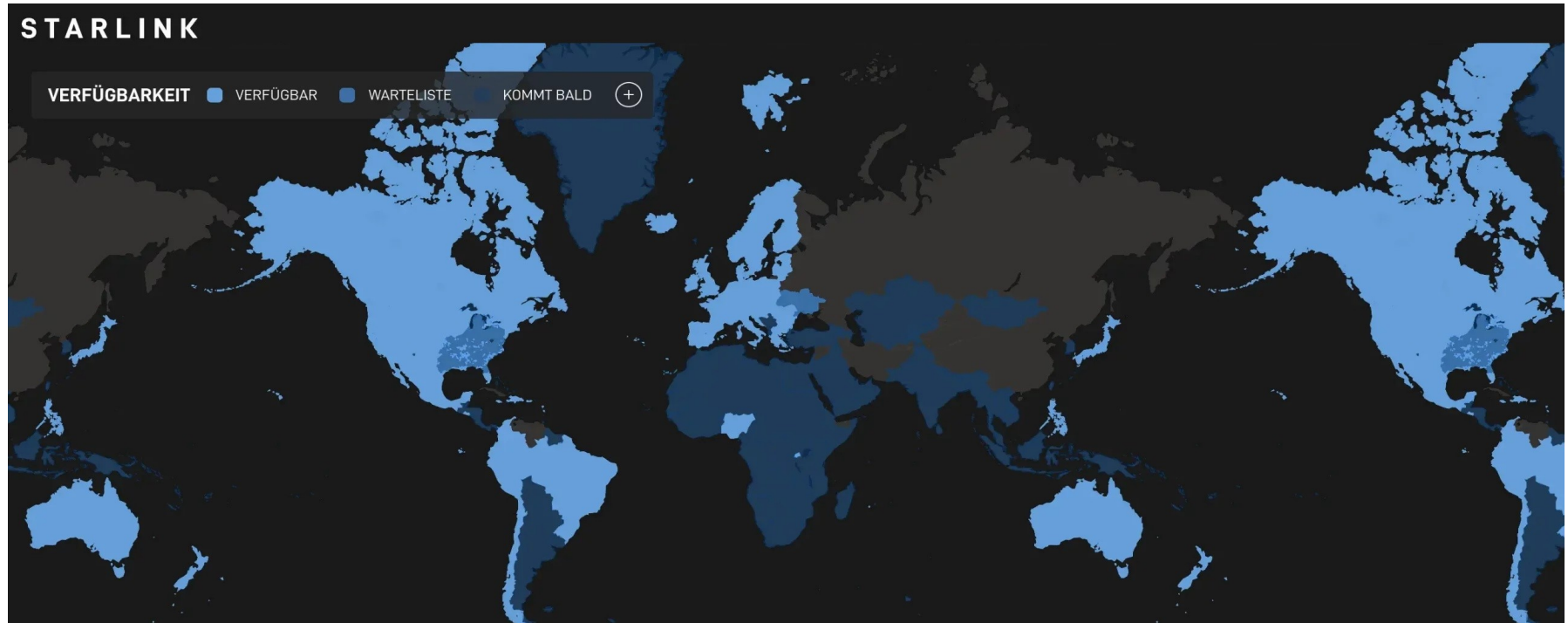
Die Internationale Astronomische Union (IAU) fürchtet, dass die Internet-Satelliten von Starlink den Nachthimmel für astronomische Beobachtungen zu sehr erhellen.

Auch macht es die Raumfahrt nicht einfacher. Vor allem aber drohen auch Konsequenzen für die Erdatmosphäre: Forscher warnen gerade davor, dass auf die Erde niedergehender Elektroschrott, der vor allem aus Aluminium besteht, die Erdatmosphäre gefährde.

Dabei kann man sich eine Welt ohne Satelliten gar nicht mehr vorstellen. Sie liefern uns TV-Programme, warnen uns frühzeitig vor Katastrophen und helfen bei der Navigation. Wie die Auswirkungen von tausenden weiteren Satelliten auf den Nachthimmel sein werden, weiß die Internationale Astronomische Union jedoch auch nicht.

Die Internationale Astronomische Union (IAU) sucht zusammen mit der American Astronomical Society (AAS) das Gespräch mit dem Betreiber von SpaceX. Dieser zeigt sich offen und experimentiert an verschiedenen Farbanstrichen. Dadurch sollen die Satelliten am Nachthimmel nicht mehr so auffallen.

Starlink - Internet aus dem Weltall 5/5



Die Karte zeigt die Starlink-Verfügbarkeit (Hellblau) im Jahr 2023.

Wo ist Starlink verfügbar?

Bis Spätsommer 2022 waren etwa 2.280 der geplanten 12.000 Satelliten aktiv. Starlink ist in vielen Ländern Europas verfügbar, darunter Deutschland, Großbritannien, Polen, Frankreich, Benelux und der Schweiz. In Deutschland gibt es bereits zwei Bodenstationen, eine in Usingen bei Frankfurt und eine in Aerzen bei Hameln.

Für wen eignet sich Starlink?

Starlink ist geeignet für Personengruppen die alternative Internet-Versorgung, abseits der gut versorgten Gebiete, benötigen und für Personengruppen die mobiles Internet brauchen für das Ferienhaus, den Schrebergarten oder für das Wohnmobil.

Was kostet Starlink monatlich?

Starlink berechnet monatlich 65 Euro für eine unlimitierte Datenflatrate mit 50 bis 200 Mbit/s im Downstream. **Hinweis:** Der Stromverbrauch ist höher als bei herkömmlichen Routern, was zusätzliche Kosten verursachen kann (Info-Stand: 2023).

Shadow Banning bei TikTok & Co. 1/3

Was ist Shadow Banning - Schattensperre?

Shadow banning, Shadowban, Ghost Banning, Comment Ghosting oder Reichweitendrosselung bezeichnet das vollständige oder teilweise Blockieren eines Benutzers beziehungsweise seiner Inhalte in einer Online-Community, sodass für den Benutzer nicht ohne Weiteres ersichtlich ist, dass er gesperrt oder gedrosselt wurde.

Der Shadowban kann meistens erst durch die Analyse der Statistiken der Social-Media-Aktivität der Follower erkannt werden. Beispielsweise sind Kommentare oder Tweets, die in einem Blog oder auf einer Medienwebseite veröffentlicht werden, für andere Personen, die von ihrem Computer aus auf diese Webseite zugreifen, nicht mehr sichtbar. Daher sinken die Interaktionen mit der Webseite bzw. dem Social-Media-Account. Shadowbans können auch als eine Form der Zensur verstanden werden, denn Betroffene verlieren so in den sozialen Medien an Reichweite.

Durch das teilweise Verbergen oder die Unkenntlichmachung von Beiträgen eines Benutzers für andere Mitglieder des Dienstes soll erreicht werden, dass der problematische oder anderweitig auffällig gewordene Benutzer unzufrieden mit der Resonanz auf seine Beiträge ist und gelangweilt oder frustriert die Webseite verlässt. Im Gegensatz zu einer kompletten Sperre wird angenommen, dass eine für den Nutzer nicht ohne Weiteres erkennbare partielle Einschränkung der Interaktion mit anderen Nutzern die unerwünschten Nutzer (etwa Spammer und Trolle) davon abhält, ein neues Konto zu erstellen, um die Sperre zu umgehen.

Wie bekommt man einen Shadowban?

Die Ursachen für einen Shadowban in klassischer Form, bei dem keine Nutzeraktivitäten mehr angezeigt werden, können vielfältig sein: ein regelmäßiger Verstoß gegen Richtlinien, regelmäßiges



Melden des Accounts von anderen Plattformnutzenden, Verwendung von Bots, die automatisiert posten oder liken. Wer sich umgekehrt an die Richtlinien der jeweiligen Plattformen hält, ist auf der sicheren Seite und riskiert keinen Shadowban.

In der Praxis ist es umstritten, ob es Shadow Banning tatsächlich gibt - Plattformen wie TikTok oder Instagram äußern sich nicht offiziell dazu. Viele Benutzer berichten jedoch von plötzlich stark eingebrochenen Reichweiten oder werden von Dritten darin bestätigt, dass Kommentare oder Likes nicht mehr für die Community sichtbar sind.

Shadow Banning bei TikTok & Co. 2/3

Wie lange dauert ein Shadowban?

Instagram und Co. sprechen nicht explizit von einem Shadowban und die tatsächlichen Gründe dafür sind nicht so leicht einsehbar. Daher gibt es auch keine offizielle Angabe darüber, wie lange ein Shadowban dauert. Die meisten Erfahrungen sprechen von 14 Tagen, bevor ein Account wieder normal nutzbar ist.

Woran erkennt man einen Shadowban - gibt es einen Test?

Im Sinne der Definition von Shadow Banning bekommt man keine Benachrichtigung, dass es einen getroffen hat. Es gibt jedoch einen einfachen Shadowban-Test, den man durchführen können:

Man veröffentlicht einen Beitrag unter weniger bekannten Hashtags. Danach können Freunde und Bekannte nach dem Hashtag auf der Plattform suchen. Wird der Beitrag nicht gefunden, scheint man von einem Shadowban betroffen zu sein.

Alternativ kann man diesen Test auch mit einem »Shadow Ban Tool« durchführen. **Hinweis:** Diese Tools befinden sich aktuell noch in einer frühen Entwicklungsphase.

Was kann man gegen einen Shadowban machen?

Wer einen Shadowban loswerden will, muss meist etwas Geduld mitbringen. Erfahrungsgemäß dauert es bei einem unabsichtlichen Verstoß um die zwei Wochen, bis alles wieder beim Alten ist.

In dieser Zeit sollte man sein Aktivitäten auf der Plattform deutlich reduzieren oder sogar völlig einstellen.

Für sensible Themen sollte man eine gut sichtbare Inhaltswarnung einfügen.

Vergeht mehr Zeit und die Beiträge oder Aktivitäten bleiben



weiterhin im Verborgenen, so kann man sich an den Support der Plattform wenden und das Problem schildern. Ist der Shadowban zu Unrecht verhängt worden, stehen die Chancen gut, wieder sichtbar zu werden.

Hinweis: Die Social-Media-Plattformen verwenden die Taktik des Shadow-Bannings, um positives Verhalten auf ihren Plattformen zu fördern. Dies kann man als Zensur ansehen oder als beeinflussende erzieherische Maßnahme betrachten, falls man mit den Richtlinien und Nutzungsbedingungen vollständig übereinstimmt. Auch sollte man daran denken, dass »unangemessene« Inhalte, die die Nutzungsbedingungen der Plattform gerade noch einhalten, zu einem Shadowban führen kann.

Shadow Banning bei TikTok & Co. 3/3

Shadowban bei TikTok

Um einen Shadowban bei TikTok zu verhindern, sollte man

- keine grenzwertigen Inhalte hochladen (nach der Meinung von TikTok, Veränderte Zeiten, andere Meinung?), zum Beispiel über Glücksspiel, gefährliche Mutproben oder ungesichertes Gebäudeklettern, urheberrechtlich geschützte Inhalte, ...
- gewerbliche Inhalte sollten immer als solche gekennzeichnet werden
- ehrliche persönliche Angaben machen.

Hält man diese Regeln ein, so wird man im Normalfall nicht betroffen oder getroffen sein von einem Shadowban.

Shadowban bei Instagram

Instagram ist bekannt dafür, sexualisierte Inhalte sofort zu blockieren und die jeweiligen Profile mit einem Shadowban zu belegen. Dies ist Teil der Community-Richtlinien, die bei den Gemeinschaftsrichtlinien des zur »Meta Plattform« zugehörigen Dienstes zu finden sind.

Weiterhin sollte man darauf achten, bei der Verwendung von Hashtags, keine sogenannten »banned hashtags« zu nutzen (gesperrte Hashtags). So gibt es eine Reihe von Wörter oder Wortkombinationen, die Gefahr laufen, gefiltert zu werden. Dazu zählt beispielsweise auch #depression.

Mit dem Online-Tool »IQ Hashtags« kann man die angedachten Hashtags prüfen, um einem etwaigen Shadow Banning zu entgehen.

Die Hashtags auf Instagram ist der Hauptmechanismus um neue Inhalte und Accounts zu entdecken.

Die Verwendung von automatisierte Tools und Bots führen bei Instagram regelmäßig zu einem Shadowban.

Der Instagram Shadowban ist zudem auch ein Weg, Spammer daran zu hindern weiter Spam versenden zu lassen, ohne dass jemand anderes in der Community dies bemerkt.

Das Kaufen von Follower führt bei Feststellung durch Instagram ebenfalls zu einem Shadowban.

Auch gehackte Accounts können bei Instagram zu einem Shadowban führen.

Shadowban und Algorithmen

Shadowbans werden zur Zeit nicht von Algorithmen durch ein mehrfaches Melden des Accounts von anderen Plattformnutzenden erteilt oder bei Verletzung der Richtlinien der Plattform oder bei »unangemessenen« Inhalten, die die Nutzungsbedingungen der Plattform gerade noch einhalten.

Shadowbans werden wahrscheinlich zunehmend auf Grundlage der Ergebnisse von automatisch ablaufenden Algorithmen ausgesprochen. Da Algorithmen selten perfekt arbeiten und nicht alle möglichen Variationen einer Sprache berücksichtigen können, ist es durchaus möglich das harmlose Inhalte zeitweise zu einem Shadowban führen können.

Auch neue Algorithmen die sich in einer frühen Entwicklungsphase befinden (z.B. Bekämpfung von Bots) können auch Nutzer (hochaktive Accounts) treffen die sich an die Regeln der Plattform halten.

Hinweis: Es wird vereinzelt inoffiziell berichtet, dass politisch unliebsame Themen ebenfalls zu einem Shadowban führen kann.

1. Allgemeines: Was ist ein Rechenzentrum?

Ein Rechenzentrum ist ein physischer Raum, ein Gebäude oder eine Einrichtung für die IT-Infrastruktur zur Erstellung, Ausführung und Bereitstellung von Anwendungen und Services sowie zur Speicherung und Verwaltung der mit diesen Anwendungen und Services zugehörigen Daten.



Mittlerweile hat sich die Infrastruktur von Rechenzentren deutlich weiterentwickelt. Die Rechenleistung der traditionellen physischen Server vor Ort wurden mit den flexiblen Möglichkeiten virtueller Netzwerke verknüpft: Viele Daten sind mittlerweile über mehrere Rechenzentren sowie öffentliche und Private Clouds (Rechen- und Speicherplattform im Internet) verbunden. Deshalb muss ein modernes Rechenzentrum in der Lage sein, über verschiedenen Standorte hinweg zu kommunizieren.

Rechenzentrum oder Serverraum: Wo liegt eigentlich der Unterschied?

Während ein Rechenzentrum in der Regel ein gesamtes Gebäude mit Servern, Speichern und allen benötigten Strukturen bezeichnet, bestehen Serverräume meist eben nur aus einem Raum in einem größeren Gebäude. Besonders für kleine und mittelständige Unternehmen, bei denen Datenmengen und Anwendungen überschaubar sind, stellen Serverräume eine gute Alternative zu einem komplexen Rechenzentrum dar. Dabei bieten viele mittlerweile eine ähnliche Ausstattung wie ein Rechenzentrum, wobei die Sicherheit und Versorgung beim Eigentümer liegt.

2. Grundlegende Betrachtungen

2.1 Warum ist ein Rechenzentrum wichtig für Unternehmen?

Die meisten Geschäftsanwendungen und -aktivitäten innerhalb eines Unternehmens erzeugen Daten, die gespeichert werden müssen. Dazu zählen beispielsweise:

- E-Mails und Dateifreigaben
- Produktivitätsanwendungen
- Webseiten
- Online-Transaktionen
- Daten in CRM-Tools (CRM ... Customer Relationship Management oder Kundenbeziehungsmanagement)
- Unternehmensressourcenplanung (ERP oder Enterprise Resource Planning)
- Datenbanken
- Big Data und künstliche Intelligenz (KI)
- virtuelle Desktops
- Kommunikations- und Kollaborationsdienste (Dienste für die Zusammenarbeit oder Mitwirkung vieler Personen)

Gerade bei großen Unternehmen, Bildungseinrichtungen oder Behörden sammeln sich riesige Datenmengen an, die sehr viele Server und viel Speicherplatz benötigen. Ein einfacher Serverraum reicht häufig nicht mehr aus, um den Datenfluss zu bewältigen. Zudem kann sich die Wartung als kompliziert erweisen. Hohe Energiekosten und in einigen Fällen sogar Überwachung rund um die Uhr, um Serverausfälle zu verhindern und Cyberangriffe abzuwehren, bringen einige Unternehmen an ihre Grenzen.

An eben diesem Punkt kommen Rechenzentren ins Spiel: Die

Daten sind an einem sicheren und rund um die Uhr überwachten Ort gespeichert. Zudem verfügt ein Rechenzentrum über eine Temperaturkontrolle, sodass die Server nicht überhitzen. Gleichzeitig gewährleistet die Notfallstromversorgung, dass die Daten ausfallsicher gespeichert sind und das Risiko von Serverausfällen sinkt.

Unternehmen, Bildungseinrichtungen oder Behörden zahlen je nach Art des Rechenzentrums meist nur für den beanspruchten Platz und den verbrauchten Strom. Dafür sparen sie Zeit bei der Verwaltung und der Infrastruktur und können sich mehr auf ihr Kerngeschäft konzentrieren.



2.2 Arten von Rechenzentren

Ein Rechenzentrum (RZ) ist ein komplexes Gebilde, bestehend aus baulich-technischen Komponenten, IT-Hardware und Software sowie einer Vielzahl technischer und organisatorischer Prozesse. Erst das Zusammenwirken dieser Elemente auf einem bestimmten Verfügbarkeitsniveau ermöglicht die Bereitstellung einer IT-Dienstleistung in der geforderten Verfügbarkeit.

Unternehmens-Rechenzentren oder Enterprise-Rechenzentrum (On-Premises): Diese Rechenzentren sind von einem Unternehmen gebaut und für dessen Endbenutzer optimiert. Das Rechenzentrum ist im Besitz eines Unternehmens und befindet sich meist auf dem Firmengelände. Somit ist das Unternehmen auch selbst für die Wartung und Verwaltung der Infrastruktur und IT-Komponenten verantwortlich. In diesem Rechenzentrum-Modell werden die gesamte IT-Infrastruktur und die Daten lokal (On-Premises) zur Verfügung gestellt. Viele Unternehmen entscheiden sich für ihre eigenen lokalen Rechenzentren, weil sie der Meinung sind, dass sie mehr Kontrolle über Daten und die Informationssicherheit haben.

Public-Cloud-Rechenzentren oder Cloud-Rechenzentren (Off-Premises): Bei dieser Off-Premise-Variante eines Rechenzentrums verwalten oder hosten (aufnehmen) öffentliche Cloud-Anbieter die Daten und Anwendungen. Die Wartung und Verwaltung fallen komplett in den Verantwortungsbereich des jeweiligen Anbieters. Bei den Cloud-Computing-Rechenzentren werden die IT-Infrastruktur-Ressourcen für die gemeinsame Nutzung durch mehrere Kunden - von einigen wenigen bis zu Millionen von Kunden - über eine Internetverbindung bereitgestellt. Cloud-Service-Anbieter haben meist kleinere Edge-Rechenzentren (edge .. Kante, Rand), die näher an den Cloud-Kunden liegen. Für

echtzeitorientierte, datenintensive Workloads (Arbeitsaufkommen) wie Big Data Analytics, künstliche Intelligenz (KI) und Content-Delivery-Anwendungen (Lieferung von Inhalten) können Edge-Rechenzentren dazu beitragen, Latenzzeiten zu minimieren und so die Gesamtleistung der Anwendungen zu verbessern.

Verwaltete Rechenzentren (Managed-Service-Rechenzentren) und Colocation-Einrichtungen: Verwaltete Rechenzentren und Colocation-Einrichtungen oder Serverhousing sind Optionen für Unternehmen, die nicht über die Räumlichkeiten, das Personal oder das Fachwissen verfügen, um einen Teil oder die gesamte IT-Infrastruktur vor Ort zu implementieren und zu verwalten, aber diese Infrastruktur nicht innerhalb den geteilten Ressourcen eines Public-Cloud-Rechenzentrums hosten möchten. In einem verwalteten Rechenzentrum mietet das Kundenunternehmen dedizierte Server, Speicher- und Netzwerkhardware vom Anbieter des Rechenzentrums und dieser übernimmt auch die Verwaltung, Überwachung und das Management.

In einer Colocation-Einrichtung besitzt das Kundenunternehmen die gesamte Infrastruktur und mietet einen speziellen Bereich, um sie in der Einrichtung zu hosten. Beim traditionellen Colocation-Modell hat das Kundenunternehmen alleinigen Zugriff auf die Hardware und die volle Verantwortung für deren Verwaltung. Dies ist ideal für den Datenschutz und die Sicherheit, aber oft unpraktisch, insbesondere bei Ausfällen oder Notfällen. Heute bieten die meisten Colocation-Anbieter Management- und Überwachungsdienste für Kunden an, die dies wünschen. Die Aufgaben einer Colocation-Umgebung reichen von einfachen Ausführungen wie der Speicherung zur Datensicherung bis hin zur Lagerung und Ausführung von grundlegenden IT-Prozessen kann ein Rechenzentrum

Rechenzentren - Konzeption, Aufbau und Security 4/35

verschiedene Aufgaben übernehmen. So fungieren einige Rechenzentren auch als Vernetzungsstelle, die verschiedene Colocation-Umgebungen verbindet. Das ist zum Beispiel für das Streamen von Filmen wichtig, bei dem sich typischerweise ein CDN (Content Delivery Network) einer Colocation-Umgebung mit einem Internetdienstanbieter (ISP) vernetzt. Verwaltete Rechenzentren (Managed-Service-Rechenzentren) und Colocation-Einrichtungen werden häufig für Remote-Datensicherungs- und Disaster-Recovery-Technologien für kleine und mittelständische Unternehmen (KMUs) verwendet.

Hyperscale- und Wholesale-Rechenzentren: Hyperscale- und Wholesale-Rechenzentren (skalierbare und sehr große Rechenzentren) hingegen sind genau auf die Anforderungen von einzelnen Unternehmen optimiert und eignen sich vor allem für Großunternehmen.

2.3 Rechenzentrum-Architektur

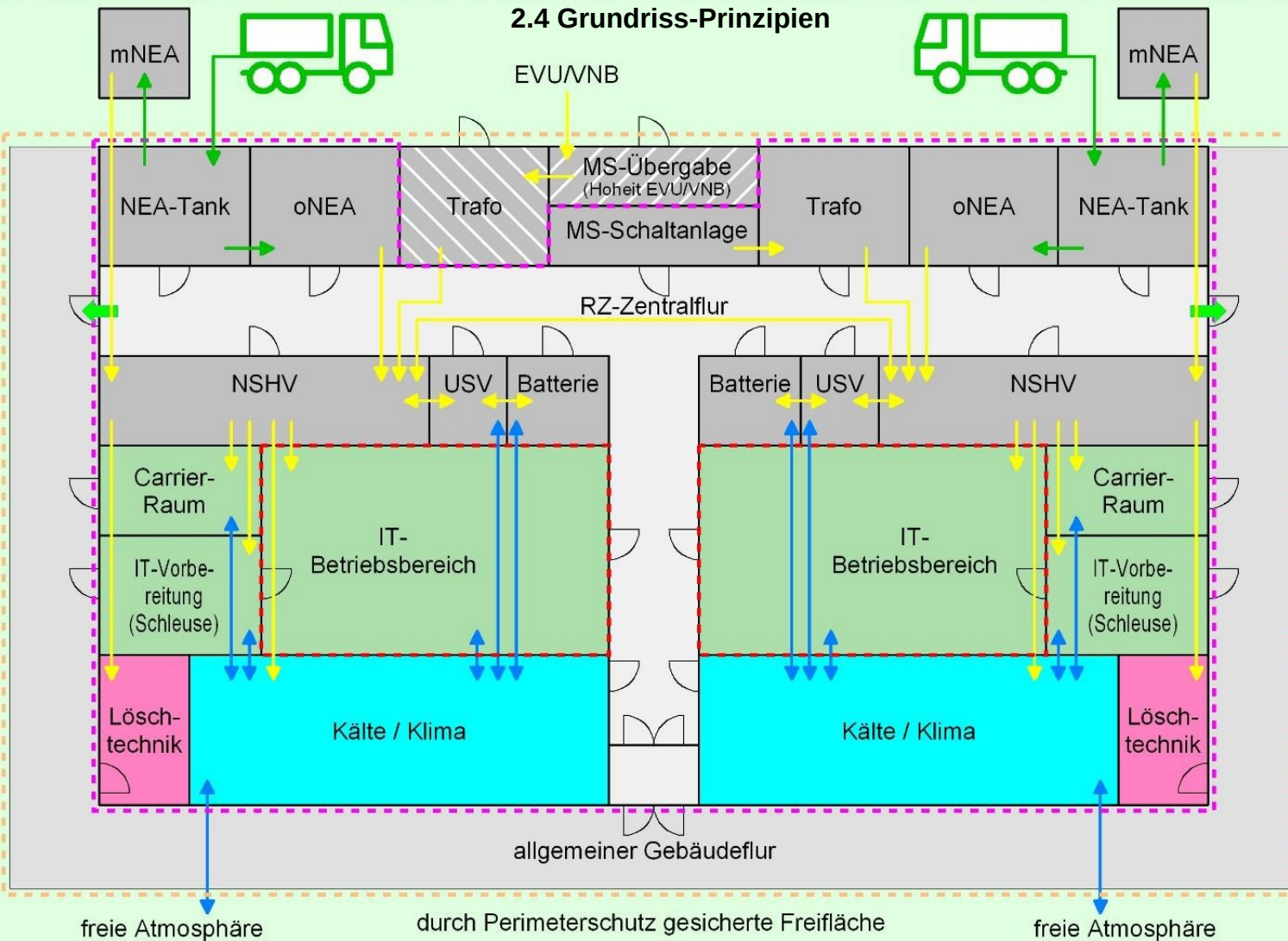
Die meisten modernen Rechenzentren, selbst interne Rechenzentren, haben sich von der traditionellen IT-Architektur, bei der jede Anwendung oder Arbeitslast auf einer eigenen dedizierten Hardware läuft, zu einer Cloudarchitektur entwickelt, bei der physische Hardwareressourcen (CPUs, Speicher, Netzwerke) virtualisiert werden. Virtualisierung ermöglicht es, diese Ressourcen von ihren physischen Einschränkungen zu lösen und zu Kapazitäten zusammenzufassen, die mehreren Anwendungen und Arbeitslasten in beliebiger Größenordnung zugewiesen werden können. Virtualisierung ermöglicht auch eine softwaredefinierte Infrastruktur (SDI), eine Infrastruktur, die voll automatisch und programmgesteuert bereitgestellt, konfiguriert, betrieben, gewartet und »heruntergefahren« werden kann.

Die Kombination aus Cloudarchitektur und softwaredefinierte

Infrastruktur (SDI) bietet Rechenzentren und ihren Nutzern viele Vorteile, darunter die folgenden:

- Optimale Auslastung der Ressourcen Rechen-, Speicherung- und Netzressourcen. Virtualisierung ermöglicht es Unternehmen oder Clouds, die meisten Benutzer mit Hardware und mit den am wenigsten ungenutzten Kapazitäten zu bedienen.
- Schnelle Bereitstellung von Anwendungen und Services. SDI-Automatisierung (SDI .. softwaredefinierte Infrastruktur) macht die Bereitstellung neuer Infrastruktur so einfach wie eine Anforderung über ein Self-Service-Portal (Selbstbedienung).
- Skalierbarkeit. Virtualisierte IT-Infrastruktur ist wesentlich einfacher zu skalieren als traditionelle IT-Infrastruktur. Selbst Unternehmen, die lokale Rechenzentren nutzen, können bei Bedarf ihre Kapazität erhöhen, indem sie Arbeitslasten in die Cloud auslagern.
- Vielzahl an Services und Rechenzentrumslösungen. Unternehmen und Clouds können Nutzern eine Reihe von Möglichkeiten bieten und bereitzustellen - alles über dieselbe Infrastruktur. Die Auswahl basiert auf den Anforderungen der Workloads (Arbeitsaufkommen) und umfassen Infrastructure as a service (IaaS), Platform as a service (PaaS) und Software as a service (SaaS). Diese Services können in einem privaten Rechenzentrum oder als Cloud-Lösungen in einer Private-Cloud-, Public-Cloud-, Hybrid-Cloud- oder Multicloud - Umgebung angeboten werden.
- Cloudnative Entwicklung. Containerisierung und serverloses Computing sowie ein robustes Open-Source-Ökosystem ermöglichen und beschleunigen Entwicklungs-Zyklen und Anwendungsmodernisierung sowie Anwendungen für die einmalige Entwicklung und Bereitstellung.

2.4 Grundriss-Prinzipien



- ➡ evtl. erforderlicher Fluchtweg
- ➡ elektrotechnische Beziehung
- ➡ klimatechnische Beziehung
- ➡ Kraftstoff-Beziehung
- - - Grundstücksgrenze / Perimeterschutz
- - - Gebäudehülle
- - - RZ-Bereich (inkl. Supportbereich)
- - - IT-Betriebs-Bereich

Grundriss-Prinzipien:

Auch wenn auf den ersten Blick keine Beziehung zwischen dem Grundriss eines Rechenzentrums (RZ) und dessen Verfügbarkeit zu vermuten ist, gibt es sie doch:

- Die Länge von Erschließungswegen sowie deren einfache Nutzbarkeit haben Einfluss auf Reaktionszeiten in einem Schadensfall.
- Die Realisierung geeigneter, voneinander getrennter Zugangsbereiche ermöglicht eine zweckmäßige Zutrittssteuerung und damit den Schutz vor Unbefugten.
- Die Realisierung von Brandabschnitten ermöglicht einen sinnvollen Aufbau von Redundanzen.

Die beiden führenden Grundprinzipien werden mit den Schlüsselworten Schalenmodell und Trennung der feinen und der groben Technik beschrieben.

Rechenzentren - Konzeption, Aufbau und Security 6/35

Schalenmodell

Im Schalenmodell sollte ein Rechenzentrum (RZ) so aufgebaut sein, dass sich Bereiche mit dem höchstwertigen Schutzgut an zentraler Stelle befinden und von anderen Räumen umgeben sind, deren Schutzbedarf nach außen hin abnimmt.

In der Abbildung auf der vorherigen Seite ist der IT-Betriebsbereich der mit dem höchstwertigen Schutzgut. Dort sind die für die Bereitstellung von IT-Dienstleistungen unmittelbar erforderlichen IT-Komponenten untergebracht und dort befinden sich auch die Daten zur Be- und Verarbeitung.

Dem IT-Betriebsbereich direkt beigeordnet sind die beiden wesentlichen Supporteinrichtungen der Strom- und Kälteversorgung: Niederspannungs-Hauptverteilung (NSHV) mit der unterbrechungsfreien Stromversorgung (USV) und Batterie sowie die Kälte- und Klimaanlage. Des Weiteren liegen der Carrier-Raum (Anbindung an das Internet) und die IT-Vorbereitung schützend zwischen IT-Betriebsbereich und allgemeinem Gebäudeflur. Gemeinsam mit der Löschtechnik und den weiteren Räumen der Energieversorgung (MS-Schaltanlage, Trafo und Netzersatzanlage) bilden die gezeigten Räume das funktionale Herz eines Rechenzentrums (RZ).

Der Zutritt zu den meisten Räumen des Rechenzentrums ist nur einem begrenzten Personenkreis zugänglich. Davon wird nur abgewichen bei Wartung und Reparatur von einigen Komponenten des Rechenzentrums durch speziell geschultes externes Personal.

Trennung der feinen und der groben Technik

Um möglichst weitgehend sicherstellen zu können, dass Personen ausschließlich solche Bereiche betreten, zu denen sie auf Grund

der dort zu erledigenden Tätigkeiten ein Zutrittsrecht haben, sollen alle technischen Komponenten - sofern möglich - räumlich voneinander getrennt untergebracht werden. So ist es z.B. zu vermeiden, dass der Zugang zur Klimatechnik durch einen RZ-Betriebsbereich hindurch erfolgt oder dass USV-Systeme (unterbrechungsfreie Stromversorgung) im Carrier-Raum (Anbindung an das Internet) aufgebaut werden.

In Fällen, in denen eine solche Trennung nicht vollständig möglich ist, sind organisatorische Maßnahmen erforderlich, um den Fortfall des Nutzens der räumlichen Trennung zu kompensieren.

Reserveflächen für Umbau und Erweiterung

Bei Hochverfügbarkeits-Rechenzentren (HV-RZ) ist es meist nicht möglich, zu ersetzende technische Einheiten erst abzubauen und die neuen erst nach deren Aufbauzeit in Betrieb zu nehmen. Es ist vielfach erforderlich, die neuen Einheiten noch während der Nutzung der abgängigen Einheiten aufzubauen, um die dann erforderliche Umschaltunterbrechung so kurz wie möglich zu halten.

Um das zu ermöglichen, sind für alle technischen Einrichtungen Reserveflächen vorzuhalten, auf denen der Neuaufbau parallel zum Weiterbetrieb der anderen Einheiten erfolgen kann. Die Größe dieser Flächen ist von der Mindestgröße der auszutauschenden Einheiten abhängig. Gibt es keine definierbare Mindestgröße, sollte die Reservefläche im Bereich von 20 bis 30 % der schon besiedelten Fläche liegen. Neben dem Nutzen, durch Reserveflächen einen unterbrechungsarmen Umbau zu ermöglichen, können solche Flächen natürlich auch für erforderliche Erweiterungen von Anlagen genutzt werden. Dabei ist aber darauf zu achten, den Verlust der potenziellen Umbaufläche zu kompensieren.

2.5 Wie ist ein Rechenzentrum (RZ) aufgebaut?

Ein Rechenzentrum besteht in der Regel aus drei Bereichen: einem Raum für die Servertechnik (IT-Betriebsbereich), einem Raum für die technische Gebäudeausrüstung und einer Schleuse.

Server-Raum

Im Serverraum stehen sich die etwa 2 Meter hohen Server- und Netzwerkschränke in geschlossenen Reihen gegenüber, jeweils Vorder- zu Vorderseite oder Rück- zu Rückseite. Entsprechend der Rechenleistung kommt es zu einer starken Wärmeentwicklung die über ein Kühlungssystem reguliert werden muss, um die Hardware vor Überhitzung zu schützen. In der Regel wird an einer Seite der Netzwerkschränke kühle Luft aus dem Boden geblasen und an der anderen Seite warme Luft nach oben abgesaugt. Die Stromverkabelung der einzelnen Netzwerkschränke verläuft meist unter einem Doppelboden. Die Datenverkabelung erfolgt von oben. Die Stromversorgung selbst ist vor allem bei Hochverfügbarkeits-Rechenzentren (HV-RZ) redundant ausgelegt, sodass es selbst bei Ausfall eines Umspannwerkes zu keinen Ausfallzeiten kommt.

Support-Technik

Im Raum für die unterstützende Technik ist die zum sicheren Betrieb der Server nötige Technik untergebracht. Hier finden sich die Installationen zur Stromversorgung und Temperaturregulierung und hier wird die Löschtechnik und Sicherheitstechnik verwaltet. Für die Sauberkeit in Rechenzentren hat sich die ISO 14644-1 Klasse 8 für Reinräume etabliert, da Staub zu Verschleißerscheinungen an der Hardware führen kann.

Sicherheitsmaßnahmen und Zutrittskontrolle

Der Sicherheit kommt im Rechenzentrum eine besondere Bedeutung zu. Umfassende Brandschutzvorkehrungen gehören

zum Standard eines jeden Rechenzentrums. Automatische Systeme zur Brandfrüherkennung und Löscheinrichtungen mit speziellen Löschgasen (Argon, CO₂ und Stickstoff) sollen dafür sorgen, dass der Schaden an der Hardware im Ernstfall möglichst gering ausfällt.

Professionelle Rechenzentrums-Anbieter verfügen zudem über ein Disaster-Recovery-Rechenzentrum, das eine Kopie des Original-Rechenzentrums mit sämtlichen Daten darstellt (Backup-Rechenzentrum oder die Umsetzung einer Zwei-Standort-Strategie). Durch ein Backup-Rechenzentrum bzw. Disaster-Recovery-Rechenzentrum sollten bei einem Totalausfall alle RZ-Nutzer innerhalb von drei Stunden wieder auf alle Applikationen zugreifen können.

Um Zugriff durch Unbefugte zu verhindern, gelten in einem Rechenzentrum strenge - im besten Fall mehrstufige - Zutrittskontrollen. Neben Alarmanlagen und Kameraüberwachung auf dem Gelände kommen in den Gebäuden digitale Authentifizierungssysteme wie Kartenleser, Fingerabdruckscanner, Handscanner oder Nummernfelder für Zugangscodes zum Einsatz. Die Zugriffskontrolle hat alle Zutritte zu den geschützten Bereichen zu protokollieren. Fehlversuche sind im System ebenfalls zu protokollieren.

Hinweis: Eine Person darf nur die Rechte haben, die sie zur Erfüllung ihrer Aufgaben tatsächlich benötigt (Minimalprinzip). Weitergehende Rechte »auf Vorrat« dürfen nicht vergeben werden. Es muss regelmäßig überprüft werden, ob Rechte noch notwendig sind. Nicht mehr erforderliche Rechte sind umgehend zurückzuziehen.

2.6 Komponenten der Rechenzentrum-Infrastruktur

Server:

Server sind leistungsfähige Computer, die Anwendungen, Dienste und Daten für Endbenutzergeräte bereitstellen. Server für Rechenzentren gibt es in verschiedenen Formen:

- Rackmount-Server sind breite, flache Standalone-Server - in der Größe eines kleinen Pizzakartons - die dafür konzipiert sind, in einem Rack platzsparend übereinander gestapelt zu werden (im Gegensatz zu einem Tower- oder Desktop-Server). Jeder Rackmount-Server verfügt über eine eigene Stromversorgung, Lüfter, Netzwerk-Switches und Ports sowie den üblichen Prozessor, Arbeitsspeicher und Speicher.
- Blade-Server sind konzipiert, um noch mehr Platz zu sparen. Jedes Blade enthält Prozessoren, Netzwerk-Controller, Arbeitsspeicher und teilweise auch Speicher. Sie sind so konzipiert, dass sie in ein Gehäuse passen, das mehrere Blades aufnimmt und die Stromversorgung, das Netzwerkmanagement und andere Ressourcen für alle Blades im Gehäuse enthält.
- Mainframes sind Hochleistungscomputer mit mehreren Prozessoren, die so viel wie ein ganzer Raum, gefüllt mit Rackmount- oder Blade-Servern, leisten können. Mainframes, als erste virtualisierbare Computer, können Milliarden von Berechnungen und Transaktionen in Echtzeit verarbeiten.

Die Wahl der Server hängt von vielen Faktoren ab, darunter der verfügbare Platz im Rechenzentrum, die Arbeitslasten, die auf den Servern ausgeführt werden, die verfügbare Leistung und die Kosten.

Speichersysteme:

Die meisten Server verfügen über eine lokale Speicherkapazität, den sogenannten Direct-Attached Storage (DAS), damit die am häufigsten verwendeten Daten (Hot Data) in der Nähe der CPU verbleiben können.

Zwei weitere Speicherkonfigurationen für Rechenzentren sind Network-Attached Storage (NAS) und Storage Area Network (SAN).

NAS bietet Datenspeicherung und Datenzugriff auf mehrere Server über eine Standard-Ethernet-Verbindung. Das NAS-Gerät ist in der Regel ein dedizierter Server mit mehreren Speichermedien - Festplattenlaufwerken (HDDs) und/oder Solid State Drives (SSDs).

Wie NAS ermöglicht ein SAN gemeinsam genutzte Speicher, aber ein SAN verwendet ein separates Netzwerk für die Daten und besteht aus einer komplexeren Mischung aus mehreren Speicherservern, Anwendungsservern und Speicherverwaltungssoftware.

Ein einziges Rechenzentrum kann alle drei Speicherkonfigurationen - DAS, NAS und SAN - verwenden, sowie Dateispeicher, Blockspeicher und Objektspeicher.

Aktive Netzwerkkomponenten: Geräte wie Router, Switches, Firewalls (Hardware) und andere Controller, die für den Betrieb eines aktiven Netzwerkes benötigt werden und die einen aktiven Stromanschluss benötigen, zählen zu den aktiven Netzwerkkomponenten.

Rechenzentren - Konzeption, Aufbau und Security 9/35

Passive Netzwerkkomponenten: Das Rechenzentrum benötigt auch passive Netzwerkkomponenten für den Betrieb eines Netzwerkes. Anders als die aktiven Netzwerkkomponenten benötigen passive Netzwerkkomponenten - wie Verkabelung, Stecker und Buchsen - jedoch keinen eigenen Stromanschluss.

Baugruppenträger: Im Gehäuse aus Metall - den sogenannten Baugruppenträgern oder Racks - sind die Serverhardware und die Netzwerkkomponenten befestigt. Eine international genormte Größe mit einer 19-Zoll-Bauweise sorgt dafür, dass die Racks mit sämtlichen Baugruppen kompatibel sind.

Netzbetrieb:

Das Netzwerk des Rechenzentrums, das aus verschiedenen Arten von Switches, Routern und Glasfaserkabeln besteht, überträgt den Netzwerkverkehr zwischen den Servern (Ost/West-Verkehr genannt) und von/zu den Servern zu den Clients (Nord/Süd-Verkehr genannt).

Wie oben erwähnt, sind die Netzservices eines Rechenzentrums typischerweise virtuell. Dies ermöglicht Erstellung von softwaredefinierten Overlay-Netzwerken, die auf der physischen Infrastruktur des Netzwerks aufbauen, um bestimmte Sicherheitskontrollen oder Service Level Agreements (SLAs) zu erfüllen.

Stromversorgung und Kabelmanagement:

Rechenzentren müssen stets verfügbar sein, auf jeder Ebene. Die meisten Server verfügen über zwei Energiequellen zur Stromversorgung. Batteriebetriebene unterbrechungsfreie Stromversorgungen (USV oder uninterruptible power supply / UPS) schützen vor Stromstößen und kurzen Stromausfällen.

Leistungsfähige Generatoren können bei einem schwerwiegenden Stromausfall einspringen. Bei Tausenden von Servern, die über verschiedene Kabel miteinander verbunden sind, ist das Kabelmanagement ein wichtiges Thema bei der Planung von Rechenzentren. Wenn Kabel zu nahe beieinander liegen, kann es zum Übersprechen kommen, was sich negativ auf die Datenübertragungsraten und die Signalübertragung auswirken kann. Wenn zu viele Kabel zusammengelegt werden, können sie außerdem übermäßige Hitze erzeugen. Beim Bau und der Erweiterung von Rechenzentren müssen Bauvorschriften und Industriestandards berücksichtigt werden, um eine effiziente und sichere Verkabelung zu gewährleisten.

Redundanz und Notfallwiederherstellung:

Ausfallzeiten von Rechenzentren sind sowohl für die Anbieter von Rechenzentren als auch für deren Kunden kostspielig. Betreiber und Architekten von Rechenzentren unternehmen große Anstrengungen, um die Ausfallsicherheit ihrer Systeme zu erhöhen. Diese Maßnahmen umfassen alles von redundanten Arrays unabhängiger Festplatten (RAIDs) zum Schutz vor Datenverlust oder -beschädigung im Falle eines Ausfalls der Speichermedien bis hin zu einer Backup-Kühlungsinfrastruktur für das Rechenzentrum, die dafür sorgt, dass die Server bei optimalen Temperaturen laufen, selbst wenn das primäre Kühlsystem ausfällt.

Viele große Anbieter von Rechenzentren verfügen über Rechenzentren in geografisch unterschiedlichen Regionen, sodass im Falle einer Naturkatastrophe oder einer politischen Störung in einer Region der Betrieb in eine andere Region verlagert werden kann, um ununterbrochene Dienste zu gewährleisten (Zwei-Standort-Strategie).

2.7 Infrastruktur-Komponenten

Der letzte Baustein, der für einen reibungslosen Betrieb des Rechenzentrums sorgt, sind die einzelnen Infrastruktur-Komponenten. Je nach Aufbau und Ausrüstung des Gebäudes fallen diese ganz unterschiedlich aus.

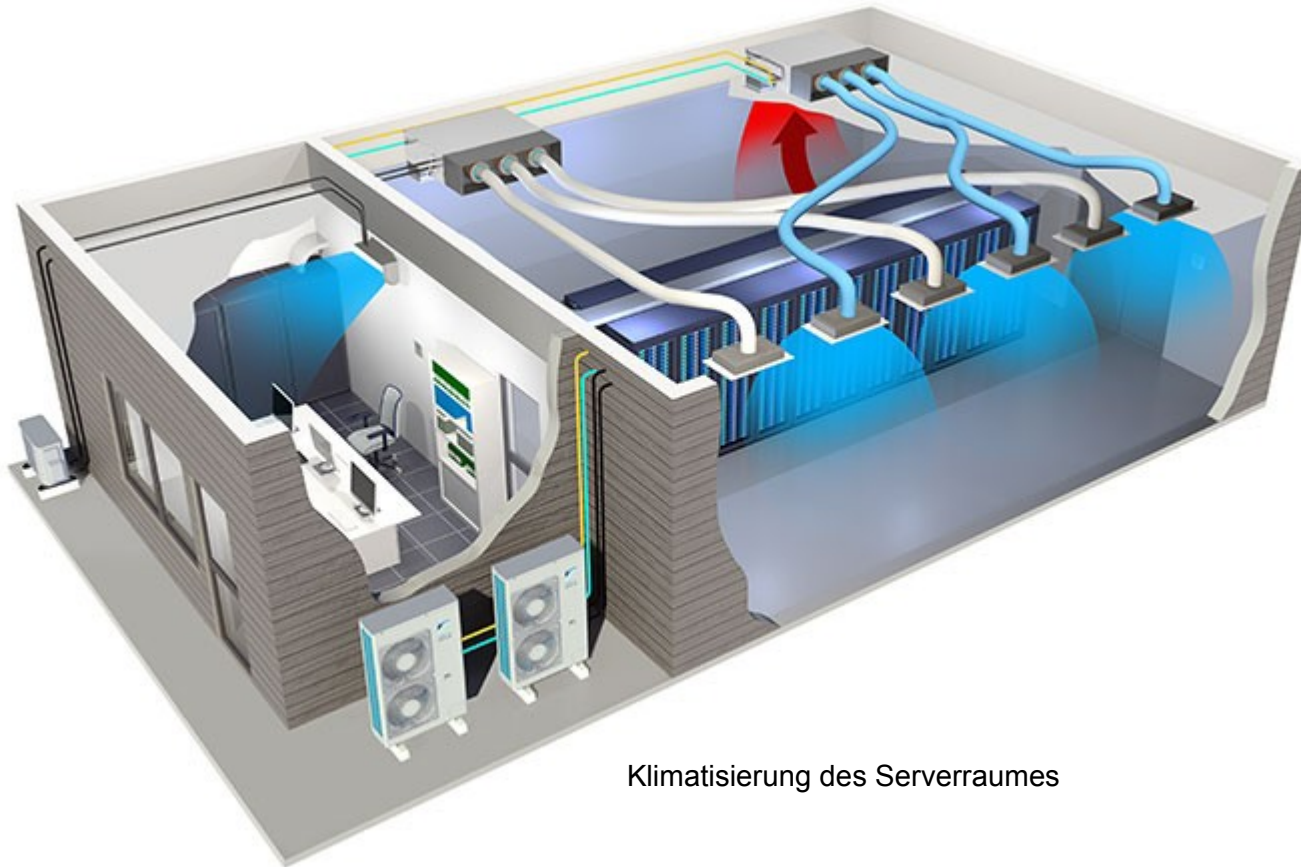
- **Umgebungskontrolle:** Eine ideale Temperatur im Rechenzentrum ist das A und O. Die große Menge an Servern erzeugt eine starke Wärme, die unkontrolliert zu Überhitzung und Ausfällen der Server führen würde. Ausgefeilte Systeme und architektonische Maßnahmen sorgen innerhalb des Rechenzentrums für einen effizienten Kühlkreislauf und zu optimale Temperaturen für die Technik.
- **Energieversorgung:** Ohne Strom läuft kein Rechenzentrum. Umso wichtiger ist es, für eine konstante, ausfallsichere Stromversorgung zu sorgen. Erreicht wird dies zum einen über redundante Stromanschlüsse, die über zwei verschiedene Versorger das Rechenzentrum mit Energie versorgen. Zum anderen überbrückt eine Batterie kurze Stromausfälle, während ein eigener Dieselgenerator bei länger anhaltenden Stromausfällen die Energieversorgung übernimmt.
- **Sicherheitstechnik:** Um die sensiblen Daten vor Dritten zu schützen, sollte nur autorisierten Personen der Zutritt zum Rechenzentrum erlaubt sein, die sich mittels Keycard oder Fingerabdruckscanner identifizieren müssen. Zusätzlich bedarf es einer modernen Videoüberwachung, die dem Personal einen konstanten Überblick über die Anlage ermöglicht. Damit bei Feuer Personal und Ausstattung geschützt sind, sollten moderne Brandschutzsysteme genutzt werden.

2.8 Kontrollmechanismen der Umgebung

Rechenzentren müssen so konzipiert und ausgestattet sein, dass sie Umgebungsfaktoren - von denen die meisten miteinander verknüpft sind - kontrollieren können, die die Hardware beschädigen bzw. zerstören und zu teuren bzw. katastrophalen Ausfallzeiten führen können.

- **Temperatur:** Die meisten Rechenzentren verwenden eine Kombination aus Luft- und Flüssigkeitskühlung, um Server und andere Hardware in den richtigen Temperaturbereichen zu halten. Bei der Luftkühlung handelt es sich im Grunde um eine Klimatisierung, genauer gesagt um eine Klimatisierung von Computerräumen (CRAC), die auf den gesamten Serverraum oder auf bestimmte Serverreihen oder -schränke ausgerichtet ist. Technologien zur Flüssigkeitskühlung pumpen die Flüssigkeit direkt zu den Prozessoren, oder in einigen Fällen werden die Server in die Kühlflüssigkeit getaucht. Zur Energieeffizienz und Nachhaltigkeit setzen Anbieter von Rechenzentren zunehmend auf Flüssigkeitskühlung die weniger Strom und Wasser als Luftkühlung benötigt.
- **Feuchtigkeit:** Eine hohe Luftfeuchtigkeit kann dazu führen, dass Geräte rosten; eine niedrige Luftfeuchtigkeit kann das Risiko elektrostatischer Ladung erhöhen (siehe nächsten Punkt). Geräte zur Kontrolle der Luftfeuchtigkeit umfassen die bereits erwähnten CRAC-Systeme, angemessene Belüftung und Feuchtigkeitssensoren.
- **Statische Elektrizität:** Bereits eine statische Entladung von 25 Volt kann Geräte beschädigen oder Daten verfälschen. Rechenzentren sind mit Geräten ausgestattet, die elektrostatische Ladung überwachen und sicher ableiten.

- **Feuer:** Aus verständlichen Gründen müssen Rechenzentren mit Brandschutzvorrichtungen ausgestattet sein, die regelmäßig getestet werden müssen.



Klimatisierung des Serverraumes

2.8 Netzersatzanlagen (NEA)

Netzersatzanlagen (NEA) haben den Zweck, bei Ausfall der Stromversorgung seitens des Energieversorgungsunternehmens (EVU) eine gleichwertige, von äußeren Einflüssen unabhängige, lokale Versorgung mit elektrischer Energie sicherzustellen. Bei der Planung von Netzersatzanlagen sind mindestens folgende Parameter zu berücksichtigen:

- die Autonomiezeit,
- das erforderliche Redundanzmodell,
- die bereitzustellende Leistung.

Autonomiezeit

Die erforderliche Autonomiezeit, also die durch die Gesamtheit technischer Maßnahmen ermöglichte autonome Laufzeit der NEA-Versorgung, definiert sich aus dem Verfügbarkeitsbedarf der in einem Rechenzentrum (RZ) erbrachten IT-Dienstleistungen und der Festlegung einer mindestens zu überbrückenden Ausfallzeit der normalen Energieversorgung seitens des Energieversorgungsunternehmens. Diese Autonomiezeit sollte

- bei einem Rechenzentrum (RZ) mit hoher Verfügbarkeit mindestens 48 h,
- bei einem Rechenzentrum (RZ) mit sehr hoher Verfügbarkeit mindestens 72 h und
- bei einem höchstverfügbaren Rechenzentrum (HV-RZ) durchaus 120 h betragen.

Der Treibstoffvorrat ist so zu dimensionieren, dass ein unterbrechungsfreier Betrieb der Netzersatzanlage (NEA) über die gesamte Autonomiezeit hinweg ohne Nachtanken sichergestellt ist.

Hinweis: Für die Lagerung des Treibstoffs der Netzersatzanlage (NEA) ist sicherzustellen, dass dessen Temperatur zu keiner Zeit unter 4 °C sinkt. Ist das nicht möglich, ist durch ein vom Motorhersteller und vom Treibstoffhersteller zugelassenes Additiv ein ausreichender Frostschutz zu bewirken.

Redundanz

Alle für die Bereitstellung der IT-Dienstleistung eines höchstverfügbaren Rechenzentrums (HV-RZ) erforderlichen Einrichtungen sind über mindestens zwei ortsfeste Netzersatzanlagen (oNEA) zu versorgen, von denen jede allein in der Lage ist, die erforderliche Leistung zu erbringen.

Zusätzlich ist für Wartungsfälle eine Anschlussmöglichkeit für eine mobile NEA (mNEA) einzurichten. Ein geeigneter Stellplatz für die mobile Netzersatzanlage (NEA) muss bereits bei der Planung eines Rechenzentrums berücksichtigt und als solcher ausgewiesen werden.

Leistung

Die ortsfesten Netzersatzanlagen (oNEA) sind samt aller zugehörigen Betriebskomponenten auf einen Dauerbetrieb unter Volllast für die Autonomiezeit auszulegen.

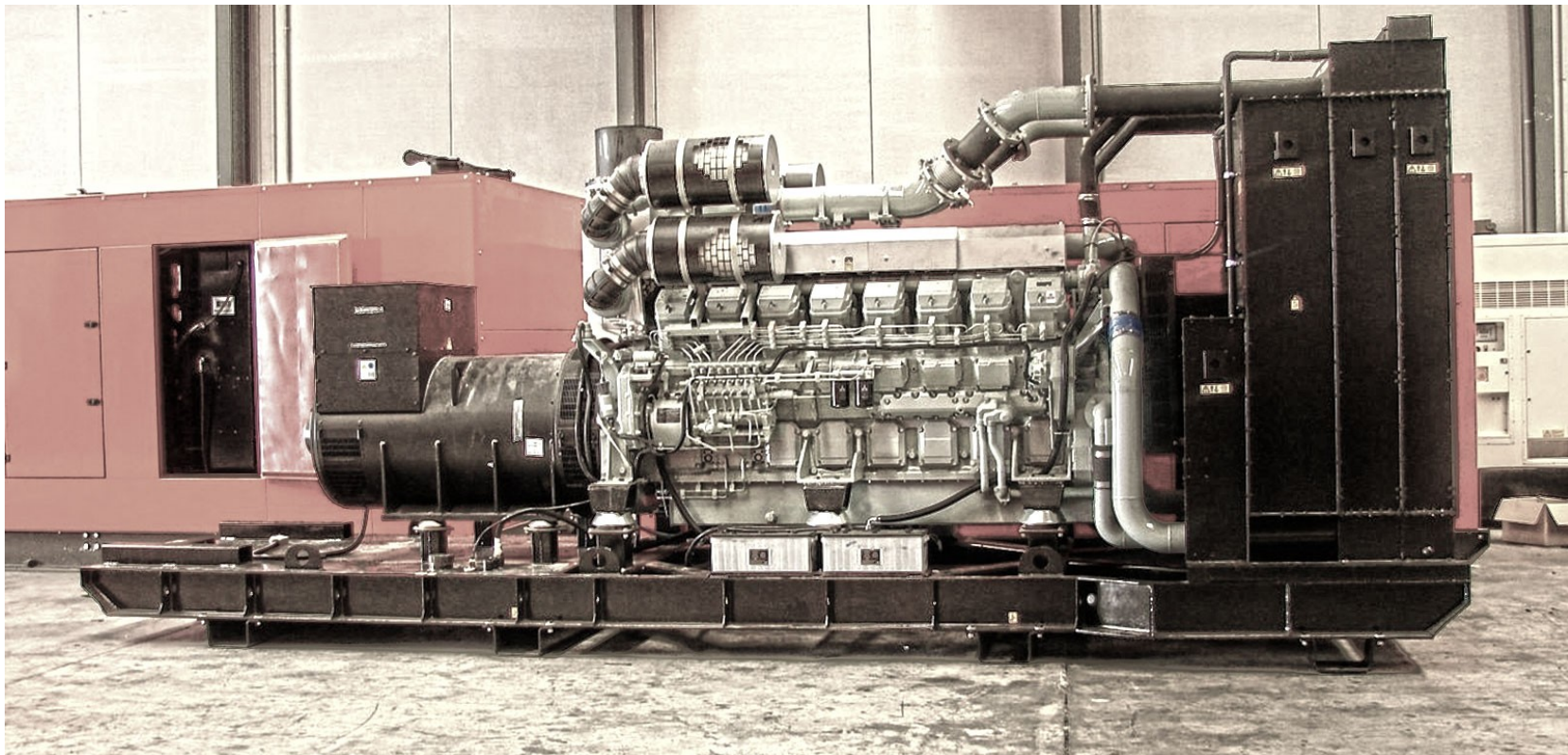
Wartezeit

Bei Ausfall der Netz-Versorgung gibt es bis zur Bereitstellung der NEA-Versorgung eine kurze Zeitspanne, in der keine Energieversorgung zur Verfügung steht, auch Dunkelphase genannt, die bestimmte Verbraucher durch USV-Systeme (unterbrechungsfreie Energieversorgung) überbrückt werden muss.

Diese Zeitspanne beträgt typisch 10 bis 20 Sekunden, kann bei Startschwierigkeiten der NEA aber auch mehrere Minuten dauern. Es ist daher nicht zweckmäßig, sofort bei Ausfall der Energieversorgung einen Shutdown zu starten, sondern damit etwas zu warten. Eine Wartezeit von ca. 5 Minuten ist als sinnvoll anzusehen.

Shutdownzeit

Die Shutdownzeit ist die Zeit, die erforderlich ist, um alle relevanten Systeme so rasch wie möglich und hinreichend geordnet herunter zu fahren, um Datenverluste zu vermeiden und ein möglichst rasches Wiederhochfahren der Systeme zu ermöglichen. Insbesondere bei Datenbanksystemen oder IT-Hardware, die bei einem schlagartigen Versorgungsausfall Schaden nehmen können, ist ein Shutdown erforderlich. Die erforderliche Dauer eines Shutdowns wird meist theoretisch festgelegt. Es empfiehlt sich aber, durch einen echten Shutdown diesen Wert von Zeit zu Zeit zu überprüfen. Ist die Shutdownzeit nicht bestimmbar, sollte in einem **ersten Ansatz** von ca. 30 Minuten ausgegangen werden. **Hinweis:** Die Brennstoffzellentechnik kann als Basis für die Netzersatztechnik genutzt werden.



2.9 Brandschutz

Rechenzentren sind in sich geschlossene Umgebungen, in denen unkontrollierte Überhitzung schnell zu einem Brand führen kann. Ein wirkungsvoller Brandschutz umfasst die drei Bereiche des baulichen, technischen und organisatorischen Brandschutzes. Damit alle Maßnahmen des Brandschutzes sinnvoll und wirksam zusammenwirken, ist ein umfassendes Brandschutzkonzept zu erstellen und umzusetzen.

Alle einander Redundanz gebenden technischen Einrichtungen sind in gegeneinander brandgeschützten Bereichen mit mindestens 90 Minuten Feuerwiderstandszeit unterzubringen.

Löschanlagen sind reaktive Systeme, denn sie kommen erst zum Einsatz, wenn ein Brand zumindest schon in der Entstehungsphase ist, also eine für die Auslösung der Löschanlage ausreichende Rauchgaskonzentration oder Temperaturerhöhung dies bewirkt hat. Für eine Löschanlage stehen zwei Arten von Löschmitteln zur Verfügung: Wasser oder Löschgas (Argon, CO₂ und Stickstoff).

Hinweis: Gebäude oder Gebäudeteile, die auf Grund ihrer Nutzung oder Bauweise zwingend mit einer wasserbasierten Löschung ausgestattet werden müssen, sind für die Unterbringung eines hochverfügbaren Rechenzentrums (HV-RZ) nicht geeignet.

Sprinkler-/Wassernebel-Feuerlöschsysteme

Wasser ist ein wirksames, bewährtes und umweltfreundliches Feuerlöschmittel. Mit speziell entwickelten Sprühköpfen, die automatisch auf die von einem Feuer ausgehende Hitze reagieren, gewährleisten Sprinkler- und Wassernebelsysteme eine effiziente Freisetzung von Löschwasser über einem potenziellen Brandherd. Bei der Planung sollten individuelle Löschanforderungen und

Umweltaspekte stets berücksichtigt werden. Darüber hinaus schützen Wassernebelsysteme die Hardware durch den Ausstoß von sehr feinen Wassertröpfchen.

Brandlöschsysteme mit rückstandsfreien Löschmitteln

Moderne Brandschutzsysteme für Rechenzentren arbeiten mit Gaslöschsysteme, die vorhandene Daten schützen und Brände bereits im Frühstadium ihrer Entstehung bekämpfen, ohne dabei Geräte zu beschädigen. Diese Systeme arbeiten mit einer leistungsstarken Kombination von Inertgasen (Argon, CO₂ und Stickstoff), um Brände ohne Beeinträchtigung der Umwelt zu löschen.



2.10 Resilienz und Verfügbarkeitsanforderungen von Rechenzentren (RZ)

Das Ziel einer erhöhten Verfügbarkeit ist nicht nur bei der Auslegung der IT-Architektur, sondern in gleichem Maße bei der Festlegung von Struktur und Dimension aller baulichen und technischen Einrichtungen anzustreben, die den Betrieb eines Rechenzentrums ermöglichen und unterstützen.

Wegen der großen Zahl von Einzelkomponenten, aus denen sich die baulich-technische Infrastruktur eines Rechenzentrums zusammensetzt und der schwer zu bestimmenden Zuverlässigkeit dieser Komponenten ist ein mathematisch präziser Wert für die zukünftige Verfügbarkeit eines Rechenzentrums in der Praxis kaum zu ermitteln.

Eine Aussage über die zukünftige Verfügbarkeit eines Rechenzentrums ist in der Praxis leichter zu gewinnen, indem die Resilienz eines Rechenzentrums betrachtet wird, also die Fähigkeit, bei Ausfällen einzelner Komponenten als Gesamtstruktur nicht vollständig zu versagen, um die angeforderten IT-Dienstleistungen in der zugesicherten Qualität stets erbringen zu können.

Ein Hochverfügbarkeits-Rechenzentrum (HV-RZ) ist so zu konzipieren, dass es folgende Eigenschaften hat:

- Bei einem Rechenzentrum mit hoher Verfügbarkeit darf schon **ein** auftretendes, störendes Ereignis,
- bei sehr hoch verfügbaren Rechenzentrum dürfen erst **zwei** (zeitgleich oder zeitnah) voneinander unabhängig auftretende, störende Ereignisse und
- bei höchstverfügbaren Rechenzentrum dürfen erst **drei** (zeitgleich oder zeitnah) voneinander unabhängig auftretende, störende Ereignisse

zu einer maximal vertretbar geringen Beeinträchtigung der Verfügbarkeit der RZ-Gesamtstruktur und der IT-Dienstleistung führen.

Die vertretbar geringe Beeinträchtigung wird unter anderem durch die maximal tolerierbare Ausfallzeit definiert. Die maximal tolerierbare Ausfallzeit bestimmt insbesondere die zur Verfügung stehende Reaktionszeit. Je geringer die maximal tolerierbare Ausfallzeit ist, desto weniger Zeit steht bei Ausfall von Komponenten für eine Reaktion zur Verfügung.

Es ist wichtig zu beachten, dass störende Ereignisse nicht allein darauf beschränkt sind, dass diese unvorhergesehen auf eine Struktur einwirken. Gleichmaßen müssen auch erforderliche Funktionsunterbrechungen von Strukturen auf Grund geplanter Inspektionen, Wartungen und Reparaturen in die Betrachtung einbezogen werden. Dabei ist zu bedenken, dass während einer geplanten Funktionsunterbrechung zusätzlich weitere unvorhergesehene Ereignisse eintreten können.

Sollte darüber hinaus für die IT-Dienstleistung tatsächlich Unterbrechungsfreiheit gefordert sein (Desaster-Toleranz), ist diese in der Regel mit einem einzelnen RZ-Standort nicht realisierbar. Dann sind meist mehrere RZ-Standorte (Stichwort: Zwei-Standort-Strategie oder mehrere Standorte) erforderlich, die sich gegenseitig Wartungsredundanz geben.

2.11 Technische Leitstelle

Die technische Leitstelle eines Rechenzentrums nimmt alle betriebsrelevanten Meldungen sowohl aus den IT-Systemen als auch aus allen Support-Einrichtungen (z.B. aus der Netzüberwachung) entgegen, wertet diese aus und veranlasst, soweit das nicht automatisch erfolgt, die erforderlichen Reaktionen. Das wesentliche Ziel der Arbeit der Leitstelle ist es, den störungsfreien Betrieb des Rechenzentrums durch vorbeugende Handlungen sicherzustellen oder durch reaktive Handlung so rasch wie möglich wiederherzustellen.

In hochverfügbaren Rechenzentren (HV-RZ) sind mindestens zwei einander Redundanz gebende Leitstellen zu betreiben. Eine Leitstelle (primäre Stelle) muss permanent (24 Stunden, 7 Tage - 24/7) reaktionsfähig sein und auf Basis der jeweiligen Meldung alle erforderlichen Maßnahmen zielgenau einleiten und koordinieren. Verliert die primäre Stelle ihre Verfügbarkeit, ist die zweite Leitstelle (Ersatzstelle) umgehend in Betrieb zu nehmen. Die maximale Dauer der Unterbrechung zwischen Ausfall der primären Stelle und voller Betriebsbereitschaft der Ersatzstelle ist unter Berücksichtigung der maximal tolerierbaren Reaktionszeiten festzulegen und in allen Fällen einzuhalten.

Alle Meldungen, die auf den technischen Leitstellen auflaufen, sollen folgende Anforderungen erfüllen:

- Meldungen erfolgen für jeden Sensor individuell. Gruppenmeldungen können ergänzend genutzt werden.
- Meldungen werden mit klar verständlichem Text mit genauer Ortsangabe und ersten einfachen Handlungsanweisungen angezeigt.

- Die Meldungen werden auf gesicherten Wegen übertragen, d.h., die Leitungen sind mindestens gegen versehentliche oder vorsätzliche Beschädigung durch einfache Mittel zu schützen.
- Bei georedundanten Standorten (Zwei-Standort-Strategie) ist für systemrelevante Meldungen zusätzlich zum lokalen Monitoring ein zentrales Monitoring zu betreiben.

Bei der Fernübertragung von Meldungen an eine vom Rechenzentrum entfernt aufgebaute Leitstelle oder an ein zentrales Monitoring müssen Integrität und Vertraulichkeit der Informationsübertragung durch geeignete kryptografische und authentisierende Mechanismen geschützt werden.

Bei der Fernsteuerung der Supporteinrichtungen von einer entfernt aufgebauten Leitstelle müssen die Steuersignale ebenfalls durch geeignete kryptografische und authentisierende Mechanismen geschützt werden. Weitere steuernde oder regelnde Eingriffe in die Einrichtungen der Supporttechnik durch Dritte (externe Dienstleister) sollte nicht in Erwägung gezogen werden.

2.12 Rechenzentrumssicherheit

Rechenzentrumssicherheit ist mit Praktiken und Vorkehrungen verbunden, die ein Rechenzentrum vor Bedrohungen, Angriffen und nicht autorisierten Zugriffen schützen. Zu den wichtigsten Komponenten der Rechenzentrumssicherheit gehören physische Sicherheit und Netzwerksicherheit. Ein Rechenzentrum ist ein zentraler Cluster von Computing- und Networking-Geräten, auf denen die geschäftskritischen Informationen eines Unternehmens, von Bildungseinrichtungen oder Behörden an einem physischen Standort gespeichert und verarbeitet werden. Unternehmen, Bildungseinrichtungen oder Behörden müssen sowohl physische als auch virtuelle Sicherheitsmaßnahmen zum Schutz ihres Rechenzentrums ergreifen. Netzwerksicherheit ist ein weiterer Aspekt beim Schutz von Rechenzentren, da Malware und andere Bedrohungen das Rechenzentrum über das Netzwerk erreichen können.

Schutz von Rechenzentren

Rechenzentren verwalten Informationen, Anwendungen und Services, die für den täglichen Geschäftsbetrieb unabdingbar sind. Unternehmen, Bildungseinrichtungen und Behörden müssen daher die von ihnen verwendeten Rechenzentren durch geeignete Sicherheitsmaßnahmen schützen. Ohne wirksame Rechenzentrumssicherheit können Datenlecks auftreten, bei denen sensible Daten oder noch schlimmer: Kundendaten offengelegt oder gestohlen werden. Datenlecks dieser Art können hohe Verluste verursachen, sowohl finanzieller Natur als in Form von Rufschädigung und Imageverlust. Durch geeignete Sicherheitspraktiken, Sensibilitätskampagnen und entsprechende Schulungen der Anwender kann verhindert werden, dass autorisierte Personen unabsichtlich Informationen offenlegen (Social Engineering), mit denen nicht autorisierte Personen Sicherheitsmechanismen umgehen können.

Physische Sicherheit

Die Maßnahmen zur Aufrechterhaltung der physischen Sicherheit eines Rechenzentrums hängen von dessen Größe ab. In Rechenzentren sind häufig viele IT-Geräte vorhanden, wie z.B. Server, Switches, Router, Infrastruktur für Strom und Kühlung sowie Telekommunikationsgeräte. Diese Ausrüstung kann sich in Schränken befinden, die einfach mit einem physischen Sperrschloss gesichert werden, oder in einem Lager, für das zusätzliche physische Sicherheitsmaßnahmen erforderlich sind (z.B. Zugangsausweis, Videoüberwachung, Alarmsysteme, Sicherheitspersonal). Der Brandschutz ist ein weiterer Aspekt der physischen Sicherheit. Da sich in Rechenzentren feuchtigkeitsempfindliche elektronische Geräte befinden, sind Löschanlagen mit chemischen Löschmitteln oder Löschgasen besser zur Brandbekämpfung geeignet als Sprinkleranlagen.

Virtuelle Sicherheit

Virtualisierungstechnologie wird heute in vielen Rechenzentren zur Abstrahierung von Servern, Netzwerken und Storages (Datenspeicher) des Rechenzentrums eingesetzt. Dank dieser Abstrahierung können IT-Administratoren die Rechenzentrumsservices remote (aus der Ferne) verwalten, Abläufe im Rechenzentrum mithilfe von Software steuern und Workloads (Arbeitsaufkommen, Arbeitsaufwand) unmittelbar, serverübergreifend und bedarfsgerecht bereitstellen. Manche Rechenzentren setzen die Virtualisierungstechnologie ein, um auf die Public Cloud (Rechen- und Speicherplattform im Internet) zuzugreifen und sie als Teil ihrer Rechenzentrumsinfrastruktur zu nutzen. Der Einsatz von Software oder Cloud-Lösungen zum Strukturieren und Verwalten des Rechenzentrums führt zwar zu flexibleren Abläufen, erhöht jedoch die Anfälligkeit des Rechenzentrums gegenüber Cyber-Angriffen.

2.13 Personal für einen reibungslosen Betrieb des Rechenzentrums

Auch wenn die meisten Rechenzentren mittlerweile stark automatisiert laufen, ist menschliches Personal unabdingbar. Die Server, das Netzwerk und die gesamte Infrastruktur müssen rund um die Uhr überwacht werden, denn nur so können Ausfälle verhindert bzw. zeitnah behoben werden, wenn Probleme auftreten. Die Aufgaben des Rechenzentrum-Personals sind in die Bereiche Systemtechnik und -verwaltung eingeteilt:

- **Systemtechnik:** Die Systemtechnik kümmert sich um alle elektrotechnischen Aufgaben in einem Rechenzentrum. Dazu zählen die Installation der Geräte, der Austausch oder die Reparatur von defekter Hardware, sowie die Verkabelung der einzelnen Komponenten.
- **Systemverwaltung:** Die Systemverwaltung kümmert sich um die serverseitige Konfiguration der Systeme und überwacht deren Betrieb. Zusätzlich ist sie für die Datensicherheit und den Datenschutz im Rechenzentrum verantwortlich.



2.14 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für Rechenzentren von besonderer Bedeutung.

Fehlerhafte Planung

Wenn ein Rechenzentrum konzipiert und dabei nicht berücksichtigt wird, es gegen elementare Gefährdungen abzusichern, besteht ein sehr hohes Ausfallrisiko. So können z.B. Standortrisiken wie Luftverkehr, Erdbeben, möglicher Starkregen (Niederschlagsmenge von mehr als 25 l/m² in einer Stunde oder mehr als 35 l/m² in sechs Stunden) oder Hochwasser die Betriebssicherheit und Verfügbarkeit gefährden. Ebenso massiv kann es sich auf den Betrieb eines Rechenzentrums auswirken, wenn durch eine fehlerhafte Konzeptionierung nicht genügend Bandbreite verfügbar ist oder die Energieversorgung am gewählten Standort nicht ausreicht.

Fehlende oder fehlerhafte Zutrittskontrollen

Fehlen Zutrittskontrollen oder sind diese unzureichend, erhöht sich die Gefahr, dass unberechtigte Personen das Rechenzentrum betreten und dort fahrlässig, z.B. aufgrund mangelnder Fachkenntnisse oder vorsätzlich Schaden anrichten. Angreifer können so z.B. schützenswerte Daten entwenden, Geräte stehlen oder Server manipulieren. Unzureichende Zutrittskontrollen wirken sich somit auf die Verfügbarkeit, Vertraulichkeit und die Integrität von Daten und IT-Komponenten aus.

Unzureichende Überwachung

Wird die im Rechenzentrum betriebene IT und Infrastruktur unzureichend überwacht und betreut, können Komponenten unbemerkt ausfallen. Dadurch wird eventuell die Verfügbarkeit und fehlerfreie Funktion des Rechenzentrums stark beeinträchtigt.

Ausfälle treten zudem oftmals schleichend ein. Ohne eine aktive Überwachung könnten diese zu spät bemerkt werden. Es ist dann oft nicht mehr möglich, rechtzeitig zu reagieren.

Unzureichende Klimatisierung im Rechenzentrum

IT-Komponenten benötigen bestimmte Betriebsbedingungen, um zuverlässig zu funktionieren. Auch setzen sie die von ihnen aufgenommene elektrische Leistung in zusätzliche Wärme um. Wenn in einem IT-Betriebsbereich die Temperatur, die Luftfeuchte oder der Schwebestoffanteil nicht innerhalb der von den Geräteherstellern vorgegebenen Grenzwerte gehalten werden, kann dies dazu führen, dass technische Komponenten nicht mehr richtig funktionieren oder ausfallen.

Feuer

Feuer ist zwar eine Gefahr, die eher selten eintritt. Entsteht aber tatsächlich ein Brand, hat dieser meist schwerwiegende Auswirkungen. Denn durch Feuer und Rauch können große Schäden entstehen. Während innerhalb des IT-Betriebsbereichs Elektrobrände die häufigste Ursache für Feuer sind, kann ein Feuer außerhalb des IT-Betriebsbereichs und insbesondere in Supportbereichen, wie der Energieversorgung (inklusive NEA - Netzersatzanlage und USV - unterbrechungsfreie Stromversorgung) oder der Klimaanlage, zahlreiche weitere Ursachen haben. Haben der IT-Betriebsbereich oder die Supportbereiche sowie andere Nachbarbereiche keinen oder nur einen unzureichenden Brandschutz, kann sich ein Feuer schnell ausbreiten und auf das Rechenzentrum übergreifen.

Wasser

Durch undichte Wasserleitungen, Starkregen, Fallrohre für

Rechenzentren - Konzeption, Aufbau und Security 20/35

Regenwasser, Hochwasser, Rohrbruch, defekte Sprinkler- oder Klimaanlage kann Wasser in das Rechenzentrum eindringen. Hierdurch können Geräte beschädigt werden und nicht mehr funktionieren. Es kann auch ein Kurzschluss ausgelöst werden, durch den einzelne Bereiche des Rechenzentrums ausfallen oder ein Brand könnte entstehen.

In nahezu allen Fällen werden Kabel, über die ein Rechenzentrum mit der Außenwelt verbunden ist, unterirdisch an das Rechenzentrum herangeführt und enden dort meist in speziell dafür vorgesehenen Räumen. Erfolgt die Gebäudeeinführung mittels vergossener Wanddurchführungen, reicht deren Dichtigkeit meist aus, um das Eindringen von Wasser zu verhindern oder auf ein beherrschbares Maß zu reduzieren. Leerohre für Kabel sind gegen das Eindringen von Wasser abzudichten.

Um das Risiko zu reduzieren, dass Regen- oder Grundwasser von außen durch Wände, Decke oder Bodenplatte in das Rechenzentrum eindringt, sollten IT-Betriebsbereiche und technische Einrichtungen der Supportbereiche weder unmittelbar unter einem Dach (Flachdach) noch unterhalb des umgebenden Oberflächenniveaus (Keller, Erdgeschoss) angeordnet werden. Ist eine solche Anordnung unvermeidbar, sind bauliche Maßnahmen umzusetzen, die das Eindringen von Wasser durch das Dach sowie durch die Außenwände weitestgehend ausschließen.

Hinweis: Sofern schützenswerte Einrichtungen eines Rechenzentrums unterhalb der Rückstauenebene (höchste Ebene, bis zu der das Wasser in einer Entwässerungs- oder Abwasseranlage ansteigen kann) verbaut sind, muss auch das Abwassersystem mit geeigneten Rückstau-Schutzeinrichtungen

(Rückstauschleife mittels eines Rohrbogens, Rückstauklappe) ausgerüstet werden.

Fehlender oder unzureichender Einbruchschutz

Selbst wenn eine gut funktionierende Zutrittskontrolle eingerichtet ist, können unbefugte Personen in ein Rechenzentrum eindringen, sofern es nicht ausreichend vor Einbrüchen geschützt wird. Täter könnten so z.B. IT-Komponenten stehlen oder manipulieren und an vertrauliche Informationen gelangen. Auch könnten sie die Geräte zerstören oder das Rechenzentrum insgesamt beschädigen.

Die Meldungen einer vorhandenen Einbruchmeldeanlage (EMA) sind mindestens auf die Alarmempfangsstelle des Haussicherheitsdienstes aufzuschalten. Die Zentrale des Haussicherheitsdienstes muss nicht unmittelbar am Standort des Rechenzentrums selbst angesiedelt sein. Die Reaktionszeit sowie die Reaktionsmöglichkeiten am jeweiligen Standort des Rechenzentrums dürfen durch die Distanz zwischen der Zentrale des Haussicherheitsdienstes und dem Standort des Rechenzentrums nicht nachteilig beeinflusst werden.

Hinweis: Der aktuelle Stand der Technik im Kontext der Drohnenabwehr bietet zahlreiche Möglichkeiten der Drohnenerkennung und des passiven Drohnenschutzes (Sichtschutz).

Ausfall der Stromversorgung

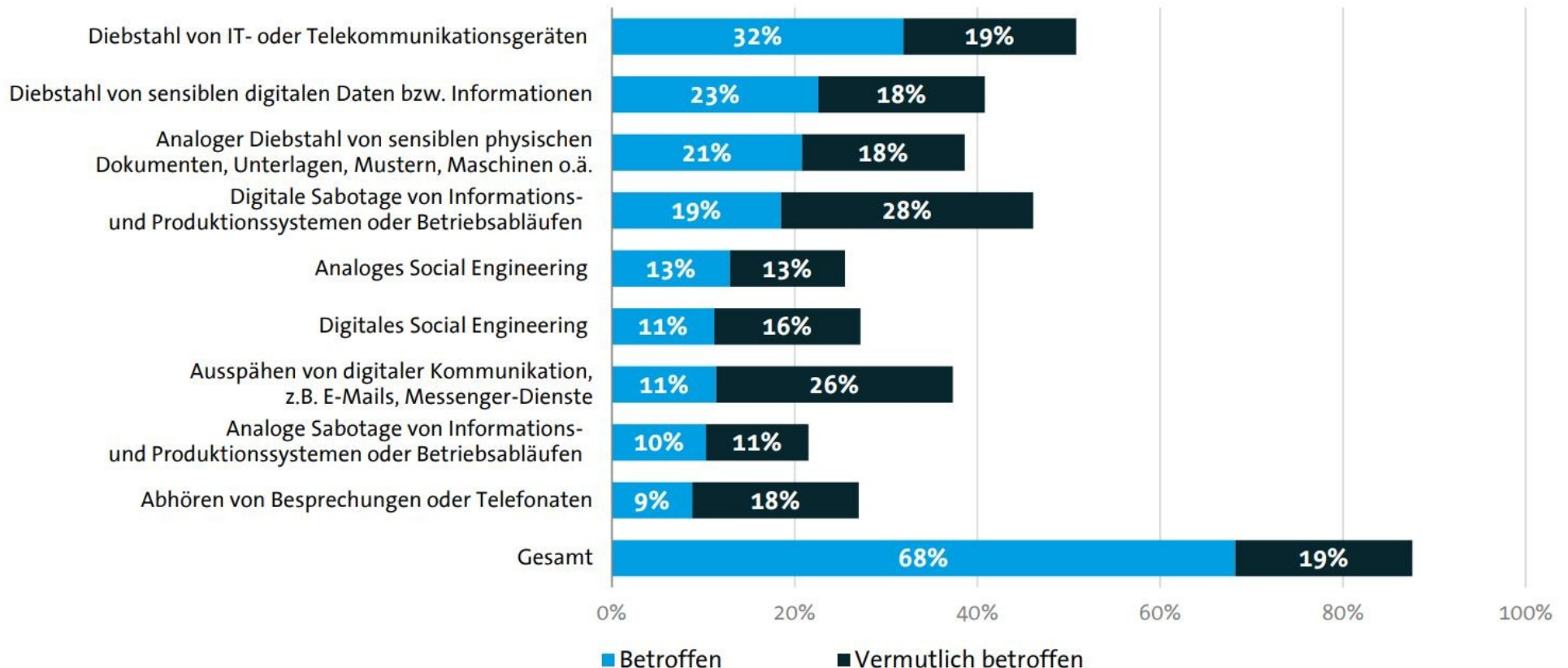
Wenn der Strom ausfällt, kann der Betriebsablauf eines Rechenzentrums und damit der Institution erheblich gestört werden. So sind bei einem Stromausfall eventuell die vom Rechenzentrum bereitgestellten IT-Services plötzlich nicht mehr erreichbar. Ebenso

können Daten verloren gehen. Zudem ist es möglich, dass durch einen plötzlichen Stromausfall IT-Systeme, TK-Systeme (technische Komponenten, Support-Einrichtungen, technische Gebäudeausrüstung) oder Überwachungstechnik beschädigt werden.

Verschmutzung

Staub und andere Verschmutzungen in einem Rechenzentrum können dazu führen, dass technische Komponenten (z. B. Lüfter) nicht mehr funktionieren. Durch Verschmutzungen verschleifen Geräte früher und fallen häufiger aus.

IT-Vorfälle in Niedersachsen



3. Anforderungen an die Planung von Rechenzentren (RZ)

Eine ganzheitliche Betrachtung der Anforderungen an ein neues Rechenzentrum ermöglicht es, alle Rahmenbedingungen und Einflussfaktoren rechtzeitig zu berücksichtigen. Es muss bei der Planung von Rechenzentren auch die Reserven, Erweiterungen oder modular erweiterbare Lösungsansätze mit berücksichtigt werden.

3.1 Basis-Anforderungen

Für ein Rechenzentrum müssen angemessene technische und organisatorische Vorgaben definiert und umgesetzt werden. Wenn ein Rechenzentrum geplant wird oder geeignete Räumlichkeiten ausgewählt werden, müssen auch geeignete Sicherheitsmaßnahmen unter Berücksichtigung des Schutzbedarfs der IT-Komponenten (insbesondere der Verfügbarkeit) mit geplant werden. Ein Rechenzentrum muss insgesamt als geschlossener Sicherheitsbereich konzipiert werden. Das Rechenzentrum muss zudem unterschiedliche Sicherheitszonen aufweisen. Dafür müssen z.B. Verwaltungs-, Logistik-, IT-Betriebs- und Support-Bereiche klar voneinander getrennt werden. Im Falle der Planung nur eines Serverraums (kein Rechenzentrum) sollte zumindest geprüft werden, ob unterschiedliche Sicherheitszonen eingerichtet werden können.

Hinweis: Bevor mit der eigentlichen Konzeption und Planung eines Rechenzentrums begonnen wird, muss zuerst ein geeigneter Standort zur Verfügung stehen oder gesucht werden.

3.1.1 Grundlage der Planung

Die Grundlage eines jeden IT-Projektes ist die klare Definition der

benötigten IT-Services in Qualität und Quantität. Das ist einfacher gesagt als getan, da die Anforderungen der Bereiche so vielfältig und unterschiedlich sind, wie die Wünsche der Benutzer des Rechenzentrums.

Von einem Rechenzentrum erwarten die Benutzer immer, dass es 24*7*365 Tage im Jahr unterbrechungsfrei zur Verfügung steht: sowohl konstant performante Anwendungen, als auch konstant sicher und unverfälscht Daten zur Verfügung stellt. Je qualifizierter und anspruchsvoller die Service Level (Dienstleistungsqualität, Servicequalität) sind, desto höher sind die Anforderungen an die Verfügbarkeit und den Schutzbedarf des Rechenzentrums. Die daraus geforderte und abgeleitete Redundanz der RZ-Architektur bestimmt die Baukosten und die jährlichen Betriebskosten sowie die zukünftigen Reinvestitionen. Bei der Definition der Service Level spielen natürlich neben den Bereitstellungszeiten, Sicherheitsaspekten, Backup-Strategien und -fenster, auch die geforderten Verfügbarkeiten zu dem unterschiedlichen Tages- und Wochenzeiten, Reaktionszeiten und benötigten Wartungsfenster eine Rolle.

Ein besonderes Augenmerk bei einem neuen Projekt, sollte auf die Dokumentation liegen. Für ein solches Projekt stellt es sich recht einfach dar: Was nicht dokumentiert ist, kann nicht richtig genutzt, gewartet, geprüft und abgenommen werden. Sicherlich sind Dokumentation und Reflektion zum Ende eines Projektes immer ein ungeliebtes Kind, aber es macht den RZ-Betrieb einfacher und sicherer.

Zu einer ganzheitlichen Lösung gehört es auch, dass ein

Betriebskonzept des neuen Rechenzentrums erstellt wird. So ist der Betreiber des Rechenzentrums in der Lage, schnell und sicher auf jede Betriebsstörung zu reagieren, auch wenn dieses nicht zum tagtäglichen Aufgabengebiet gehört. Der Abschluss des Projektes wird durch die Erstellung eines Notfallkonzepts abgerundet. So ist der IT-Betrieb auf Notfälle, Krisen oder Katastrophen stets organisatorisch gut vorbereitet. Fehler kann man nicht vermeiden, Krisen und Naturkatastrophen nicht verhindern. Aber die Konzepte versetzen den IT-Betreiber in die Lage, schnell, sicher und professionell auf viele Eventualitäten reagieren zu können.

Hinweis: Für alle Gewerke der Energieversorgung, technischen Gebäudeausrüstung (TGA) sowie der Kühlungs- und Lüftungsanlagen ist ein einheitliches und durchgängiges Bezeichnungssystem aufzubauen und dauerhaft einzuhalten. Innerhalb eindeutig bezeichneter und dadurch von anderen sicher unterscheidbaren Verteilungen, Schaltschränken, usw. darf es jede Bezeichnung nur ein einziges Mal geben. Auch für Elemente wie Pumpen, Melder usw. darf jede Bezeichnung nur ein einziges Mal vergeben werden.

3.1.1 Bildung von Brandabschnitten

Es müssen geeignete Brand- und Rauchabschnitte für die Räumlichkeiten eines Rechenzentrums festgelegt werden. Die Brand- und Rauchabschnitte müssen über den baurechtlich vorgeschriebenen Rahmen hinaus auch Schutz für die darin befindlichen technischen Einrichtungen und deren Verfügbarkeit bieten. Es muss verhindert werden, dass sich Brand und Rauch ausbreiten.

3.1.3 Energieversorgung von Rechenzentren (RZ)

Bei den Planungen der Energieversorgung sind hinsichtlich der

Dimensionierung aller Komponenten einige Kriterien unbedingt zu berücksichtigen:

- Im normalen Dauerbetrieb darf die Auslastung der Energieversorgung bei maximal 85 % der verfügbaren Anschlussleistung liegen.
- Bei betriebsüblichen Spitzenlasten darf die Auslastung der Energieversorgung bei maximal 95 % der verfügbaren Leistung liegen.
- Es sind Reserven bereitzustellen (dauerhaft oder individuell zuschaltbar), die auch für besondere Betriebszustände, z.B. Ausfall der regulären Energieversorgung, die Einhaltung der vorgenannten Grenzwerte sicherstellen.

Hinweis: Die Einspeisung aus dem Stromverteilnetz in ein Hochverfügbarkeits-Rechenzentrum (HV-RZ) soll aus einer möglichst hohen Hierarchiestufe des Verteilnetzes heraus erfolgen und darf ab diesem Punkt keine anderen Kunden versorgen.

3.1.2 Einsatz einer unterbrechungsfreien Stromversorgung (USV)

Für alle betriebsrelevanten Komponenten des Rechenzentrums muss eine unterbrechungsfreie Stromversorgung (USV) installiert werden. Da der Leistungsbedarf von Klimaanlage oft zu hoch für eine USV ist, muss mindestens die Steuerung der Anlagen an die unterbrechungsfreie Stromversorgung angeschlossen werden. Im Falle eines Serverraums sollte je nach Verfügbarkeitsanforderungen der IT-Systeme geprüft werden, ob der Betrieb einer USV notwendig ist. Die USV muss ausreichend dimensioniert sein. Bei relevanten Änderungen an den Verbrauchern muss überprüft werden, ob die vorhandenen USV-Systeme noch ausreichend dimensioniert sind. Bei USV-Systemen mit Batterie als

Energiespeicher muss die Batterie im erforderlichen Temperaturbereich gehalten werden. Sie sollte dazu vorzugsweise räumlich getrennt von der Leistungselektronik der USV platziert werden. Die USV muss regelmäßig gewartet und auf Funktionsfähigkeit getestet werden. Dafür müssen die vom Hersteller vorgesehenen Wartungsintervalle eingehalten werden.

3.1.3 Notabschaltung der Stromversorgung

Es muss geeignete Möglichkeiten geben, elektrische Verbraucher im Rechenzentrum spannungsfrei zu schalten. Dabei muss darauf geachtet werden, ob und wie eine vorhandene USV räumlich und funktional in die Stromversorgung eingebunden ist. Werden klassische Not-Aus-Schalter eingesetzt, muss darauf geachtet werden, dass darüber nicht das komplette Rechenzentrum abgeschaltet wird. Die Notabschaltung muss sinnvoll parzelliert (in sinnvolle Teilbereiche unterteilen) und zielgerichtet erfolgen. Alle Not-Aus-Schalter müssen so geschützt sein, dass sie nicht unbeabsichtigt oder unbefugt betätigt werden können.

3.1.4 Einhaltung der Lufttemperatur und -feuchtigkeit

Es muss sichergestellt werden, dass die Lufttemperatur und Luftfeuchtigkeit im IT-Betriebsbereich innerhalb der vorgeschriebenen Grenzwerte liegen. Die tatsächliche Wärmelast in den gekühlten Bereichen muss in regelmäßigen Abständen und nach größeren Umbauten überprüft werden. Eine vorhandene Klimatisierung muss regelmäßig gewartet werden. Die Parameter Temperatur und Feuchtigkeit müssen mindestens so aufgezeichnet werden, dass sich rückwirkend erkennen lässt, ob Grenzwerte überschritten wurden und dass sie bei der Lokalisierung der Ursache der Abweichung sowie bei der Beseitigung der Ursache unterstützend genutzt werden können.

3.1.5 Zutrittskontrolle

Der Zutritt zum Rechenzentrum muss kontrolliert werden. Die Zutrittskontrolle dient dem Schutz der Vertraulichkeit und der Integrität der im Rechenzentrum (RZ) vorhandenen Informationen. Die Zutrittsrechte müssen nach festgelegten Vorgaben vergeben werden. Für im Rechenzentrum tätige Personen muss sichergestellt werden, dass diese keinen Zutritt zu IT-Systemen außerhalb ihres Tätigkeitsbereiches erhalten. Alle Zutrittsmöglichkeiten zum Rechenzentrum müssen mit Zutrittskontrolleinrichtungen ausgestattet sein. Jeder Zutritt zum Rechenzentrum muss von der Zutrittskontrolle individuell erfasst werden. Es muss regelmäßig kontrolliert werden, ob die Regelungen zum Einsatz einer Zutrittskontrolle eingehalten werden. Die Anforderungen der Institution an ein Zutrittskontrollsystem müssen in einem Konzept ausreichend detailliert dokumentiert werden.

Hinweis: Unbefugte sind nicht nur externe Personen, auch Mitarbeiter eines hochverfügbaren Rechenzentrums (HV-RZ) oder im Rahmen entsprechender Vereinbarungen gleichgestellte Mitarbeiter externer Firmen sind in Bereichen, für die sie nicht ausdrücklich im Rahmen der Erfordernisse ihrer Arbeit ein Zutrittsrecht haben, als Unbefugte zu betrachten.

3.1.6 Verschließen und Sichern

Alle Türen des Rechenzentrums müssen stets verschlossen gehalten werden. Fenster müssen möglichst schon bei der Planung vermieden werden. Falls sie doch vorhanden sind, müssen sie ebenso wie die Türen stets verschlossen gehalten werden. Türen und Fenster müssen einen dem Sicherheitsniveau angemessenen Schutz gegen Angriffe und Umgebungseinflüsse bieten. Sie müssen mit einem Sichtschutz versehen sein. Dabei muss beachtet werden,

dass die bauliche Ausführung aller raumbildenden Elemente in Bezug auf die erforderliche Schutzwirkung gleichwertig sein muss.

3.1.7 Einsatz einer Brandmeldeanlage

In einem Rechenzentrum muss eine Brandmeldeanlage installiert sein. Diese muss alle Flächen überwachen. Alle Meldungen der Brandmeldeanlage müssen geeignet weitergeleitet werden. Die Brandmeldeanlage muss regelmäßig gewartet werden. Es muss sichergestellt werden, dass in Räumen des Rechenzentrums keine besonderen Brandlasten vorhanden sind.

3.1.8 Einsatz einer Lösch- oder Brandvermeidungsanlage

In einem Rechenzentrum muss eine Lösch- oder Brandvermeidungsanlage nach aktuellem Stand der Technik installiert sein. Ist dies nicht möglich, muss durch technische (insbesondere durch eine flächendeckende Brandfrüherkennung) und organisatorische Maßnahmen (geschultes Personal und Reaktionspläne für Meldungen der Brandfrüherkennung) sichergestellt sein, dass unmittelbar, innerhalb von maximal 3 Minuten auf Meldungen der Brandfrüherkennung reagiert wird. Es muss beachtet werden, dass darüber hinausgehende baurechtliche Anforderungen hinsichtlich der Ausstattung mit Handfeuerlöschern davon unberührt bleiben. Die Feuerlöscher müssen so angebracht werden, dass sie im Brandfall leicht zu erreichen sind. Jeder Feuerlöscher muss regelmäßig geprüft und gewartet werden. Alle Mitarbeiter, die ein Rechenzentrum betreten dürfen, müssen in die Benutzung der Handfeuerlöscher eingewiesen werden.

3.1.11 Inspektion und Wartung der Infrastruktur

Für alle Komponenten der baulich-technischen Infrastruktur müssen mindestens die vom Hersteller empfohlenen oder durch

Normen festgelegten Intervalle und Vorschriften für Inspektion und Wartung eingehalten werden. Inspektionen und Wartungsarbeiten müssen protokolliert werden. Brandschotten müssen daraufhin geprüft werden, ob sie unversehrt sind. Die Ergebnisse müssen dokumentiert werden.

3.1.9 Automatische Überwachung der Infrastruktur

Alle Einrichtungen der Infrastruktur, wie z. B. Leckageüberwachung, Klima-, Strom- und USV-Anlagen, müssen automatisch überwacht werden. Erkannte Störungen müssen schnellstmöglich in geeigneter Weise weitergeleitet und bearbeitet werden.

3.1.10 Einsatz einer Brandfrüherkennung

Ein Rechenzentrum muss mit einer Brandfrüherkennungsanlage ausgestattet werden. Die Meldungen der Brandfrüherkennung müssen an eine ständig besetzte Stelle geleitet werden, die eine Kontrolle und Schutzreaktion innerhalb von maximal 3 Minuten veranlassen kann. Alternativ muss eine automatische Schutzreaktion erfolgen. Um ein ausgewogenes Verhältnis zwischen Brandschutz und Verfügbarkeit zu erreichen, muss sichergestellt werden, dass sich einander Redundanz gebende Einrichtungen nicht gemeinsam im Wirkungsbereich der gleichen Spannungsfreischaltung befinden.

3.1.11 Vermeidung und Überwachung nicht erforderlicher Leitungen

In einem Rechenzentrum dürfen nur Leitungen verlegt werden, die der unmittelbaren Versorgung der im Rechenzentrum aufgebauten Technik (in der Regel IT- und gegebenenfalls Kühltechnik) dienen. Ist es aus baulichen Gründen unabwendbar, Leitungen durch das Rechenzentrum zu führen, um andere Bereiche als die des Rechenzentrums zu versorgen, muss dies einschließlich

Begründung dokumentiert werden. Die Risiken, die von solchen Leitungen ausgehen, müssen durch geeignete Maßnahmen minimiert werden, z.B. durch Einhausung und Überwachung. Meldungen aus der Überwachung der Leitungen müssen unverzüglich hinsichtlich der Gefährdungsrelevanz geprüft und bewertet werden. Gegenmaßnahmen müssen entsprechend der erkannten Gefährdungsrelevanz zeitgerecht umgesetzt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik und sie sollten grundsätzlich erfüllt werden.

3.2.1 Perimeterschutz für das Rechenzentrum

Für Rechenzentren sollte ein Perimeterschutz (Freigeländeüberwachung) existieren. Je nach festgelegtem Schutzbedarf für das Rechenzentrum und abhängig vom Gelände sollte der Perimeterschutz aus folgenden Komponenten bestehen:

- äußere Umschließung oder Umfriedung,
- Sicherungsmaßnahmen gegen unbeabsichtigtes Überschreiten einer Grundstücksgrenze,
- Sicherungsmaßnahmen gegen beabsichtigtes gewaltloses Überwinden der Grundstücksgrenze,
- Sicherungsmaßnahmen gegen beabsichtigtes gewaltsames Überwinden der Grundstücksgrenze,
- Freiland-Sicherungsmaßnahmen,
- äußere Personen- und Fahrzeugdetektion,
- Maßnahmen zur Beweissicherung (z.B. Videoaufzeichnung),
- Zuluftöffnungen und andere Öffnungen sind gegen Sabotage-Angriffe zu schützen, sowie eine
- automatische Alarmierung.

3.2.2 Planung und Installation von Gefahrenmeldeanlagen (GMA)

Basierend auf dem Sicherheitskonzept des Gebäudes sollte geplant werden, welche Gefahrenmeldeanlagen für welche Bereiche des Rechenzentrums benötigt und installiert werden. Hierüber hinaus sollte festgelegt werden, wie mit Alarmmeldungen umzugehen ist. Das Konzept sollte immer angepasst werden, wenn sich die Nutzung der Gebäudebereiche verändert. Es sollte eine zum jeweiligen Einsatzzweck passende Gefahrenmeldeanlage (GMA) installiert werden. Die Meldungen der GMA sollten unter Beachtung der dafür geltenden Technischen Anschlussbedingungen (TAB) auf eine Alarmempfangsstelle aufgeschaltet werden. Die ausgewählte Alarmempfangsstelle muss jederzeit erreichbar sein. Sie muss technisch sowie personell in der Lage sein, geeignet auf die gemeldete Gefährdung zu reagieren. Der Übertragungsweg zwischen eingesetzter GMA und Alarmempfangsstelle sollte entsprechend den TAB und nach Möglichkeit redundant ausgelegt werden. Alle vorhandenen Übertragungswege müssen regelmäßig getestet werden.

3.2.3 Einsatz einer Netzersatzanlage (NEA)

Die Energieversorgung eines Rechenzentrums aus dem Netz eines Energieversorgungsunternehmens sollte um eine Netzersatzanlage (NEA) ergänzt werden. Wird eine NEA verwendet, muss sie regelmäßig gewartet werden. Bei diesen Wartungen müssen auch Belastungs- und Funktionstests sowie Testläufe unter Last durchgeführt werden. Der Betriebsmittelvorrat (Treibstoff) einer NEA muss regelmäßig daraufhin überprüft werden, ob er ausreichend ist. Außerdem muss regelmäßig kontrolliert werden, ob die Vorräte noch verwendbar sind, vor allem um die sogenannte Dieselpest zu vermeiden. Nach Möglichkeit sollte statt Diesel-Kraftstoff schwefelarmes Heizöl verwendet werden. Die Tankvorgänge von

Brennstoffen müssen protokolliert werden. Aus dem Protokoll muss die Art des Brennstoffs, die genutzten Additive, das Tankdatum und die getankte Menge hervorgehen.

3.2.4 Blitz- und Überspannungsschutzeinrichtung

Es sollte auf Basis der aktuell gültigen Norm ein Blitz- und Überspannungsschutzkonzept erstellt werden. Dabei sind die für den ordnungsgemäßen Betrieb des Rechenzentrums (RZ) erforderlichen Blitzschutz zonen festzulegen. Alle Einrichtungen des Blitz- und Überspannungsschutzes sollten ein Mal im Jahr einer umfassenden Prüfung unterzogen werden. Die Ergebnisse der Prüfung sind zu dokumentieren. Festgestellte Mängel sind innerhalb von wenigen Werktagen zu beheben. Die ordnungsgemäße Mängelbeseitigung ist durch eine erneute Prüfung der betroffenen Bereiche nachzuweisen.

Hinweis: Außenanlagen mit galvanisch leitenden Verbindungen in das Innere eines Gebäudes dürfen nicht mit der Blitz-Fangeinrichtung verbunden werden. Ziel dieser Maßnahmen ist es zu verhindern, dass bei einem Blitzeinschlag in die Fangeinrichtung des Gebäudes Blitzteilströme in das Gebäude geleitet werden, die dort Schäden verursachen können.

3.2.5 Klimatisierung im Rechenzentrum

Es sollte sichergestellt werden, dass im Rechenzentrum geeignete klimatische Bedingungen geschaffen und aufrechterhalten werden. Die Klimatisierung sollte für das Rechenzentrum ausreichend dimensioniert sein. Alle relevanten Werte (Temperatur, Feuchte, Schwebstoffgehalt und Frischluftanteil) sollten ständig überwacht werden. Weicht ein Wert von der Norm ab, sollte automatisch eine Alarmmeldung weitergeleitet werden. Die Klimaanlage sollten in IT-Betriebsbereichen möglichst ausfallsicher sein.

3.2.6 Durchführung von Funktionstests der technischen Infrastruktur

Die technische Infrastruktur eines Rechenzentrums sollte regelmäßig (zumindest ein- bis zweimal jährlich) sowie nach Systemumbauten und umfangreichen Reparaturen getestet werden. Die Ergebnisse sollten dokumentiert werden. Besonders ganze Reaktionsketten sollten einem echten Funktionstest unterzogen werden.

3.2.7 Anlagen zur Löschung oder Vermeidung von Bränden

Ein Rechenzentrum sollte mit einer automatischen Lösch- oder Brandvermeidungsanlage ausgestattet werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für ein Rechenzentrum exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

3.3.1 Ausweichrechenzentrum

Es sollte ein geografisch separiertes Ausweichrechenzentrum aufgebaut werden. Das Ausweichrechenzentrum sollte so dimensioniert sein, dass alle Prozesse der Institution aufrechterhalten werden können. Auch sollte es ständig einsatzbereit sein. Alle Daten der Institution sollten regelmäßig ins Ausweichrechenzentrum gespiegelt werden. Der Schwenk auf das Notfallrechenzentrum sollte regelmäßig getestet und geübt werden. Die Übertragungswege in das Ausweichrechenzentrum sollten geeignet abgesichert und entsprechend redundant ausgelegt sein.

3.3.2 Durchführung von Staubschutzmaßnahmen

Bei Baumaßnahmen in einem Rechenzentrum sollten geeignete Staubschutzmaßnahmen definiert, geplant und umgesetzt werden. Personen, die selbst nicht an den Baumaßnahmen beteiligt sind, sollten in ausreichend engen Zeitabständen kontrollieren, ob die Staubschutzmaßnahmen ordnungsgemäß funktionieren und die Regelungen zum Staubschutz eingehalten werden.

3.3.3 Zweckmäßiger Aufbau der Verkabelung im Rechenzentrum

Kabeltrassen in Rechenzentren sollten sehr sorgfältig geplant und ausgeführt werden. Trassen sollten hinsichtlich Anordnung und Dimensionierung so ausgelegt sein, dass eine Trennung der Spannungsebenen sowie eine sinnvolle Verteilung von Kabeln auf den Trassen möglich ist und dass auch für zukünftige Bedarfsmehrung ausreichend Platz zur Verfügung steht. Zur optimalen Versorgung von IT-Hardware, die über zwei Netzteile verfügt, sollte ab der Niederspannungshauptverteilung für die IT-Betriebsbereiche eine zweizügige sogenannte A-B-Versorgung aufgebaut werden. Einander Redundanz gebende Leitungen sollten über getrennte Trassen verlegt werden.

3.3.4 Einsatz von Videoüberwachungsanlagen

Die Zutrittskontrolle und die Einbruchmeldung sollten durch Videoüberwachungsanlagen ergänzt werden. Eine Videoüberwachung sollte in das gesamte Sicherheitskonzept eingebettet werden. Bei der Planung, Konzeption und eventuellen Auswertung von Videoaufzeichnungen muss der Datenschutzbeauftragte immer mit einbezogen werden. Die für eine Videoüberwachung benötigten zentralen Technikkomponenten sollten in einer geeigneten Umgebung geschützt aufgestellt werden. Es sollte regelmäßig überprüft werden, ob die

Videoüberwachungsanlage korrekt funktioniert und ob die mit dem Datenschutzbeauftragten abgestimmten Blickwinkel eingehalten werden.

3.3.5 Redundante Auslegung von unterbrechungsfreien Stromversorgungen (USV)

USV-Systeme sollten modular und so aufgebaut sein, dass der Ausfall durch ein redundantes Modul unterbrechungsfrei kompensiert wird. Sofern für die IT-Betriebsbereiche eine zweizügige sogenannte A-B-Versorgung aufgebaut ist, sollte jeder der beiden Strompfade mit einem eigenständigen USV-System ausgestattet sein.

3.3.6 Redundante Auslegung von Netzersatzanlagen (NEA)

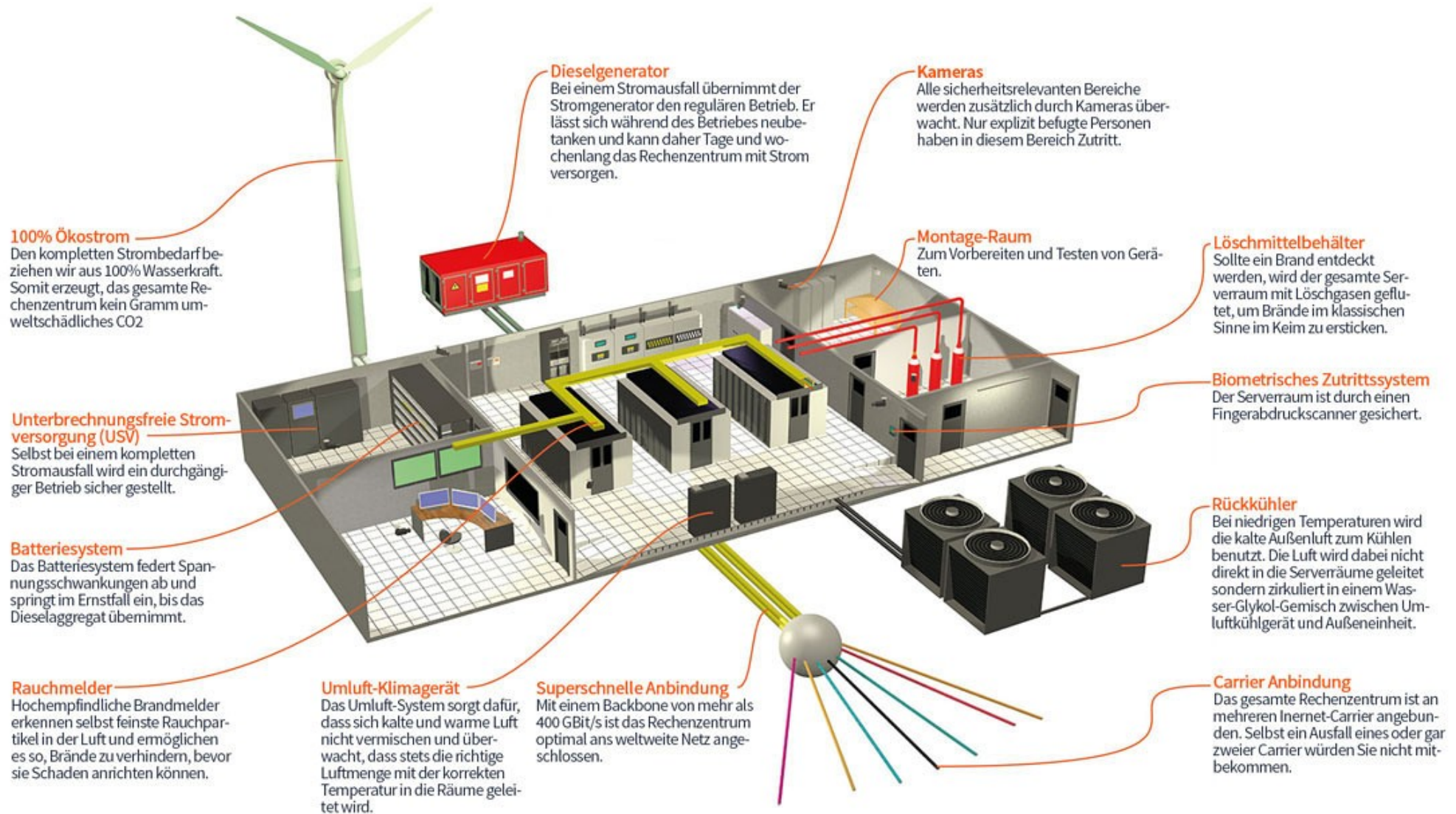
Netzersatzanlagen sollten redundant ausgelegt werden. Hinsichtlich der Wartung müssen auch redundante NEA entsprechend dem Stand der Technik und der aktuellen Normen behandelt werden.

3.3.7 Einsatz von höherwertigen Gefahrenmeldeanlagen

Für Rechenzentren mit erhöhtem Schutzbedarf sollten nur dafür geeignete Gefahrenmeldeanlagen eingesetzt werden.

3.3.8 Schutz gegen statische Aufladung

In allen Bereichen, in denen technische Einrichtungen vorhanden sind, von deren ordnungsgemäßer Funktion die Bereitstellung der Dienstleistungen eines Rechenzentrums (RZ) abhängig ist und die durch Spannungsschläge auf Grund statischer Aufladung beschädigt werden können, sind mindestens elektrostatisch ableitfähige Bodenbeläge zu verwenden, leitfähig zu verkleben und an das Erdungssystem anzuschließen. In allen anderen Bereichen sind mindestens antistatische Bodenbeläge zu verwenden.



4. Planung, Konzeption und Bau von schlüsselfertigen Rechenzentren (RZ)

Die Anforderungen an ein eigenes Rechenzentrum sind hoch: Dieses muss sicher, hochverfügbar und redundant ausgelegt sein. Zudem sind Klima- und Elektrokonzepte aufgrund hoher Wärmelasten optimal abzustimmen.

Studien kommen zu dem Ergebnis, dass bis 2030 mit einer Absenkung der CO₂-Emissionen von Rechenzentren um 30 Prozent zu rechnen ist. Grundlage für diese Entwicklung sind Virtualisierung, bessere Klima- und Abwärmekonzepte sowie energiesparende Technologien.

Auch sollten die technischen Geräte (Racks, Klimatisierung, ...) von einem oder von verschiedenen Herstellern kompatibel sein, d.h. die technische Anbindung, die Außenmaße und andere wesentliche Eigenschaften der Geräte müssen bereits während der Planung geprüft und gegebenenfalls in Absprache mit den Herstellern angepasst werden.

Basierend auf einer Risikoanalyse, sowie den technischen und rechtlichen Anforderungen, wird eine Detailplanung und Kostenschätzung erstellt.

- Gebäude- und Raumplanung
- Sicherheitskonzepte infolge von Wasser, Brand, etc.
- Datenspeicher- und Verarbeitungssysteme
- Raum-in-Raum-Konzepte
- Bautechnik und Elektrotechnik
- Klima- und Lüftungstechnik
- Technik für Nutzung von Abwärme
- Sicherheits- und Feuerlöschtechnik

4.1 Unterbrechungsfreie Stromversorgung (USV)

Die USV-Anlage kommt nur höchst selten zum Einsatz, gleichzeitig ist der Aufwand, die Batterien vorzuhalten, sehr hoch. Mittels Modernisierung, Batterie-Monitoring und gegebenenfalls einer Erweiterung kann die USV auch als Stromspeicher genutzt werden. Dazu wird bei Ungleichgewichten Strom aus dem öffentlichen Netz gespeichert und zu einem anderen Zeitpunkt wieder zurückgespeist oder im eigenen Unternehmen genutzt: Die ursprüngliche Backup-Funktion bleibt dabei natürlich erhalten.

4.2 Risiko- und Schwachstellenanalyse

Sicherheit hat Priorität! Mit einer umfassenden Risikoanalyse wird eine Entscheidungsplattform geschaffen, die die Grundlage für die Ausarbeitung von konkreten Konzepten und Handlungsalternativen bildet. Eine Risikoanalyse beinhaltet u.a.:

- Analyse von Anforderungen, Prozessen, IT-, TK- und Sicherheitsproblematiken (TK ... techn. Komponenten)
- Risiko-, Schwachstellen- und Netzwerkanalyse
- Rechtliche und wirtschaftliche Auswirkungen
- Energieversorgung und Klimatisierung
- Brandfrühsterkennung und Löschanlagen
- Zutrittskontrolle und Monitoring

4.3 Netzwerk-Verkabelung

Neben der Netzwerkanalyse und -design wird von dem ausführenden Unternehmen in der Regel auch die fachgerechte Verlegung und Installation der Kabelkanäle und Netzkabel für Kupfer und Lichtwellenleiter (Spleiß-Arbeiten aller Leitungs- und Kabelspezifikationen) im kompletten Gebäudekomplex ausgeführt.

Bei besonders hohen Anforderungen an die Ausfallsicherheit gilt es gegebenenfalls, bei Steckern auf höchste Qualität zu achten: Dazu gehört eine spezielle Oberflächenbehandlung, die dafür sorgt, dass Stecker schmutzabweisend und selbstreinigend sind, um Verbindungsprobleme auszuschließen.

- Strukturierte Verkabelungssysteme
- Backbone-Verkabelung über Lichtwellenleiter
- Singlemode- und Multimodefasern (Glasfaserkabel)
- Kupfer-Verkabelung bis zum Arbeitsplatz
- Abnahmemessungen für Kat. 6, Kat. 7, Kat.8 und Glasfaserkabel

Hinweis: Die Verlegung der Kabel und Leitungen ist lage- und tiefenrichtig zu dokumentieren. Die Dokumentation der Verlegung der Kabel und Leitungen ist bei der Planung und Durchführung von Erdarbeiten im Bereich solcher Kabel und Leitungen zu berücksichtigen.

4.4 Bau- und Projektmanagement

In jeder Phase des Projektes sollten immer Ansprechpartner zur Verfügung stehen. Das ausführende Unternehmen, das sämtliche Baumaßnahmen ausführt bzw. überwacht, übernimmt in der Regel die Bauleitung und die Überwachung der Fremdinstallationen. Nach Ausführung aller Arbeiten wird das Rechenzentrum schlüsselfertig an den Betreiber des Rechenzentrums übergeben.

- Server/Netzwerkschränke
- Klimatisierung und Löschanlagen
- Brandfrühsterkennung (z.B. Rauchdetektion sowie einer Gaslöschanlage über einen 3-stufigen Brandschutz)
- Zutrittskontrolle und Monitoring

- Stromversorgung und Stromverteilung
- Unterbrechungsfreie Stromversorgung (USV)
- Netzwerkverkabelungen
- WLAN-Infrastruktur

4.5 Brandschutztraining

Mit der zuständigen Feuerwehr kann man sogar den Ernstfall proben, indem bei einem simulierten Brandfall der Serverraum mit realen Löschgas (Stickstoff, Argon, CO₂) geflutet wird.

Nach dem abgeschlossenen Training des Betreibers mit der zuständigen Feuerwehr, sollte der Serverraum schnellstmöglich wieder begehbar gemacht werden. Dazu muss das Löschgas abgesaugt und der Luft-Sauerstoff sollte dem Serverraum anschließend wieder zugeführt werden.

Die gewonnenen Erkenntnisse einer erfolgreichen Übung sollten in die Dokumentation für den Notfall, sowie beim Neubau von anderen Rechenzentren mit einfließen.

4.6 Modernisierung von Datenverteilern

- Austausch von Verteilerschränken
- Neustrukturierung der Komponentenanzahl
- Säuberung von Verteilerschränken
- Dokumentation der passiven Infrastruktur
- Erstellung von Messprotokollen einer vorhandenen Netzwerkverkabelung
- usw.

4.7 Sichere Stromversorgung und USV

Ohne unterbrechungsfreie Stromversorgung (USV) ist kein Rechenzentrum denkbar. Sollte die Hauptstromversorgung ausfallen, greifen übergangsweise die Batterien der USV-Anlage bis Dieselgeneratoren die Stromversorgung übernehmen. Neue intelligente Konzepte rund um Batterien und Batterieraum verändern derzeit traditionelle Systeme: So werden moderne, wartungsfreie Batterien im klimatisiert ausgelegten Batterieraum durch intelligente Ladeelektronik kontinuierlich trainiert. Sie können bei einem kompletten Ausfall der externen Stromversorgung etwa zehn Minuten das Rechenzentrum im Volllast-Betrieb versorgen. In dieser Zeit werden die Dieselgeneratoren hochgefahren, die dann auch für längere Zeiträume die Stromversorgung gewährleisten.

4.8 Energiesparen mit Gleichstromversorgung

Eine interessante Strategie in Bezug auf den Nachhaltigkeitsgedanken verfolgen insbesondere Hyperscaler (skalierbare Rechenzentren). Hier wird durch die USV-Anlage der von außen kommende Wechselstrom in Gleichstrom umgewandelt, um die Batterien für die Notstromversorgung aufzuladen. Der positive Effekt ist, dass durch den Einsatz von Gleichstrom die Wärmeabgabe und der Energieverbrauch deutlich verringert wird. Traditionell wird der Gleichstrom im Problemfall wieder in Wechselstrom für die Versorgung der IT-Hardware umgewandelt. Neue Konzepte basieren jedoch darauf, nur Gleichstrom im Rechenzentrum zu verwenden um auf die Umwandlung in Wechselstrom verzichten können (Energieeinsparung). Das Open Compute Project (OCP) und die Initiative Open19 wollen mit offenen Spezifikationen und der Energieversorgung der Racks mit Gleichstrom dazu beitragen, Ineffizienzen im Data Center zu beseitigen.

Hinweis: Eine USV ist trotz ihrer Eigenschaft, Spannungs-

schwankungen auch zu höheren Werten hin abzufangen, keinesfalls als Mittel des Überspannungsschutzes anzusehen. USV-Systemen muss, wie jedes andere elektrische Gerät auch, ein ordnungsgemäßer Überspannungsschutz vorgeschaltet werden.

4.9 Security, Brandschutz und Umgebungskontrollsysteme

Im Rechenzentrum gelten höchste Security-Standards, das gilt nicht nur für die Abwehr von Cyberangriffen, sondern auch bei baulicher Sicherheit, bei der Zutritts- und Zugriffskontrolle sowie redundant ausgelegten Systemen. Ein ausgefeilter Brandschutz spielt eine entscheidende Rolle, denn an kaum einem Ort findet sich Energie derart konzentriert wie in einem Rechenzentrum. Ein dichtes Netz aus Brandmeldern und ein Brandfrüherkennungs-System sind deshalb ebenso wichtig wie eine Löschanlage. Dabei wird die Luft im Rechenzentrum ständig angesaugt und die Partikel-Konzentration mittels Laserlicht gemessen. Im Fall eines Feuers, z.B. durch einen Kurzschluss, wird in der Regel automatisch ein Alarm bei der Feuerwehr ausgelöst. Die Löschanlage flutet das Rechenzentrum im Brandfall mit ungiftigem Stickstoff, der die Flammen erstickt. Dabei kann der Gesamtbetrieb dennoch aufrechterhalten werden.

4.10 Nachhaltige Klimatisierung und Abwärmenutzung

Auch die Klimatisierung ist von entscheidender Bedeutung, denn die Hardware gibt die benötigte Energie fast zu 100 Prozent wieder als Wärme ab. Zugleich könnte ein zu starker Temperaturanstieg die empfindliche Hardware schädigen. Einhausungen für Warm- und Kaltgänge haben sich mittlerweile als Standard durchgesetzt. Mit neuen Konzepten wie der Abwärme-Nutzung wird versucht, die durch die RZ-Hardware erzeugte Wärme zum Beispiel zur Heizung von anderen Gebäudeteilen zu verwenden.

4.11 Innerer Rechenzentrumsbereich: Die Server-Racks in intelligenter Architektur

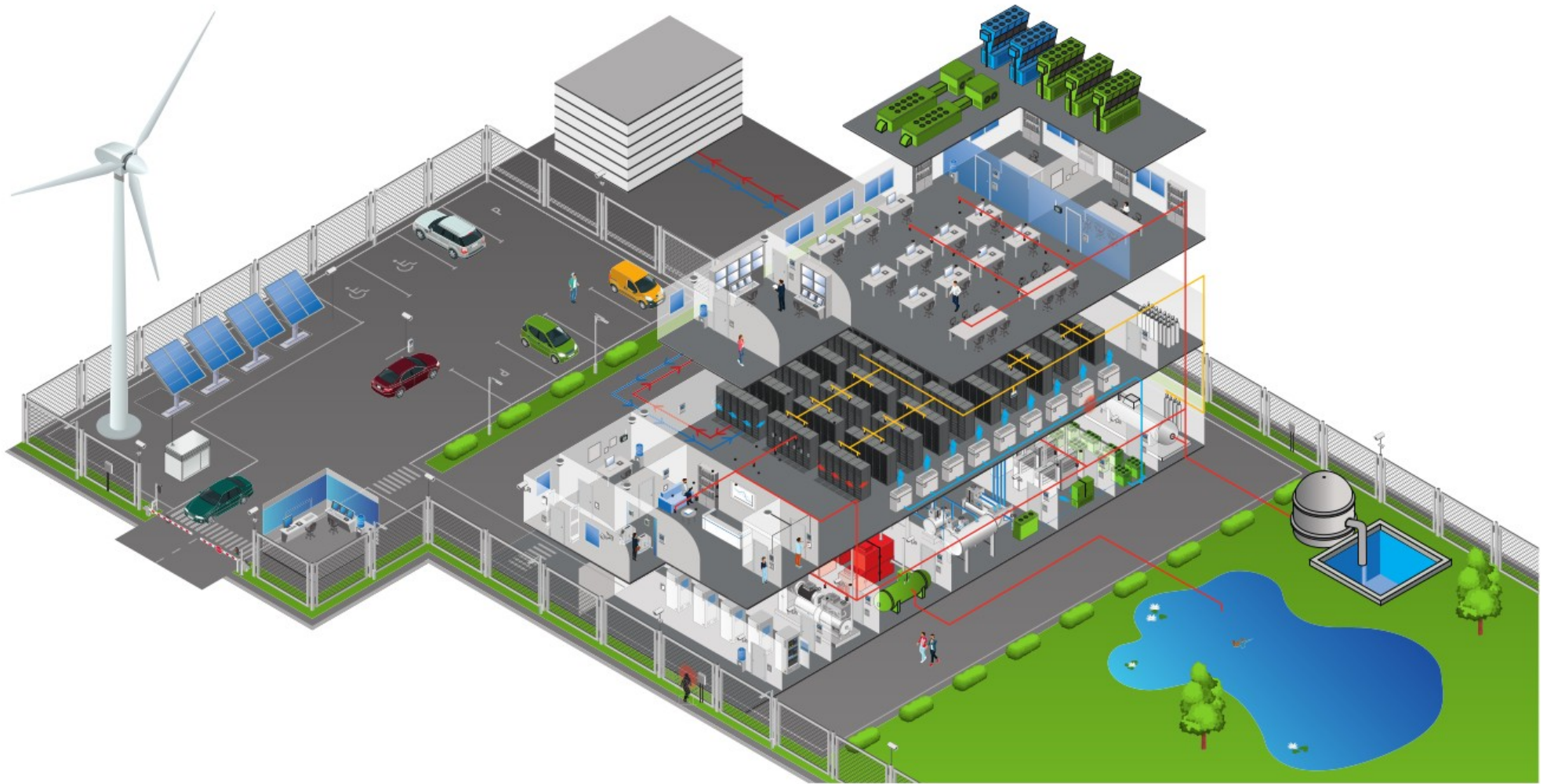
In der Regel wird die Wärmereduzierung zudem durch die Konstruktion eines doppelten Bodens im Server-Raum unterstützt. Das Prinzip ist simpel - die warme Luft, die von den Servern ausgeblasen wird, wird durch ein Umluftkühlgerät angesaugt, durch einen Wärmetauscher abgekühlt und schließlich wieder zu den Racks geleitet. Durch diese Luftzirkulation ist sichergestellt, dass im Herz des Rechenzentrums, in dem die Server, Storages- und Netzwerksysteme in standardisierten 19-Zoll-Racks geordnet sind, eine angemessene Raumtemperatur herrscht.

Zeitgemäße Racks (rack ... Regal, Gestell) sind bei hoher Belegungsdichte so flexibel und platzsparend wie möglich ausgelegt, lassen sich individuell an IT-Anwendungen anpassen und sollten hinreichend Raum für die Verkabelung bieten. Dies gewinnt insbesondere vor dem zunehmenden Einsatz von Spine-Leaf-Architekturen an Bedeutung, da hier weitaus mehr Kabel zum Einsatz kommen als bei konventionellen Ansätzen. Zukunftssicherheit bringt darüber hinaus auch die Fähigkeit der Racks, bei Bedarf einfach und schnell, IT-Hardware für neue Anwendungen austauschen zu können.

4.12 RZ-Verkabelung: Strukturiert und ausfallsicher

Die passiven Netzwerk-Komponenten wie Kabel und Stecker, die alle Systeme redundant untereinander und mit dem Internet verbinden, sollten sowohl für Kupfer- als auch für Glasfaserverkabelung genutzt werden können. Für den Erfolg einer Rechenzentrumskonzeption und den störungsfreien Betrieb sorgt eine ausfallsichere und strukturierte Verkabelung, die aktuellen Standards folgt. Die Technologie im Rechenzentrum (RZ) ist weiter im Wandel: Deshalb muss eine Verkabelung alle aktuellen und

zukünftigen Kommunikationssysteme unterstützen und sich nicht nur dem Übertragungsprotokoll, sondern auch den Endgeräten gegenüber neutral verhalten: Ansonsten besteht die Gefahr, dass künftige Änderungen der Rechenzentrums-Infrastruktur erhebliche Kosten mit sich bringen.



Legende: Linienfarben

Rot: Brandschutz – Hellblau: Gebäudeautomation – Gelb: Server – Dunkelblau: Remote Services

5. Hinweise zur Ausfallsicherheit von Rechenzentren (RZ)

Um die Ausfallsicherheit eines normalen Rechenzentrums zu erhöhen, sollte man ein größeres Rechenzentrum in zwei kleinere Rechenzentren aufteilen.

Die beiden Rechenzentren sollten zusätzlich an entfernten Standorten (Zwei-Standort-Strategie) aufgebaut werden und nur durch separate Datenleitungen miteinander verbunden sein.

Das Backup des einen Rechenzentrums wird zu dem jeweils anderen Rechenzentrum übertragen und dort auch gespeichert.

Die beiden Rechenzentren sollten so dimensioniert werden, dass bei einem kompletten Ausfall eines Rechenzentrums der Notbetrieb durch das andere Rechenzentrum übernommen werden kann.

Hinweis: Das Zurückspielen eines Backups sollte mindestens einmal im Jahr durch das Personal trainiert werden. Dafür kann man eventuell speziell vorgehaltene Hardware nutzen, die auch für andere Testszenarien genutzt werden kann.



Tier-System: Qualitätsstufen für Rechenzentren

Das englische Wort **Tier** wird in der Informatik und in der Informationstechnologie häufig verwendet und kann je nach Zusammenhang unterschiedliche Bedeutungen haben. Wörtlich übersetzt heißt es lediglich **Stufe**, **Schicht**, **Ebene** oder **Rang** und bezeichnet eine bestimmte Position in einem hierarchischen Modell, bei dem die unteren Positionen direkt von den darüber liegenden abhängig sind.

Das Konzept Tier ist universell ausgelegt und dient unter anderem für Bezeichnungen bei der Hardware, bei Netzwerkprotokollen und Netzwerkschichten sowie in der Informationstechnologie. In Kombination mit Servern und Rechenzentren steht Tier in zwei unterschiedlichen Zusammenhängen. Es bezeichnet sowohl die Anbindung beziehungsweise den Betreiber der Infrastruktur anhand seiner Stellung innerhalb des globalen Netzwerks sowie die Qualitätsstufen in einem Datacenter (Rechenzentrum), die teilweise durch Zertifizierungen abgesichert sein können.

Hinweis: Die Tier-Topologie wurde Ende der 1990er Jahre vom Uptime Institut mit Sitz in den USA, weltweit als Standard eingeführt. Das Tier Modell berücksichtigt primär nur die Verfügbarkeit oder Uptime und wenige weitere Kriterien.

Was sind Tier als Qualitätsstufen in Rechenzentren (RZ)?

Bei einem Datacenter (RZ) dienen Tier's als eine von mehreren möglichen Bezeichnungen für Qualitätsstufen, die von dem Betreiber garantierte Verfügbarkeit widerspiegeln. Als Rahmen für die Referenz nutzt die Skala dabei ein Kalenderjahr, in dem ein System wie zum Beispiel ein virtueller oder dedizierter Server maximal für eine bestimmte Zeit ausfallen darf. Diese Frist deckt



alle potentiellen Gründe ab und schließt somit ausdrücklich Ereignisse wie Wartungsarbeiten, Administration der Software oder Schäden an der Hardware sowie oft ebenfalls Fälle von »höherer Gewalt« - etwa Naturkatastrophen oder Unterbrechungen der Stromversorgung - mit ein. Bei der Verfügbarkeit für ein Datacenter (RZ) werden vier unterschiedliche Stufen unterschieden:

- **Tier 1** gewährleistet eine Verfügbarkeit von mindesten 99,671 Prozent oder eine maximale Ausfallzeit von 28,8 Stunden im Jahr
- **Tier 2** gewährleistet eine Verfügbarkeit von mindesten 99,749 Prozent oder eine maximale Ausfallzeit von 22,7 Stunden im Jahr
- **Tier 3** gewährleistet eine Verfügbarkeit von mindesten 99,982 Prozent oder eine maximale Ausfallzeit von 1,6 Stunden im Jahr
- **Tier 4** gewährleistet eine Verfügbarkeit von mindesten 99,995 Prozent oder eine maximale Ausfallzeit von 26,3 Minuten im Jahr

Rechenzentren – Tier-Standards und Datensicherheit 2/9

Die Zertifizierungen der Datacenter (RZ) finden einerseits durch die Betreiber selbst und andererseits durch unabhängige Institute statt, die zum Beispiel die Konformität mit wichtigen Standards wie der 2019 in Kraft getreten DIN EN 50600 überprüfen. Darüber hinaus nehmen einige Anbieter und Portale im Internet eigene Zertifizierungen vor, indem sie meist mit Hilfe von automatisierten Skripten die Erreichbarkeit von Rechenzentren in regelmäßigen Abständen kontrollieren und statistisch auswerten. Offizielle Zertifizierungen anhand internationaler Normen durch unabhängige Unternehmen und Organisationen finden bei einem Datacenter (RZ) lediglich auf den ausdrücklichen Antrag des Betreibers statt und sind nicht gesetzlich vorgeschrieben, sondern erfolgen ausschließlich auf freiwilliger Basis. Zu diesen Zertifizierungen gehören etwa ebenfalls allgemeine Standards für wirtschaftliche Betriebe wie die ISO 9001, die das Qualitätsmanagement beschreibt oder ISO 14000 ff, das Richtlinien für das Umweltmanagement, den Ausstoß von CO₂ und die Verwendung regenerativer Energien enthält.

Welche alternativen Systeme für Qualitätsstufen bei Rechenzentren (RZ) existieren?

Ein Nachteil des Tier Modells besteht darin, dass seine Zertifizierungen primär die Verfügbarkeit oder Uptime berücksichtigen und wenige weiteren Kriterien enthalten. Aus diesem Grund haben sich mittlerweile andere Einteilungen etabliert, die die Qualitätsstufen für ein Datacenter in einem komplexeren Zusammenhang ermitteln. So besitzt etwa das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** ein eigenes Analysemodell und vergibt für diese Zertifizierungen an überprüfte Rechenzentren. Es umfasst sechs verschiedene Qualitätsstufen, die ebenfalls die Verfügbarkeit widerspiegeln:

- **VK 0** steht für eine Verfügbarkeit bis 95 Prozent oder maximal

zwei bis drei Wochen Downtime im Jahr

- **VK 1** steht für eine Verfügbarkeit zwischen 95 Prozent und 99 Prozent oder maximal 90 Stunden Downtime im Jahr
- **VK 2** steht für eine Verfügbarkeit zwischen 99 Prozent und 99,9 Prozent oder maximal 9 Stunden Downtime im Jahr
- **VK 3** steht für eine Verfügbarkeit zwischen 99,9 Prozent und 99,99 Prozent oder maximal 60 Minuten Downtime im Jahr
- **VK 4** steht für eine Verfügbarkeit zwischen 99,99 Prozent und 99,999 Prozent oder maximal 5 Minuten Downtime im Jahr
- **VK 5** steht für eine Verfügbarkeit von 100 Prozent und erlaubt keinerlei Downtime 24/7/365 über ein Jahr

Eine weitere populäre Einteilung für Qualitätsstufen an Rechenzentren stellt das von dem TÜV entwickelte **Trusted Site Infrastructure (TSI)**, das in seiner ersten Version 2001 veröffentlicht wurde und seit dieser Zeit stark an Bedeutung gewinnt. Inzwischen zählt es zu den häufigsten unabhängigen Zertifizierungen für Datacenter und wurde mit TSI.EN50600 ergänzt, um ebenfalls Zertifizierungen für die neue Euronorm ausstellen zu können. Es berücksichtigt unter anderem ebenfalls die physische Sicherheit von Rechenzentren anhand von Abständen zu gefährdeten Betrieben wie petrochemischen Einrichtungen, Hochwassergebieten, Flughäfen und anderen Risikofaktoren.

Zertifizierungen durch das TSI kennen vier unterschiedliche Level für Datacenter:

- **Level 1** - mittlere Verfügbarkeit mit einem grundlegenden Schutz zum Betrieb von Rechenzentren
- **Level 2** - erweiterte Verfügbarkeit mit redundanten Strukturen für die Versorgung von Energie, Anbindung an das Netzwerk und Klimakontrolle

Rechenzentren – Tier-Standards und Datensicherheit 3/9

- **Level 3** - hohe Verfügbarkeit (Hochverfügbarkeit) mit permanenter Betriebskontrolle 24/7/365, gesicherter und redundanter Versorgung und Brandbeherrschung
- **Level 4** - sehr hohe Verfügbarkeit (Höchstverfügbarkeit) für dedizierte Datacenter mit umfassender Absicherung im Vorfeld und Wartungstoleranzen

Die Ansprüche an ein Datacenter haben sich in den letzten Jahren erheblich gewandelt und stellen mittlerweile in vielen Bereichen Anforderungen, die in der Vergangenheit ausschließlich bei systemkritischen Einrichtungen wie Polizei, Feuerwehr und Streitkräften oder der Energieversorgung bestanden. Auf diesen Umstand ist zurückzuführen, dass sich neben den Tier

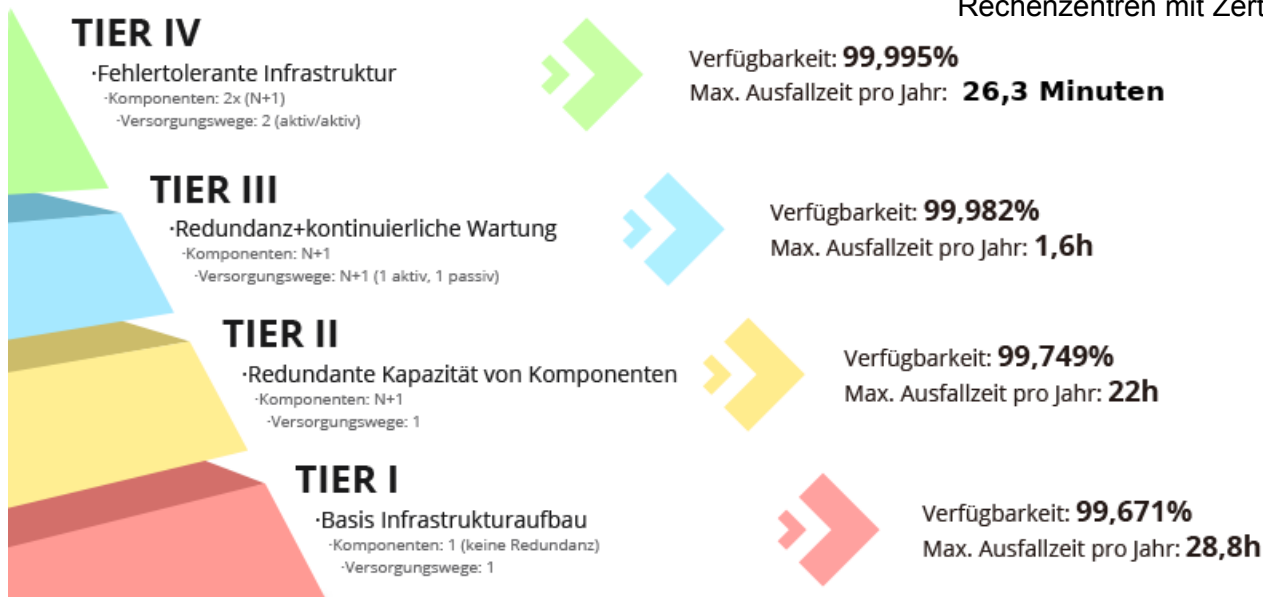
unabhängige Zertifizierungen für Rechenzentren wie TSI und DIN EN 50600 zunehmend etablieren, obwohl keine rechtliche Verpflichtung zu diesen besteht.

Welches Datacenter empfiehlt sich für einen bestimmten Zweck?

Rechenzentren mit Tier 1 und 2 oder TSI Zertifizierungen nach VK 0 und VK 1 galten lange Zeit als ideal für kleine Unternehmen, private und öffentliche Webseiten, weil sie eine hohe Leistung zu einem günstigen Preis anboten. In der Praxis spielen sie allerdings heute kaum noch eine relevante Rolle, weil durch die Professionalisierung der Datacenter und die Verwendung von redundanten Systemen und ausfallsicherer Hardware die Verfügbarkeit stark angestiegen ist. Aus diesem Grund empfehlen die meisten IT-Experten, Rechenzentren mit Zertifizierungen der Stufe Tier 3 für

Anwendungen, die kurze Ausfälle ohne kritische Folgen tolerieren - etwa interne Plattformen in einem Unternehmen oder für die Buchhaltung.

Kommerzielle Webseiten, Onlineshops, Server für das Gaming und zeitkritische Prozesse etwa in der Industrie sollten Datacenter mit der maximalen Verfügbarkeit Tier 4 beziehungsweise Zertifizierungen nach TSI VK 4 oder höher verwenden, um eine permanente Erreichbarkeit 24/7/365 bei geringer Latenz und Server Response Time (SRT) zu gewährleisten.



Hinweis: Alle Bewertungs-Systeme bieten eine verlässliche Bewertungsgrundlage für die Planung, Umsetzung und Inbetriebnahme neuer Rechenzentren sowie für die leistungstechnische Optimierung und die sicherheitstechnische Weiterentwicklung bestehender Rechenzentren.

Rechenzentren – Tier-Standards und Datensicherheit 4/9

Tier-Klassen - Klassifizierung von Sicherheit in Rechenzentren

Bei der Wahl des richtigen Rechenzentrums ist zu beachten, dass sie sich zum Teil erheblich in ihrer Leistungsfähigkeit unterscheiden. Das betrifft nicht nur Systemtechnik, Energieeffizienz und Datensicherheit, sondern vor allem auch die Verfügbarkeit. Die sogenannte Tier-Klasse gibt Auskunft über die Qualität eines Rechenzentrums und gilt als Maßstab für seine Ausfallsicherheit.

IT-Systeme und Server dürfen zu keinem Zeitpunkt ausfallen, sondern müssen permanent zur Verfügung stehen. Unternehmen sind auf eine zuverlässige Unterstützung durch die IT-Infrastruktur angewiesen. Aus diesem Grund arbeiten die meisten Unternehmen bereits mit virtuellen und redundanten Servern und Speichersystemen. Moderne Rechenzentren sind daher auf eine Hochverfügbarkeit ausgelegt.

Die technische Infrastruktur in einem Datacenter muss so ausgelegt sein, dass die Ausfallsicherheit der IT-Systeme gewährleistet ist.

Tier-Klassen - Weltweiter Standard für die Sicherheit von Rechenzentren

Das amerikanische Uptime Institute, das mit über 1.500 Zertifizierungen in fast 100 Ländern einen weltweiten Standard für die Sicherheit von Rechenzentren definiert hat, klassifiziert in vier sogenannten Tiers (englisch: Rang, Level oder Stufe).

Die vier Tier-Klassen, die in der TIA-942 (Telecommunications Infrastructure Standard für Data Centers) vorgenommen wurden, legen die Ausfallsicherheit und die Verfügbarkeit eines Rechenzentrums fest. Das bedeutet, jedes Tier steht für einen bestimmten Rang, den das Datacenter und seine Infrastruktur erfüllen muss.

Die Tier-Klassen im Überblick

Die wichtigsten Unterscheidungskriterien für die Tier-Klassen 1 bis 4 sind Redundanz und Verfügbarkeit. Hierbei ist wichtig zu erwähnen, dass jede Tier-Klasse über alle erforderlichen Komponenten der darunter liegenden Stufe verfügt. Tier 1-Rechenzentren verfügen über die einfachste Infrastruktur und gelten dabei als wenig zuverlässig. Tier 4-Rechenzentren hingegen sind im Aufbau sehr komplex und verfügen über die meisten redundanten Komponenten - sie gelten als hochverfügbar. Bei einer Hochverfügbarkeit liegt die Wahrscheinlichkeit, dass ein Datacenter einsatzbereit ist, bei nahezu 100%. Die Ausfallzeit pro Jahr liegt entsprechend lediglich im Minutenbereich.

Tier 1 (keine Redundanz und hohes Ausfallrisiko):

Ein Tier-1-Rechenzentrum verfügt über einen einzigen Pfad für Strom und Kühlung. Tier 1 fordert die geringste Entwärmungsleistung von 220 bis 320 Watt pro Quadratmeter. Es bietet eine erwartete Betriebszeit von 99,671%, d. h. max. 28,8 Stunden Ausfallzeit pro Jahr.

- Basis-Infrastrukturaufbau ohne Redundanz
- Komponenten zur Versorgung und Verteilung von Energie und Kühlung nur einfach vorhanden
- nur geplante Wartungen möglich (bei Wartungen muss der Betrieb der Systeme komplett unterbrochen werden, hohes Ausfallrisiko des Datacenters)
- sehr hohe Ausfallzeit pro Jahr

Ein Tier-1-Rechenzentrum schützt vor Unterbrechungen durch menschliches Versagen, nicht jedoch vor unerwarteten Störungen oder Ausfällen. Das Rechenzentrum muss für vorbeugende Wartung und Reparaturen vollständig abgeschaltet werden, da sonst das Risiko ungeplanter Unterbrechungen steigt und ein

Rechenzentren – Tier-Standards und Datensicherheit 5/9

Systemausfall schwerwiegende Folgen haben könnte.

Tier 2 (einfache Redundanz im Rechenzentrum):

Ein Tier-2-Rechenzentrum verfügt über redundante Kapazitäten. Es verfügt über einen einzigen Strom- und Kühlungspfad sowie über einige redundante Komponenten und Backup-Komponente. Tier 2 fordert eine Entwärmungsleistung von 430 bis 540 Watt pro Quadratmeter. Die erwartete Betriebszeit beträgt 99,741%, d. h. max. 22 Stunden Ausfallzeit pro Jahr.

- Strom- und Kühlungskomponenten redundant vorhanden (**N+1**-Redundanz)
- einige redundante Komponenten, Verteilungspfad für Stromversorgung und Kühlung sind einfach ausgelegt
- massive Störungen oder Totalausfall möglich
- hohe Ausfallzeit pro Jahr

Die redundanten Komponenten können entfernt werden, ohne dass es zu einer Abschaltung kommt. Ein Tier-2-Rechenzentrum bietet bessere Wartungsmöglichkeiten und Sicherheit vor Störungen, aber wie bei einem Tier-1-Rechenzentrum wirkt sich eine unerwartete Abschaltung einer Tier-2-Einrichtung auf das System aus.

Tier 3 (Fehlertoleranz des Systems erhöht):

Ein Tier-3-Rechenzentrum ist gleichzeitig wartbar. Es verfügt über mehrere Stromversorgungs- und Kühlungspfade sowie über Systeme zur Aktualisierung und Wartung, ohne dass es abgeschaltet werden muss. Die Entwärmungsleistung liegt bei 1.070 bis 1.620 Watt pro Quadratmeter. Es hat eine erwartete Betriebszeit von 99,982%, was max. 1,6 Stunden Ausfallzeit pro Jahr bedeutet. Eine Tier-3-Rechenzentrum erfordert alle

Komponenten, die auch in einem Tier-2-Rechenzentrum vorhanden sind, aber diese Rechenzentren müssen zusätzlich eine **N+1**-Redundanz aufweisen:

- **N** bezieht sich auf die erforderliche Kapazität zur Unterstützung der vollen IT-Last
- **+1** steht für eine zusätzliche Komponente für Sicherungszwecke
- mehrere Pfade für Stromversorgung und Kühlung
- Aktualisierungs- und Wartungsarbeiten an einzelnen Komponenten während des laufenden Betriebs möglich
- mehrere Brandabschnitte erhöhen die Ausfallsicherheit
- geringe Ausfallzeit pro Jahr

Die **N+1**-Redundanz stellt sicher, dass eine zusätzliche Komponente in Betrieb genommen wird, wenn das primäre Element ausfällt oder vom Personal für geplante Wartungsarbeiten entfernt wird. Im Gegensatz zu Tier 1 und Tier 2 müssen diese Systeme nicht abgeschaltet werden, wenn eine Wartung oder ein Austausch erforderlich ist. Damit wird der IT-Betrieb des Rechenzentrums während einer Wartung nicht beeinträchtigt.

Tier 4 (Fehlertoleranz des Systems erhöht):

Ein Tier 4-Rechenzentrum ist vollständig fehlertolerant aufgebaut. Es verfügt über mehrere unabhängige und physisch isolierte Systeme, die als redundante Kapazitätskomponenten und Verteilungswege fungieren. Die Trennung ist notwendig, damit beide Systeme nicht durch ein Ereignis beeinträchtigt werden können. Die Entwärmungsleistung liegt dabei über 1.620 Watt pro Quadratmeter. Ein Tier 4-Rechenzentrum hat eine erwartete Betriebszeit von 99,995%, was max. 26,3 Minuten Ausfallzeit pro Jahr bedeutet.

Rechenzentren – Tier-Standards und Datensicherheit 6/9

Tier 4-Rechenzentren verfügen entweder über **2N**- oder **2N+1**-Redundanz:

- **2N**-Redundanz (oder **N+N**-Redundanz) bedeutet, dass die Einrichtung ein vollständig gespiegeltes, unabhängiges System in Bereitschaft besitzt. Wenn eine Primärkomponente ausfällt, wird eine identische Backup-Kopie in Betrieb genommen, um den weiteren Betrieb sicherzustellen.
- Das **2N+1**-Modell bietet die doppelte Betriebskapazität (**2N**) und eine zusätzliche Sicherungskomponente (**+1**) für den Fall, dass ein Ausfall eintritt, während ein sekundäres System aktiv ist.
- vollständig fehlertolerant eingerichtet
- Komponenten und Leitungswege sind redundant ausgelegt
- hohe Kosten
- Ausfallzeit pro Jahr im Minutenbereich

Fällt ein Gerät aus oder kommt es zu einer Unterbrechung im Verteilungspfad, wird der IT-Betrieb nicht beeinträchtigt. Wenn jedoch die redundanten Komponenten oder Verteilungspfade zu Wartungszwecken abgeschaltet werden, kann das Rechenzentrum im Falle eines Ausfalls einem höheren Störungsrisiko ausgesetzt sein. Aus diesem Grund garantiert ein Tier-4-Rechenzentrum keine hundertprozentige Betriebszeit.

Auch wenn ein Tier 4-Rechenzentrum wesentlich komplexer aufgebaut ist als ein Tier 1-Datacenter, muss es nicht unbedingt immer die beste Lösung für ein Unternehmen sein. Tier 1-Infrastrukturen können für Unternehmen erhebliche Risiken bergen, während Investitionen in ein Tier 4-Rechenzentrum unter Umständen unangemessen hoch ausfallen können. Unternehmen sollten sich daher von erfahrenen Rechenzentrumsexperten beraten lassen.

Hinweis: Noch vor einigen Jahren lag die mittlere Wärmelast bei etwa 0,5 Kilowatt pro Quadratmeter. Durch die zunehmende Integration und Packungsdichte der IT-Komponenten ist der Mittelwert inzwischen bei mehr als 3 Kilowatt pro Quadratmeter angekommen. Zudem sind immer noch Klimageräte im Betrieb, die bis zu 60 Prozent des Energiebedarfs eines Datacenters ausmachen.

Was bedeutet »Hochverfügbarkeit«?

Der Begriff Verfügbarkeit bezeichnet die Wahrscheinlichkeit, dass ein System zu einem gegebenen Zeitpunkt tatsächlich wie geplant benutzt werden kann. Die Verfügbarkeit wird dabei als Verhältnis aus Ausfallzeit (Downtime) und Gesamtzeit eines Systems bemessen:

$$\text{Verfügbarkeit} = \text{Uptime} / (\text{Downtime} + \text{Uptime})$$

oder

$$\text{Verfügbarkeit (\%)} = 1 - \text{Ausfallzeit} / (\text{Produktionszeit} + \text{Ausfallzeit})$$

Die Hochverfügbarkeit (abgekürzt auch HA, abgeleitet von engl. high availability) bezeichnet also die Fähigkeit eines Systems, bei Ausfall einer seiner Komponenten einen uneingeschränkten Betrieb zu gewährleisten.

Für »Hochverfügbarkeit« muss die Wahrscheinlichkeit, dass ein System verfügbar ist, über 99,99% liegen. Die jährliche Ausfallzeit muss demnach im Minutenbereich liegen.

Fehlertolerante Systeme

Fehlertolerante Systeme erreichen eine besonders hohe Verfügbarkeit, weil sie mithilfe von intelligenter Software auf nahezu

Rechenzentren – Tier-Standards und Datensicherheit 7/9

alle erdenklichen Fehlerursachen reagieren können. Zusätzlich eliminiert der Aufbau fehlertoleranter Systeme Ursachen für Single Points of Failure (SPOF; einzelne Fehlerstelle). Ein SPOF bezeichnet eine einzelne Komponente, die für die korrekte und zuverlässige Funktionsfähigkeit des Gesamtsystems zwingend erforderlich ist. Dies schließt auch das Design des Netzwerkes und der Speichertechnik mit ein: So kann ein ausgefallener Netzwerkswitch bereits dazu führen, dass der Service des Gesamtnetzwerkes nicht mehr verfügbar ist. Durch die Herstellung von Redundanz und automatischer Lastenverteilung können SPOF-Risiken (Single Points of Failure; einzelne Fehlerstelle) eingedämmt werden. Dafür werden die einzelnen Hardware- und Netzwerk-Komponenten wie Router und Switches des selben Typs mehrfach angelegt. Im Falle eines Ausfalls kann die redundante Komponente die Aufgabe der Anderen übernehmen. Bei besonders hohen Verfügbarkeitsanforderungen kann auch die gesamte Rechnerhardware in Form eines Standby-Systems gespiegelt werden.

Es ist jedoch zu beachten, dass eine hohe Verfügbarkeit nicht nur auf physischer Infrastruktur-Ebene bestimmt wird. Die organisatorischen und ausführenden Strukturen sind für einen sicheren Betrieb der Infrastruktur nicht weniger entscheidend. Dazu zählen beispielsweise:

- geschultes Servicepersonal
- Bereithalten von Ersatzteilen
- Abschluss von Wartungsverträgen
- Instruktionen über das Verhalten im Fehler- oder Notfall
- schnelle, exakte Kommunikationsführung
- nachvollziehbare Protokollierung der Ereignisse

Die wichtigsten, zertifizierungsfähigen Normen auf

organisatorischer Ebene sind ISO/IEC 27001 (Norm für Information Security Management Systems, kurz ISMS) mit Anlehnung an den IT-Grundschutz sowie ISO/IEC 20000 (Norm für IT-Service-Management, kurz ITSM). Für die Standards ISO/IEC 27001 und ISO/IEC 20000, ist ergänzend auch jeweils ein Leitfaden mit Best Practice Anweisungen vorhanden. Gemeint sind ISO/IEC 27002 und ITIL (IT Infrastructure Library).

Zertifizierungen in Europa - Gleicher Standard, andere Institute

Die Klassifizierung von Verfügbarkeitsklassen nach der Definition des Uptime Institute hat sich weitgehend durchgesetzt. Als Zertifizierer spielt das Uptime-Institute, das Rechenzentren in den Phasen Design (Bauplanung), Bau und Betrieb zertifiziert, hierzulande allerdings kaum eine Rolle. Weitaus stärker verbreitet ist der Standard Trusted Site Infrastructure (TSI). Der Kriterienkatalog der TSI wurde von TÜV Informationstechnik (TÜViT) bereits 2001 entwickelt und berücksichtigt inzwischen auch die Anforderungen der europaweit geltenden Norm für Rechenzentren EN 50600. So stellen in Deutschland sowohl der TÜV Nord und Süd Zertifizierungen aus, die sich zwar unterscheiden, aber in etwa die gleichen Voraussetzungen abfragen. Das Zertifikat des TÜV Rheinland hierüber lautet beispielsweise »Reliable Data Center«. Dieses Zertifikat weist nach, dass entsprechende Anforderungen nach dem Prüfkatalog für Reliable Data Center (RDC; zuverlässiges Rechenzentrum) erfüllt wurden.

Bei der Wahl der passenden Zertifizierung ist jedoch zu beachten, dass die verschiedenen Normen unterschiedliche Schwerpunkte setzen. Während bestimmte Normen den Fokus auf die organisatorische Ebene legen, zielen andere Standards auf physische Sicherheit ab. Diese beinhalteten z.B. Anforderungen für die Beurteilung und Behandlung von Informationssicherheitsrisiken

Rechenzentren – Tier-Standards und Datensicherheit 8/9

entsprechend den individuellen Bedürfnissen der Organisation und spezifiziert die Implementierung geeigneter Sicherheitsmechanismen.

EN 50600 ist die erste europaweit länderübergreifende Norm, die mit einem ganzheitlichen Ansatz umfassende Vorgaben für Planung, Neubau und Betrieb eines Rechenzentrums macht - von der Planung der Gewerke, Baukonstruktion, Elektroversorgung, Klimatisierung und Verkabelung sowie über Sicherheitssysteme bis zum Rechenzentrums-Betrieb.

Geht es um rein wirtschaftliche Kennzahlen, existieren nochmals andere Normen. Darüber hinaus sind bei der Zertifizierung und der Prüfung eines Rechenzentrums fünf Hauptkriterien zu beachten. Hierzu gehören neben der Standortwahl und der Gebäudekonstruktion auch Klimatechnik, Telekommunikation und Verkabelung sowie der Sicherheitsaspekt. Bei der Vielzahl und Übersichtlichkeit an Einstufungen, Kriterien und möglichen Zertifikaten ist es ratsam, sich bei der Wahl des passenden Rechenzentrums mit der notwendigen Zertifizierung- bzw. Sicherheitsstufe beraten zu lassen.

Ist die Qualitätsprüfung von Rechenzentren vorgeschrieben?

ISO-Normen, Qualitätsstufen und Zertifizierungen sind nicht verpflichtend und werden durch Betreiber von Rechenzentren freiwillig oder über unabhängige Organisationen wie TÜV Süd durchgeführt.

Umso wichtiger ist es für Investoren, Mieter und Endnutzer, auf die transparente Angabe der Qualitätsstufe zu achten. Betreiber von Rechenzentren wiederum stärken ihre Vertrauenswürdigkeit durch eine zertifizierte Verfügbarkeit und Sicherheit.

Welches Rechenzentrum-Tier ist nun das Richtige?

Obwohl höhere Tiers einen zuverlässigeren Service bieten, bedeutet dies nicht zwangsläufig, dass ein Tier 4-Rechenzentrum für die Bedürfnisse eines Unternehmens am besten geeignet ist. Unternehmen verschiedener Art tendieren in der Regel zu bestimmten Tiers. Letztendlich ist es eine Entscheidung des Eigentümers, welche Stufe für die geschäftlichen Anforderungen am besten geeignet ist.

Ein kleiner Leitfaden für die Entscheidung:

- **Tier 1:** Tier 1-Rechenzentren eignen sich am besten für kleine Unternehmen und Neugründungen, die die günstigste und kosteneffizienteste Hosting-Option wünschen. Kleine Unternehmen ohne Dauerbetrieb oder einfache IT-Anforderungen sind toleranter gegenüber häufigen Ausfallzeiten.
- **Tier 2:** Diese Rechenzentren sind die erste Wahl für kleine und mittlere Unternehmen, die eine kostengünstige, aber zuverlässigere Option als ein Tier-1-Rechenzentrum suchen. Kleine oder mittelgroße Unternehmen nutzen in der Regel Tier-2-Rechenzentren, um Datensicherungen oder nicht unternehmenskritische Datenbanken zu hosten (aufnehmen).
- **Tier 3:** Tier 3-Rechenzentren sind die ideale Wahl für große Unternehmen mit komplexen IT-Anforderungen, die zusätzliche Ausfallsicherheiten benötigen. Unternehmen, die kritische und umfangreiche Datenbanken, insbesondere Kundendaten, hosten, entscheiden sich in der Regel für diese Klasse.
- **Tier 4:** Diese Rechenzentren eignen sich für Unternehmen mit ausreichendem Budget und unternehmenskritischen Anforderungen. Regierungsorganisationen und große Unternehmen mit wichtigen Servern und intensiven Kunden- oder Geschäftsanforderungen sind die Hauptnutzer eines Tier-4-Rechenzentrums.

In der Regel sind die gewünschte Verfügbarkeit der Daten, die Datensicherheit, die Kosten und die Betriebszeit (geringe oder keine Ausfallzeiten) die wichtigsten Faktoren bei der Wahl einer Stufe.

Es ist sehr wichtig, wo man seine Daten aufbewahrt. Daher ist es von entscheidender Bedeutung, die Unterschiede zwischen den verschiedenen Tiers (**siehe auch:** alternativen Systeme für Qualitätsstufen) zu kennen, die Daten hosten (aufnehmen).

Exploit - EternalBlue 2/3

Windows-Betriebssysteme. Bis Mai 2019 hatten sämtliche mit den USA in Konkurrenz stehenden Mächte auf staatlicher oder nichtstaatlicher Ebene Gebrauch von EternalBlue gemacht oder gar eigene Programme rund um die Software entwickelt und auch angewendet.

Hinweis: In den aktuellen Windows-Versionen ist SMBv1 standardmäßig deaktiviert. Ist etwas deaktiviert, so kann Malware auf infizierten Rechner SMBv1 auch wieder aktivieren.

Entwicklung von EternalBlue

EternalBlue wurde von der Nationalen Sicherheitsbehörde der Vereinigten Staaten als Teil ihres umstrittenen Programms entwickelt, bei dem Schwachstellen in der Cybersicherheit gehortet und zu Waffen umfunktioniert werden, anstatt die Schwachstellen an den entsprechenden Anbieter zu melden.

Vor dem Bekanntwerden war EternalBlue eine der nützlichsten Schwachstellen im Cyber-Arsenal der NSA, die in unzähligen Geheimdienst- und Terrorismusbekämpfungsmissionen eingesetzt wurde.

Die NSA hat angeblich fast ein Jahr lang nach einem Fehler in der Software von Microsoft gesucht. Nachdem sie ihn gefunden hatte, entwickelte die NSA EternalBlue, um die Sicherheitslücke auszunutzen.

Die NSA nutzte EternalBlue etwa fünf Jahre lang, bevor sie Microsoft über dessen Existenz informierte. Seitdem hat Microsoft die NSA und andere Regierungsstellen aufgefordert, eine digitale Genfer Konvention zu unterstützen, die ein Ende der Anhäufung von Softwareschwachstellen durch Nationalstaaten fordert.

Wie funktioniert EternalBlue?

Der EternalBlue-Exploit nutzt SMBv1-Schwachstellen in älteren Versionen von Microsoft-Betriebssystemen aus. SMBv1 wurde Anfang 1983 als Netzerkommunikationsprotokoll entwickelt, um den gemeinsamen Zugriff auf Dateien, Drucker und Ports zu ermöglichen. Es war im Wesentlichen eine Möglichkeit für Windows-Rechner, miteinander und mit anderen Geräten über Remote-Dienste zu kommunizieren.

EternalBlue nutzt Schwachstellen in SMBv1 aus, um bösartige Datenpakete einzufügen und Malware über das Netzwerk zu verbreiten. Die Schwachstelle nutzt dabei die Art und Weise aus, wie Microsoft Windows speziell erstellte Pakete von bösartigen Angreifern behandelt oder besser gesagt falsch behandelt. Alles, was der Angreifer tun muss, ist ein böswillig erstelltes Paket an den Zielservers zu senden und schon breitet sich die Malware aus und ein Cyberangriff ist die Folge.

Das Microsofts Patch schließt die Sicherheitslücke vollständig und verhindert damit Versuche Malware oder andere Versuche der digitalen Infiltration mithilfe des EternalBlue-Exploits zu implementieren. Aber ein Hauptproblem bleibt bestehen - für viele Windows-Versionen muss das Software-Update installiert werden, um Schutz zu bieten.

Hinweis: EternalBlue ist immer noch am leben und am Entwicklungs-Horizont warten bereits die Nachfolger oder sind schon aktiv.

Es ist dieses Hauptproblem, das EternalBlue eine so lange Lebensdauer verleiht - viele Menschen und sogar Unternehmen versäumen es, ihre Software regelmäßig zu aktualisieren, wodurch ihre Betriebssysteme ungepatcht und somit anfällig für EternalBlue

Exploit - EternalBlue 3/3

und andere Angriffe bleiben. Bis zum heutigen Tag beläuft sich die Zahl der ungepatchten anfälligen Windows-Systeme auf mehrere Millionen.

Wie wird EternalBlue bei Cyberangriffen eingesetzt?

EternalBlue wurde bekanntlich zur Verbreitung der Ransomware »WannaCry« und »Petya« verwendet. Die Sicherheitslücke kann jedoch für jede Art von Cyberangriff verwendet werden, einschließlich Cryptojacking (illegales schürfen von Kryptowährung) und wurmartiger Malware. Der NSA-Hack öffnete jedem Angreifer die Tür, um ein bösesartiges Paket an einen anfälligen Server zu senden, der den Patch zur Behebung von CVE-2017-0144 noch nicht angewendet hat.

WannaCry

Der Name sagt schon alles. »WannaCry« ist der Name eines weltweiten Ransomware-Angriffs, der durch den EternalBlue-Exploit ermöglicht wurde. Wie man am Namen sieht haben selbst Hacker eine humorvolle Seite.

Der WannaCry-Cyberangriff begann am 12. Mai 2017 und hatte sofort weltweite Auswirkungen. Die Ransomware verbreitete sich mit einer Geschwindigkeit von 10.000 Geräten pro Stunde und infizierte an einem einzigen Tag über 230.000 Windows-PC's in 150 Ländern. Obwohl keine spezifischen Ziele erkennbar waren, waren einige große Namen und Einrichtungen betroffen, darunter FedEx, die Universität von Montreal, LATAM Airlines, die Deutsche Bahn und vor allem der Gesundheitsdienst des Vereinigten Königreichs, der National Health Service (NHS, Tausende von Terminen und Operationen wurden abgesagt).

Petya

Petya ist ein weiterer Ransomware-Cyberangriff, der die

EternalBlue-Schwachstelle nutzte, um Schaden anzurichten.

»Petya« kam eigentlich Anfang 2016 auf den Markt, also noch vor »WannaCry«, allerdings ohne großes Aufsehen und ohne großen Schaden anzurichten. Die erste Version von »Petya« wurde über einen böseartigen E-Mail-Anhang verbreitet und war eine ziemlich gewöhnliche Form von Ransomware. Die Petya-Ransomware verschlüsselt Dateien und verlangt für die Freigabe der Dateien ein Lösegeld in Bitcoin.

Hinweis: Das Lösegeld sollte niemals gezahlt werden. Man sollte lieber über ein gutes und funktionierendes Backup-Konzept nachdenken und es auch umsetzen.

Dank EternalBlue und dem unglücklichen Erfolg von »WannaCry« erhielt die Petya-Ransomware eine zweite Chance auf Zerstörung. Im Juni 2017 wurde »NotPetya« unter Verwendung des EternalBlue-Exploits eingesetzt und dieses Mal wurde »Petya« deutlichst bemerkt.

Der Hauptunterschied zwischen der ersten und zweiten Version von »Petya« bestand darin, dass »NotPetya« (Petya V2) darauf abzielte, ein System vollständig zu deaktivieren. Egal ob das Lösegeld gezahlt wurde oder nicht, es gab keine bekannten erfolgreichen Gegenmaßnahmen durch die Betroffenen. Der Cyberangriff verschlüsselte dauerhaft die Master File Table (MFT) und den Master Boot Record (MBR) eines Computers.

Schätzungen zufolge belaufen sich die Kosten für »NotPetya« auf über 10 Milliarden US-Dollar und für »WannaCry« auf rund 4 Milliarden US-Dollar. Einige große Namen wurden ziemlich hart getroffen, darunter das Schifffahrtsunternehmen Maersk, das Kurier- und Logistikunternehmen FedEx und Merck Pharmaceuticals.

Spracheingabe unter Windows 1/3

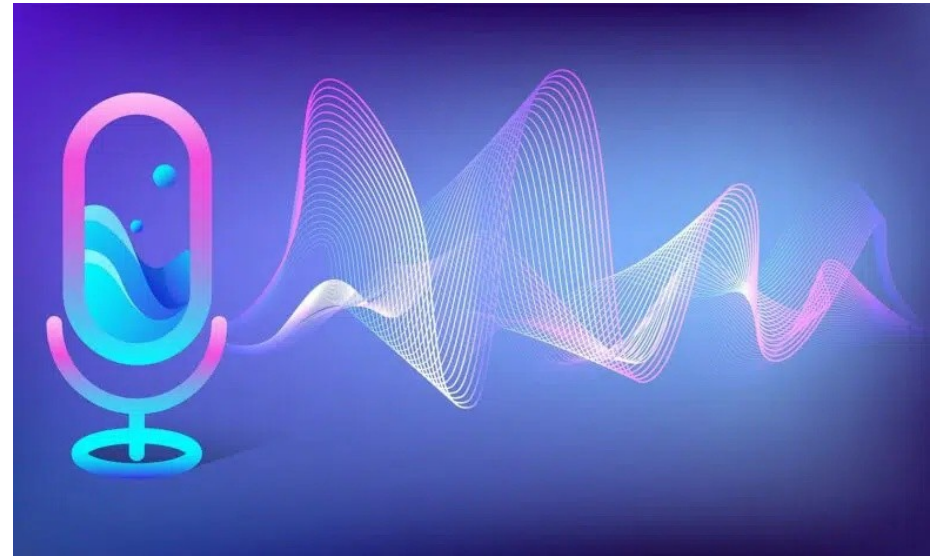
Bereits in Windows 10 hat Microsoft eine Sprachsteuerung (Voice Access) implementiert und mit dem Update auf Windows 11 22H2 noch einmal überarbeitet. Mit der Sprachsteuerung kann man nicht nur Windows-Sprachbefehle erteilen, sondern sie beinhaltet auch eine Diktierfunktion.

Spracherkennung oder Voice Access

Damit die Sprachsteuerung und Diktierfunktion in Windows funktioniert, muss man zunächst ein Mikrofon in Windows einrichten. Die dafür notwendigen Funktionen findet man in den Einstellungen unter **System -> Sound** im Bereich Eingabe. Neben dem klassischen Mikrofon an einem Headset oder als eigenständige Hardware kann man auch auf integrierte Mikrofone in Laptops oder Webcams zurückgreifen. Diese sind jedoch für die Spracherkennung nicht so gut geeignet, da Hintergrundgeräusche und die größere Entfernung zum Sprecher potenzielle Störquellen darstellen können.

Die Spracherkennung in Windows funktioniert für viele Sprachen, darunter auch Deutsch und muss zunächst aktiviert werden. Dann kann man Texte in Windows-Anwendungen diktieren, z.B. in eine Textverarbeitung wie Microsoft Word oder auch in einen der vielen kostenlosen Texteditoren. Eine weitere Funktion sind die Sprachbefehle. Mit Sprachbefehlen kann man Windows in begrenztem Umfang steuern und bestimmte Funktionen ausführen lassen.

Damit auch andere Apps auf das Mikrofon zugreifen können, muss man dies in den Datenschutzeinstellungen von Windows erlauben. Hier kann man global festlegen, ob der Zugriff auf das Mikrofon erlaubt ist und darunter für die einzelnen Apps anpassen. Für die Sprachsteuerung und das Diktieren ist eine Freigabe jedoch nicht erforderlich.



Eine weitere Voraussetzung ist die Aktivierung der Spracherkennung. Die dazu notwendige Funktion findet man in den Einstellungen von Windows 11 unter **Barrierefreiheit -> Spracherkennung**.

Um die Windows 11 Sprachsteuerung zu aktivieren, muss man den Schalter bei Windows-Spracherkennung auf »an« schalten. Sobald die Spracherkennung aktiviert ist, kann man die Spracherkennung mit der Windows-Tastenkombination **[WIN] + [STRG] + [S]** starten.

Beim ersten Aufruf startet Windows den Assistenten zur Spracherkennung, welcher einen durch den Einrichtungprozess für das Mikrofon führt. Zum Abschluss der Spracherkennung kann man die Genauigkeit der Spracherkennung noch verbessern, indem man in Windows die Spracherkennung mit einem Lernprogramm selbst trainieren kann.

Spracheingabe unter Windows 2/3

Man kann das Training aber auch auf einen späteren Zeitpunkt verlegen und das Lernprogramm überspringen. Man findet das Lernprogramm später in der klassischen **Systemsteuerung** -> **Spracherkennung** -> **Computer trainieren**.

Im letzten Schritt muss man noch den Aktivierungsmodus der Sprachsteuerung festlegen. Windows bietet einen manuellen und Stimmaktivierungsmodus.

Im manuellen Modus muss die Spracherkennung jedes Mal über die Tastenkombination **[STRG] + [WIN]** oder über das Mikrofon-Symbol in der Taskleiste erst aktiviert werden, während der stimmaktive Modus mit »**Zuhören starten**« aktiviert wird.

Windows mit Sprachbefehlen steuern

Nach Abschluss der Einrichtung wird man auf eine Microsoft-Webseite »Befehle der Windows-Spracherkennung« in Windows 10 und Windows 11 weitergeleitet. Damit ist die Einrichtung abgeschlossen.

Mit **[WIN] + [STRG] + [S]** startet oder deaktiviert man die Sprachsteuerung.

Wenn man den manuellen Modus zur Spracherkennung ausgewählt hat, sieht man ein kleines Fenster auf dem Desktop mit dem Status der Spracherkennung und man muss erst auf das Mikrofon-Symbol in den Fenster klicken oder **[STRG] + [WIN]** drücken, um die Spracherkennung zu starten.

Im Automatik-Modus sieht das Fenster dagegen etwas anders aus, erst mit dem Sprach-Befehl »**Zuhören starten**« wird die Sprachsteuerung aktiviert.

Mit dem Sprach-Befehl »**Was kann ich sagen**« erhält man eine Liste aller Befehle der Windows-Spracherkennung.

Diktatfunktion unter Windows nutzen

Wenn man die Spracherkennung aktiviert hat, steht in Windows 10 und 11 auch die Diktatfunktion zur Verfügung. Diese lässt sich mit der Tastenkombination **[WIN] + [H]** aktivieren oder auch über das Mikrofon-Symbol in der Taskleiste starten. Windows blendet dann ein Icon ein und signalisiert, dass es für das Diktat bereit ist und zuhört.

Wenn man nun mit dem Sprechen beginnt, werden die Worte in Text umgewandelt und in der aktuell geöffneten App bzw. Programm eingefügt.

Neben dem eigentlichen Text versteht die Diktatfunktion auch Befehle für das Diktieren wie **neue Zeile**, **neuer Absatz**, **Kleinschreibung WORT**, **Großschreibung WORT**, **WORT auswählen**, **Punkt**, **Komma**, **Tab** und viele Kommandos mehr (für WORT das entsprechende Wort einsetzen).

Unterschied Spracherkennung und Sprachzugriff

Der wesentliche Unterschied zwischen Sprachzugriff und Spracherkennung ist, dass der Sprachzugriff die Diktierfunktion und die Windows 11 Sprachsteuerung in einem Modul vereint. Der Sprachzugriff ist eine Neuerung in Windows 22H2 und derzeit nur in englischer Sprache verfügbar (Stand: 2023).

Spracheingabe unter Windows 3/3

Befehle der Windows-Spracherkennung

Mithilfe der Spracherkennung kann man unter Windows (Windows 10 und 11) den Computer nur mit der Stimme bedienen - ganz ohne Tastatur oder Maus.

Um die verfügbaren Sprach-Befehle zu erhalten, sagt man einfach »**Was kann ich sagen?**«.

Hinweis: Die Spracherkennung ist nicht für alle Sprachen verfügbar.

In der folgenden Tabellen bedeutet ein fett formatiertes Wort oder Ausdruck, dass es sich um ein Beispiel handelt. Der Ausdruck ist durch den entsprechenden Ausdruck zu ersetzen, um das gewünschte Ergebnis zu erhalten.

Aktion

Menü »Start« öffnen
Öffnen der Suche
Doppelklicken auf ein Element

Wechseln zu einer geöffneten App

Einfügen eines neuen Absatzes
oder einer neuen Zeile in einem
Dokument
Markieren eines Worts in einem
Dokument
Auswählen eines Worts und
Beginn der Korrektur

Sprachbefehl

Start
Windows S drücken
Doppelklick auf **Papierkorb**
Doppelklick auf **Computer**
Doppelklick auf **Dateiname**
zu Paint wechseln
zu WordPad wechseln
zu **Programmname** wechseln
Anwendung wechseln

neuer Absatz; neue Zeile

Wort auswählen

Wort korrigieren

Aktion

Markieren und Löschen
bestimmter Wörter
Aktualisieren der Liste der zurzeit
verfügbaren Sprachbefehle
Spracherkennungsmodus
aktivieren
Spracherkennungsmodus
deaktivieren
Einfügen der numerischen
Darstellung einer Zahl (z. B. 3
anstelle des Worts drei)
Platzieren des Cursors vor
einem bestimmten Wort
Platzieren des Cursors nach
einem bestimmten Wort

zum Anfang des aktuellen
Satzes wechseln
zum Ende des aktuellen Satzes
wechseln
Markieren des gesamten Texts
im aktuellen Dokument
Großschreibung des ersten
Buchstabens eines Worts
Umwandeln aller Buchstaben eines
Worts in Kleinbuchstaben
Komma schreiben
Semikolon schreiben
Punkt schreiben
Doppelpunkt schreiben
und vieles mehr [...]

Sprachbefehl

Wort löschen

Sprachbefehle aktualisieren

Zuhören starten

nicht mehr zuhören

Zahlen **Wert**

zu **Wort** wechseln

zur Position nach **Wort**
wechseln

zum Satzanfang wechseln

zum Satzende wechseln

Alle auswählen

Großschreibung **Wort**

Kleinschreibung **Wort**

Komma

Semikolon

Satzendpunkt; Punkt

Doppelpunkt

Was ist eine Lootbox?

Als Lootboxen (virtueller Behälter oder virtuelle Schatzkiste) werden virtuelle Kisten in Computer-, Konsolen- oder App-Spielen bezeichnet, die verschiedene zufällige virtuelle Gegenstände enthalten. Der Spieler erhält die Lootboxen kostenlos, kann diese aber auch finden oder erhält sie geschenkt. In vielen Spielen wird dem Spieler angeboten, weitere Lootboxen gegen echtes Geld zu kaufen.

Hinweis: Der Kauf kann dabei durch eine Spielwährung oder Echtgeld stattfinden, meistens aber muss die Spielwährung wiederum mit Echtgeld gekauft werden.

Das Wort »Lootbox« setzt sich aus dem englischen Substantiv für Beute »Loot« und für Kiste »box« zusammen. Eine Lootbox ist dementsprechend eine Beutekiste, mit unbestimmten Inhalt.

Sie können kosmetische Gegenstände beinhalten, die das Aussehen des Avatars des Spieler, seiner Rüstung oder Kleidung verändern. Sie können aber auch Gegenstände beinhalten, die den Spielverlauf zu Gunsten des Spielers beeinflussen. Dies können mehr Rohstoffe, bessere Waffen, stärkere Rüstungen, mehr Energie oder Beschleunigung von Produktionsprozessen sein.

Warum sind »Lootboxen« in die Kritik geraten?

- Lootboxen stehen in der Kritik Spieler zu verführen, Geld für Lootboxen auszugeben in der Hoffnung das in der Lootbox gewünschte, seltene oder besondere Gegenstände enthalten sind.
- Entwicklern wird vorgeworfen, dass Lootboxen Gegenstände enthalten, die durch den eigentlichen Spielverlauf nicht



erworben werden können. Durch den Kauf erlangen die Käufer der Lootboxen ein deutlichen Vorteil gegenüber den Nicht-Käufern (Pay2Win). Die ungleiche Ausgangslage entscheidet nun über Sieg oder Niederlage und nicht mehr das Können oder das taktische Geschick der Spieler.

- Lootboxen werden auch kritisiert, weil sie dafür sorgen, dass ein eigentliches kostenloses Spiel durch kostenpflichtig erwerbbarer Lootboxen zu einem teuren Spaß werden kann.
- Lootboxen wird ein Suchtpotential vorgeworfen, da es sich bei ihrer Mechanik, um Glücksspiel handeln soll. Laut Kritikern wecken Lootboxen falsche Hoffnungen und motivieren Spieler weitere Lootboxen zu öffnen.

Reaktionen von Gesetzgebern (Info-Stand: 2024)

Spieleentwickler machen durch Lootboxen normalerweise zusätzlichen Profit. Lootboxen sind allerdings ein Glücksspiel und die Spieleentwickler werden dafür kritisiert, durch deren Implementation Spielsucht auszulösen und die Spieler finanziell auszunutzen. In manchen EU-Staaten wurden Lootboxen in den letzten Jahren daher gesetzlich reguliert, allerdings noch nicht in Deutschland.

Deutschland: Im bayrischen Landtag wurde ein Antrag eingebracht, um das Mindestalter für ein Lootboxen-Spiel auf 18 Jahre heraufzusetzen. Der Antrag wurde abgelehnt, erhielt aber Zuspruch von einigen Parteien.

Deutschland: Die USK (Unterhaltungssoftware Selbstkontrolle) fordert, dass Eltern sich mit dem Thema auseinandersetzen und ihre Kinder darüber aufklären. **Hinweis:** Eltern können den Kauf von Zusatzinhalten kontrollieren, indem sie den Kauf systemweit deaktivieren oder keine Zahlungsdaten hinterlegen. Käufe von Kindern ohne Zustimmung der Eltern können oft auch rückabgewickelt werden. Info von game (Verband der deutschen Games-Branche) - 2024

Belgien: Die belgische Glücksspiel-Kommission sieht in Lootboxen einen Verstoß gegen das Glücksspielgesetz und fordert ein EU-weites Verbot. Unter anderem begründet der belgische Justizminister Koen Geens seine Forderung damit, dass die Mischung - aus dem Spielen eines Spiels und der Möglichkeit Glücksspiel zu betreiben, gefährlich für die psychische Gesundheit von jungen Menschen sei.

Vereinigtes Königreich: Die britische Glücksspiel-Behörde (UK Gambling Commission) sprach sich dagegen aus, Lootboxen mit

Glücksspiel gleichzusetzen und äußerte sich, dass sie nicht unter das britische Glücksspiel-Gesetz fallen. Die Behörde begründet ihre Entscheidung damit, dass die gewonnenen Preise nur im Spiel selbst eingesetzt werden können und keine Möglichkeit auf Auszahlung besteht. **Hinweis:** Das Unterhaus im Vereinigten Königreich **forderte** im September 2019, dass Lootboxen als Glücksspiel eingestuft werden sollen.

Niederlande: Auch die niederländische Glücksspiel-Behörde kam mit Hilfe einer Studie zu dem Ergebnis, vier von zehn Spielen mit Lootboxen verstießen gegen das Glücksspielgesetz. Kommt es zu keiner Änderung des Geschäftsmodells ist es der Behörde gestattet, Strafen oder Verbote zu verhängen. Über die genauen Namen der Spiele gibt die Behörde keine Auskunft. Jedoch sind die Kriterien einer Beurteilung, ob es sich um einen Gesetzesverstoß handelt, genau festgelegt.

USA: In den USA gibt es derzeit keine einheitliche Regelung bezüglich Lootboxen. Einige Bundesstaaten, wie Kalifornien und Washington, haben jedoch Untersuchungen durchgeführt, um festzustellen, ob Lootboxen als Glücksspiel betrachtet werden sollten.

China: Der chinesische Kulturminister legte fest, dass Lootboxen reguliert werden sollen. Entwickler sollen genaue Informationen über die Lootboxen veröffentlichen. Diese Informationen sind unter anderem: der Name der Box, Inhalt der Box, Besitzer, Menge der Gegenstände und Chancen auf bestimmte Gegenstände.

Fazit: Die Debatte um Lootboxen und das Glücksspielrecht ist nach wie vor aktuell und es ist unklar, in welche Richtung sich die rechtlichen Rahmenbedingungen entwickeln werden.

Die Spine-Leaf-Architektur ist eine moderne Netzwerk-Architektur für Datacenter und soll die Engpässe der klassischen Rechenzentrumsarchitektur, zum Beispiel lange Umschaltzeiten und komplexe Verwaltung, neutralisieren.

In Datacenter nimmt bereits seit geraumer Zeit die Zahl der virtualisierten Applikationen zu. Dieser Trend erhöht den Bedarf an leistungsstarken Gigabit-Ethernet-Verbindungen.

Während früher das Verhältnis der extern und intern gerouteten Verbindungen bei vier zu eins lag, hat sich das Verhältnis heute längst umgekehrt. Auf Grund der hohen Nutzung von Plattform-Virtualisierungen kommen auf eine externe Verbindung vier interne Verbindungen. Das hat die logische Konsequenz, dass ein wesentlicher Anteil des Datenflusses in Zukunft innerhalb eines Datacenter zwischen virtuellen Servern ablaufen wird.

Netzwerk-Topologien auf dem Prüfstand

IT-Infrastruktur-Planer müssen nun handeln und ihre Routing-Strategien und Netzwerk-Topologien an die aktuellen Trends anpassen. Übrigens, unter einer Topologie versteht man die Art und Weise wie Netzwerkgeräte miteinander verbunden sind und wie die Hosts untereinander kommunizieren. Eine herkömmliche Netzwerk-Topologie besteht in der Regel aus drei Schichten:

- Core-Layer (Kernschicht): In dieser Ebene sind die Aggregations-Switches miteinander verbunden (Aggregation ... Gruppierung, Anhäufung, Zusammenballung). Zugleich wird mit Netzwerken außerhalb des Rechenzentrums kommuniziert.
- Aggregation-Layer (Aggregationsschicht) oder Distribution-Layer: Auf dieser Ebene kommunizieren die Zugriffs-Switches miteinander.
- Access-Layer (Zugriffsschicht): Über diese Ebene haben sich die Benutzer mit dem Netzwerk verbunden.



Die Zugriffsschicht ist mit der Aggregationsschicht redundant verbunden sowie auch mit der Kernschicht. Die Aggregationsschicht verbindet angrenzende Access-Layer-Switches und Datacenter-Reihen. Die Kernschicht sorgt für Routing-Services zu anderen Teilen des Rechenzentrums sowie auch zu solchen, die außerhalb verortet sind. Damit sind das Internet oder andere Außenstellen gemeint.

Eine solche klassische Client-Server-Topologie wird auch als North-to-South-Routing bezeichnet. Das bedeutet, der North-South-Traffic fließt in einem Routing-Modell erst nach unten und dann wieder nach oben. Der Datenverkehr wird absichtlich von den Verbindungsknoten fern gehalten.

Was die Skalierbarkeit angeht, so ist diese traditionelle dreischichtige Router-Architektur durchaus praxistauglich. Jedoch können sich leicht »Flaschenhälse« (Latenzen) zwischen den beschriebenen Ebenen bilden. Solche Engpässe können auch durch redundante Links entstehen, sofern sie verwendet werden. Kein Wunder, denn dieses vertikale Routing-Schema wurde in der Vergangenheit für ein externes Routing konzipiert.

Spine-Leaf-Architektur als Lösungsansatz

Da eine zunehmende Verbreiterung von virtualisierten Servern in horizontale Routing-Verbindungen erfordert, ist es angezeigt, dass die Rechenzentrums-Planer auf eine andere Router-Topologie umstellen und die Datenlaufzeit optimieren. Das heißt, an die Stelle der herkömmlichen Topologie tritt idealerweise eine Spine-Leaf-Architektur (spine ... Rückgrat, leaf ... Blatt, Laubblatt).

Damit also die Zwischenebenen wie bei der klassischen Aggregationsschicht wegfallen, müssen die Router direkt über eine vernetzte Kreuzverbindung angebunden werden. Für eine solche Topologie hat sich der Name East-to-West-Routing durchgesetzt. Bei einem East-West-Traffic verteilen sich also die Netzwerk-Segmente auf mehrere Zugriffs-Switches und die Hosts müssen Verbindungsknoten passieren - im Gegensatz zum North-South-Traffic.

Das Strukturmodell einer Spine-Leaf-Architektur sieht dann folgendermaßen aus: Core-Layer, Spine-Layer und Leaf-Layer. An der oberen Ebene ist der Core-Layer und der Leaf-Layer bildet die untere Ebene. Wobei hier der Leaf-Layer dem Access-Layer entspricht und daran die Server und Speichereinheiten angeschlossen sind.

Das Entscheidende: Die Leaf-Switches sind eng verflochten und mit den Spine-Switches verbunden. Diese Verflechtung soll garantieren, dass zwischen den Leaf- beziehungsweise Access-Switches nicht mehr als ein Hop (Weg von einem Netzknoten zum nächsten Netzknoten) besteht. Daraus resultiert eine deutliche Reduktion der Latenzzeit. Engpässe zwischen den Leaf-Switches bzw. Access-Switches treten nun nicht oder nur ganz selten auf.

Spine-Leaf-Topologie ist Standard

In den Designs der Portfolios von Netzanbietern findet man heute meist nur noch Leaf-Spine. Da die beiden Schichten, Zugriff und Aggregation erweitert sind, kann ein Host mit einem anderen über jeden beliebigen Leaf-Switch in Verbindung treten. Zudem weiß man immer, dass der Datenverkehr nur über den Eingangs-Leaf-Switch, den Spine-Switch und den Ausgangs-Leaf-Switch fließt.

Auf diese Weise kann das Verhalten von Anwendungen vorhergesagt werden. Im Falle von mehreren Multi-Tiered-Webanwendungen (tiered ... abgestuft) ist das von entscheidender Bedeutung. Das gilt zum Beispiel auch für High-Performance-Computing-Cluster und Hochfrequenz-Handel.

Der prinzipielle Aufbau der Spine-Leaf-Architektur

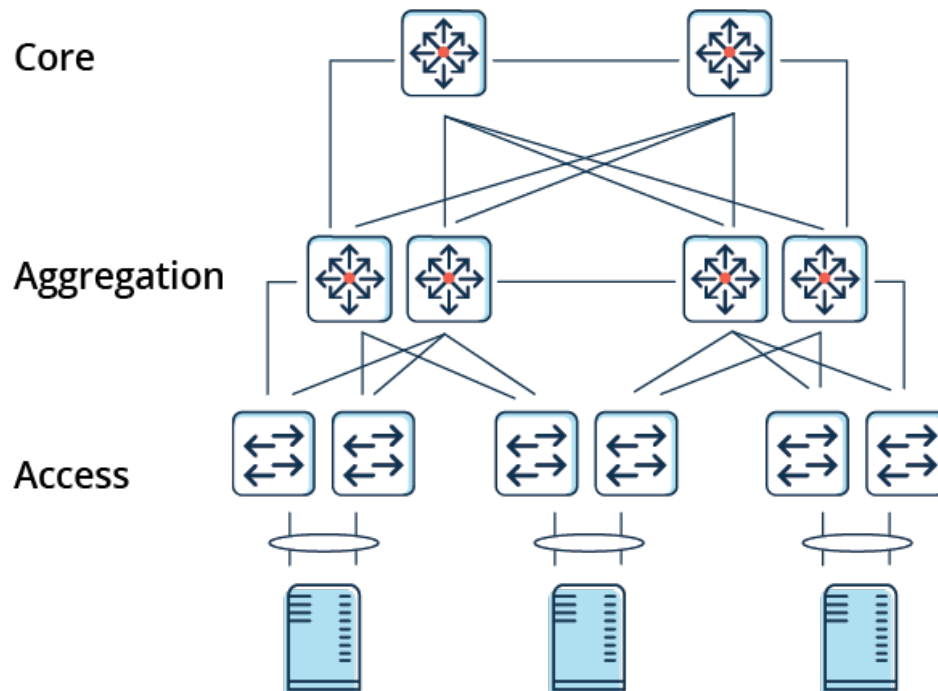
An den Switches der Leaf-Ebene (Access-Layer) sind beispielsweise Server oder Datenspeicher angeschlossen. Da jeder Leaf-Switch eine Verbindung zu jedem Spine-Switch besitzt, ist sichergestellt, dass in die Kommunikation von einem Endpunkt zum anderen Endpunkt maximal ein Spine-Switch involviert ist. Sind beide Endpunkte am gleichen Leaf-Switch angeschlossen, bleibt der Verkehr vollständig innerhalb der Leaf-Ebene.

An den Spine-Switches selbst befinden sich keine Access-Geräte. Sie sind für das schnelle Switching der Daten zwischen den Leaf-Switches zuständig. Die Spine-Switches sind dafür optimiert und zeichnen sich durch eine hohe Switching-Leistung aus. Ist eine Core-Ebene an die Spine-Ebene angeschlossen, übernimmt diese unter anderem die Aufgabe, den Traffic zu fremden Rechenzentren oder in das Internet zu leiten.

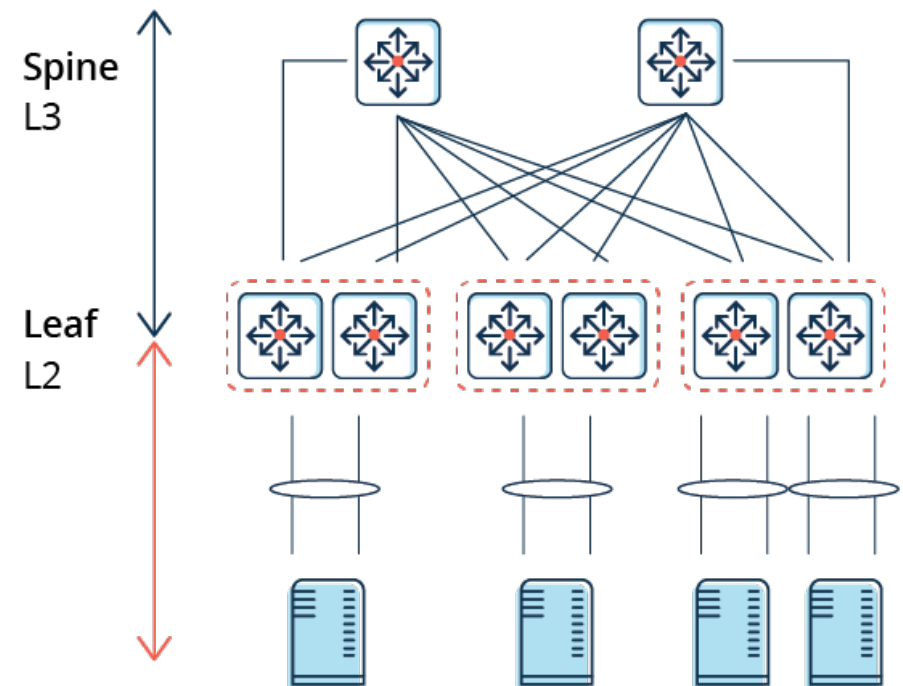
Die Spine-Leaf-Architektur kommt in modernen Rechenzentren zum Einsatz. Sie stellt eine Alternative zu herkömmlichen Netzwerk-Topologien mit Core-, Aggregation- und Access-Ebene dar. In der Spine-Leaf-Architektur sind die Leaf-Switches mit den Spine-Switches vollvermascht.

Die Spine-Leaf-Architektur besteht aus den beiden Ebenen der Leaf- und der Spine-Switches. Je nach Realisierung kann noch eine dritte Ebene, die Core-Ebene, hinzukommen. Ist keine Core-Ebene vorhanden, bilden die Spine-Switches das Core des Netzwerks. Die Leaf-Switches stellen die Access-Schicht dar. Sie sind voll mit den Spine-Switches vermascht. Jeder Leaf-Switch besitzt eine eigene Verbindung zu jedem Spine-Switch.

Traditional 3-Tier Architecture



2-Tier Spine-Leaf Architecture



Switching und Routing in der Spine-Leaf-Architektur

Grundsätzlich sind Spine-Leaf-Architekturen auf dem Layer 2 (Switching) oder dem Layer 3 (Routing) realisierbar. Die Links zwischen der Spine- und der Leaf-Ebene können daher geroutet oder geschwitcht sein. Im Gegensatz zu einfachen Spanning-Tree-Topologien (spanning tree ... aufspannender Baum), in denen einzelne Verbindungen zur Vermeidung von Netzwerkschleifen keine Daten übertragen und sich in einem logischen Blockier-Status befinden, sind in der Spine-Leaf-Architektur alle Verbindungen weiterleitend. Der Spanning-Tree-Algorithmus ist hier durch andere Algorithmen wie das Shortest Path Bridging (SPB) ersetzt.

Ein weiterer Layer-2-Algorithmus, der häufig in Spine-Leaf-Architekturen zum Einsatz kommt, ist TRILL (Transparent Interconnection of Lots of Links). Beide Protokolle (SPB, TRILL) sorgen in einer geschwitchten Umgebung dafür, dass die Endpunkte schleifenfrei auf dem jeweils kürzesten Weg erreichbar sind. Sie verwenden für die Wegberechnung das so genannte Shortest Path First Computing. Das **Spanning-Tree-Protokoll** (STP) ist für die Spine-Leaf-Architektur **ungeeignet**, da es keine parallelen Pfade berücksichtigen kann.

Die Kapazität wird der Spine-Leaf-Architektur ebenfalls verbessert, da STP nicht mehr benötigt wird. STP ermöglicht zwar redundante Pfade zwischen zwei Switches, es kann jedoch niemals mehr als ein Pfad aktiv sein. So kommt es, dass Pfade häufig überzeichnet werden. Umgekehrt bauen Spine-Leaf-Architekturen auf Protokolle wie ECMP-Routing (Equal-Cost-Multipath-Routing), um den Verkehr auf allen verfügbaren Pfaden auszugleichen und gleichzeitig noch Netzwerk-Loops, Schleifen zu vermeiden.

TRILL und SPB ermöglichen die intelligente Wegfindung und sorgen für die benötigte Performance. Sowohl TRILL als auch SPB

können im Gegensatz zum Spanning-Tree-Protokoll Multipfade und eine größere Anzahl von Netzknoten bedienen. SPB ist im IEEE-Standard 802.1aq definiert. Die Spezifizierung von TRILL ist im RFC 6326 der IETF zu finden.

Eine **vollständige** Layer-3-Spine-Leaf-Architektur routet jeden Link. Hierfür kommen Routing-Protokolle der Schicht 3 wie OSPF (Open Shortest Path First) zum Einsatz. Sie finden ebenfalls den kürzesten Weg zum Ziel und verhindern die Bildung von Routing-Schleifen.

Vor- und Nachteile der Spine-Leaf-Architektur

Gegenüber Strukturen mit Core-, Aggregation- und Access-Layer oder einfachen Hub-and-Spoke-Architekturen bietet die Spine-Leaf-Architektur eine Vielzahl von Vorteilen. Die Vollvermaschung der Leaf-Switches mit den Spine-Switches stellt sicher, dass zwischen beiden Ebenen nicht mehr als ein Hop (Weg von einem Netzknoten zum nächsten Netzknoten) besteht. Dies sorgt für kurze, genau vorhersagbare Latenzzeiten. Gleichzeitig minimiert sich die Wahrscheinlichkeit für Engpässe zwischen der Spine- und Leaf-Ebene, da eine Vielzahl paralleler Verbindungen vorhanden sind und jeder Leaf-Switch seine exklusive Leitung zu jedem Spine-Switch nutzen kann.

Ein weiterer Vorteil dieser Architektur ist die hohe Redundanz. Fällt eine Verbindung aus, stehen weitere Möglichkeiten zur Verfügung, das gewünschte Ziel zu erreichen. Intelligente Link- oder Routing-Protokolle wie SPB, TRILL oder OSPF sorgen dafür, dass die jeweils kürzeste, schleifenfreie Verbindung automatisch berechnet und bereitgestellt werden kann.

Spine-Leaf-Architekturen können im Gegensatz zu Strukturen mit Core-, Aggregation- und Access-Layer, die überwiegend für den so genannten Nord-Süd-Verkehr ausgelegt sind, auch Querverkehr

(Ost-West-Verkehr) sehr performant und ohne Engstellen (Flaschenhälse) bedienen. Neue Knoten lassen sich ohne Veränderung der existierenden Topologie einbinden. Es müssen lediglich die vollvermaschten Verbindungen für die neuen Knoten bereitgestellt werden. Die Architektur ist bis zu einer gewissen Größe gut skalierbar. Allerdings wächst die Anzahl der benötigten Verbindungen mit der Zunahme an Switches sehr stark. Wird beispielsweise nur ein einzelner Spine-Switch hinzugefügt, muss für jeden Leaf-Switch ein neuer Link bereitgestellt werden.

Im WAN-Umfeld sind Spine-Leaf-Architekturen eher unüblich, da der Aufwand und die Kosten für die Vollvermaschung der beiden Netzebenen zu groß sind. Zur Anbindung von WAN-Außenstellen kommt meist eine einfache, sternförmige Hub-and-Spoke-Architektur zum Einsatz.

Gegenüberstellung von Spine-Leaf-Architektur und Hub-and-Spoke-Architektur

Eine einfache Hub-and-Spoke-Architektur ist für die Verbindung von Switches untereinander in einem Datacenter unüblich. Lediglich die Anbindung von Endgeräten an einen Leaf-Switch (Access-Switch) weist eine Hub-and-Spoke-Architektur auf. Obwohl es sich logisch gesehen um eine Ethernet-Bus-Architektur handelt, ist jedes Endgerät sternförmig mit einem einzigen Link an den Switch angebunden. Bei der Kommunikation des Endgeräts mit einem zentralen Service oder mit einem anderen Endgerät ist immer der eigene Switch involviert. Der Begriff Hub (Nabe, Radnabe) steht in diesem Fall für den Switch und der Begriff Spoke (Speiche, Radspeiche) für die Verbindung zum Endgerät.

Verbindet man Switches untereinander per Hub-and-Spoke-Architektur über einen zentralen Switch, entstehen Engpässe sobald Datenverkehr zwischen den äußeren Switches auftritt, da

sämtlicher Traffic über den zentralen Switch geführt werden muss. Zudem stehen im Gegensatz zur Spine-Leaf-Architektur keine redundanten Verbindungen zur Verfügung. Typische Anwendungsbereiche für Hub-and-Spoke-Architekturen sind Filialnetze oder VPN-Anbindungen. In einem Filialnetz sind Außenstellen sternförmig über jeweils eine WAN-Verbindung an eine Zentrale angebunden. Sämtlicher Verkehr, auch der zwischen Filialen, muss immer über die Zentrale geführt werden. VPN-Netze bilden auf beliebigen Netzstrukturen eine logische Hub-and-Spoke-Architektur und führen ebenfalls sämtlichen Traffic über den zentralen VPN-Punkt.

Zusätzlich zu der höheren Leistung, bietet die Spine-Leaf-Architektur eine bessere Skalierbarkeit. Es können weitere Spine-Switches hinzugefügt und mit jedem Leaf-Switch verbunden werden, wodurch die Kapazität noch weiter erhöht wird. Genauso können neue Leaf-Switches nahtlos eingefügt werden, wenn die Port-Dichte problematisch wird. In beiden Fällen muss für diese Ausbreitung der Infrastruktur (Scale-Out) das Netzwerk nicht erst neu gestaltet werden und es entstehen dabei auch keine Ausfälle.

Die Hub-and-Spoke-Architektur eines Netzwerks hat die Form eines Sterns. Die verschiedenen Kommunikationsendpunkte (Spokes) sind jeweils mit einer Netzwerkverbindung mit dem zentralen Netzwerkknoten, dem Hub, verbunden. Sämtlicher Netzwerkverkehr fließt über den Hub.

Die Hub-and-Spoke-Architektur eines Netzwerks erinnert an den Aufbau eines Rads mit Speichen (Spokes) und Nabe (Hub). Die einzelnen Endpunkte des Netzes sind sternförmig über jeweils genau eine Netzwerkverbindung mit dem zentralen Netzwerkknoten verbunden. Möchten einzelne Endpunkte miteinander kommunizieren, werden die Daten zunächst an den zentralen Knoten und dann weiter zum Endpunkt übermittelt. Es existieren keine direkten Verbindungen zwischen den einzelnen Endpunkten. Der Hub ist zentraler Knoten im Netzwerk und an jeglicher Kommunikation beteiligt. Ohne den Hub ist kein Datenaustausch möglich. Die Anzahl benötigter Leitungen lässt sich in einem Hub-and-Spoke-Netz sehr einfach bestimmen. Sie entspricht der Anzahl der zu verbindenden Endpunkte (ohne den zentralen Hub).

Hub-and-Spoke-Architekturen kommen sowohl im Local Area Network (LAN) als auch im Wide Area Network (WAN) zum Einsatz. Zusätzlich ist eine Unterscheidung zwischen physischen und logischen Hub-and-Spoke-Architekturen möglich. Beispielsweise lässt sich auf einem physisch voll- oder teilvermaschten Netzwerk ein logisches Hub-and-Spoke-Netzwerk realisieren.

Typisch ist die Hub-and-Spoke-Architektur für kleinere geschaltete LAN-Umgebungen mit einem einzelnen Switch, bei denen die Endgeräte mit Hilfe von Twisted-Pair-Kabeln alle mit dem zentralen Switch verbunden sind. Obwohl das LAN logisch gesehen eine Bus-Struktur hat, handelt es sich physisch um eine Stern-Struktur. Größere LANs mit vielen Switchen verwenden für die Vernetzung

der Switches untereinander andere Architekturkonzepte wie beispielsweise die Spine-Leaf-Architektur.

Drahtlose Netzwerke wie das WLAN verwenden ebenfalls häufig die Hub-and-Spoke-Architektur. Endgeräte sind dabei per Funk mit einem zentralen WLAN-Router oder WLAN-Accesspoint verbunden, der den kompletten Verkehr steuert. Weitere Beispiele für Hub-and-Spoke-Netzwerke sind Telefonanlagen mit ihren einzeln angeschlossenen Telefonen oder mobile Funkzellen mit ihren angemeldeten Mobiltelefonen.

Andere Netzwerkarchitekturen sind teilvermaschte, vollvermaschte, ringartige und baumartige Netzwerke oder Bus-Strukturen.

Physische und logische Hub-and-Spoke-Architekturen

In Netzwerken ist es wichtig, eine Unterscheidung zwischen logischer und physischer Architektur zu treffen. Die physische Architektur bezieht sich auf die tatsächlich vorhandenen Verbindungen zwischen zwei Netzknoten. Existiert beispielsweise ein zentraler Switch, an den alle Endgeräte per Kabel angeschlossen sind, handelt es sich um eine physische Stern- oder Hub-and-Spoke-Topologie.

Logische Architekturen beziehen sich auf die Kommunikationsströme höherer Schichten. So lassen sich beispielsweise auf einem voll- oder teilvermaschten Netzwerk, in dem einzelne Netzknoten physisch auch untereinander verbunden sind, völlig andere logische Topologien einrichten. Das Routing kann so konfiguriert sein, dass trotz einer direkten physischen Verbindung zwischen den Kommunikationspartnern A und B sämtlicher Verkehr über einen zentralen Router C fließen muss.

Logische Hub-and-Spoke-Architekturen sind häufig bei VPN-

Verbindungen im Internet vorzufinden. Filialen oder einzelne Rechner bauen dabei über das Internet einen verschlüsselten Tunnel zu einem zentralen VPN-Punkt auf. Obwohl im Internet andere Kommunikationswege zwischen den einzelnen Filialen oder Rechnern existieren, wird der komplette Datenverkehr grundsätzlich über den VPN-Tunnel zur Zentrale transportiert und erst von dort zum Ziel. Möchten Filialen oder Rechner untereinander kommunizieren, ist immer die VPN-Zentrale involviert.

Vor- und Nachteile der Hub-and-Spoke-Architektur

Einer der wichtigsten Vorteile der Hub-and-Spoke-Architektur ist, dass das Netzwerk eine sehr einfache und übersichtliche Struktur hat. Jeder Endknoten besitzt genau eine Verbindung zum zentralen Knotenpunkt. Weitere Verbindungen existieren nicht. Um mit der Zentrale Daten auszutauschen, ist eine Verbindung zu verwenden. Möchten zwei Endknoten miteinander Daten austauschen, sind zwei Verbindungen involviert. Übertragungszeiten lassen sich sehr gut abschätzen und **Störungen sind schnell eingegrenzt** und gefunden.

Im Vergleich zu teil- oder vollvermaschten Netzen sind weniger Verbindungen notwendig. Dies ist besonders im WAN vorteilhaft, da lange Datenverbindungen sehr kostspielig sein können. Vorteilhaft kann eine Hub-and-Spoke-Topologie aus Security-Sicht sein. Da der komplette Verkehr über den zentralen Hub geführt wird, kann er dort sehr gut kontrolliert, überwacht oder ver- bzw. entschlüsselt werden.

Eines der Hauptprobleme der Hub-and-Spoke-Architektur ist die fehlende Redundanz im Netzwerk. Fällt der zentrale Hub aus, ist das ganze Netzwerk gestört. Kein Endpunkt kann mehr kommunizieren. Bei einem Ausfall einer Verbindung von einem

Endknoten zum Hub ist die komplette Kommunikation für diesen Endknoten gestört. Alternative Leitungswege existieren nicht. Möchten man sich gegen Ausfälle absichern, sind die zentralen Knoten und die einzelnen Verbindungen mehrfach bereitzustellen. Große, komplexe Netzwerke mit mehreren zentralen Kommunikationspunkten lassen sich mit einfachen Sternstrukturen nicht abbilden. Hier müssen andere Topologien wie teilvermaschte Strukturen zum Einsatz kommen.

Die Hub-and-Spoke-Architektur im WAN

Die Hub-and-Spoke-Architektur ist im WAN-Bereich typisch für Filialnetze. Einzelne Filialen oder Außenstellen eines Unternehmens sind über eine WAN-Verbindung an die Zentrale oder die Hauptstelle angebunden. Je nach Entfernung der Filiale zur Zentrale kann die WAN-Verbindung unterschiedliche Längen haben. Grundsätzlich erhält man aber ein Sternnetz. Außenstellen können nicht direkt miteinander Daten austauschen, sondern müssen immer den Weg über die Zentrale wählen. Da in der Regel die für die Arbeit benötigten Anwendungen in der Zentrale gehostet sind, ist der überwiegende Traffic auch auf den Datenleitungen zur Zentrale zu vermuten. Für moderne Kommunikationsprotokolle wie Voice over IP (VoIP), bei denen Endgeräte Sprachdaten nach dem Verbindungsaufbau direkt untereinander austauschen, ist die Hub-and-Spoke-Architektur nachteilig.

Gegenüberstellung der Hub-and-Spoke-Architektur und der Spine-Leaf-Architektur

Zur Verbindung von Switches untereinander in großen modernen LAN-Umgebungen kommt in der Regel keine Hub-and-Spoke-Architektur zum Einsatz. In diesem Bereich hat sich die so genannte Spine-Leaf-Architektur durchgesetzt. Meist besteht das Spine-Leaf-Modell aus zwei oder drei Ebenen. Dies sind in dreischichtigen Modellen die Core-Ebene, die Spine-Ebene und die Leaf-Ebene und

in zweischichtigen Modellen die Spine- und die Leaf-Ebene. Über die Leaf-Ebene erfolgt der Anschluss der Geräte. Sie bildet den Access-Layer.

Die einzelnen Leaf-Switches (Access-Switches) sind vollvermascht mit den Switches der Spine-Ebene verbunden. Über die Spine-Ebene gelangen die Daten direkt zu anderen Leaf-Switches. In Modellen mit einer zusätzlichen Core-Ebene können die Core-Switches das zentrale Switching oder Routing übernehmen. Die Core- oder Leaf-Ebene ist zuständig für die Verbindung zu anderen Rechenzentren oder anderen Netzwerken wie beispielsweise dem Internet.

Die Vollvermaschung stellt sicher, dass jeder Access-Switch Daten genau über einen Hop zu einem Spine-Switch senden kann. Latenzzeiten werden minimiert und unnötige Hops vermieden. Fällt eine einzelne Verbindung aus, sind weitere redundante Wege vorhanden, auf denen Daten gesendet werden können.

Die Spine-Leaf-Architektur bietet gegenüber einfachen Hub-and-Spoke-Topologien eine Vielzahl von Vorteilen. Sie ist wesentlich performanter und ausfallsicherer. Im Gegensatz zur Hub-and-Spoke-Architektur ist sie nicht nur für Verkehr von und zu zentralen oder externen Anwendungen, sondern auch sehr gut für Querverkehr der Endpunkte untereinander geeignet. Dies kommt modernen **virtualisierten** Rechenzentren sehr entgegen.

Was ist ein Metaversum oder ein Leben in einer virtuellen Parallelwelt?

Eine eindeutige Definition des Metaversum oder Metaverse existiert derzeit nicht. Vielmehr gibt es Diskussionen, was das Metaverse sein könnte, was es nicht ist, was es sein sollte bzw. sein muss und was zum zu ihm gehört.

Das Metaversum ist eine Verknüpfung aus der realen und den virtuellen Welten (ein betretbares Internet). Es ist also ein virtueller Ort, an dem sich reale Menschen begegnen, um dort miteinander zu interagieren. Diese Erweiterung der realen Welt ist darauf ausgelegt, dass die Teilnehmer physisch in die virtuelle Welt eintauchen können.

Gleichzeitig ist es durchaus denkbar, an realen Ereignissen über die virtuelle Welt hinweg in Echtzeit teilzuhaben. Das macht das Metaversum in vielen Bereichen zu einer wichtigen Grundlage für die persönliche, ortsunabhängige Weiterbildung. Die physische Welt wird demnach in eine digitale transferiert, in der wir uns frei bewegen können.

Der wichtigste Aspekt des Metaversum ist die Interaktion mehrerer Teilnehmer innerhalb des virtuellen Raums.

Merkmale des Metaverse

Folgende Eigenschaften und Merkmale eines Metaverse lassen sich heute bereits definieren:

- in Echtzeit gerenderte, nicht begrenzte, persistente, beständige 3D-Räume, in denen sich Nutzer als Avatare frei bewegen
- kollektive 3D-Räume, in denen Nutzer erkunden, gestalten, spielen, arbeiten, soziale Kontakte knüpfen und Geschäfte führen, ohne sich im selben physischen Raum zu befinden



- Firmen »besitzen« das Metaverse nicht, da es sich um eine kollektiv geteilte technische Infrastruktur handelt
- Geräte- und systemübergreifende virtuelle Räume lassen sich von Nutzern erschaffen und für andere Nutzer zugänglich machen
- Extended- und Mixed-Reality-Technologien kommen zum Einsatz und ermöglichen Interaktionen zwischen digitalen und realen Räumen, z. B. VR-Brillen, Digital Assistants, Smart/Voice User Interfaces (VUI), neurale Chips, Machine Learning, künstliche Intelligenzen und künstliche neuronale Netzwerke
- kompatible virtuelle und reale Währungen bilden eine einheitliche Ökonomie für digitale und physische Räume
- eine Totalität von virtuellen und physischen Räumen setzt kompatible technische Standards, Protokolle, Interoperabilität, digitalen Besitz, Blockchain-Technologien und einheitliche Gesetzgebungen voraus

Metaverse: Woher kommt die Idee?

Der Begriff Metaverse taucht erstmals 1992 in Neal Stephenson's Roman »Snow Crash« auf, die Idee ist jedoch deutlich älter. In dem Roman »Snow Crash« agieren Menschen durch programmierte Avatare miteinander. »Meta« steht dabei für jenseits und »verse« für Universum.

Die Verschmelzung und Interaktion der Realität mit virtuellen 3D-Räumen findet sich auch im Cyberpunk-Genre der 1980er-Jahre ebenso wie in modernen Film-Interpretationen wie »The Matrix« (1999) und »Ready Player One« (2018) wieder.

Metaversum und seine Möglichkeiten

Das Metaversum bietet nicht nur Nutzern neue Möglichkeiten, virtuelle Räume zu erleben. Auch Firmen eröffnen sich neue E-Commerce-Optionen. Die Corona-Krise zeigte, wie flexibel eine vernetzte Welt auf eingeschränkte Kontakte reagieren kann, wenn sich das soziale und geschäftliche Leben ins Metaverse verlagert. Vor allem in Hinsicht auf die Live-Analyse von Nutzerdaten, Onlineshopping und Kryptowährungen wie Bitcoin eröffnet das Metaverse neue Marketing-Strategien. Dazu zählen Möglichkeiten, um Kundengruppen zu erweitern, der eigenen Marke Sichtbarkeit zu verschaffen sowie mit Kunden direkt und weltweit zu interagieren.

Metaversum als Zukunftsvision

Facebooks CEO Mark Zuckerberg (CEO: Chief Executive Officer, Geschäftsführer, oberster Leiter des operativen Geschäfts) zählt zu den stärksten Verfechtern und größten Investoren in Sachen Metaverse. 2021 kündigte er an, Facebook in den kommenden Jahren in ein Metaverse-Unternehmen zu verwandeln. Facebook stellt viele Millionen Dollar Fördermittel für die Forschung bereit, um die Entwicklung von Forschungs- und Entwicklungsprogramme

zum Metaverse voranzutreiben. Metaverse ist laut Facebook die neue »Computing-Plattform« der Zukunft. Aus diesem Grund investiert der Onlinegigant geschätzt mehrere Milliarden Dollar jährlich in die Entwicklung von Grundlagentechnologien.

Facebooks aktuell größtes Metaverse-Projekt heißt »Horizon Workrooms« und konzentriert sich auf das »Metaverse for Work«. Derzeit unterstützt »Horizon Workrooms« neue Formen hybrider Arbeitsmodelle. Horizon-Nutzer können in Form von Avataren in virtuellen Konferenzräumen mit Kollegen an anderen Orten aktiv zusammenarbeiten. Mitzudenken sind hier auch Remote-Trainingsprogramme, Weiterbildungsmöglichkeiten oder Kundenberatungen. Mit geschätzt drei Milliarden aktiven Nutzern pro Monat ist Facebook das größte Social-Media-Unternehmen der Welt. Das »Metaverse for Work« ist also nur ein erster Schritt in eine Welt, in der Nutzer im Metaversum interagieren, gestalten, spielen und kaufen, ohne einen physischen Ort zu teilen.

Wie funktioniert das Metaversum?

In das Metaversum gelangt man mit einer VR- oder AR-Brille (**VR-Brille**: virtual reality display oder VR display, **AR-Brille**: augmented reality display oder AR display). Oder auch mit dem Smartphone oder Tablet. Mit einem 3D-Avatar bewegt man sich durch die virtuelle Welt, trifft Freunde auf einen Spaziergang oder geht zu Arbeitsmeetings. Dabei ist die Schnittstelle zwischen virtueller und realer Welt ein wichtiger Faktor. Denn Gegenstände aus der echten Welt können ganz einfach eingescannt und in das Metaversum übertragen werden.

Durch das Metaversum kann es auch zu einem Paradoxon (Hybrid Work Paradoxon) kommen. Einerseits profitieren die Beschäftigten von der hybriden und flexiblen Arbeit, andererseits wünschen sie sich mehr persönliche Kontakte. Das Metaverse **kann** dazu beitragen, diese Gegensätze zusammenzuführen.

Virtueller Grunderwerb und NFT-Grundstücke im Metaverse

»Metaverse« wird als virtuelle, erweiterte Realität verstanden, die darauf abzielt, die »reale Welt« einerseits nachzubilden und andererseits zu erweitern. Das Metaverse soll nicht nur Arbeitsplatz und soziales Netzwerk sein, sondern auch ein Ort, in dem man seine Freizeit verbringen und etwaigen Aktivitäten nachgehen kann. Derzeit ist auch ein regelrechter Hype um den Erwerb von digitalen Grundstücken im Metaverse erkennbar, die insbesondere als digitaler Marktplatz und neuer Raum für Werbung dienen können.

Der Hype um das Metaverse geht auch mit dem Boom von Kryptowährungen einher, die zu Transaktionszwecken im Metaverse verwendet werden. Bitcoin und Ethereum sind als jene mit der größten Marktkapitalisierung zu nennen. Neben Kryptowährungen spielen auch NFTs, also Non-Fungible-Token, eine große Rolle, zumal Grundstücke im Metaverse als solche erworben werden.

NFTs sind Einträge in einem dezentralen Hauptbuch (distributed ledger) und nicht austauschbare Token auf Blockchain-Basis. Sie basieren auf der gleichen Technologie wie Kryptowährungen, sind im Unterschied zu diesen grundsätzlich jedoch nicht teilbar und somit einzigartig. Durch den Erwerb eines NFTs, der etwa auf ein Kunstwerk verlinkt, wird ein einzigartiger Standort auf der Ethereum-Blockchain erworben, die auf eine Textdatei im Internet verweist, die jeder einsehen kann. Innerhalb dieser Textdatei befindet sich eine weitere URL, die auf das Kunstwerk selbst verweist und für jedermann einsehbar ist. Der Kauf von Krypto-Kunst oder eines sonstigen NFTs ist daher grundsätzlich der Kauf einer Zeile in einem fälschungssicheren Hauptbuch (das auch als Transaktionsliste verstanden werden kann), die auf eine öffentlich gehostete Datei verweist.



Die Idee und der antizipierte Aufstieg des Metaverse birgt eine Vielzahl neuer Anwendungsfälle für die Blockchain-Technologie. Ein derzeit finanziell florierender Bereich betrifft Plattformen wie etwa »Decentraland« (gehört zu den NFT-Games). »Decentraland« ist eine dezentralisierte 3D-Plattform für virtuelle Realität, die aus einer Vielzahl an virtuellem »Bauland« besteht. Solch virtuelles Land in »Decentraland« basiert ganz generell auf NFTs, die mittels der Kryptowährung »MANA« erworben werden können. Vereinfacht gesagt ist »Decentraland« somit eine Plattform für den Kauf und Verkauf von virtuellem Land und Immobilien im Metaverse.

Andere bekannte Plattformen mit teils unterschiedlichen Anwendungen sind »The Sandbox« (gehört zu den NFT-Games), »Somnium Space« (gehört zu den NFT-Games), »Upland« (gehört zu den NFT-Games) und »OpenSea« (OpenSea ist eine NFT-Auktionsplattform).

Virtuelle Immobilien können in Form eines NFT mittels eines NFT-Smart-Contracts erworben werden. Smart Contracts folgen der If-Then-Else-Regel und entsprechenden Attributen über die Ethereum-Blockchain (on-chain NFT). Sobald die Zahlung abgewickelt ist, wird der NFT über eine entsprechende Plattform an den Erwerber übertragen. Schon im Rahmen dieses Schrittes können sich jedoch schon erste rechtliche Fragestellungen ergeben.

Während viele Erwerber der Ansicht sind, das »Eigentum« an einem NFT erworben zu haben, oder den NFT selbst als Eigentumsnachweis qualifizieren, so ist der NFT eher als eine Rechnung im Rahmen einer Transaktion zu verstehen. Käufer und Verkäufer interagieren miteinander und der NFT begründet die entsprechende Rechnung. Programmierseitig kann diese »Rechnung« auch an »etwas« außerhalb der Blockchain (off-chain) verlinken, etwa einer Cloud oder einem zentralisierten Hardware-Server oder eben innerhalb der Ethereum-Blockchain.

Dieses »etwas« ist in aller Regel ein einfaches Bild (.jpeg). Der NFT (die Rechnung) sagt auch nichts über die Transaktion selbst aus. Um diese beurteilen zu können, müsste man vielmehr die jeweiligen Geschäftsbedingungen des NFT-Smart-Contracts prüfen.

Weitere rechtliche Probleme können sich schon auf sachenrechtlicher Ebene ergeben. So können einem NFT selbst keine Attribute zugesprochen werden. Der faktische Erwerb ist der zwischen den ursprünglichen Parteien ausbedungene Inhalt. Der Wert des NFTs folgt demnach grundsätzlich dem Vertragsinhalt. Ein Problem ist jedoch, dass kein Vertrag zwischen dem initialen primären Käufer und den nachfolgenden sekundären Erwerbern vorliegt (sowie allen weiteren Erwerbern im Nachgang). Im weiteren liegt auch kein vertragliches Verhältnis zwischen Sekundärkäufern und dem ursprünglicher Aussteller des NFTs vor.

Es gibt nun jedoch Plattformen, die NFTs ausstellen und für die entsprechenden Verträge gewisse Rahmenbedingungen vorsehen, wie etwa, dass diese NFTs auch nur auf dieser einen Plattform verwendet werden können bzw. sollen. Sollte nun ein solcher NFT auf bzw. über eine andere Plattform vertrieben werden, so besteht das Risiko, dass die Geschäftsbedingungen nicht übertragen werden. Sofort stellt sich die Frage, wieviel der NFT nun tatsächlich (außerhalb der vertraglich vorgesehenen Plattform) wert ist und welcher (vertragliche) Inhalt nun tatsächlich mit einem NFT übertragen bzw. erworben wird.

Nun kann es sein, dass eine Plattform NFTs mit gewissen Vorteilen (perks) ausstellt, wie den Zugang zu einer bestimmten Kommunikationsplattform mit Gleichgesinnten. Die Plattforminhaber könnten nachträglich jedoch »ihre Meinung ändern« und den Zugang aus diversen Gründen entziehen. Fraglich in diesem Zusammenhang ist, ob die Geschäftsbedingungen eines jeden ausgestellten NFTs an die nächsten Erwerber übertragen werden. Sollte die Anwendbarkeit dieser Geschäftsbedingungen scheitern, etwa weil die Plattforminhaber in keinem Vertragsverhältnis mit allen nachgeschalteten Käufern stehen, dann besteht das Risiko, dass der Erwerber keine rechtliche Möglichkeit hat, seine »Rechte« gegen die Plattforminhaber durchzusetzen.

Neben konsumentenschutzrechtlichen Fragestellungen stellt sich auch die Frage im Rahmen des NFT-Erwerbs, dem keine Geschäftsbedingungen beigelegt sind, was mit dem NFT dann eigentlich erworben wird. Es besteht daher das Risiko, dass mit dem NFT nichts erworben wird. Denn ein NFT ist mit einem Hyperlink vergleichbar, wobei der zugrunde liegende Gehalt oder Inhalt sich im Laufe der Zeit durchaus ändern kann oder ab einer gewissen Transaktionsanzahl intransparent wird. Da der Grunderwerb im Metaverse über NFTs erfolgt, liegt auch in diesem

Fall ein solches Risiko vor.

Großteils wird der Grunderwerb im Metaverse jedoch aufgrund der Rückverfolgbarkeit des »Eigentums« in der Ethereum-Blockchain als relativ sicher qualifiziert, weil eine »Grundbuchstauglichkeit« (Land Register, Register of Land Titles) der on-chain Einträge angenommen wird. Es ist zu erwarten, dass in Zukunft die Möglichkeiten, Teile von NFTs (fractionalized NFTs) zu erwerben, zunehmen werden, was neue Entwicklungen und weitere rechtliche Fragestellungen im Bereich der Immobilieninvestitionen bringen könnte.

Generell gilt auch, dass das Metaverse kein rechtsfreier Raum ist. Alle geltenden Bestimmungen zum Vertragsrecht im Allgemeinen und zum Immobilienrecht im Besonderen finden auch im Metaverse Anwendung. Vor dem Kauf eines virtuellen Grundstücks ist aber jedenfalls Vorsicht geboten und die Prüfung der Geschäftsbedingungen der jeweiligen Plattform ratsam.

Viele Millionen Dollar für virtuelles Land (Info-Stand: 2021)

Der Weg in Richtung digitale Zukunft scheint klar: Auf »Decentraland« und »The Sandbox« wechseln digitale Grundstücke momentan für Millionenbeträge die Besitzer. Und das ist kein Spielgeld.

Die Firma Republic Realm hat gerade 4,3 Millionen US-Dollar für eine Landfläche auf der Game-Plattform »The Sandbox« bezahlt. Laut der Datenfirma Nonfungible.com ist das der bisher größte Deal mit virtuellen Immobilien.

Zuvor hatte bereits die kanadische Kryptofirma Tokens.com 2,5 Millionen US-Dollar für Flächen in Decentraland investiert. Laut

Krypto-Internetseite Dapp sind vor einiger Zeit in einer Woche auf den größten Metaverse-Seiten Ländereien für insgesamt mehr als 100 Millionen US-Dollar verkauft worden.

Barbados eröffnet virtuelle Botschaft (Info-Stand: 2021)

In dieser virtuellen Welt der Zukunft wird es in Kürze sogar schon die erste virtuelle Botschaft geben: Der Karibikstaat Barbados will sie am 1. Januar 2022 eröffnen, als erstes Land überhaupt. Sie soll unter anderem bei der Beschaffung von Visa behilflich sein.

Worauf sollte man achten, wenn man Grundstück im Metaverse kauft?

Die meisten Grundstücke im Metaverse bezahlt man in Ethereum. Die Preise beginnen oft erst bei einigen tausend Euro. Daher spekulieren sehr viele Investoren auf einen steigenden Preis des digitalen Lands im Metaverse. Das Risiko vergessen hierbei allerdings viele.

Verlieren Kryptowährungen stark an Wert, kann man hohe Verluste in echter Währung erleiden, selbst wenn der Krypto-Preis für das digitale Land steigen sollte.

Die Anzahl an Metaversen steigt zudem rapide. Es ist also wichtig, sich vorher ausführlich mit dem jeweiligen NFT-Game auseinanderzusetzen. Denn es kann durchaus vorkommen, dass ein Metaverse irgendwann nicht mehr weiterentwickelt wird.

Der gesamte Sektor steckt noch in den Kinderschuhen. Deshalb sollte einem bewusst sein, dass das in digitales Land investierte Geld kein seriöses Investment darstellt. Es dient stattdessen vor allem dem Spaß, als Treffpunkt in der digitalen Welt und mit etwas Glück kann man auch noch Geld verdienen.

Was ist Telegram?

Telegram ist eine Cloud-basierte Instant-Messaging-App, die 2013 ins Leben gerufen wurde und seitdem eine treue Benutzerbasis gewonnen hat. Sie wurde von Pavel und Nikolai Durov entwickelt, zwei russischen Brüdern, die vor allem für die Entwicklung einer Social-Networking-Plattform (die russische Facebook-Alternative VKontakte) bekannt geworden sind.

Die App bietet eine geheime Chat-Option mit Ende-zu-Ende-Verschlüsselung, sowie eine reguläre Chat-Variante, die in der Telegram-Cloud verschlüsselt wird. Sie ist für die Betriebssysteme iOS, macOS, Android, Windows Phone, Windows und Linux verfügbar.

Telegram - Ende-zu-Ende-Verschlüsselung?

Die App verfügt über zwei Schichten von Verschlüsselung. Private und Gruppen-Cloud-Chats unterstützen die **Server-zu-Client-Verschlüsselung**, während geheime Chats von der **Client-zu-Client-Verschlüsselung** profitieren. Die Telegram-Verschlüsselung basiert auf einer 2048-Bit-RSA-Verschlüsselung, einer symmetrischen 256-Bit-AES-Verschlüsselung und einem sicheren Diffie-Hellman-Schlüsselaustausch.

Anders als bei den vielen anderen Messengern sind Chats bei Telegram **nicht automatisch Ende-zu-Ende-verschlüsselt**. Es gibt zwar für die Kommunikation die Funktion der verschlüsselten Übertragung der Nachrichten auf den Cloud-Server. Auf den Servern selbst jedoch kommt das Telegram-eigene Protokoll MTPROTO zum Einsatz, das keine Ende-zu-Ende-Verschlüsselung vorsieht.

Dritte sowie Telegram-Mitarbeiter selbst können so durchaus mit geringen Aufwand auf die in der Cloud gespeicherten Inhalte zugreifen. Dies ist ein spezielles Sicherheitsproblem bei Telegram.



Es ist wichtig zu erwähnen, dass MTPROTO nur für Standard-Cloud-Chats auf mobilen Geräten gilt und standardmäßig **keine automatische** Ende-zu-Ende-Entschlüsselung bietet. MTPROTO hat deswegen bereits sehr viel Kritik erhalten. Dieses in Telegram verwendete symmetrische Verschlüsselungsschema gilt nicht als besonders sicher. Das Protokoll macht es möglich, jeden Chiffretext in einen anderen Chiffretext zu verwandeln, der sich zur gleichen Nachricht wieder entschlüsseln lässt.

Das Problem mit der E2E-Verschlüsselung (E2E ... Ende-zu-Ende) von Telegram ist, dass sie nicht standardmäßig angewendet wird. Die meisten Chats (Cloud-Chats) auf Telegram werden sicher verschlüsselt, während sie zwischen den Geräten und den Servern von Telegram übertragen werden. Sobald Chat-Nachrichten auf den Telegram-Servern ankommen, werden sie mit MTPROTO verschlüsselt, während sie auf den Servern ruhen. Telegram kann jedoch Chat-Daten lesen, da es die Ver- und Entschlüsselung der Nachrichten auf den Servern übernimmt.

Andere Messaging-Dienste, wie z.B. **Signal**, **Threema** (kostenpflichtig) oder auch WhatsApp, wenden standardmäßig die Ende-zu-Ende-Verschlüsselung (E2E-Verschlüsselung) auf alle Kommunikationen an. Der Dienst kann diese Nachrichten (E2E-Verschlüsselung) nicht lesen. Nur der Absender und der

Empfänger können E2E-verschlüsselte Nachrichten lesen. Mit anderen Worten: Jeder Dienst, der E2E-Verschlüsselung für **alle** seine Nachrichten verwendet, ist sicherer als Telegram.

Telegram unterstützt Ende-zu-Ende-Verschlüsselung nur für drei Arten von Kommunikation: **Geheime Chats** (nur als Einzel- und **nicht** als Gruppenchats verfügbar), **Sprachanrufe** und **Videoanrufe**.

Geheime Chats sind Chats, die nicht auf Telegram-Servern gespeichert werden und nur für die am Chat beteiligten Geräte zugänglich sind. Geheime Chats sollten genauso sicher sein wie MTPROTO es eben erlaubt, aber die Benutzer müssen daran denken, sie einzuschalten. Bei Nutzung der geheimen Chats kann man dann (teils durchaus technisch begründet) auf einige gewohnte Funktionen nicht mehr zugreifen.

Sprach- und Videoanrufe werden automatisch E2E-verschlüsselt, was sie ebenfalls so sicher macht, wie MTPROTO es eben erlaubt.

Hinweis 1: Aus der Datenschutzerklärung von Telegram: »Wir können auch automatisierte Algorithmen zur Analyse von Nachrichten in **Cloud-Chats** verwenden, um Spam und Phishing zu unterbinden.«

Hinweis 2: Die Benutzer müssen diese Funktion (E2E-Verschlüsselung) jedoch bei geheimen Chats aktiv einschalten - und zwar bei jedem einzelnen aufs Neue. Für sämtliche Gruppenchats ist diese Option nicht verfügbar. Nur bei Sprach- und Videoanrufen ist sie standardmäßig aktiviert.

Hinweis 3: Ein weiteres Problem bei Telegram, dass nach wie vor unklar ist, wer genau welche Server betreibt und wo diese im

Einzelnen stehen. Der Unternehmenssitz selbst liegt offiziell in Dubai (Info-Stand: 2024). Auch in der öffentlichen Kommunikation hält sich Telegram mit Transparenz weitestgehend zurück.

Wie verarbeitet Telegram personenbezogene Daten?

Zuallererst umfasst das Verfahren von Telegram zur Verhinderung von Spam und anderen Missbrauch, das Sammeln von Informationen wie IP-Adressen, Gerätedetails, Historie von Benutzernamensänderungen und mehr. Für die Speicherung holt sich Telegram vorab pauschal die Einwilligung der Nutzer. Diese Daten werden, wenn sie gesammelt werden, für maximal 12 Monate gespeichert, bevor sie gelöscht werden. Das gibt böswilligen Dritten viel Zeit, um Zugriff darauf zu erhalten.

Zweitens ist es Telegram-Moderatoren erlaubt, Standard-Chat-Nachrichten zu lesen, die als Spam und Missbrauch (Verletzung der Telegram-Regeln) gekennzeichnet wurden (z.B. durch automatisierte Algorithmen), um festzustellen, ob dies stimmt oder auch nicht. Das ist zwar eine vernünftige Praxis, aber es bedeutet auch, dass andere lesen können, was man dort schreibt.

Schließlich kann die App auch aggregierte Metadaten (gesammelte und zusammengefasste Daten, ermöglicht auch die Erstellung von Bewegungsprofile) speichern, um sich besser an die Benutzer anzupassen. Zum Beispiel, um eine personalisierte Liste von den häufigsten Kontakten zu erstellen, die angezeigt wird, wenn man das Suchmenü öffnet.

Keines dieser drei Konzepte ist in der digitalen Welt unbekannt. Allerdings müssen sich die Nutzer darüber bewusst sein, wie ihre sensiblen Daten von der App gehandhabt werden.

Mit wem teilt Telegram die Daten?

Neben den anderen Nutzern, mit denen man über die App kommuniziert, gibt Telegram in seiner Datenschutzrichtlinie weitere mögliche Datenziele an. Erstens, und das ist offensichtlich, teilt Telegram die persönlichen Daten seiner Nutzer mit seiner Muttergesellschaft und einem Gruppenmitglied, das Support für seine Dienste anbietet.

Allerdings behält sich Telegram auch das Recht vor, IP-Adresse und Telefonnummer an staatliche Behörden weiterzugeben (man kann Telegram auch über ein VPN aufrufen). Dies geschieht allerdings nur, wenn das Unternehmen einen Gerichtsbeschluss erhält, der besagt, dass ein Nutzer unter Terrorismusverdacht steht.

Das Unternehmen selbst schreibt zum Thema Datenanfragen von Drittparteien (Info-Stand: 2021): »Bis zum heutigen Tag haben wir 0 Byte Nutzerdaten an Dritte weitergegeben, einschließlich aller Regierungen.« Die Daten aus den Cloud-Chats würden »in mehreren Rechenzentren rund um den Globus gespeichert, die auf verschiedenen juristischen Personen verteilt sind und damit von mehreren Gerichtsbarkeiten gesteuert werden«. Schlüssel und zugehörige Daten würden nie am selben Standort gespeichert. Um Telegram zu einer Offenlegung von Daten zu zwingen, müssten demnach Gerichtsbeschlüsse aus mehreren Ländern einheitlich die Herausgabe anordnen, so Telegram.

Vor- und Nachteile von Telegram

Vorteile von Telegram:

- Open-Source-Apps und Telegram-Datenbank-Bibliothek
- selbstzerstörende Nachrichten
- Benutzer können auf mehreren Geräten gleichzeitig eingeloggt sein

- unterstützt Zwei-Schritt-Authentifizierung
- DSGVO-konform (DSGVO ... Datenschutz-Grundverordnung der Europäischen Union)
- **Nachteile von Telegram:**
- Registrierung erfordert eine Telefonnummer
- E2E-Verschlüsselung nur für geheime Chats (nicht als Gruppenchats verfügbar), Sprachanrufe und Videoanrufe
- keine Überprüfung (Audits) durch Dritte
- Servercodes sind nicht quelloffen (kein Open-Source)
- Telegram protokolliert IP-Adresse und andere Benutzerdaten, wie Gerätedetails, Historie von Benutzernamensänderungen, Metadaten (ermöglicht Bewegungsprofile), Telefonbuch, Beitritt zu Kanälen und Gruppen (öffentlich sichtbar)
- Administrator kann als Spam-markierte persönliche Nachrichten lesen

Fazit zu Telegrams Sicherheit

Telegram ist zumindest nicht in dem Maße sicher, wie es sich gerne darstellt. Nichtsdestotrotz hat es seine Vorteile gegenüber anderer Messenger. Wenn man im Vorfeld die richtigen Sicherheitsvorkehrungen trifft, ist Telegram mit seiner großen Nutzerbasis ein Ort, an dem man sich mit anderen Personen verbinden und unterhalten kann. Wenn man jedoch extrem auf eigene Privatsphäre bedacht ist, sollte man vielleicht lieber die Finger von dem Messenger lassen. Wichtige oder sehr personenbezogene Daten sollten dort auf jeden Fall nicht geteilt werden. Denn Telegram ist in der Tat nicht so sicher, wie das Unternehmen es darstellt.

Insgesamt lohnt es sich, bei Messenger-Diensten stets kritisch zwischen Komfort, Sicherheit und den eigenen Überzeugungen abzuwägen und **genauer** hinzusehen.

Shodan: Suchmaschine für verwundbare Geräte und Systeme die mit dem Internet verbunden sind

Shodan (<https://www.shodan.io>) wurde 2009 vom Softwareentwickler John Matherly ins Leben gerufen, der 2003 die Idee der Suche nach mit dem Internet verbundenen Geräten konzipiert hat. Der Name Shodan ist ein Hinweis auf SHODAN, der künstlichen Intelligenz aus der Videospiel-Serie »System Shock«.

Shodan wurde seitdem eingesetzt, um Systeme mit niedrigen Sicherheits-Vorkehrungen zu finden, einschließlich Steuerungssystemen für die kritische Infrastruktur. In vielen Fällen ist die einzige Software, die benötigt wird, um eine Verbindung zu diesen Systemen herzustellen, ein beliebiger Webbrowser.

Mit Hilfe von Shodan kann man alles finden, was eine Netzwerkadresse besitzt - von bestimmten Computertypen über SCADA-Systeme (Supervisory Control and Data Acquisition, Überwachungs- und Datenbeschaffungssysteme), Überwachungskameras, IoT Geräte (Internet of things ... Internet der Dinge), Smart-Home-Systeme, Industriesteuerungen, Ampel- und Verkehrssteuerungen, Maschinen, Wind- und Solarparks bis hin zu spezieller IT-Hardware und Anwendungen. Die zugänglichen Geräte müssen mindestens über einen offenen Port verfügen.

Shodan sammelt Daten meist auf Webservern (HTTP/HTTPS über die Ports 80, 8080, 443, 8443), sowie FTP (Port 21), SSH (Port 22), Telnet (Port 23), SNMP (Port 161), SIP (Port 5060) und Real Time Streaming Protocol (RTSP, Port 554). Letztere werden regelmäßig für den Zugriff auf Webcams und deren Videostream verwendet.

Hinweis: Diese Geräte und Systeme sind teilweise auch ohne Passwort oder mit dem Standardpasswort der Hersteller (siehe auch: Bedienungsanleitungen der Hersteller) zugänglich.



Shodan wird auch gerne von Netzwerkprofis als Tool für die Schwachstellenbewertung genutzt. Shodan durchforstet dann das Internet und verarbeitet die Banner und andere Informationen, die diverse Geräte zurückliefern. Anhand dieser Daten kann Shodan ermitteln, welche Datenbank und Version am weitesten verbreitet ist, wie viele Webcams sich an einem bestimmten Standort befinden sowie Marke und Modell der Geräte und vieles mehr.

Die von Shodan gesammelten Daten (Metadaten) enthalten meist Informationen über die Serversoftware, unterstützte Optionen, eine Begrüßungsseite oder ähnliches, die der Server in seiner Interaktion mit dem anfragenden Client übermittelt hat.

Man könnte einwenden, dass Webseiten wie Shodan es Angreifern ermöglichen, Schwachstellen aufzuspüren und auszunutzen. Wahr ist aber auch, dass Netzwerk- und Sicherheitsspezialisten in der Lage sein müssen, genauso viel zu sehen wie ein Angreifer, um effektive Verteidigungsmaßnahmen ergreifen zu können.

Zugriff auf die Suchmaschine Shodan

Shodan liefert derzeit zehn Ergebnisse an Benutzer ohne und 50 an diejenigen mit einem Benutzerkonto. Wenn Benutzer die Beschränkung entfernen möchten, müssen sie einen Grund angeben und eine Gebühr entrichten. Die primären Nutzer von Shodan sind Internetsicherheitsspezialisten, Forscher (Marktforschung) und Strafverfolgungsbehörden (Info-Stand: 2023).

Hinweis: Das reine Suchen im Internet nach öffentlich erreichbaren Geräten oder Systemen ist nicht strafbar. Sobald aber versucht wird, in gefundene Systeme einzudringen und Sicherheitsmechanismen zu umgehen oder Sicherheitslücken auszunutzen, unterliegt dies in der Regel der Strafverfolgung.

Arbeitsweise von Shodan

Shodan scannt mit dem Internet verbundene IP-Adressen nach offenen Ports ab und analysiert die Ergebnisse. Diese werden in eine Datenbank eingetragen, die der Anwender nach bestimmten Schlagworten durchsuchen und nach Kriterien filtern kann. Beispielsweise kann die Datenbank nach Begriffen wie »Webcam«, »Smart-TV«, »Printer« oder »MongoDB« durchsucht werden. Werden Einträge zu den Begriffen gefunden, stellt sie Shodan mit einigen Zusatzinformationen dar.

Besitzt man ein Shodan-Konto, lassen sich die Ergebnisse mit Filtern weiter eingrenzen. Filter sind Beispielsweise »city:Hamburg«, »country:Germany« oder »os:Windows« und weitere. Neben der reinen Suche bietet Shodan einige weitere Funktionen. Es lassen sich zum Beispiel die am häufigsten verwendeten Suchbegriffe der Shodan-Benutzer auflisten.

Ohne ein Shodan-Konto lässt sich die Suchmaschine zwar grundsätzlich nutzen, doch sind die Funktionen und

Suchmöglichkeiten stark eingeschränkt. Soll Shodan mit vollen Rechten verwendet werden, muss der Nutzer Informationen über sich preisgeben und sich kostenpflichtig registrieren. Dies soll die missbräuchliche Nutzung eindämmen.

Während die Suchmaschine kostenlos nur eine beschränkte Anzahl an Suchergebnissen ausgibt, erhalten Nutzer mit kostenpflichtigem Konto vollständige Ergebnislisten. Weitere kostenpflichtige Optionen stellt Shodan bei Bedarf zur Verfügung.

Einsatzmöglichkeiten der Suchmaschine

Shodan ist für viele verschiedene Zwecke einsetzbar. Die wichtigsten Anwendungsbereiche sind:

- IT-Sicherheitsanalysen
- Forschungszwecke
- Penetrationstests
- Strafverfolgung
- Aufspüren von Sicherheitslücken und Geräteschwachstellen
- Überprüfung der Gefährdung der Privatsphäre
- Überprüfung der eigenen Smart-Home- oder IoT-Umgebung
- Sicherheitschecks industrieller Anlagen und Steuerungen
- Hacking

Alternativen jenseits von Shodan

Neben Shodan existieren allerdings noch weitere Suchmaschinen, die ähnlich vorgehen und das Internet nach verbundenen Geräten und Systemen durchsuchen - eine davon ist **Censys**.

Insecam.com ist eine spezielle Suchmaschine für Webcams. Für die Suche nach Webcams wird man im Internet noch weitere Suchmaschinen finden.

SHODAN-Webcam - RSSOwl

File Edit View Go Feeds News Tools Window Help

Feeds

- SHODAN-Administration (282)
- SHODAN-Cisco (91)
- SHODAN-CMS (28)
- SHODAN-Common Files (9)
- SHODAN-Default Credentials (17)
- SHODAN-DNS Server (6)
- SHODAN-Firewall (2)
- SHODAN-FTP (73)
- SHODAN-Languages (8)
- SHODAN-Operating System (59)
- SHODAN-Printer (14)
- SHODAN-Router (52)
- SHODAN-SCADA and ICS (107)
- SHODAN-Server Modules (10)
- SHODAN-Television (56)
- SHODAN-VOIP (102)
- SHODAN-Web Server (318)
- SHODAN-Webcam (52)**
 - SHODAN: linux upnp avtech
 - SHODAN: netcam (10)
 - SHODAN: dcs 5220 (5)
 - SHODAN: Server: GeoHttpServer (7)
 - SHODAN: TeleEye (6)
 - SHODAN: Vivotek Network Camera
 - SHODAN: imagatek ipcam (6)
 - SHODAN: sq-webcam (3)
 - SHODAN: Boa ipcam (5)
 - SHODAN: Server: SQ-WEBCAM (3)**
- SHODAN-Windows (9)
- SHODAN-ZENworks (10)

SHODAN-Webcam

All News Ungrouped Classic

Title	Date	Author
79.114.125.74:80	8/15/13 12:24 PM	
79.114.125.74:80	8/15/13 12:24 PM	
124.10.32.143:80	8/15/13 12:23 PM	
82.79.74.247:80	8/15/13 12:23 PM	
82.79.74.247:80	8/15/13 12:23 PM	
116.3.82.73:80	8/15/13 12:23 PM	
99.135.235.80:80	8/15/13 12:17 PM	
99.135.235.80:80	8/15/13 12:17 PM	
58.152.119.219:80	8/15/13 12:15 PM	
118.80.72.162:80	8/15/13 11:45 AM	
92.39.128.162:80	8/15/13 11:43 AM	
190.128.162.162:80	8/15/13 11:32 AM	
70.88.72.162:80	8/15/13 11:45 AM	
202.130.68.142:80	8/15/13 11:43 AM	
123.17.149.25:80	8/15/13 11:32 AM	

SHODAN RSS feed shows webcam found open at 82.79.74.247:80

82.79.74.247:80

Thursday, August 15, 2013 12:23

HTTP/1.0 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH: 2906

HTTP header reveals it is a SQ-WEBCAM device

Schlussbetrachtung

Systeme und Geräte die nicht mit dem Internet verbunden sind, können nicht gefunden werden und damit auch nicht **aus dem Internet** angegriffen werden.

Aus technischen Gründen ist die Anbindung ans Internet oftmals einfach nur grob fahrlässig und häufig auch nicht notwendig.

Falls Systeme und Geräte unbedingt mit dem Internet verbunden sein müssen, so sollte dies über hohe und aktuelle Hürden geschehen. Diese Zugriffsmöglichkeiten müssen **regelmäßig** von außen wie auch von innen qualifiziert geprüft werden.

Jahrzehntelang war das vorherrschende Datenmodell in der Anwendungsentwicklung das relationale Datenmodell, das Daten in Tabellen aus Zeilen und Spalten speicherte. Zum Erstellen und Bearbeiten dieser relationalen Tabellen wurde die Structured Query Language (SQL) verwendet. SQL-Datenbanken modellieren Datenbeziehungen als Tabellen. Die Zeilen in der Tabelle stehen für eine Sammlung zusammengehöriger Werte eines Objekts oder einer Entität. Jede Spalte in der Tabelle stellt ein Datenattribut dar, ein Feld (oder eine Tabellenzelle) speichert den tatsächlichen Wert des Attributs. Mit einem relationalen Datenbankmanagementsystem (RDBMS) kann man auf die Daten auf viele verschiedene Arten zugreifen, ohne die Datenbanktabellen selbst zu reorganisieren.

NoSQL-Datenbanken (NoSQL ... Not Only SQL) wurden speziell für bestimmte Datenmodelle entwickelt und speichern Daten in flexiblen Schemas, die sich leicht für moderne Anwendungen skalieren lassen.

NoSQL-Technologien sind schon seit den 1960er Jahren unter verschiedenen Namen bekannt. Richtig populär sind sie aber erst mit der Umstrukturierung der Datenlandschaft geworden. Also seit Entwickler die großen und vielfältigen Datenmengen bewältigen müssen, die in der Cloud, auf dem Mobilgerät, in den Social Media und durch Big Data generiert werden.

Die Begrifflichkeit des NoSQL kam erstmals 1998 auf und wurde für eine Open Source-Datenbank des Entwicklers Carlo Strozzi verwendet, die keine Möglichkeit des SQL-Zugriffs beinhaltete. Er selbst allerdings weist darauf hin, dass zwischen Datenbanken, die kein SQL verwenden und Datenbanken, die vom relationalen Ansatz Abstand nehmen, unterschieden werden muss. Heute versteht man unter NoSQL den letzteren Fall.

Die nicht-relationalen NoSQL-Datenbanken zeichnen sich vor allem



durch zwei Kriterien aus, zum einen werden Daten nicht in Tabellen (Zeilen und Spalten, keine festgelegten Tabellenschemata) gespeichert und zum anderen ist die Abfragesprache **nicht** SQL (SQL ... Structured Query Language), was auch durch den Namen Not Only SQL deutlich wird. Bei NoSQL-Datenbanken werden Joins (Verbindungen, Koppelungen) in der Regel vermieden.

Eine Besonderheit der NoSQL-Databases ist außerdem die horizontale Skalierung (zusätzliche Server). Relationale SQL-Datenbanken sind vertikal skaliert und stützen ihre gesamte Leistungskraft auf einen einzelnen Server. Um ihre Kapazitäten zu erhöhen, müsste in einen stärkeren Server investiert werden – das ist auf Dauer nicht nur teuer, sondern schränkt auch die Möglichkeiten in der Anwendungsentwicklung ein. NoSQL-Lösungen verteilen die Daten in der Regel auf mehrere Server. Erhöht sich die Datenmenge, werden einfach neue Server hinzugefügt. Dadurch können NoSQL-Datenbanken ohne Probleme große Datenmengen speichern und verarbeiten, wodurch sie sich vor allem für Big-Data-Anwendungen eignen.

Allerdings bedeutet NoSQL nicht, dass gar keine SQL-Datenbanken eingesetzt werden, sondern dass nicht nur SQL-Datenbanken im

Einsatz sein können. Es gibt Varianten mit gemischten Datenbanken, wie auch solche ohne SQL-Datenbanken. Beides wird unter dem Oberbegriff NoSQL zusammengefasst.

Moderne Anwendungen stehen vor mehreren Herausforderungen, die durch NoSQL-Datenbanken gelöst werden können. Anwendungen verarbeiten beispielsweise große Datenmengen aus unterschiedlichen Quellen wie sozialen Medien, intelligenten Sensoren und Datenbanken von Drittanbietern. All diese unterschiedlichen Daten passen nicht immer genau in das relationale Modell der SQL-Datenbanken. Die Durchsetzung tabellarischer Strukturen **kann** zu Redundanz, Datenduplizierung und Leistungsproblemen im großen Maßstab führen.

Was sind die Vorteile von NoSQL Lösungen?

Diese Datenbanksysteme bieten einige Vorteile gegenüber traditionellen SQL Lösungen, die im Big Data Umfeld ausschlaggebend sind. Die folgenden Faktoren sind in nahezu allen NoSQL-Datenbanken umgesetzt:

- NoSQL-Datenbanken sind für bestimmte Datenmodelle und Zugriffsmuster optimiert. Diese ermöglichen eine höhere Leistung, als wenn man versuchen würde, ähnliche Funktionen mit relationalen Datenbanken zu erreichen.
- In der Praxis gibt es verschiedene Datenabfragen, die herkömmliche relationale Datenbanken nicht oder nur mit sehr viel Aufwand unterstützen.
- NoSQL-Datenbanken sind in der Regel so konzipiert, dass sie durch die Verwendung von verteilten Hardware-Clustern skaliert werden können, im Gegensatz zu einer Skalierung durch das Hinzufügen teurer und robuster Server. Einige Cloud-Anbieter übernehmen diese Vorgänge im Hintergrund als vollständig verwaltete Dienstleistung. Weitere Eigenschaften sind eine sehr

schnelle Datenverarbeitung, sie stellen auch keine so hohen Ansprüche an die Datenschemata und können somit die Daten schneller speichern.

- Die meisten NoSQL-Datenbanken sind Open-Source-Software und können somit komplett kostenlos genutzt werden, inklusive des Datenbankmanagements.
- NoSQL-Datenbanken bieten in der Regel flexible Schemata, die eine schnellere und iterativere Entwicklung ermöglichen (iterativ ... sich wiederholend). Das flexible Datenmodell macht NoSQL-Datenbanken ideal für halbstrukturierte und unstrukturierte Daten. Eine relationale Datenstruktur hingegen kann das Datenmodell sehr stark einschränken.
- NoSQL-Datenbanken bieten hochfunktionelle APIs (application programming interface oder Programmierschnittstelle) und Datentypen, die speziell für ihre jeweiligen Datenmodelle entwickelt wurden.

Typen von Datenmodellen bei NoSQL-Datenbanken

Die meisten nicht relationalen Hochleistungsdatenbanken - manchmal als »Not Only SQL« bezeichnet - können stark strukturierte Daten, die in Tabellen gespeichert wurden - auch verarbeiten. Allerdings sind sie nicht wie relationale Datenbanken (Abfragesprache: SQL) auf starre Datenmodelle beschränkt.

Die vier **häufigsten** Typen von NoSQL-Datenbanken:

- Schlüssel-Wert (Key-Value-Datenbanken oder Key-Value Stores): Schlüssel-Wert-Typen eignen sich am besten, wenn ein Schlüssel bekannt und der zugehörige Wert des Schlüssels unbekannt ist. Schlüsselwertdatenbanken (z.B. »Redis«, »Riak«, »Amazon DynamoDB«, »Oracle NoSQL«, ...) sind hochgradig partitionierbar und ermöglichen eine horizontale Skalierung auf einem Niveau, das andere Arten von NoSQL-Datenbanken

möglicherweise nicht erreichen. Eine Schlüsselwertdatenbank speichert Daten als eine Sammlung von Schlüsselwertpaaren, in denen ein Schlüssel als eindeutiger Identifikator dient. Schlüssel und Werte können alles sein, von einfachen Objekten bis hin zu komplexen zusammengesetzten Objekten. Anwendungsfälle wie Gaming, Werbung und IoT eignen sich besonders gut für das Schlüssel-Werte-Datenspeicherungsmodell.

- Dokument (dokumentenorientierte Datenbanken oder Document Stores): Dokumentdatenbanken (z.B. »MongoDB«, »CouchDB«, ...) erweitern das Konzept von Schlüssel-Wert-Datenbanken, indem sie ganze Dokumente in Gruppen zusammenfassen, die als Sammlungen bezeichnet werden. Dokumentdatenbanken verfügen über das gleiche Dokumentmodellformat, das Entwickler in ihrem Anwendungs-code verwenden. Sie speichern Daten als JSON- Objekte, die flexibel, halbstrukturiert und hierarchisch aufgebaut sind. Aufgrund des flexiblen, semi-strukturierten und hierarchischen Aufbaus der Dokumente und Dokument-datenbanken können diese entsprechend den Anforderungen der Anwendungen weiterentwickelt werden. Das Dokumentdatenbankmodell eignet sich gut für Kataloge, Benutzerprofile und Content-Management-Systeme, bei denen jedes Dokument einzigartig ist und sich im Laufe der Zeit weiterentwickelt.
- Spaltenorientiert (spaltenorientierte Datenbanken oder Wide-Column Stores): Spaltenorientierte Datenbanken (z.B. »Apache Cassandra«, »Hbase«, »Google Bigtable«, ...) speichern Daten und Abfragen effizient in Datenzeilen, die platzsparend sind und Vorteile bei der Abfrage bestimmter Datenbankspalten bieten.
- Graphdatenbanken: Graphdatenbanken (z.B. »Neo4j«, »Amazon Neptune«, »DataStax Graph«, »JanusGraph«, ...) basieren auf einem Modell aus »Knoten« und »Kanten«, die die Vernetzung von Daten darstellen - z.B. die Beziehungen zwischen Personen in einem sozialen Netzwerk oder Bewegungsmuster von Webseitenbenutzer. Der Zweck einer Graphdatenbank besteht also darin, das Entwickeln und Ausführen von Anwendungen zu vereinfachen, die mit hochgradig verbundenen Datensätzen arbeiten. Sie verwenden Knoten zur Speicherung von Dateneinheiten und Edges (edge .. Kante, Rand) zur Speicherung von Beziehungen zwischen Einheiten und stark verbundenen Datensätzen. Ein Edge hat immer einen Startknoten, einen Endknoten, einen Typ und eine Richtung. Er kann Eltern-Kind-Beziehungen, Aktionen, Besitzverhältnisse und Ähnliches beschreiben. Die Anzahl und Art der Beziehungen in einem Knoten ist nicht beschränkt. Typische Anwendungsfälle sind Social Networking, Empfehlungsmodule, Betrugserkennung und Wissens-diagramme.
- In-Memory-Datenbanken (Hauptspeicher-Datenbanken): Während andere nicht-relationale Datenbanken Daten auf Festplatten oder SSDs speichern, sind In-Memory-Datenspeicher so konzipiert, dass kein Zugriff auf Festplatten erforderlich ist. Sie eignen sich ideal für Anwendungen, die Reaktionszeiten im Mikrosekundenbereich erfordern (Workloads mit niedriger Latenz) oder große Verkehrsspitzen aufweisen. Man kann sie in Gaming- und Ad-Tech-Anwendungen für Features wie Bestenlisten und Echtzeitanalysen verwenden.
- Datenbanken durchsuchen (Suchmaschinendatenbank): Eine nichtrelationale Suchmaschinendatenbank widmet sich der Suche nach Dateninhalten, z.B. nach Anwendungsausgabeprotokollen, die von Entwicklern zur Problembehandlung verwendet werden. Sie verwendet Indizes, um ähnliche Merkmale unter den Daten zu kategorisieren und die Suchfunktion zu vereinfachen. Suchmaschinendatenbanken sind für die Sortierung unstrukturierter Daten wie z.B. Bilder und Videos optimiert.

Auswahl von NoSQL-Datenbanken

Bei der Auswahl einer NoSQL-Datenbank und deren unterstützten Datenmodell, muss man sich zuerst darüber Klarheit verschaffen,

- über die Art der anfallenden Daten und deren möglichen Entwicklungen in der Zukunft,
- über die Art und Weise der Datenspeicherung (zentrale Speicherung an einem Ort oder verteilte Speicherung an vielen Standorten)
- über die Erweiterungsfähigkeit der Hard- und Software der Datenbank,
- über den Einsatz einer proprietären, urheberrechtlich geschützten Software oder einer quelloffenen Software (Open Source Software)
- über die Art und Weise der Datenabfragen und deren möglichen zukünftigen erforderlichen Erweiterungen,
- über eine mögliche Migration (ohne Datenverlust) zu einer anderen Datenbank,
- über die Vernetzung der Daten und
- über die erforderlichen Zugriffsberechtigungen für den Zugriff auf die Daten.

Hinweis: Bei der Auswahl einer Datenbank sollte man immer viel Geduld mit einbringen. Eine nachträglicher Austausch einer Datenbank ist immer zeit- und kostenintensiv.

Anwendungsmöglichkeiten für NoSQL-Datenbanksysteme

Datenmodelle auf der Grundlage von NoSQL eignen sich für alle Unternehmen, die auf flexible, skalierbare, leistungsstarke und funktionsstarke Datenbanken angewiesen sind, sei es für Gaming, E-Commerce (z.B. Speicherung von Produktkatalogdaten, deren Produkte unterschiedliche Attribute aufweisen), Big-Data-Analysen

(z.B. um schnell veränderliche, umfangreiche Daten zu analysieren), IoT-Apps (Internet of Things), Echtzeit-Web-Apps oder für ähnliche oder andere Zwecke.

ACID Eigenschaften von SQL Datenbanken

Klassische relationale Datenbanken erfüllen die vier sogenannten ACID Eigenschaften. Diese besagen, dass die wichtigste Anforderung an eine Datenbank ist, den Wahrheitsgehalt und die Aussagekraft der Daten zu erhalten. In vielen Fällen werden Datenspeicher als »Single Point of Truth« gesehen, somit wäre es fatal, wenn fehlerhafte Informationen gespeichert und weitergegeben werden.

Die vier Eigenschaften umfassen folgende Punkte:

- **Atomicity (A):** Datentransaktionen, z.B. die Eintragung eines neuen Datensatzes oder das Löschen eines alten, sollen entweder ganz oder gar nicht ausgeführt werden. Für andere Benutzer ist die Transaktion erst sichtbar, wenn sie vollständig ausgeführt ist.
- **Consistency (C):** Diese Eigenschaft ist erfüllt, wenn jede Datentransaktion die Datenbank von einem konsistenten in einen neuen konsistenten Zustand überführt.
- **Isolation (I):** Wenn mehrere Transaktionen gleichzeitig stattfinden, muss der Endzustand derselbe sein, als wenn die Transaktionen getrennt voneinander stattfinden würden. Das heißt die Datenbank sollte den Stresstest bestehen. Also nicht durch Überlastung zu falschen Datenbanktransaktionen kommen.
- **Durability (D):** Die Daten innerhalb der Datenbank dürfen sich nur durch eine Transaktion ändern und nicht durch äußere Einflüsse veränderbar sein. Ein Softwareupdate darf beispielsweise nicht versehentlich dazu führen, dass sich Daten ändern oder womöglich gelöscht werden.

Erfüllt NoSQL die ACID Eigenschaften?

NoSQL Lösungen können generell die ACID Eigenschaften nicht einhalten, obwohl es Ausnahmen gibt, wie beispielsweise die Graphdatenbanken, die alle Konzepte erfüllen. NoSQL Datenbanken werden in vielen Fällen über mehrere Geräte und Server verteilt. Dadurch können deutlich größere Datenmengen gleichzeitig verarbeitet und gespeichert werden, was eine Hauptanforderung an diese Systeme ist. Dadurch erfüllen sie jedoch die Eigenschaft der Konsistenz nicht. Angenommen wir haben eine NoSQL Datenbank auf zwei physischen Servern realisiert, von denen einer in Deutschland und der andere in den USA steht. Die Datenbanken enthalten die Kontostände und -transaktionen von deutschen und amerikanischen Kunden. Dabei sind die deutschen Konten in Deutschland und die amerikanischen Konten auf dem amerikanischen Server gespeichert.

Es kann nun aber vorkommen, dass ein deutscher Kunde eine Überweisung auf ein amerikanisches Konto vornimmt. Dann werden beide Datenspeicher verändert und sind in diesem Bearbeitungszeitraum inkonsistent. Dadurch kann es vorkommen, dass eine Datenbankabfrage gestartet wird während die Verarbeitung in Deutschland bereits abgeschlossen ist, die Verarbeitung in den USA aber noch in Arbeit ist. In diesem Zeitfenster (»Inconsistency Window«), stimmen die Daten in der Datenbank nicht überein und sind damit inkonsistent. Bei relationalen Datenbanken kommt dies nicht vor.

Anwendungsfälle von NoSQL-Datenbanken

Man kann NoSQL-Datenbanken verwenden, um eine Vielzahl von hochleistungsfähigen mobilen, Internet der Dinge (IoT)-, Spiele- und Webanwendungen zu erstellen. Das Spektrum der NoSQL-Datenbanken und ihre jeweiligen Anwendungsfälle sind breit gefächert. Obwohl es schwierig ist, eine repräsentative Auswahl an

Anwendungsfällen zu präsentieren, werden im Folgenden einige Beispiele als Denkanstöße aufgezeigt.

Datenverwaltung in Echtzeit: Mit NoSQL-Datenbanken können Sie Empfehlungen, Personalisierungen und eine verbesserte Benutzererfahrung in Echtzeit bereitstellen. Disney+ beispielsweise stellt seine umfangreiche digitale Inhaltsbibliothek mit Hilfe der NoSQL-Datenbanktechnologie für mehr als 150 Millionen Subscriber (Teilnehmer, Abonnenten, Info-Stand: 2023) bereit.

Cloud-Sicherheit: Man kann Graphdatenbanken verwenden, um komplexe Beziehungen innerhalb von Daten zu erkennen. Zum Beispiel hilft »Wiz« seinen Kunden, ihre Sicherheitslage zu verbessern, indem es die kritischsten Risiken identifiziert und beseitigt. Das Unternehmen verwendet ein in »Amazon Neptune« gespeichertes Graphenmodell, um die toxische Kombination von Risikofaktoren aufzudecken, die kritische Risiken darstellen. Die »Wiz-Risiko-Engines« durchlaufen den Graphen und stellen innerhalb von Sekunden eine Reihe von miteinander verbundenen Risikofaktoren in einem Sicherheitsgraphen zusammen. **Hinweis:** »Amazon Neptune« ist ein Graphdatenbank-Service, mit hoher Skalierbarkeit und Verfügbarkeit und wurde entwickelt um Milliarden von Beziehungen in Sekunden abfragen zu können.

Hochverfügbare Anwendungen: Verteilte NoSQL-Datenbanken eignen sich hervorragend für den Aufbau von Anwendungen mit hoher Verfügbarkeit und geringer Latenz für das Messaging (Kurznachrichtendienst, Kurzmitteilungsservice), die sozialen Medien, Dateifreigaben und vieles mehr. Zum Beispiel hat »Snapchat« mehr als 290 Millionen Nutzer (Info-Stand: 2023), die täglich Milliarden von Bildern und Videonachrichten senden. Snapshat nutzt NoSQL-Datenbanksysteme, um die mittlere Latenzzeit beim Versenden von Nachrichten deutlich zu reduzieren.

Wie funktionieren NoSQL-Datenbanken?

NoSQL-Datenbanken verwenden verschiedene Datenmodelle für den Zugriff auf und die Verwaltung von Daten. Diese Arten von Datenbanken sind speziell für Anwendungen optimiert, die flexible Datenmodelle, ein großes Datenvolumen und eine niedrige Latenzzeit erfordern. Dies wird durch Lockerung der Beschränkungen der Datenkonsistenz bei relationalen Datenbanken erreicht. Je nach Datenmodell gibt es Unterschiede bei der Implementierung. Viele NoSQL-Datenbanken verwenden jedoch Javascript Object Notation (JSON), ein offenes Datenaustauschformat, das Daten als eine Sammlung von Name-Wert-Paaren darstellt.

Beispiel für eine NoSQL-Datenbank

Modellierung des Schemas für eine einfache Buchdatenbank:

In einer relationalen Datenbank wird ein Buchdatensatz oft zerlegt (oder »normalisiert«) und in separaten Tabellen gespeichert. Die Beziehungen der Daten werden dabei durch Primär- und Fremdschlüsselbeschränkungen definiert. In diesem Beispiel hat die Tabelle Bücher Spalten für ISBN (international standard book number), Buchtitel und Auflagennummer, die Tabelle Autoren hat Spalten für AutorenID und Autorenname. Die Tabelle Autoren-ISBN verfügt über die Spalten Autoren-ID und ISBN. Das relationale Modell soll es der Datenbank ermöglichen, die referenzielle Integrität zwischen Tabellen in der Datenbank durchzusetzen, es zur Reduzierung der Redundanz zu normalisieren und im Allgemeinen für die Speicherung zu optimieren.

- In einer NoSQL-Datenbank wird ein Bucheintrag normalerweise als Dokument gespeichert. Für jedes Buch werden der Artikel, die ISBN, der Buchtitel, die Auflagennummer, der Autorenname und die Autoren-ID als Attribute in einem einzigen Dokument

gespeichert. In diesem Modell sind die Daten für eine intuitive Entwicklung und horizontale Skalierbarkeit optimiert.

Wann sollten Sie NoSQL-Datenbanken SQL-Datenbanken vorziehen?

Eine NoSQL-Datenbank eignet sich am besten für die Verarbeitung unbestimmter, unzusammenhängender oder sich schnell ändernder Daten. Sie ist für Entwickler intuitiv zu bedienen, wenn die Anwendung das Datenbankschema vorgibt. Man kann es für Anwendungen verwenden, bei denen:

- Flexible Schemas benötigt werden, die eine schnellere und iterativere Entwicklung ermöglichen.
- Die Leistung Vorrang vor einer starken Datenkonsistenz und der Aufrechterhaltung von Beziehungen zwischen Datentabellen hat (referentielle Integrität, Unverfälschtheit, Unversehrtheit).
- Eine horizontale Skalierung durch Sharding (Aufteilung auf viele Server) zwischen Servern erforderlich ist.
- Strukturierte, halbstrukturierte und unstrukturierte Daten unterstützt werden sollen.

Man muss nicht immer zwischen einem nicht-relationalen und einem relationalen Datenbankschema entscheiden. Man kann auch eine Kombination aus SQL- und NoSQL-Datenbanken verwenden. Dieser hybride Ansatz ist weit verbreitet und gewährleistet, dass jeder Workload (Arbeitsaufkommen) der richtigen Datenbank zugeordnet wird, um ein optimales Ergebnis zu erzielen.

Wie findet man die richtige NoSQL Datenbank?

Die Auswahl einer geeigneten NoSQL Datenbank hängt von verschiedenen Faktoren ab und nicht immer muss von einer klassischen relationalen Datenbank zu einer NoSQL-Datenbank gewechselt werden. Hier sind einige Punkte, die bei der Auswahl

berücksichtigt werden sollten:

- **Datenmodell:** NoSQL Datenbanken gibt es für verschiedenste Datenmodelle, wie Dokument-, Schlüssel-Wert-, Spalten- der Graphdaten. Es sollte eine Datenbank gewählt werden, die zum eigenen Datenmodell passt, um die vollen Vorteile der Datenbank nutzen zu können.
- **Skalierbarkeit:** Not-Only SQL Datenbanken sind dafür bekannt, horizontal skalierbar zu sein, um auch bei großen Datenmengen und vielen Abfragen noch schnelle Antwortzeiten gewährleisten zu können. Vor der Einrichtung einer Datenbank sollte sich vergewissert werden, dass die Skalierbarkeit einfach möglich ist und vom eigenen Team und der Hardware ohne weiteres umgesetzt werden kann.
- **Leistung:** Je nach Art der Anwendung wird die Leistung einer Datenbank unterschiedlich bewertet. Bei der einen Anwendung, werden sehr häufig kleine Datenmengen in die Datenbank geschrieben, während bei anderen Anwendungen einmal am Tag große Mengen aufgenommen werden müssen. Vor Auswahl der Datenbank sollte der Leistungsumfang definiert werden, um eine möglichst passende Datenbank auszuwählen und anschließend zu prüfen, ob die Performance auch umgesetzt werden kann.
- **Konsistenz:** Abhängig von der Anforderung an die Datenkonsistenz schränkt sich die Auswahl an Datenbanken massiv ein. Bei der Wahl der NoSQL-Datenbank sollte berücksichtigt werden, welchen Konsistenzgrad die Daten aufweisen sollten, damit es zu keinen Problemen in der Praxis kommt.
- **Dauerhaftigkeit:** Im Bereich der Dauerhaftigkeit sollte bewertet werden, wie stark die Daten vor Verlust geschützt werden sollten. Dabei muss geprüft werden, wie sich die Datenbank bei einem Systemausfall verhält und welche Daten anschließend

wiederhergestellt werden müssen.

- **Einfachheit der Nutzung:** Die Benutzerfreundlichkeit spielt auch eine wichtige Rolle bei der Auswahl einer geeigneten Datenbank. Es sollte darauf geachtet werden, wie selbstständig die Nutzer die neue Datenbank bedienen können und geprüft werden, ob möglicherweise Schulungen nötig sind (z.B. Graphdatenbank Neo4j mit einer gewöhnungsbedürftigen Abfragesprache). Außerdem sollte geprüft werden, wie sich die Datenbank an die bestehenden Systeme, beispielsweise über APIs (application programming interface), anbinden lässt.
- **Kosten:** Abschließend dürfen auch die Lizenz- und Nutzungskosten nicht vergessen werden, die über die Gesamtbetriebszeit entstehen können. Zusätzlich zu den reinen Nutzungskosten sollten hier auch Kosten für das Hosting und die Wartung mit berücksichtigt werden.

Wenn diese Faktoren bei der Auswahl einer NoSQL Datenbank berücksichtigt werden, lässt sich eine geeignete Datenbank für die jeweilige Anwendung finden und die wesentlichen Kriterien der Anwendung können erfüllt werden.

Fazit

- NoSQL-Datenbanken sind eine beliebte Alternative zu herkömmlichen relationalen Datenbanken.
- Sie sind für die Verarbeitung großer Mengen unstrukturierter oder halbstrukturierter Daten konzipiert.
- NoSQL-Datenbanken bieten hohe Skalierbarkeit, Verfügbarkeit und Fehlertoleranz.
- Zu den wichtigsten Faktoren gehören die Datenmodellierung, Skalierbarkeit, Konsistenz, Verfügbarkeit und Sicherheit.
- Zu den beliebtesten NoSQL-Datenbanken gehören »MongoDB«, »Cassandra«, »Couchbase«, »Redis« und »Amazon DynamoDB« und einige weitere.

Was versteht man unter einer relationalen Datenbank?

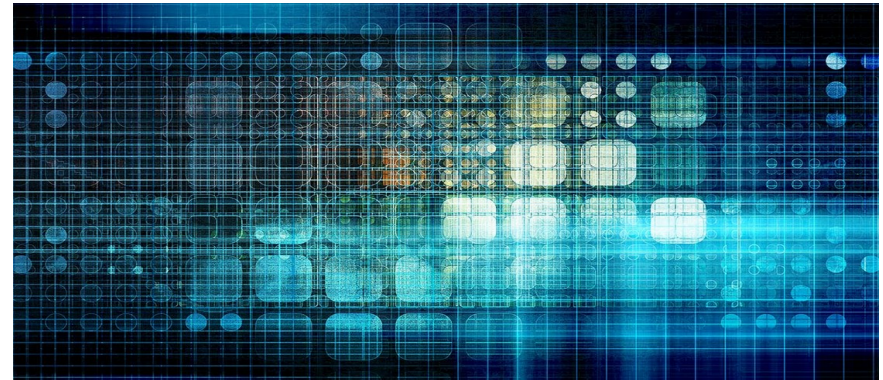
Das relationale Datenbankmodell ist das am weitesten verbreitete Konzept zur rechnergestützten Datenverwaltung. In relationalen Datenbanken werden Informationen als Datensätze strukturiert in Tabellen gespeichert und zur Abfrage verfügbar gemacht. Die Tabellen und Datensätze stehen über Schlüssel miteinander in Beziehung. Ein Datensatz besteht dabei aus mehreren Wertebereichen, die über Tabellenspalten bestimmten Attributen zugeordnet sind. **Hinweis:** Theoretisch handelt es sich jedoch auch bei analogen Informationssammlungen, wie beispielsweise bei einer Bibliothek, um eine Datenbank.

Die intuitivste Art und Weise diese Informationen abzuspeichern ist in tabellarischer Form, also in Zeilen und Spalten. Für viele Daten, wie z.B. im Rechnungswesen, bietet sich diese Darstellung an, da die Daten dadurch immer eine feste, strukturierte Form aufweisen. Solche Datenbanken in tabellarischer Form bezeichnet man als relationale Datenbanken, abgeleitet von dem mathematischen Konzept der Relationen (Beziehungen).

Was ist die Normalisierung von Datenbanken?

Einer der Grundbegriffe der relationalen Datenmodellierung ist die Normalisierung. Die Normalisierung bezeichnet ein Konzept aus dem Datenbankdesign mit dem Ziel, die Redundanzen, also die Dopplungen in der Datenbank, zu eliminieren. Dadurch lässt sich Speicherplatz sparen und außerdem kommt es nicht mehr zu Anomalien (Unregelmäßigkeiten, Abweichungen bei Abfragen). Diese wiederum erschweren die automatische Datenverarbeitung, sowie die Pflege der Datenbank. Normalisierung ist also eine Strategie, Redundanzen in relationalen Datenbanken zu beseitigen.

Merksatz: Als Normalisierung bezeichnet man also die Überführung einer Datenbanktabelle in eine Normalform höheren



Grades. Die Überführung in eine Normalform geringeren Grades wird als Denormalisierung bezeichnet.

Normalisierung und ihre Ziele

Unter Normalisierung eines relationalen Datenbankmodells versteht man die Aufteilung von Attributen in mehrere Relationen (Tabellen) mithilfe der Normalisierungsregeln und deren Normalformen, sodass eine Form entsteht, die keine vermeidbaren Redundanzen mehr enthält.

Mit der Normalisierung einer Datenbank sollen folgende Ziele erreicht werden:

- **Beseitigung von Redundanzen:** Durch die Normalisierung können doppelte Daten gelöscht werden, ohne dass die Datenbank selbst Informationen verliert. Das spart Speicherressourcen und führt dadurch auch zu schnelleren Abfragen. Außerdem verringert es das Potenzial von Fehlern, da bei einer Änderung immer alle redundanten Datensätze geändert werden müssten. Redundanzfrei bedeutet also, dass Daten entfernt werden können, ohne dass es zu Informationsverlusten kommt.

- **Anomalien:** Vermeidung von Anomalien (funktionelle und transitive Abhängigkeiten). Redundante Daten führen zu semantischen Anomalien (Bedeutungsfehler). Diese wiederum erschweren die automatische Datenverarbeitung sowie die Pflege der Datenbank.
- **Datenmodell:** Durch die Normalisierung ergibt sich oft auch automatisch ein übersichtliches, klar strukturiertes und einheitliches Datenmodell. Eine große Tabelle wird nämlich oft in mehrere, überschaubare Tabellen aufgeteilt.

Welche Normalformen (NF) gibt es?

Um doppelte und mehrwertige Wertebereiche (Tabelleninhalte) zu vermeiden, sind im Rahmen relationaler Datenbankmodelle drei aufeinander aufbauende Normalformen (1NF, 2NF, 3NF) entwickelt worden. In der Praxis sind nur drei Normalformen (1NF, 2NF, 3NF, gutes Kosten-Nutzen-Verhältnis) von Bedeutung. **Hinweis:** In der Theorie gibt es jedoch mindestens fünf Normalformen.

Bei einer Normalform handelt es sich um einen definierten Zielzustand. Für jede Normalform wurden spezielle Anforderungen festgelegt, die erfüllt sein müssen, wenn dieser Zielzustand eintreten soll.

Hierbei ist wichtig, dass die Normalformen aufeinander aufbauen. Das bedeutet, dass eine hohe Normalform nur dann erfüllt ist, wenn auch **alle vorhergegangenen Normalformen** erfüllt sind.

Hinweis: In der Datenbankentwicklung ist die Dritte Normalform oft ausreichend, um die perfekte Balance aus Redundanz, Performance und Flexibilität für eine Datenbank zu gewährleisten. Natürlich gibt es auch Sonderfälle, z.B. im wissenschaftlichen Bereich, wo eine Datenbank bis zur 5. Normalform normalisiert werden kann bzw. muss.

Normalisierung und Abhängigkeiten

Die Normalisierung von Daten in einer Datenbank bringt auch funktionale Abhängigkeiten zwischen den Informationen mit sich. Jeder Relationstyp (Tabelle) hat verschiedene Informationen in sich und besitzt damit auch unterschiedliche Ausprägungen von funktionalen Abhängigkeiten.

Dabei wird zwischen der funktionalen, voll funktionalen und transitiven Abhängigkeit unterschieden.

Funktionale Abhängigkeit: Eine funktionale Abhängigkeit zwischen Attribut Y und Attribut X liegt dann vor, wenn es zu jedem X genau ein Y gibt.

Voll funktionale Abhängigkeit: Eine vollständig funktionale Abhängigkeit liegt dann vor, wenn das Nicht-Schlüsselattribut nicht nur von einem Teil der Attribute eines zusammengesetzten Schlüsselkandidaten funktional abhängig ist, sondern von allen Teilen eines Relationstyps (Tabelle).

Die vollständig funktionale Abhängigkeit wird mit der 2. Normalform (2NF) erreicht.

Transitive Abhängigkeit: Eine transitive Abhängigkeit liegt dann vor, wenn Y von X funktional abhängig und Z von Y, so ist auch dann Z von X funktional abhängig. Diese Abhängigkeit ist transitiv. Die transitive Abhängigkeit wird mit 3. Normalform (3NF) erreicht.

1. Normalform (1NF)

Die 1. Normalform ist erreicht, wenn alle Datensätze atomar sind. Das heißt, dass jedes Datenfeld lediglich **einen** Wert enthalten darf. Außerdem sollte sichergestellt sein, dass jede Spalte nur Werte desselben Datentyps (Numerisch, Text, ...) enthält.

Folgende Beispiele müssen entsprechend verändert werden, damit eine Datenbank in der 1. Normalform vorliegt:

Beispiel 1

Adresse: Hauptstraße 1, 12345 Berlin

Die Adresse muss auf 4 Datenfelder (Straße, Hausnummer, PLZ, Ort) verteilt werden.

Straße: Hauptstraße

Hausnummer: 1

PLZ: 12345

Ort: Berlin

Beispiel 2

Rechnungsbetrag: 128,45 €

Der Rechnungsbetrag muss auf 2 Datenfelder (Betrag, Währung) verteilt werden.

Betrag: 128,45

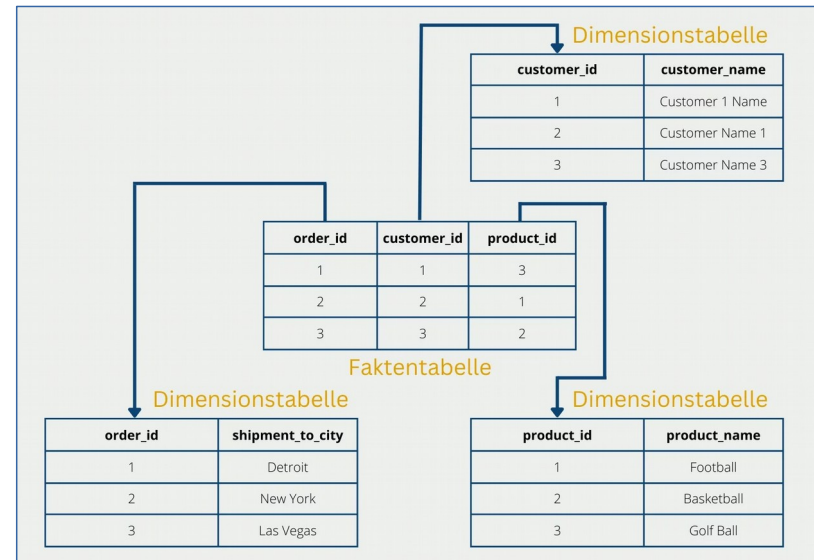
Währung: €

Definition der ersten Normalform (1NF): Die 1. Normalform (1NF) ist immer dann gegeben, wenn alle Informationen in einer Tabelle atomar (je Feld nur einen Wert desselben Typs) vorliegen.

2. Normalform (2NF)

Die 2. Normalform ist erfüllt, wenn die erste Normalform erfüllt ist und außerdem jede Spalte (Nichtschlüsselattribut) in einer Zeile voll funktional abhängig ist vom Primärschlüssel.

Der Primärschlüssel bezeichnet ein Attribut (Beifügung), das zur eindeutigen Identifikation einer Datenbankzeile verwendet werden kann. Dazu zählen beispielsweise die Rechnungsnummer zur Identifikation einer Rechnung oder die Ausweisnummer zur Identifikation einer Person.



Konkret bedeutet dies in der Anwendung, dass alle Merkmale ausgelagert werden müssen, die nicht ausschließlich vom Primärschlüssel abhängig sind. In der Praxis führt dies dann oft zu einem sogenannten Sternschema (siehe Bild).

In unserem Beispiel ist der Kundenname nicht vom Primärschlüssel **order_id** der ursprünglichen Tabelle abhängig. Deswegen muss der Kundenname in einer neuen Tabelle ausgelagert werden. Lediglich der Fremdschlüssel **customer_id** referenziert dann auf die neue Tabelle, sodass keine Information verloren geht.

Definition der zweiten Normalform (2NF): Ein Relationstyp (Tabelle) befindet sich genau dann in der 2. Normalform (2NF), wenn er sich in der ersten Normalform (1NF) befindet und jedes Nichtschlüsselattribut von jedem Schlüsselkandidaten voll funktional abhängig ist.

3. Normalform (3NF)

Die 3. Normalform liegt vor, wenn die beiden vorhergehenden Normalformen erfüllt sind und es zusätzlich **keine** sogenannten transitiven Abhängigkeiten gibt. Das bedeutet, die Nicht-Schlüssel-Attribute sind **voneinander funktional unabhängig**.

Eine transitive Abhängigkeit liegt vor, wenn ein Attribut, welches kein Primärschlüssel ist, nicht nur von diesem abhängt, sondern auch von anderen Attributen. Transitive Abhängigkeiten sind in der 3. Normalform nicht zulässig.

Beispiel: Eine Tabelle, in der die Rechnungsnummer, die Produktnummer und der Preis enthalten sind, dann haben wir es höchstwahrscheinlich mit einer transitive Abhängigkeit zu tun. Der Preis des Produktes hängt nämlich nicht wirklich von der Rechnungsnummer ab, sondern vielmehr von der Produktnummer, da für jedes Produkt ein fester Preis definiert ist. Diese Abhängigkeit kann man auflösen, indem man die Produkte in eine neue Tabelle auslagert und somit das Attribut Preis aus der ursprünglichen Tabelle herausfällt.

Hinweis: Datenbankentwickler können mit der Dritten Normalform die perfekte Balance in ihrem Datenmodell herstellen, um neue Probleme aus der realen Welt in ein relationales Datenbankmodell einzupflegen.

Definition der dritten Normalform (3NF): Ein Relationstyp (Tabelle) befindet sich genau dann in der 3. Normalform, wenn er sich in der 2. Normalform (2NF) befindet und kein Nichtschlüsselattribut transitiv von einem Kandidatenschlüssel abhängt.

Redundanzen in Datenbanken

Redundanzen sind doppelte Informationen in einer Datenbank bzw.

Datenbank-Tabelle. Man spricht von einer redundanzfreien Datenbank, wenn alle doppelte Informationen entfernt werden können, ohne dass ein Informationsverlust stattfindet. Redundanzen in Datenbanken sind immer ein Zeichen für ein schlechtes Datenbankdesign.

Wie kann man Redundanzen vermeiden?

Redundanzen können mittels der Normalisierung entfernt werden. Die Normalisierung entfernt doppelte Informationen, ohne dass ein Informationsverlust in anderen Relationen (Tabellen) stattfindet.

Wann lässt man Redundanzen zu?

Ab und zu kann eine Redundanz aber auch wahre Wunder wirken, wenn es um die Performance in einer Datenbank geht. Besonders in anderen Fällen von relationalen Datenbanken, wie im Data Warehouse oder im Business Intelligence-Bereich, werden ganz bewusst Redundanzen eingebaut, um zeitaufwändige und performance-aufwändige SQL-Abfragen zu verbessern. In solchen Fällen spricht man von der »**Kontrollierten Redundanz**«, die mithilfe der Denormalisierung von Datenbanken erreicht wird.

Was sind die Grenzen der Normalisierung?

Relationale Datenbanken werden in die verschiedenen Normalformen überführt, um die Datenintegrität und eine effiziente Datenspeicherung zu gewährleisten. Jedoch bieten die Normalformen nicht nur Vorteile, sondern man stößt auch an Grenzen, die bei der Arbeit mit Datenbanken beachtet werden sollten.

Grenzen der Datenbanknormalisierung:

- 1. Auswirkungen auf die Leistung:** Eine normalisierte Datenbank kann starke Auswirkungen auf die Abfrageleistung haben. Mit der zunehmenden Form werden komplexere Joins (Datenbank-

- Tabellen mittels Abfragen verbinden) und mehr Abfragen nötig, um Daten zu erhalten. Dies führt vor allem bei großen Datenmengen zu erheblich langsameren Abfragen. Dies wird noch zusätzlich dadurch verstärkt, dass durch die Normalisierung mehr Tabellen nötig werden und dadurch eine zusätzliche Komplexität eingeführt wird.
2. **Datenredundanz:** Das Hauptziel der Normalisierung ist die Beseitigung von Datenredundanzen, durch die Aufteilung der Daten in unterschiedliche Tabellen. Dies führt neben der zusätzlichen Komplexität auch zu deutlichen Leistungseinbußen bei der Datenabfrage. Deshalb können Denormalisierungstechniken genutzt werden, um eine gewisse Datenredundanz zuzulassen und dafür die Leistungsfähigkeit zu erhalten.
 3. **Erhöhte Komplexität:** Die erhöhte Komplexität der Normalisierung führt vor allem zu aufwendigen und umfangreichen Abfragekonstruktionen. Dies führt dazu, dass die Nutzer genügend Kenntnisse in SQL und Datenbankdesign haben müssen, um die Daten richtig abzufragen. Außerdem müssen auch die Administratoren entsprechend die Normalisierungsprinzipien kennen, um die Datenbank effektiv verwalten zu können.
 4. **Herausforderungen bei der Wartung:** Die Wartung und Verwaltung einer normalisierten Datenbank sollte nicht unterschätzt werden. Denn auch die Änderung oder Löschung von Daten kann Operationen in verschiedenen Tabellen erfordern. Wenn diese nicht stattfinden, ist das Risiko für Inkonsistenzen (Unstimmigkeiten) hoch.
 5. **Flexibilität und Anpassungsfähigkeit:** Neben der Instandhaltung wird natürlich auch die Erweiterung und Anpassung deutlich komplexer. Das Hinzufügen von neuen Attributen oder Änderungen in der Datenstruktur erfordern aufgrund der Normalisierung meist auch Änderungen in verschiedenen Tabellen.
 6. **Gleichgewicht zwischen Normalisierung und Leistung:** Nicht immer ist eine höhere Normalisierungsform auch die optimale Wahl für ein Datenbanksystem. Es muss im Einzelfall ein Gleichgewicht zwischen ausreichender Normalisierung, Datenintegrität und Denormalisierung für eine optimale Leistung gefunden werden.
 7. **Kompromisse bei der Berichterstellung und Analyse:** Neben der Datenspeicherung an sich, sollten bei der Konzeption von Datenbanken auch die nachfolgenden Prozesse, wie beispielsweise das Berichtswesen berücksichtigt werden. Durch die Normalisierung kann es auch hier zur Beeinträchtigung von Performance (Leistungsverhalten) kommen, wenn das aggregieren (vereinen) der Daten deutlich länger dauert.
 8. **Kontextspezifische Überlegungen:** Die Normalisierung sollte im Einzelfall für die Anwendung geprüft werden und eine entsprechende Entscheidung getroffen werden. Dazu zählt beispielsweise auch die Prüfung der Datentypen und ob diese normalisiert werden sollten. Beispielsweise bei Protokollen kann es passieren, dass höhere Normalisierungsstufen nicht wirklich vorteilhaft sind.
- Die Normalisierung von Datenbanksystemen sichert zwar die Datenintegrität, jedoch hat es auch einen großen Einfluss auf die Arbeit mit Datenbanken. Deshalb ist eine sorgfältige Bewertung der Kompromisse zwischen Normalisierung und Leistung unumgänglich. Nur dann ist eine effektive Datenverwaltung möglich.
- Was ist das Konzept der Denormalisierung?**
- Die Denormalisierung ist eine Methode zur Optimierung der Datenbankleistung, indem gezielte Redundanzen in ein normalisiertes Datenbankschema eingeführt werden. Während die Normalisierung eigentlich versucht diese Redundanzen zu beseitigen, setzt die Denormalisierung diese gezielt ein, um die

Abfrageleistung zu verbessern und die Effizienz des Systems zu steigern. Durch die absichtliche Duplizierung von Tabellen oder einer weniger stark aufgeteilten Struktur, wird der Bedarf für komplexe Joins (Datenbank-Tabellen mittels Abfragen verbinden) bei der Datenabfrage verringert und somit die Abfrageleistung erhöht. Bei der Denormalisierung werden verschiedene Techniken genutzt, wie zum Beispiel:

- **Abflachen von Tabellen:** Hierbei werden mehrere Tabellen in einer einzigen zusammengefasst, um den Bedarf für Joins zu verringern. Dadurch lassen sich Abfragen deutlich vereinfachen und die Leistung wird verbessert, da nicht so viele Leseoperationen getätigt werden müssen.
- **Hinzufügen redundanter Daten:** Bei diesem Ansatz werden Daten aus einer Tabelle dupliziert mit dem Ziel die Notwendigkeit von Joins zu verringern. Auch hierdurch wird die Abfrageleistung verbessert. Diese Methode macht vor allem Sinn für häufig abgefragte Informationen.
- **Abgeleitete Spalten einführen:** Ein weiteres Mittel der Denormalisierung ist die Einführung von berechnenden Spalten, die abgeleitete oder berechnete Werte enthalten. Dadurch müssen diese nicht während einer Abfrage berechnet werden, wodurch sich wiederum die Leistung verbessern lässt.

Die Denormalisierung kommt vor allem bei Anwendungen zum Einsatz, in denen die Abfrageleistung einen hohen Stellenwert hat, wie beispielsweise beim »Data Warehousing« (Warengeschäft mit Daten) und dem »Business Intelligence« (systematische Unternehmensanalyse). Jedoch muss natürlich beachtet werden, dass es aufgrund dieser Methoden zu Dateninkonsistenzen kommt oder kommen kann. Zusätzlich ist der Speicherbedarf auch höher, da Daten gezielt doppelt gespeichert werden.

Genauso wie die Normalisierung, sollte auch die Nutzung der Denormalisierung gut durchdacht sein und abhängig vom Anwendungsfall genutzt werden. Es kann keine allgemeingültige Aussage getroffen werden, ob grundsätzlich auf die Normalisierung oder die Denormalisierung zurückgegriffen werden sollte. Vielmehr sollte ein gesundes Gleichgewicht zwischen beiden Extremen gefunden werden, das den Anforderungen entspricht.

Weitere Normalformen für Datenbanken

Neben den 3 wichtigsten Normalformen (1NF, 2NF, 3NF) gibt es noch weitere Normalformen.

Nullte Normalform in einer Datenbank

Die Nullte Normalform liegt in vielen Fällen während der Anforderungsanalyse einer Datenbank vor (Entwicklungsphase einer Datenbank). Die Anforderungsanalyse in der Datenbankentwicklung beginnt mit dem Sammeln (Aggregation) von unstrukturierten und unsortierten Informationen aus den verschiedensten Fach- oder Datenbereichen.

R.-Nr.	Datum	Name	Straße	Ort	Artikel	Anzahl	Preis
187	01.01.2012	Max Mustermann	Musterstr. 1	12345 Musterort	Bleistift	5	1,00 €

Definition der Nullten Normalform: Eine Relationstyp (Tabelle) befindet sich in der Nullten Normalform, wenn alle Datenelemente, Informationen der realen Welt in einer Tabelle zusammengefasst und aufgelistet sind. Die Tabelle liegt dann in der Nullten Normalform vor, d. h. sie ist noch **nicht** normalisiert.

Vierte Normalform (4NF)

Die 4. Normalform schließt an die Boyce-Codd-Normalform und deren normalisierte Datenmodellierung an.

Zusätzlich muss zum Erreichen der 4. Normalform (4NF) die Bedingung erfüllt sein, dass Abhängigkeiten von mehrwertigen Attributmengen trivial sind und eine Attributmenge der Schlüsselkandidat der Relation ist. Das bedeutet, dass keine Redundanz in funktional abhängigen Attributen existieren können.

Definition der Vierten Normalform (4NF): Ein Relationstyp befindet sich genau dann in der 4. Normalform (4NF), wenn er sich in der Boyce Codd Normalform (BCNF) befindet und für jede mehrwertige Abhängigkeit einer Attributmenge Y von einer Attributmenge X gilt: Die mehrwertige Abhängigkeit ist trivial oder X ist ein Schlüsselkandidat der Relation (Tabelle).

Anders ausgedrückt, die 4. Normalform ist erfüllt, wenn die 3. Normalform erfüllt ist und wenn **keine paarweise auftretenden mehrwertigen Abhängigkeiten** vorhanden sind.

Ein Beispiel für eine triviale Abhängigkeit ist z.B., dass zu einem Kunden alle bestellten Artikel gespeichert werden. Identifiziert die **KundenNr** nicht nur einen Artikel sondern eine ganze Liste verschiedener Artikel, spricht man von einer mehrwertigen Abhängigkeit. Die Relation ist dennoch in der 4. Normalform, da die Abhängigkeit trivial und die **KundenNr** der Schlüsselkandidat der Tabelle ist.

Um die mehrwertigen Abhängigkeiten aufzulösen, muss die Tabelle aufgeteilt werden. Durch die Aufteilung in mehrere Tabellen, wird die mehrwertige Abhängigkeit in eine triviale aufgelöst wird. Dadurch entsteht eine zusätzliche Referenztabelle, die meist nur eine neue Spalte enthält. Die **Primär-Fremdschlüssel-Beziehungen** bleiben weiterhin bestehen. Die Aufteilung muss sicherstellen, dass alle Daten der Ausgangstabelle wieder zusammengesetzt werden können. Darüber hinaus dürfen keine

Daten verloren gehen, wenn ein Datensatz gelöscht wird.

In der Praxis wird die 4. Normalform normalerweise nicht verwendet. Bei der Erstellung relationaler Datenmodelle hat sich die 3. NF als praxistauglich erwiesen und wird in der überwältigenden Mehrheit relationaler Datenmodelle eingesetzt. 1. und 2. NF kommen nur dann zum Einsatz, wenn Daten in Systeme geladen werden oder eine Normalisierung, aufgrund einer geringeren Relevanz und zugunsten einer besseren Performance, in den Hintergrund tritt (z.B. Reporting).

Boyce Codd Normalform (BCNF oder 3.5NF)

Die Boyce-Codd-Normalform (BCNF) ist eine Weiterentwicklung der 3. Normalform (3NF). In der 3. Normalform kann es vorkommen, dass ein Teil eines Schlüsselkandidaten funktional abhängig ist von einem Teil eines anderen Schlüsselkandidaten. Die Boyce-Codd-Normalform verhindert diese funktionale Abhängigkeit. Als Schlüsselkandidat wird ein Attribut oder eine Attributkombination bezeichnet, die einen Datensatz eindeutig identifizieren (also einen Primärschlüssel bilden). Die BCNF braucht nur dann angewendet zu werden, wenn mehrere Schlüsselkandidaten vorhanden sind und sich diese teilweise überlappen. Ist in der Relation (Tabelle) nur ein Kandidatenschlüssel vorhanden oder es liegt keine Überlappung bei mehreren Kandidatenschlüsseln vor, befindet sich die Relation automatisch in der Boyce-Codd-Normalform.

Definition der Boyce-Codd-Normalform (BCNF): Ein Relationstyp ist genau dann in Boyce-Codd Normalform (BCNF), wenn jede Determinante (Bestimmungsgröße) vom Relationstyp ein Kandidatenschlüssel ist. Die Boyce-Codd Normalform ist die höchste Normalform auf der Basis funktioneller Abhängigkeiten. Eine Relation (Tabelle), die sich in der Boyce-Codd Normalform befindet ist auch gleichzeitig in der 3. Normalform (3NF).

Beispiel für eine Boyce-Codd-Normalform (BCNF)

Ausgangspunkt der folgenden Betrachtung ist die Tabelle Rechnung, die um die Spalte **LagerOrt** erweitert wurde. Der **LagerOrt** gibt an wo der Artikel im Lager abgelegt wurde.

ReNr	ArtNr	LagerOrt	Anzahl
100100	1010	22	1
100100	1020	15	2
100100	1030	9	5
100103	1040	13	10
100104	1040	13	6

Die zusammengesetzten Schlüsselkandidaten sind **ReNr-ArtNr** und **ReNr-LagerOrt**. Zwischen **ArtNr** und **LagerOrt** besteht eine funktionale Abhängigkeit, die nichts mit der Rechnungsnummer zu tun hat, daher ist die Relation (Tabelle) zwar in 3. Normalform, aber nicht in der Boyce-Codd-Normalform.

Das Attribut **ArtNr** ist hier die Determinante für den Lagerort, aber das Attribut **LagerOrt** ist nur ein Teil eines Schlüsselkandidaten und somit funktional abhängig zum Attribut **ArtNr**.

Das gleiche gilt für die umgekehrte Richtung, da auch über den Lagerort die Artikelnummer bestimmt werden kann.

Die Abhängigkeit wird durch eine Aufteilung der Daten in zwei Tabellen gelöst.

Aus der Ausgangstabelle entstehen so zwei neue Tabellen, die über einen Primärschlüssel verbunden sind.

Neue Tabelle: Rechnung-Artikel

ReNr	ArtNr	Anzahl
100100	1010	1
100100	1020	2
100100	1030	5
100103	1040	10
100104	1040	6

Neue Tabelle: Artikel-Lagerort

ArtNr	LagerOrt
1010	22
1020	15
1030	9
1040	13
1040	13

Fünfte Normalform (5NF)

Die 5. Normalform beschäftigt sich, wie die 4. Normalform, mit mehrwertigen Abhängigkeiten.

Die Voraussetzung der 5. Normalform ist eine Relation in der 4. Normalform, zudem müssen alle Schlüsselkandidaten der Relation (Tabelle) auch Schlüssel der Teilmengen der Relation sein.

Das heißt, die ausgegliederten Attribute müssen Schlüssel auch der neu entstehenden Relationen (Tabellen) sein.

Hinweis: In der 5. Normalform ist es **nicht mehr möglich**, die Relationstypen weiter in Relationstypen eines geringeren Grades zu zerlegen, so dass der Ursprungszustand nur mit Informationsverlust wieder hergestellt werden kann.

Ein Relationstyp befindet sich genau dann in der 5. Normalform (5NF), wenn er sich in der 4. Normalform (4NF) befindet und für jede Abhängigkeit (R_1, R_2, \dots, R_n) folgendes gilt: Die Abhängigkeit ist trivial oder jedes R_i aus (R_1, R_2, \dots, R_n) ist Schlüsselkandidat der Relation. Die 5. Normalform (5NF) wird unter anderem als »Project Join Normalform (PJNF)« bezeichnet.

Ziel der Fünften Normalform (5NF)

Die 5. Normalform dient anders als die anderen Normalformen dazu, neue Informationen zu entdecken. Richtig angewendet ergeben sich neue Zusammenhänge in den Daten.

Die 5. Normalform wird nur angewandt, wenn man mögliche Verbindungen aus drei Beziehungen ausdrücken möchte und keine konkreten Verbindungen zwischen drei Tabellen abbildet.

Beispiel für die Fünfte Normalform

Die Tabelle enthält Informationen darüber welches Produkt eines Herstellers von welchem Kunden gekauft wurde. Dabei bietet jeder Hersteller verschiedene Produkte an, die von verschiedenen Kunden gekauft werden.

HerstellerNr	ProduktBez	KundeNr
1	Stift 1	006
1	Ordner 1	007
2	Ordner 2	006
3	Kopierpapier	007

Keiner der Kunden kauft alle Produkte eines Herstellers und keines der Produkte wird von allen Kunden gekauft. Das bedeutet, dass alle Attribute der Tabelle relevant sind, um die Information zu speichern wer was bei wem gekauft hat. In der Relation liegen keine mehrwertigen Abhängigkeiten vor, da Produkte und Kunden zusammen eine wichtige Information abbilden.

Der Schlüsselkandidat der Tabelle besteht aus allen drei Attributen. Aufgrund dessen müssen drei einzelne Relationen (Tabellen) erstellt werden, um die Mehrwertigkeit aufzulösen.

Neue Tabelle: Hersteller-Produkt

HerstellerNr	ProduktBez
1	Stift 1
1	Ordner 1
2	Ordner 2
3	Kopierpapier

Neue Tabelle: Produkt-Kunde

ProduktBez	KundeNr
Stift 1	006
Ordner 1	007
Ordner 2	006
Kopierpapier	007

Neue Tabelle: Hersteller-Kunde

HerstellerNr	KundeNr
1	006
1	007
2	006
3	007

Die ursprüngliche Relation wurde in eine triviale Abhängigkeit aufgelöst. Eine weitere Zerlegung ist nicht mehr möglich.

HerstellerNr	ProduktBez	KundeNr
1	Stift 1	006
1	Ordner 1	007
1	Ordner 1	006
1	Stift 1	007
2	Ordner 2	006
3	Kopierpapier	007

Bei einem Join (Datenbank-Tabellen mittels Abfragen verbinden) auf alle Tabellen entstehen neue Zeilen, die es ursprünglich nicht in der Tabelle gab. Dadurch entsteht ein Informationsverlust, da nicht mehr erkennbar ist, welche Informationen zu Beginn enthalten waren.

Anomalien in Datenbanken

Anomalien in Datenbanken treten bei einer nicht existierenden oder fehlerhaften Normalisierung auf. Es existieren drei Arten von Datenbank-Anomalien, die Einfüge(Insert)-Anomalie, die Änderungs(Update)-Anomalie und die Lösch>Delete)-Anomalie. In der Datenbankentwicklung ist die 3. Normalform oft ausreichend, um die perfekte Balance aus Redundanz, Performance und Flexibilität für eine Datenbank zu gewährleisten. Sie eliminiert auch die meisten Anomalien in einer Datenbank, aber nicht alle.

Einfüge(Insert)-Anomalien

Bei einem fehlerhaften oder inkorrekten Datenbankdesign kann es bei der Einfüge-Anomalie passieren, dass Daten gar nicht in die Datenbank übernommen werden, wenn zum Beispiel der Primärschlüssel keinen Wert erhalten hat oder eine unvollständigen Eingabe von Daten zu Inkonsistenzen führt.

Änderungs(Update)-Anomalie

Bei der Änderungs-Anomalie, auch Update-Anomalie genannt, werden gleiche Attribute eines Datensatzes in einer Transaktion nicht automatisch geändert. So entsteht eine Inkonsistenz der Daten.

Lösch>Delete)-Anomalie

Bei einer Löschanomalie kann es passieren, dass ein Benutzer einer Datenbank aktiv Informationen löschen will und damit indirekt, aufgrund des fehlerhaften Datenbankdesigns, andere zusammenhängende Informationen ebenfalls parallel löscht.

Warum normalisiert man nicht alle Datenmodelle?

Eine zu starke Normalisierung der Daten hat negative Folgen. Durch die Normalisierung werden zusätzliche Tabellen benötigt, die administrativen Aufwand erzeugen (z.B. Speicherplatz, Berechtigung, referenzielle Integrität). Zudem verlangsamt es die Abfragegeschwindigkeit, da die Tabellen erst mithilfe von Joins (Datenbank-Tabellen mittels Abfragen verbinden) verknüpft werden müssen. Daher wird besonders in der Datenanalyse und dem Reporting - die Normalisierung aufgehoben, um durch Redundanz Ergebnisse schneller abzurufen.

Vor- und Nachteile der Normalisierung

Durch die Normalisierung einer Datenbank weist das Zielschema weniger Redundanz auf als das Ausgangsschema. Normalisierung erleichtert somit die Pflege einer Datenbank.

Andererseits geht die Normalisierung von Datenbanken immer mit der Auslagerung von Attributen in separate Tabellen einher. Dies bedeutet, dass logisch zusammengehörige Daten nicht mehr gemeinsam in einer Tabelle gespeichert werden. Möchte man Daten, die auf verschiedene Tabellen aufgeteilt wurden, zusammenführen, ist zunächst ein Join für die Abfragen erforderlich.

Was kann man mit einer Bildersuche anfangen?

Man hat ein Bild von jemandem, aber man weiß nicht, wer es ist oder was das Bild bedeutet. Für die Bildersuche kann man mehrere Online-Tools zur Suche verwenden. Für die Bildersuche sind Google (images.google.com) und TinEye (www.tineye.com) zur Zeit die beliebtesten Online-Tools.

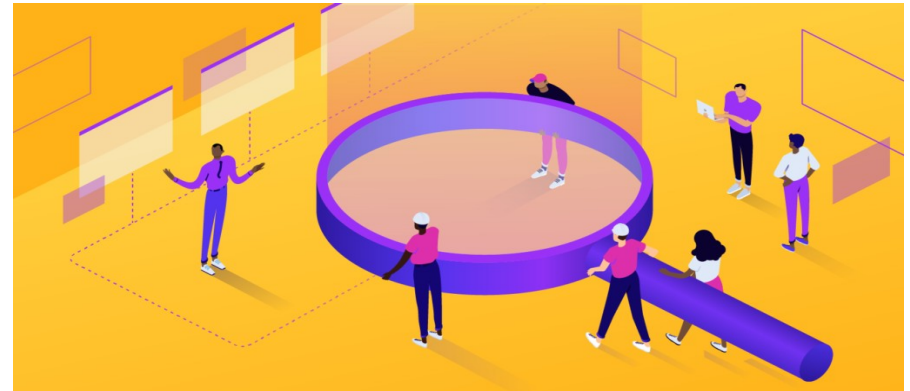
Möglichkeiten und Ergebnisse der Bildersuche:

- andere Kopien von einem Bild zu finden
- das Original von einem Bild aufspüren
- um nach Personen zu suchen oder
- um mehr Informationen über das Bildmotiv (Bücher, Pflanzen, Pilze, Schilder mit Straßennamen, Symbole, ...) zu erhalten

Die Google-Bildersuche ist ein mächtiges Tool, welches wahrscheinlich den meisten Menschen im alltäglichen Gebrauch ausreichen wird. Manchmal lohnt es sich durchaus, auch über den Tellerrand zu schauen.

Anonyme Bildersuche mit Ixquick: Wer seine Bildersuche nicht offenlegen will, kann dafür Ixquick (ixquick.com/deu/) nutzen. Die Suche nach Bildern läuft auch unter Ixquick sehr einfach ab: Man gibt den gewünschten Begriff ein oder verfeinert die Suchanfrage mit der »Erweiterten Suche«. In den Sucheinstellungen von Ixquick kann man einstellen, ob die Suchanfragen gefiltert werden sollen, von welchen Servern die Ergebnisse stammen sollen und vieles mehr. Die meisten Bilder und die dazugehörigen Webseiten kann man sich dann anonym über den Ixquick-Proxy ansehen.

Die freie Mediensuche – Wikimedia: Wikimedia Commons (https://commons.wikimedia.org/wiki/Main_Page?uselang=de) ist in



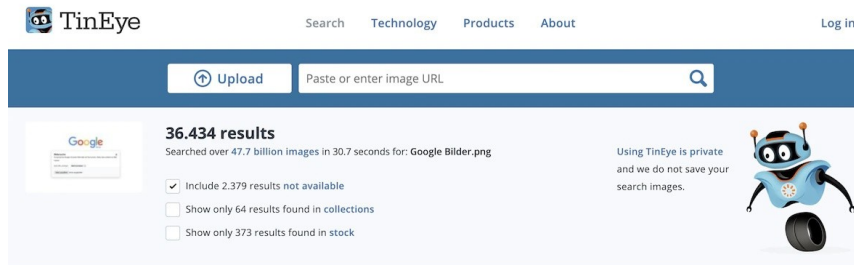
dem Sinne eigentlich keine Bildersuchmaschine, dennoch kann man hier einiges an wiederverwertbarem Material finden. Wikimedia ist eine Mediensammlung für gemeinfreien und frei-lizenzierten Inhalte (Bilder, Animationen, Audio- und Videodateien).

Von der Oberfläche her ähnelt Wikimedia - wie der Name es schon verrät - der Online-Enzyklopädie Wikipedia. Die Suchfunktionen sind etwas gewöhnungsbedürftig. Dafür kann man die unter der Creative-Commons-Lizenz geteilten Bilder, unter Angabe der Quelle, frei weiterverwenden.

Kindgerechte Bildersuche mit Picsearch: Der große Vorteil von Picsearch (picsearch.de) ist der starke Familienfilter. So werden Gewalt und anrühige Inhalte gut herausgefiltert, sodass sich Picsearch vor allem für den Familienrechner anbietet.

Die Rückwärts-Bildersuchmaschine - TinEye: Im Gegensatz zu den anderen hier vorgestellten Suchmaschinen liefert die Reverse-Image-Search TinEye (www.tineye.com) nicht die »hübschesten« Blumenmotive und Bilder von Katzenbabys, wenn man dies oder

ähnliches in das Suchfeld eingibt. Auf der Webseite von TinEye kann man eigene Bilder hochladen oder mit der URL eines bestimmten Bildes nach dessen Ursprung und den Webseiten suchen, die dieses Bild oder optisch sehr ähnliche Bilder verwenden.



Die Rückwärts-Bildersuchmaschine - Image Search: Mit Image Search (www.image-search.org) kann man online Bilder finden. Mit der umgekehrten Bildersuche (Reverse Image Search) kann man ähnliche Bilder auf verschiedene Arten (über die direkte Eingabe von Bilder - meist per Drag and Drop, Schlüsselworte, URL eines Bildes - die mittels der rechten Maustaste in die Zwischenablage kopiert wurde) mit jedem kompatiblen Gerät finden.

Die Funktion »My Photos« von Google: Wer viel fotografiert und die Fotos im Anschluss im Internet an vielen verschiedenen Orten präsentiert, verliert möglicherweise schnell den Überblick. Mit der Funktion »My Photos« macht die Google-Suche es möglich, die vielen eigenen hochgeladenen Fotos und Bilder im Netz wiederzufinden. Auch muss man sich als Nutzer so nicht mehr darum bemühen, die Bilder entsprechend in Kategorien einzuordnen, da Google dies bereits erledigt. Dank der »My Photos«-Suche kann man zum Beispiel alle Bilder aus dem Urlaub, vom Geburtstag oder von einer Hochzeit sofort und schnell

sich ausgeben lassen. Dies bietet vor allem bei vielen Bildern eine ausreichende Menge an Komfort.

Mit einem Bild bei Google suchen

Mit Google (images.google.com) kann man mehr über ein Bild oder Objekte erfahren. man hat beispielsweise die Möglichkeit, ein Foto einer Pflanze aufzunehmen und damit nach Informationen oder ähnlichen Bildern zu suchen.

Mögliche Ergebnisse:

- Suchergebnisse für Objekte auf dem Bild
- ähnliche Bilder
- Webseiten mit dem Bild oder einem ähnlichen Bild

Bild per Drag-and-drop hinzufügen

- Suchen Sie auf Ihrem Computer das Bild, mit dem Sie suchen möchten.
- Rufen Sie google.com oder google.de auf.
- Klicken Sie auf das Kamera-Symbol auf der rechten Seite des Suchfeldes.
- Ziehen Sie das Bild in das Suchfeld.

Mit einer URL suchen

- Rufen Sie auf Ihrem Computer die Webseite mit dem Bild auf, das Sie verwenden möchten.
- Kopieren Sie die URL, indem Sie zuerst mit der rechten Maustaste auf das Bild und dann auf **Bildadresse kopieren** klicken.
- Rufen Sie google.com oder google.de auf.
- Klicken Sie auf »Suche anhand von Bildern«.
- Fügen Sie die URL in das Textfeld unter **Bildlink einfügen** ein.
- Klicken Sie auf **Suchen**.

Wie finde ich den Urheber eines Fotos heraus?

Hier ist eine einfache Möglichkeit, dies herauszufinden. Man startet entweder den Browser oder die Google-App auf dem Smartphone. Nun kann man die betreffende Webseite aufrufen, auf der sich das Bild befindet. Nun kann man das Kontextmenü des Bildes aufrufen oder man tippt etwas länger mit dem Finger auf die Aufnahme und wählt danach die Option »In Google nach dem Bild suchen«. Der Browser öffnet daraufhin einen neuen Tab und startet die Rückwärtssuche. In der Regel findet man dann die Quelle des Fotos, also den Urheber oder den Ort, an dem es veröffentlicht wurde.

Kostenlose Lizenzen für Bilder mit Creative-Commons

Mit Creative-Commons-Lizenzen kann man Bilder kostenlos verwenden, solange man die Quellenangabe nicht vergisst. Allerdings gibt es auch Einschränkungen, wie und in welchem Kontext man die Bilder verwenden darf. Man sollte unbedingt beim Herunterladen der Bilder auf die Lizenzbedingungen achten.

BGH-Urteil: Google darf Thumbnails verwenden

Der Bundesgerichtshof (BGH) kam zu dem Schluss, dass Google bei der Verwendung von Thumbnails bei der Bildersuche keine Urheberrechte verletzt.

Der BGH begründet sein Urteil damit, dass es Suchmaschinen erlaubt sei, kleine Vorschaubilder in den Ergebnislisten zu zeigen. Diese Thumbnails machen es Nutzern möglich, schnell einen Eindruck von den gesuchten Bildern zu bekommen, ohne die entsprechenden Seiten dazu öffnen zu müssen. Der BGH befand außerdem, dass die Suchmaschinen für das Zeigen der kleinen Vorschaubilder in der Regel keine Gebühren zahlen müssen. Das Urteil des BGH ist in der Fachwelt als wegweisend angesehen. Es bedeutet, dass Suchmaschinen nun auch wesentliche Elemente

von Bildern zeigen dürfen, wenn sie diese in ihren Ergebnislisten anzeigen. Dies kann den Nutzern helfen, das gesuchte Bild schnell und einfach zu finden. Auf der anderen Seite müssen jedoch Urheber mehr denn je darauf achten, dass ihre Bilder nicht unberechtigt verwendet werden.

Google Lens: KI-basierte Bilderkennung für mehr Komfort

Mit »Google Lens« kann man mit dem Smartphone noch schneller auf Googles KI-basierten Bilderkennung zugreifen. Die mobile Bilderkennung ermöglicht es Texte, Gegenstände, Tiere, Pflanzen, Barcodes und vieles mehr zu erkennen und zuzuordnen. Ob man nach einem bestimmten Stoff, einer Pflanze oder sogar einem Ort sucht - »Google Lens« hilft dabei, schnell die gewünschten Informationen zu erhalten.

Mit »Google Lens« kann man von Dingen Informationen bekommen, indem man einfach die Smartphone-Kamera auf ein Objekt richtet. »Google Lens« erkennt dies und liefert die relevanten Informationen dazu. »Google Lens« kann beispielsweise das Rezept für ein Gericht anzeigen, wenn man ein Foto von einem Restaurant-Teller macht oder es zeigt Informationen zu Sehenswürdigkeiten an, wenn man beispielsweise von einem Gebäude ein Foto macht.

Google-Rückwärtsbildersuche: Echt oder Fälschung?

Nicht jedes Foto das man im Internet findet ist eine Fälschung. Aber wenn man ein gefundenes Bild überprüfen möchte, dann ist die Google-Rückwärtsbildersuche (Google Reverse Image Search) ein gutes Hilfsmittel. Dabei kann man einfach ein Foto hochladen und Google zeigt an, wo es bereits veröffentlicht wurde. So kann man schnell herausfinden, ob es sich um ein echtes oder ein gefälschtes Bild handelt. Mit ein wenig Recherche kann man so relativ schnell herausfinden, ob das Bild, authentisch oder manipuliert wurde.

Wie suche ich jemanden anhand eines Fotos?

Ausgangsbasis ist in der Regel das Bild einer Person und vielleicht noch ein Name dazu und sonst nichts. Dann hat man verschiedene Möglichkeiten vermisste oder gesuchte Personen zu finden.

Google Images – Bildersuche im Netz

Google Images besteht seit 2001 und ist ein Suchdienst von Google, mit dem Bildersuchen im Web durchgeführt werden können. Zusätzlich zum Bild können weitere Informationen eingegeben werden, so zum Beispiel Name, Wohnort oder Beruf. Mit der Bilder-Suchmaschine kann das Web auf drei verschiedene Arten durchsucht werden:

- Ein vorhandenes digitales Bild, wahlweise vom eigenen Computer oder aus dem Internet, wird einfach per Drag and Drop in das Suchfeld von Google Images gezogen.
- Über das Kamerasymbol kann ein Foto direkt hochgeladen werden. Per Klick wird das Startbild für die Suche ausgewählt.
- Ist die Suchgrundlage im Netz vorhanden, kann auch einfach die Bild-URL als Ausgangspunkt verwendet werden. Über das Kamerasymbol kann die zuvor kopierte URL eingefügt werden.

Suchen nach Bildern im Netz mit TinEye

Ein weiterer Suchdienst, der das Auffinden von Personen über Bilder und Fotos möglich macht, ist TinEye. Der Suchdienst wird häufig verwendet, um die Verbreitung eigener Bilder im Netz zu überprüfen - oder eben auch, um gezielt nach bestimmten Bildern und Personen zu suchen. Der Dienst ermöglicht ebenfalls die Suche nach Bildern anhand von Bildausschnitten.

Um eine Bildersuche über TinEye zu starten, wird die Bilddatei vom Rechner per Drag and Drop in das Suchfeld der Webseite gezogen.

Social Media – Suche in der Netzgemeinde

Hilft die Bildersuche im Netz nicht weiter, dann ist auch eine Suche über die Social Media Portale üblich. Über die Freundesliste kann das Foto verbreitet werden.

Allerdings gibt es hier einen rechtlichen Punkt zu beachten: Grundsätzlich dürfen Fotos von Personen im Netz nur mit deren Einwilligung veröffentlicht werden. Wer also diesen Weg wählt, geht eventuell ein Risiko ein und kann von der gesuchten Person rechtlich belangt werden.

Häufig werden auch vermisste Kinder per Facebook oder über andere Social Media Kanäle gesucht. Hier helfen auch die Initiativen für vermisste Kinder und weitere Organisationen, die sich auf diese Fälle spezialisiert haben.

Internet-Adressen:

Google-Images: images.google.com

Fotos von Personen und Haustieren suchen:

photos.google.com/people

TinEye: www.tineye.com

Ixquick: ixquick.com/deu/

Personensuche: <https://www.personensuche.de>

Wikimedia Commons:

https://commons.wikimedia.org/wiki/Main_Page?uselang=de

Picsearch: picsearch.de

Image Search: www.image-search.org

Spionage per Smart-TV

Bereits seit mehreren Jahren haben die Hersteller von Heimelektronik und Fernsehgeräten das Internet entdeckt. Fast jedes aktuelle Gerät ist mit einem Ethernet-Port oder einem WLAN-Adapter ausgerüstet. Und die smarten Geräte tun das, was in ihren smarten Namen bereits enthalten ist - sie sammeln Daten und werten diese auch fleißig aus.

Außerdem sind Geräte, die mit dem Internet verbunden sind, auch immer eine lohnendes Ziels für Cyberkriminelle.

Was kann ein Smart-TV?

Nutzerinnen und Nutzer können das smarte TV-Gerät - wie auch jedes Tablett oder ein Smartphone - mit dem Internet verbinden. Dadurch ergibt sich im Vergleich zu konventionellen Fernsehern eine ganze Bandbreite von zusätzlichen Funktionen:

- Zugriff auf die Mediathek mehrerer TV-Sender, um sich z.B. eine verpasste Sendung ansehen,
- Nutzung von Streamingdiensten wie »Netflix« oder »Amazon Prime«, für den Zugriff auf unzählige Serien, Filme und Dokumentationen,
- Videoplattformen wie »YouTube« oder »Vimeo« sind direkt am Fernseher abrufbar,
- Zugriff auf Musikdateien aus dem Internet,
- im Internet surfen, wie auf einem normalen Computer (nur nicht so komfortabel)
- die Videotelefonie über das smarte Fernsehgerät nutzen,
- Zugriff auf Fotos und Videos, die man auf Cloud-Diensten gespeichert hat,
- Spiele-Apps kann man am Fernseher auch ohne Konsole spielen und



- Inhalte von mobilen Geräten kann man auf das Smart-TV übertragen und dort anzeigen lassen.

In der Regel funktioniert die Steuerung der Menüs auf dem Bildschirm des Smart TVs mit der Fernbedienung intuitiv. Neuere Modelle bieten aber auch die Möglichkeit, die Steuerung über Sprachbefehle oder eine Touch-Fernbedienung durchzuführen.

Heimlicher Spion im Wohnzimmer?

Ein Smart-TV kann - je nach den Funktionen, die man aktuell nutzt - unzählige Informationen über die Nutzerinnen und Nutzer sammeln, z.B. wer wann wie lange welches Programm konsumiert hat.

Die Daten über das persönliche Nutzungsverhalten werden von den TV-Herstellern regelmäßig an Dritte, etwa an App-Anbieter, weiterverkauft.

Teilweise können sogar private Gespräche und Szenen, die sich vor dem Fernseher abspielen, mitgeschnitten und weitervermittelt werden. In Hinblick auf die Sicherheitslücken des Smart-TV ist deshalb oft vom »Spion im Wohnzimmer« die Rede. Die Agentur der Europäischen Union für Cybersicherheit (ENISA) hat schon 2015 vor der Gefahren für die Privatsphäre gewarnt, die von Smart-TVs ausgehen. Das Bundeskartellamt 2020 hat darauf hingewiesen, dass Smart-TV-Hersteller oft gegen geltendes Recht verstoßen. Seitdem haben einige Hersteller in dieser Hinsicht nachgebessert, auch um keine Bußgelder zu riskieren. Doch noch immer gibt es beim Smart-TV Sicherheitslücken.

Das sind einige Gefahren, die Nutzerinnen und Nutzer kennen sollten:

- Smart TVs verfügen meistens über eine eingebaute Kamera (**Hinweis:** es gibt auch schwer zu entdeckende Kameras mit einer ausfahrbaren Linse). Was die einzelnen Hersteller und App-Entwickler über diese Kamera mitschneiden, ist für Nutzerinnen und Nutzer oft nur schwer herauszufinden.
- Die Funktion der Sprachbefehle ist bequemer als die konventionelle Fernbedienung. Dafür kann der Fernseher aber auch die Geräusche und Gespräche belauschen, auch wenn dies nicht beabsichtigt ist.
- Ist das Smart-TV mit anderen Geräten verknüpft, etwa mit dem Smartphone, so können die Hersteller ein Cross-Device-Tracking (geräteübergreifende Erfassung) betreiben. Das heißt, sie sammeln die Daten der Nutzerinnen und Nutzer und erstellen ein Nutzungsprofil über verschiedene Geräte hinweg.
- Wie alle internetfähigen Geräte können auch Smart TVs zur Zielscheibe von Cyberangriffen durch Hacker werden. Je mehr smarte Geräte im Haus sind, desto wichtiger ist die Absicherung des privaten WLAN (Router) durch ein starkes Passwort.

Praktische Empfehlungen für die Sicherheit beim Smart TV

Mit einigen einfachen Maßnahmen können Nutzerinnen und Nutzer das Smart-TV ein Stück sicherer machen - ohne auf dessen Vorteile komplett verzichten zu müssen.

- Man sollte sich möglichst noch vor dem Kauf informieren, wie man die Mikrofone, Kameras und die Erfassung persönlicher Daten deaktivieren kann. Falls eine Änderung der Einstellungen gar nicht vorgesehen ist, so sollte man sich unbedingt für ein anderes Modell entscheiden.
- Als erstes sollte man die Kamera in den Einstellungen deaktivieren, falls vorhanden und nicht wirklich benötigt. Noch besser: Man klebt die Kamera mit einem schwarzen Klebeband oder einem Stück Karton ab. Nur so verhindert man mit einiger Sicherheit, dass die TV-Hersteller oder Hacker private Szenen aus dem Wohnzimmer mitschneiden können.
- Sofort nach dem ersten Anschließen des neuen Fernsehers sind in den Einstellungen des Geräts die Erfassung persönlicher Daten sowie die Weitergabe der Daten so weit wie möglich einzuschränken. **Hinweis:** Man sollte sich nicht auf die Standard-Sicherheitseinstellungen verlassen.
- Die Anbindung des Smart-TV an das private primäre WLAN ist keine gute Idee. Idealerweise sollte man für solche speziellen Geräte ein zweites WLAN nutzen. Möglich ist das etwa unter Verwendung von Gastnetzwerken (siehe auch: Bedienungsanleitung, Internet) die man nur für sich selbst nutzt. Man sollte auch dafür sorgen, dass die dort eingebundenen Geräte nicht untereinander kommunizieren können.
- Man sollte auf die Sprachsteuerung und Videotelefonie verzichten. Beide Funktionen mögen auf den ersten Blick reizvoll klingen, sind aber auch mit einer besonders intensiven Datenerfassung (Personalisierung: Stimm- und Gesichtserkennung) verbunden.

- Die Deaktivierung aller sonstigen Funktionen (z.B. ACR, Automatic Content Recognition oder automatische Inhaltserkennung), die man ohnehin nicht nutzen will, ist immer eine gute Idee. Die Hersteller der smarten Fernseher benutzen in den Einstellungen verschiedene Namen für die ACR-Technologie (Viewing Information Services, SyncPlus, Viewing Data, Smart Interactivity, Live Plus, interaktive TV-Einstellungen, Samba Interactive TV, ...).
- Apps deinstallieren: Auch auf dem smarten Fernseher sind Apps vorinstalliert oder man hat selbst ein paar Anwendungen installiert (Hinweis: Apps sammeln auch Daten). Dazu zählen Anwendungen wie HbbTV (Hybrid Broadcast Broadband TV), das meist auf dem roten Knopf auf der Fernbedienung hinterlegt ist. Betätigt man diesen Button, so liefert HbbTV Hintergrundinformationen aus dem Netz zur aktuellen Sendung. Deshalb sollten alle unnötigen oder nicht mehr genutzte Apps deinstalliert oder deaktiviert werden.
- Shopping-Tour vermeiden: Man sollte darauf verzichten, über den Smart TV zu surfen, einzukaufen oder Dinge zu konsumieren, wenn sensible Daten - wie Bankverbindungen, Kontodaten oder sonstige Nutzerdaten - abgefragt werden. So kann man sich auf einfachen Wege schützen.
- Die Aktualisierung der Software des Smart-TVs schließt in der Regel einige Sicherheitslücken (siehe auch: aktuelle Sicherheitslücken zum Gerät, die dem Internet bekannt sind). Um die Updates nicht manuell durchführen zu müssen, kann man die Updates über die Geräteeinstellungen automatisieren.
- Internetverbindung trennen: Wenn es hart auf hart kommt und man sich unsicher fühlt, so kann man das Smart TV auch einfach vom Internet trennen. Nachteil: Streamingdienste können dann nicht mehr genutzt werden. In diesem Fall stellt sich dann auch die Frage nach der Sinnhaftigkeit der Anschaffung eines smarten Fernsehers.

Welche Informationen können smarte Fernseher erfassen?

Der erste Schritt ist immer, sich darüber bewusst zu werden, dass man - egal mit welchem Gerät man sich im Internet bewegt - einen digitalen Fingerabdruck hinterlässt.

Hinsichtlich des Datensammelns muss man zwischen drei verschiedenen Kategorien unterscheiden:

- **Informationen zum Gerät:** IP-Adresse, Standort, Gerätenummer oder Werbe-ID
- **Nutzerdaten:** Geburtsdatum, Kontaktdaten, Mail-Adresse oder auch Bankdaten
- **Nutzerverhalten am TV:** Interaktionen des Nutzers mit dem Fernsehgerät, beispielsweise Cursorbewegungen oder besuchte Webseiten
- **ACR-Technologie (Automatic Content Recognition):** Daten sammeln mittels der automatische Inhaltserkennung (ACR) der genutzten Fernsehprogramme.

Dementsprechend sollte man sich stets die Fragen stellen, welche Informationen der smarte Fernseher überhaupt sammeln kann und welche Daten man mit anderen unbekannten Personen, Gruppen, Organisationen, Firmen, usw. teilen möchte.

Welche Art von Daten sammeln Smart-TVs?

Die Smart-TV-Überwachung nutzt eine ACR-Technologie (Automatic Content Recognition oder automatische Inhaltserkennung), um Daten zu sammeln und an Werbetreibende und Datenbroker (Datenhändler) zu verkaufen. Dabei wird das Zuschauerprofil um demografische Daten (Alter, Ethnizität, Geschlecht, Bildungsstand, ...) und der aktuellen IP-Adresse ergänzt. Diese Daten können auch Informationen liefern über den Standort und

eventuell auch über den sozioökonomischen Status der Nutzer. Anschließend kann den Nutzern auf mehreren Geräten (Smart-TV, Smartphone und Computer) gezielt Werbung für Produkte angezeigt werden, entsprechend der eingeordneten Nutzer-Kategorie. Unternehmen geben häufig an, dass sie durch diese Datenerfassung das Kunden- und Fernseherlebnis der Nutzer verbessern wollen, aber viele Smart-TVs können die Nutzer auch auf ungeahnte und vielfältige Weise überwachen. Unter Smart-TV-Spionage fällt außerdem das illegale Eindringen in ein WLAN-Netzwerk, um Zugriff auf den smarten Fernseher zu erlangen.

Bundeskartellamt: Smart TVs werden bezüglich des Datenschutzes teilweise als mangelhaft eingestuft

Das bei internetfähigen Fernsehgeräten Handlungsbedarf besteht, erkannte 2020 auch schon das Bundeskartellamt. In einem umfangreichen Bericht hat sich das Bundeskartellamt dem Thema Smart-TVs gewidmet. Die Behörde kommt darin zu dem Schluss, dass viele Hersteller massiv gegen die Datenschutz-Grundverordnung (DSGVO) verstoßen. Die Geräte sammeln dabei umfangreiche Informationen über ihre Besitzer, die vorwiegend zu Werbezwecken verwendet werden. Der Untersuchung des Bundeskartellamts zufolge können die Geräte Daten über das Fernsehverhalten, die App-Nutzung, das Surf- und Klickverhalten sowie biometrische Daten wie die Stimme oder Cursorbewegungen weitergeben. Das häufigste Ziel dieser Datenerfassung ist eine zielgerichtete, personalisierte Werbung oder sogar für crossmediale Werbezwecke (medienübergreifende Werbung).

Um die Datenschutzeinstellungen zu ändern, ist ein enormer Aufwand notwendig. Man muss sich durch die Systemeinstellungen kämpfen und dort nach den entsprechenden Optionen (mit schwer verständlichen Menüeinträgen) suchen, um sie zu deaktivieren,

soweit die Hersteller dies auch vorgesehen haben. Außerdem fehlt es an garantierter IT-Sicherheit, durch die Bereitstellung zeitnaher Updates seitens des Herstellers.

Darüber hinaus haben die Experten auch die IT-Sicherheit der Geräte unter die Lupe genommen. Bei etlichen Herstellern sei nicht gewährleistet, dass die Sicherheitsstandards auch in der Zukunft aufrechterhalten werden, etwa durch regelmäßige Softwareaktualisierungen. Keines der untersuchten Unternehmen mache verbindliche Angaben dazu, wie lange für ihre Produkte Sicherheitsupdates zuverlässig bereitgestellt werden.

Welche Arten von Spionage sind mittels Smart TV möglich?

2017 zeigten Forscher an der Universität von Washington beispielsweise auf, wie man mittels einer Software über das Soundsystem eines Smart-Geräts die Bewegungen von Personen in einem Raum verfolgen konnte. Dies funktioniert, indem fast nicht erkennbare Chirp-Signale (chirp ... zirpen) in der Musik versteckt werden. Diese Signale prallen am menschlichen Körper ab und fungieren mit den Gerätemikrofonen wie Sonarsignale. Die Software konnte innerhalb von etwa 7 Metern vom Gerät mehrere Personen mit einer Genauigkeit von ca. 18 cm erkennen.

Bei einem weiteren, im Frühjahr 2017 demonstrierten Hacking-Angriff, werden Funksignale eingesetzt, um altbekannte Schwächen in den auf Smart-TVs ausgeführten Webbrowsern auszunutzen. Im Grunde nutzen die Hacker Sicherheitslücken in den TV-Webbrowsern aus und betten mithilfe eines billigen Funksenders einen Code in ein abnormales TV-Signal ein. Wenn dieses Signal ausgestrahlt wird, können Hacker die Fernseher im Sendebereich kontrollieren. Anschließend können sie sich Kontrolle über andere Geräte verschaffen und Aktivitäten in den betreffenden Haushalten

überwachen. Bei einer neuen Spionagemethode wird ein neuronales Netzwerk und ein neuer, von Forschern an der Universität von Tel Aviv und an der Cornell University gemeinsam entwickelter Algorithmus eingesetzt, um Muster in Datenströmen von verschlüsselten Videos zu analysieren, z.B. von »Netflix«, »Amazon« und »YouTube«, um herauszufinden, was sich die smarten TV-Nutzer ansehen. Dazu braucht ein Hacker lediglich Zugriff auf das betreffende WLAN-Netzwerk.

So funktioniert's: Video-Streams werden in der Regel in Segmenten übertragen, den Bursts (data burst ... Datenpakete, Datenbündel), und über die variable Bitratenkomprimierung komprimiert. Bursts der gleichen Länge können somit unterschiedliche Datenmengen enthalten. Durch Messen der Bits pro Segmentlänge wird ein digitaler Fingerabdruck erstellt, der mit anderen, ausgewählten Videos verglichen werden kann, sobald das Muster bekannt ist.

Bei dieser neuen Methode muss das neuronale Netz anhand einer digitalen Fingerabdrucks-Bibliothek geschult werden, mit der ein Cyberkrimineller dann die abgegriffenen Daten mit denen der jeweiligen Videos vergleicht. Es ähnelt dem Vergleich von Fingerabdrücken, aber die Genauigkeit nach der Schulung beträgt nur 99 %.

Gerüchteweise wurden diese und wahrscheinlich noch andere Methoden, von einigen staatlichen Behörden bereits eingesetzt. Die wichtigsten anderen Funktionen umfassen einen **gefälschten AUS-Modus und eine WLAN-Neuverbindung**, damit Benutzer denken, dass das smarte Fernsehgerät ausgeschaltet sei, wenn es in Wahrheit weiter aufzeichnet. Außerdem waren gerüchteweise Strategien geplant, mithilfe von ähnlichen Methoden Videos aufzunehmen und diese über das WLAN des Fernsehers zu übertragen.

Diese Szenarien sind auf jeden Fall beunruhigend, aber am wahrscheinlichsten ist es, dass die Sehgewohnheiten der Nutzer von Smart-TV-Herstellern überwacht und die Informationen dann an Marketingunternehmen verkauft werden. Anders ausgedrückt, erfolgt die Spionage oft durch den Hersteller der smarten Fernseher. Im Februar 2017 wurde »Vizio« durch die »Federal Trade Commission« eine Strafe von 2,2 Millionen Dollar auferlegt. Das Unternehmen hatte die Sehgewohnheiten seiner Kunden (die smarten Fernseher wurden durch die IP-Adresse identifiziert) verfolgt und die Informationen dann an Inserenten (Anzeigenkunden) verkauft. Andere TV-Hersteller praktizieren ähnliche Spionagemethoden, aber bisher konnte kein Verkauf solcher Daten an Marketingunternehmen nachgewiesen werden.

Am effektivsten lassen sich Cybersicherheits-Risiken vermeiden, wenn keine Verbindung zum Internet besteht. In unserer modernen Welt ist dies aber nicht immer praktikabel.

Zusatzinfos über HbbTV

Das Hybrid Broadcast Broadband TV (HbbTV) ist ein Standard, nach dem Fernsehgeräte zusätzliche Informationen des eingeschalteten Senders abrufen. Dabei handelt es sich in den meisten Fällen um Programminformationen. Teilweise findet man allerdings auch Mediatheken-Angebote, um ältere Sendungen abzurufen, höher aufgelöste Versionen der Teletext-Seiten oder Zusatzangebote wie etwa eingeblendete Ticker-Nachrichten. Werbeclips werden ebenfalls über diese Technik verbreitet. Meistens macht ein eingeblendeter roter Button auf die HbbTV-Angebote aufmerksam, die man dann über einen ebenfalls roten Knopf auf der Fernbedienung erreicht und startet. Damit das funktioniert, wird beim Einschalten eines Senders automatisch dessen HbbTV-Website geladen. Dadurch erfahren die

Sendeanstalten dann bereits, wann sich wie viele Zuschauer in ihr Programm eingeklinkt haben. Doch häufig bleibt es nicht bei diesen anonymen Auswertungen. Teilweise werden auch die IP-Adressen sowie der Typ des smarten Fernsehgeräts erfasst. Durch das Setzen eines Cookies, was auch die einfachen Browser der Smart-TVs erlauben, lässt sich der Anwender sehr einfach identifizieren. Der Sender erfährt, zu welchen Zeiten der Nutzer fernsieht und bei welchen Sendungen er sich zuschaltet. Bei einigen Sendern übermittelt der Fernseher sogar im Minutentakt ein Signal, dass er noch aktiv und das Programm des Senders noch eingeschaltet ist. Mit allen diesen Daten lässt sich im Laufe der Zeit ein recht genaues Profil des Zuschauers und seiner Vorlieben anlegen.

Bei der Auswertung der Daten greifen die Sender auch gerne auf die Hilfe von »**Google Analytics**« zurück. Nun kann man zwar sagen, dass diese Auswertungen nicht über das hinausgehen, was auch von nahezu jeder größeren Webseite an Daten erfasst wird. Das Setzen von Cookies ist gängige Praxis und »Google Analytics« und andere Programme für die Auswertung von Besucherdaten sind ebenfalls weit verbreitet. Dass die Aufdeckung dieser Praktiken durch eine Studie der TU Darmstadt im Jahr 2014 ein so großes Medienecho hervorrief, hängt aber wohl damit zusammen, dass der Fernseher noch mehr als der PC als Bestandteil des Privatlebens angesehen wird. Zudem ist das Tracking von Zuschauern **ohne vorherige Information** der Nutzer juristisch äußerst fragwürdig.

HbbTV-Aufrufe verhindern

Es gibt verschiedene Wege, wie man sich schützen kann. Am einfachsten ist natürlich das Abziehen des Netzkabels beziehungsweise das Deaktivieren des WLAN-Clients.

Allerdings verzichtet man dadurch nicht nur auf viele praktische TV-Angebote im Internet, sondern man kann auch nicht mehr über das

smarte TV-Gerät auf die lokalen Netzwerkressourcen zugreifen.

Die zweite Methode besteht darin, HbbTV (Hybrid Broadcast Broadband TV) abzuschalten. Jedes Fernsehgerät bietet in der Regel dafür in seinen Menüs eine entsprechende Einstellung an.

Die dritte Methode ist aufwendiger, erlaubt jedoch eine feine Steuerung der Internetzugriffe. Man verwendet dazu die Filter, die nahezu jeder Router zur Verfügung stellt und die oftmals unter Bezeichnungen wie »Kindersicherung« den Zugang zu definierten Websites versperren.

Man legt durch Filterregeln erlaubte Internetseiten (Whitelist) explizit fest. Damit beschränkt man die Internet- und LAN-Zugriffe des smarten Fernsehers auf einige ausgewählte Adressen. Für das Surfen im Internet eignet sich ohnehin das Tablett oder Notebook deutlich besser. Teilweise ist beim Anlegen der Whitelist ein wenig Probieren erforderlich. Einige Internetdienste erfordern den Aufruf von zusätzlichen Webadressen, sonst funktionieren sie nicht. Damit etwa »Youtube« sich wie gewohnt bedienen lässt, muss auch der Zugriff auf »Google« erlaubt sein.

Man kann aber auch, eine Blacklist anlegen, die gezielt den Zugriff auf die HbbTV-Seiten der Sender blockiert. Bei der Vielzahl der Programme würde das aber einen erheblich höheren Aufwand bedeuten.

Hinweis: Die Whitelist einiger Router steuern lediglich den direkten Zugriff auf eine Webseite. Wenn diese wiederum von sich selbst aus weitere Seiten aufruft, etwa die Auswertung der Zugriffe durch spezielle Webseiten, lassen die Router dies häufig zu. Verhindern kann man das nur über eine Blacklist, die jedoch, wie bereits erwähnt, eine umfangreiche und mühevollen Konfiguration erfordert.

Was aber, wenn das Gerät seine Daten nicht über HTTP oder HTTPS an die Sender schickt, sondern einen Schleichweg über einen anderen Kanal wählt? Um dies zu verhindern, muss man noch sämtliche andere Ports schließen, die für den Datenverkehr im Internet verwendet werden. Dies lässt sich ebenfalls bei vielen Routern konfigurieren (Voraussetzung: ausreichendes Hintergrundwissen).

Wie gefährlich ist Google Analytics?

Im Zusammenhang mit dem Tracking im Internet und der Erfassung der Daten wird immer wieder »Google Analytics« genannt. Dabei handelt es sich um ein Tool zur Datenverkehrsanalyse, das die Besucher einer Webseite nicht nur zählt, sondern auch ihre Wege über die verschiedenen Seiten beobachtet, ebenso wie die Dauer und wie lange die Benutzer dort verweilen, welches Betriebssystem und welchen Browser die Benutzer verwenden, wo der Standort ist und welche Werbefbanner die Benutzer anklicken. Obwohl »Google Analytics« kostenlos ist, handelt es sich dabei um eine sehr professionelle und umfassende Anwendung. Datenschutzrechtlich ist der Dienst allerdings umstritten, da er die Daten ohne Einwilligung und Wissen der Benutzer erhebt und auch die IP-Adresse der Nutzer erfasst.

Falls ein Besucher bei einem Google- Account angemeldet ist, lassen sich die Analytics-Daten mit seinem Benutzerprofil verknüpfen.

Kritisch gesehen wird auch, dass die Auswertungen auf einem Google-Server in den USA landen. Internetnutzer können die Erfassung ihrer Daten durch »Google Analytics« verhindern, indem sie das Ausführen von Javascript auf Webseiten in ihrem Browser verbieten. Eine andere Möglichkeit ist, die Domain google-analytics.com im Router auf eine Blacklist zu setzen.

Die amerikanische FBI gibt folgende Empfehlungen

- Nutzer sollten genau wissen, welche Features, Funktionen das Smart TV hat und wie man diese kontrollieren kann (siehe auch: Internetsuche - Modellname des TV, Datenschutz, ...).
- Die Nutzer sollten sich nicht auf die Standard-Sicherheitseinstellungen des Fernsehgeräts verlassen. Man sollte auch unbedingt Bescheid wissen, wie man Mikrofone, Kameras und das Sammeln von Daten abstellen kann.
- Wenn die Kamera des Geräts nicht deaktiviert werden kann, hilft auch ein schwarzes Klebeband, das man auf die Kameralinse kleben kann.
- Man sollte regelmäßig prüfen, ob der Hersteller des TV-Geräts Sicherheitsupdates bereitstellt (Einstellungen: automatisierte Updates).
- Man sollte auf jeden Fall die Datenschutzbestimmungen des TV-Herstellers und der verwendeten Streaming-Dienste prüfen. Dort müssen die Nutzer eintragen, welche Daten gesammelt werden dürfen, wie und wo diese Daten gespeichert werden und was mit den Daten gemacht werden darf.

Fazit

Je mehr smarte Geräte die Verbraucher einsetzen, desto umfassender ist auch digitaler Fingerabdruck der TV-Nutzer. Gleichzeitig wird aus Sicht der Nutzer der smarten Geräte die Datenverarbeitung aber immer intransparenter.

Moderne smarte Geräte die von den Verbrauchern genutzt werden, verringern aktuell den Datenschutz und die Datensicherheit der Nutzer. Dies Phänomen ist als sogenanntes Privacy Paradox bekannt. Das Privacy Paradox kann nur durch umfangreiches Wissen über die smarten Geräte im privaten und familiären Umfeld aufgelöst werden.

Historie des Memex-Projektes

Der Memex (Memory Extender ... Gedächtnis-Erweiterer) ist ein als möglichst menschengerechtes, einfach bedienbares Wissensfindungs- und Verwertungssystem konzipierter Kompakt-Analog-Rechner, der 1945 von Vannevar Bush fiktiv vorgestellt wurde. Das Prinzip lag auch der bereits 1931 in den USA patentierten Statistischen Maschine von Emanuel Goldberg zugrunde. Vannevar Bush war ein Pionier des Analogrechners, folglich entspricht sein Bild des Memex als eines elektro-mechanischen Informationssystems dem damaligen Stand der Technik (Terminologie, Relationierung, Indizierung und Mikroverfilmung). Die Möglichkeiten von Digitalrechnern waren damals noch nicht abzusehen. Obwohl der Memex stets eine technisch-wissenschaftliche Utopie blieb, gab Memex seither beständig Ideen zum »Büro der Zukunft« vor. So wäre er nicht nur die erste Hypertext-Maschine, sondern auch der mikrofilmbasierte Vorläufer des Personal Computers gewesen. Im Digitalzeitalter hat das Microsoft-Forschungsprojekt »MyLifeBits« die Ideen Vannevar Bushs als Leitgedanken wieder aufgenommen.

Was ist Memex?

Die Defense Advanced Research Projects Agency (DARPA), das Forschungsprojekte für das US-Verteidigungsministerium durchführt, entwickelt eine Suchmaschine namens Memex. Sie soll sich wesentlich besser eignen, auf bestimmte Aufgabengebiete zugeschnittene Recherchen durchzuführen.

Die US-Forschungsbehörde DARPA hat Teile von »Memex« unter Open-Source-Lizenzen veröffentlicht, aus denen die spezialisierte Suchmaschine für das »Darknet« (»Tor«) besteht. Mit »Memex« soll auch das »Deep Web« und vor allem das Tor-Netzwerk durchsucht werden können. Auch die Entwickler des Tor-Projektes haben beim Bau des Systems geholfen.



Im Gegenzug finanziert die Behörde für einige Jahren Verbesserungen im Tor-Netzwerk, die den Datenverkehr beschleunigen und die Sicherheit der Nutzer erhöhen sollen.

Das Tor-Projekt wolle im Gegenzug der DARPA und somit den Fahndern ein besseres Verständnis des Netzwerks vermitteln, aber keinesfalls die Anonymität der Benutzer gefährden.

Mit »Memex« kann man stark eingegrenzte Recherchen besser auszuführen, als es herkömmliche Web-Suchmaschinen aktuell können.

Ein Haupt-Einsatzgebiet für »Memex« ist vor allem die Verbrechensbekämpfung, etwa im Bereich des organisierten Menschenhandels oder der Drogenfahndung. Memex soll dabei auch Inhalte indizieren, die nur sehr kurz online sind oder in Teilen des Netzes liegen, die nicht umfassend von üblichen Suchmaschinen abgedeckt werden.

Tor-Chefentwickler: Kriminelle schaden dem Anonymisierungs-Projekt (Stand: 2015)

Unter anderem arbeitet das Tor-Projekt mit den Entwicklern von »Memex« zusammen und wird im Gegenzug finanziell unterstützt.

Tor-Entwicklungschef Roger Dingledine äußerte sich dazu und versicherte, es ginge den Tor-Entwicklern nur darum, den Fahndern und DARPA-Entwicklern ein besseres Verständnis des Tor-Netzes zu vermitteln. Man wolle nichts unternehmen, was die Sicherheit des Anonymitäts-Netzwerkes untergraben könne. Ein Ziel von »Memex« ist es, sogenannte Hidden Services (verborgene Dienste) im Tor-Netz zu finden und zu durchsuchen - etwa illegale Drogen-Marktplätze.

Entwicklungschef Roger Dingledine vertritt die Einstellung, dass Hidden Services, deren Adressen öffentlich verfügbar seien, auch gefunden werden dürfen. Kriminelle seien zwar nur eine geringe Prozentzahl der Tor-Nutzer, würden dem Projekt aber sehr schaden.

Trotzdem sei man vorsichtig, welche Informationen man an die Memex-Entwickler weitergebe. Der Leiter des Projektes habe ihm versichert, es sei nicht das Ziel, Tor löchrig zu machen. Grundsätzlich geht es bei »Memex« eher darum, sehr viel Informationen aus vielen Quellen zu sammeln und mit Big-Data-Werkzeugen automatisch zu analysieren.

Die Memex-Bausteine befinden sich unter einer Handvoll von Open-Source-Lizenzen. Links zu den einzelnen Projekten bei »GitHub« finden sich im Open Catalog der DARPA. Allerdings stellt die Behörde so gut wie keine Dokumentation zur Verfügung, wie die freigegebenen Komponenten der DARPA-Software »Memex«, der

vielen verschiedenen Drittanbieter, zusammenpassen. Auch der Mix aus verschiedenen Lizenzen kann die Weiterbenutzung in anderen Projekten erheblich erschweren. Besonders für Software, die der Gemeinfreiheit (»Public Domain«) unterliegt, ist das in einigen Rechtssystemen bedenklich, da der Begriff »Public Domain« keine Lizenz, sondern die Abwesenheit einer solchen darstellt.

Die Memex-Suchmaschine wurde für die Verbrechensbekämpfung entwickelt (Stand: 2015)

Die »Memex« genannte Suchmaschine soll sich für Recherchen, die auf bestimmte Aufgabengebiete zugeschnitten sind, besser als die üblichen Suchmaschinen eignen - insbesondere bei der Verbrechensbekämpfung. Selbst spezielle Suchmaschinen für das Tor-Netzwerk eignen sich nur begrenzt für die Verbrechensbekämpfung.

Mit »Memex« sollen Recherchierende wesentlich besser mit den Ergebnissen hantieren, sie auf neue Art organisieren und besser in Teilergebnissen weitersuchen können. Die DARPA hat der amerikanischen Reportagereihe »60 Minutes« und dem Magazin »Scientific American« eine Demonstration von »Memex« gegeben. In einem Video von »60 Minutes« sieht man zum Beispiel Informationen die als Graphen oder Karten aufbereitet wurden.

Vor allem aber durchsuche »Memex« einen wesentlich größeren Anteil der im Netz verfügbaren Informationen. Laut Chris White, dem für »Memex« zuständigen Manager, erschließen die üblichen Suchmaschinen nur **etwa fünf Prozent** der Informationen im Web.

Der Rest, das sogenannte »Deep Web« oder »Dark Web« (»Tor-Netzwerk«) besteht zum Teil aus unstrukturierten Daten, etwa Sensordaten oder Daten »anderer Geräte«, die sich nicht von

traditionellen Suchmaschinen erfassen lassen.

Hinweis: »Memex« soll nicht nur Webseiten im Tor-Netzwerk (»Dark Web«) sammeln und indizieren, sondern auch Inhalte im sogenannten »Deep Web« entdecken.

Außerdem gibt es temporäre Seiten, die schneller wieder verschwinden, als Suchmaschinen sie erfassen können, sowie Informationen, die nur mit spezieller Software zugänglich sei, etwa über das Tor-Netzwerk. Im Schutz dieses »Dark Web« floriert der Menschenhandel sowie der Handel mit illegalen Drogen und Waffen.

»Memex« oder zumindest ein Teil der Implementierung, ist offensichtlich erfolgreich bereits im Einsatz, insbesondere bei der Fahndung nach Menschen- und Drogenhändlern und bei der Bekämpfung der Kinderpornografie.

Die gesammelten Informationen, darunter auch von Werbeeinblendungen, werden zusammen mit Standortdaten durch »Memex« visualisiert und sollen es den Fahndern erlauben, Bewegungsprofile möglicher Täter zu erstellen.

Laut dem Bericht im »Scientific American« wurde das Werkzeug von der New Yorker Bezirksstaatsanwaltschaft in 20 Untersuchungen zum Menschenhandel eingesetzt. Grundsätzlich soll sich »Memex« aber auch für die Fahndungen in anderen Bereichen sowie zur Terrorismusbekämpfung eignen.

Suchmaschinen für das Tor-Netzwerk (Stand: 2015)?

Das Tor-Netzwerk sorgt sich um die Anonymität seiner Benutzer, wie also können Suchmaschinen dort überhaupt funktionieren?

Damit Hidden Services dennoch erreichbar sind, benötigen sie wie im normalen Web eine Adresse, die normalerweise jedoch in Form eines Hashwerts vorliegt. Die Tor-Adresse der Suchmaschine Duckduckgo lautet <http://3g2upl4pq6kufc4m.onion>. Diese Adresse lässt sich nur in einem Tor-kompatiblen Browser öffnen. Duckduckgo liefert übrigens auch über seine Tor-Adresse nur Resultate aus dem normalen Web.

Jeder Hidden Service generiert regelmäßig einen Beschreibungswert, den sogenannten Descriptor. Dieser Descriptor enthält eine Liste der Knoten, über die der Hidden Service aktuell erreichbar ist und eine Identifikationsnummer, die Descriptor-ID, die ihrerseits ein Hashwert ist. Dieser Hashwert ändert sich alle 24 Stunden. Der Hashwert wird über einen Distributed Hash Table (DHT) in den sogenannten Hidden Services Directories veröffentlicht, die wiederum auf ausgewählten Tor-Konten liegen.

Dieser dynamische Aufbau sorgt für Anonymität, stellt aber ein Hindernis für Suchmaschinen dar, die aktuelle Ergebnisse liefern wollen. Die Crawler der Suchmaschinen müssen sich nämlich an den DHTs (Distributed Hash Table) orientieren, um eine Verbindung zu dem Hidden Service herzustellen, den sie indizieren wollen.

Es gibt aber noch ein weiteres Problem: Ein solcher Tor-Knoten kann genutzt werden, um die Descriptor-IDs zu manipulieren und so einen DDoS-Angriff (DDoS ... distributed denial of service oder verteilte Dienstblockade) innerhalb des Tor-Netzwerks zu starten. Solche Angriffe gibt es immer wieder und sie lassen sich erst beenden, wenn die Betreiber des Tor-Netzwerks einen solchen Knoten identifizieren und abschalten. Mit Hilfe einer neuen Finanzierungsrunde durch die DARPA soll das Tor-Protokoll in den nächsten Monaten modernisiert werden, so dass beispielsweise

versteckte Dienste auf mehreren Hosts laufen können. Das soll nicht nur DDoS-Angriffe mildern, sondern auch den steigenden Datenverkehr innerhalb des Netzwerks besser verteilen. So will das Tor-Netzwerk eine vergleichbare Surfgeschwindigkeit erreichen, wie sie im normalen Web üblich ist. Zudem soll die Verschlüsselung des Identitätsschlüssels der jeweiligen Hidden Services erhöht werden, und das Original des Schlüssels soll auch offline gespeichert werden können.

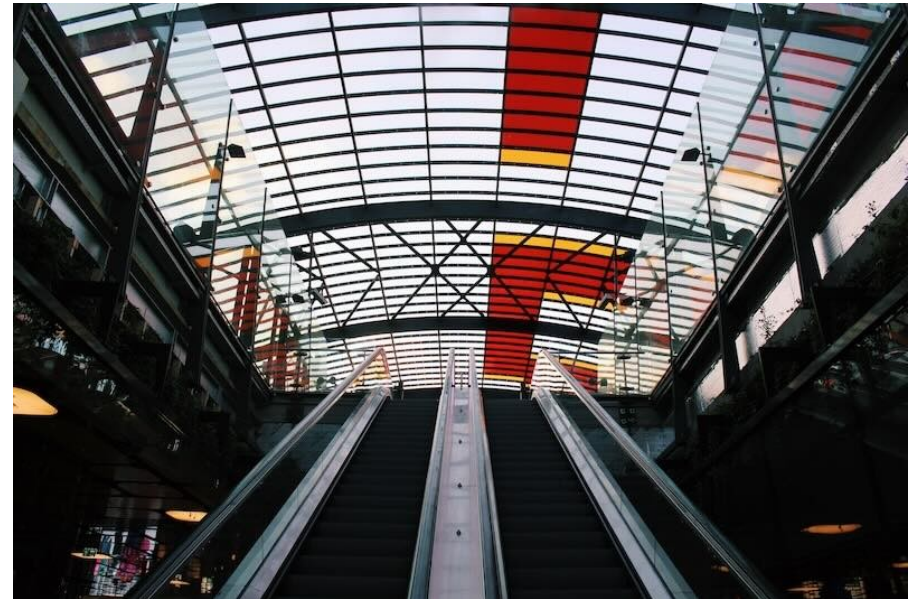
Suchmaschinen im Tor-Netzwerk haben es also ungleich schwerer, aktuelle und zuverlässige Suchergebnisse zu liefern, wenn sie überhaupt aufgerufen werden können. Auf der zentralen Anlaufstelle »The Hidden Wiki« (http://zqkltwi4fecvo6ri.onion/wiki/index.php/Main_Page) gibt es eine Liste von Suchmaschinen, von denen viele nicht immer erreichbar sind und einige lediglich eine Liste von Onion-Seiten bereitstellen, die es teilweise gar nicht mehr gibt.

Die Arbeitsgruppe Kritische Infrastrukturen (AG KRITIS, Webseite: ag.kritis.info) ist eine Gruppe von Fachleuten, die sich die Verbesserung der IT-Sicherheit und Resilienz von Kritischen Infrastrukturen (KRITIS) gemäß § 2 (10) BSI-Gesetz zum Ziel gesetzt hat. Die AG KRITIS wurde 2018 im Nachgang zum 34. Chaos Communication Congress des CCC (Chaos Computer Club) im Rahmen eines Arbeitstreffens gegründet und sieht sich selbst als unabhängig von Unternehmen und Wirtschaftsverbänden.

Der Grundgedanke der Gründung der AG KRITIS im Jahr 2018 war, dass die Ressourcen der Bundesrepublik Deutschland zur Reaktion auf Großschadenslagen durch Cyber-Vorfälle im Bereich der Kritischen Infrastrukturen nicht ausreichen, um die Auswirkung der dadurch verursachten Krisen und Katastrophen zu bewältigen. 2019 wurde schließlich die Loslösung vom CCC beschlossen, um größtmögliche Unabhängigkeit und Neutralität zu erreichen.

Die Mitglieder der AG KRITIS werden regelmäßig als Sachverständige befragt oder zitiert, z.B. zu Sicherheitslücken, dem IT-Sicherheitsgesetz oder sonstigen Themen rund um die Kritische Infrastrukturen und Digitalisierung.

Die AG KRITIS besteht aus 44 Fachleuten (Stand: 2023), die sich täglich mit Kritischen Infrastrukturen (KRITIS) gemäß § 2 des BSI-Gesetzes beschäftigen. Die Mitglieder sind unter anderem in den KRITIS- Sektoren: Energie, Gesundheit, Ernährung, Transport und Verkehr, Finanz- und Versicherungswesen, Informationstechnik und Telekommunikation, Wasser sowie Staat und Verwaltung als auch Medien und Kultur dienstlich aktiv. Die Arbeitsgruppe stimmt sich aktuell zweiwöchentlich telefonisch bzw. über Videokonferenzen ab und trifft sich unregelmäßig zu Workshops. Neben zwei Leitern sind einzelne Mitglieder als offizielle Sprecher der AG KRITIS benannt.



Hinweis: Seit November 2020 ist die AG KRITIS im Online-Kompendium Cybersicherheit in Deutschland des BMI (Bundesministerium des Inneren) als relevanter Akteur der deutschen Cybersicherheitslandschaft aufgeführt.

KRITIS-Dachgesetz (KRITIS-DachG)

Das KRITIS-Dachgesetz reguliert ab dem Jahr 2024 die Resilienz und physische Sicherheit Kritischer Infrastrukturen. Das Gesetz setzt die EU-Direktive **EU RCE** (EU 2022/2557) in Deutschland durch zusätzliche Pflichten für Betreiber kritischer Anlagen um (z.B. Meldepflichten, physische Sicherheit, Personal und Krisenmanagement).

Mit Cyber-Grooming oder Internet-Grooming wird die gezielte Manipulation Minderjähriger sowie junger Volljähriger über das Instrument Internet bezeichnet.

Der Begriff »Cybergrooming« setzt sich aus den englischen Begriffen »cyber« (dt. ...Internet) und »grooming« (dt. ... Pflege, Zurechtmachen oder auch sexuelle Anmache, Anbahnung mittels der Informationstechnik) zusammen.

Das Ziel von Cybergrooming ist, das Opfer in eine Falle zu locken, um Straftaten wie sexuell motivierte Übergriffe bis hin zur Vergewaltigung zu begehen. Die Kontaktaufnahme erfolgt mit dem konkreten Ziel, sexuellen Missbrauch oft über viele Jahre hinweg online oder offline bei realen Treffen anzubahnen. Dies geschieht per Chat, Fotos, Videos, Sexting (Versenden freizügiger oder erotischer Bilder und Texte per Mobiltelefon), Erpressung z.B. mit Hilfe pornografischer Videoaufnahmen. Der Begriff Cybergrooming wird im allgemeinen auch für sexuelle Belästigung im Internet verwendet.

Hinweis: Wie auch bei der Verbreitung und dem Besitz von kinderpornografischen Schriften, treten bei Cyber-Grooming vermehrt minderjährige Tatverdächtige in Erscheinung.

Mitunter besteht auch »nur« ein rein finanzielles Interesse organisierter Krimineller, mittels Erpressung (Veröffentlichung von intimen Fotos oder Videos).

Vorgehen der Täter

Der Täter baut zunächst, teilweise über mehrere Monate oder sogar Jahre, Vertrauen auf - um dann Straftaten wie etwa die Anfertigung kinderpornografischer Aufnahmen oder sexuellen Missbrauch an arglosen Kinder und Jugendliche zu verüben. Das



englische Wort Grooming (striegeln, zurechtmachen, vorbereiten) bezieht sich hierbei darauf, dass den potentiellen Opfern durch einige Täter zu Beginn geschmeichelt wird oder Geschenke gemacht werden. Darüber hinaus manipulieren die Täter oftmals die Wahrnehmung der Opfer. Dies führt in vielen Fällen dazu, dass die Betroffenen ihre Erlebnisse für sich behalten.

Ogleich es sich dabei um eine Erscheinungsform von Cyber-Grooming handelt, ist aktuell noch nicht bekannt, wie oft sich der sexuelle Missbrauch tatsächlich von der virtuellen in die reale Welt verlagert. Einer Studie zufolge wurde zuletzt im Jahr 2010 durchschnittlich fast jeder sechzigste Jugendliche im Alter von 15 Jahren bei einem Treffen mit einer älteren Online-Bekanntschaft sexuell belästigt. Mit einem persönlichen Treffen außerhalb des Internets gehen die Minderjährigen in jedem Fall ein großes Risiko ein, da den Opfern die wahre Identität des Täters meist nicht bekannt ist. Um sich wiederum zu vergewissern, dass der Täter es

tatsächlich mit einem Kind zu tun hat, bringt dieser häufig vor einem Treffen die Kontaktdaten des Opfers in Erfahrung und überprüft selbstige auf Richtigkeit.

Das Internet als Tatort

Das Internet bietet aus Sicht der Täter eine äußerst effektive Möglichkeit, Kontakt zu potentiellen Opfern aufzunehmen. Insbesondere auf die Gefahr von Online-Spielen wies die ProPK (Polizeiliche Kriminalprävention der Länder und des Bundes) im Jahr 2020 hin. In diesem Zusammenhang rückte vor allem das Online-Spiel »Fortnite« in den Vordergrund, das mit diversen Fällen von Cyber-Grooming in Verbindung gebracht wurde. Die dort vorhandene Chat-Funktion und die meist zufällige Konstellation der Spiel-Teams bietet laut ProPK die Möglichkeit, sich den minderjährigen Nutzern unbemerkt anzunähern.

Aber auch andere soziale Netzwerke und Plattformen werden von den Tätern aktiv zur Kontaktaufnahme genutzt. Die grundsätzliche Attraktivität des Internets im Rahmen von Cyber-Grooming lässt sich durch diverse Eigenschaften erklären, die dieses Medium mit sich bringt:

- vermeintliche Anonymität
- unbegrenzte räumliche und zeitliche Verfügbarkeit
- extrem schnelle und breitflächige Übermittlung von Information und Kommunikation

Die Profile der Kinder und Jugendlichen geben dabei ausreichend Informationen an den Täter preis, um Gemeinsamkeiten vorzutäuschen und damit eine gewisse Verbundenheit herstellen zu können. Nicht selten geben sich die Täter dabei als ungefähr gleichaltrig aus oder stellen sich als verständnisvolle Erwachsene mit ähnlichen Erfahrungen und Interessen dar. So gewinnen sie

das Vertrauen ihrer Opfer mit dem Ziel, sie zu manipulieren. In vielen Fällen bringen sie die Kinder dazu, ihnen freizügige Selbstporträts zu senden. Die Fotos werden dann teilweise als Druckmittel gegen die Minderjährigen eingesetzt, um sie zu weiteren Handlungen zu bewegen. Einige Täter verfolgen außerdem das Ziel, sich auch »offline« mit den minderjährigen Opfern zu treffen, um sie zu missbrauchen. Zugleich schwinden die Schutzmechanismen aus der analogen Welt, weil sich die Kinder in ihren eigenen vier Wänden sicher fühlen. Das Internet führt zwar zu einer gewissen Distanz zwischen Opfer und Täter, jedoch bietet es mithilfe von textlichen und visuellen Inhalten ausreichend Platz für Intimität. Insbesondere durch die Nutzung von Webcams könne eine »Art sexueller Voyeurismus im virtuellen Raum« entstehen.

Präventionsmaßnahmen

Auf erster Ebene wird vor allem von Seiten der Familien-, Sozial- oder Schulpolitik Aufklärungsarbeit geleistet. Hierbei steht die Sensibilisierung im Umgang mit Medien und dem Internet, insbesondere in sozialen Netzwerke und Spiele-Plattformen, im Vordergrund. Ziel sollte stets sein, Opfer und begleitende Personen oder »unbeteiligte« Zuschauer zu stärken und die potentiellen Täter auf die Konsequenzen ihrer Handlung hinzuweisen. Zudem werden Maßnahmen getroffen, die die Tatbegehung erschweren. Hierzu zählen beispielsweise Sperr- oder Meldefunktionen in dem jeweiligen Portal, aber auch die Kontrolle von relevanten Internetseiten.

Eltern sollten mit ihren Kindern gemeinsam vereinbaren, dass bei einer Nutzung von Online- Diensten niemals private Daten wie die Adresse und Telefonnummer mitgeteilt werden sollten. Sie sollten sie dafür sensibilisieren, dass es Menschen gibt, die sich als Kinder oder verständnisvolle Gesprächspartner ausgeben und sehr raffiniert vorgehen, um ihr wahres Alter oder ihre wahren Absichten

zu verbergen. Sie sollten mit ihnen das Thema Cybergrooming besprechen und aufzeigen, ab welchen Zeitpunkt ein Chat gefährlich werden kann.

Zuletzt sollten, nachdem die Straftat bereits begangen wurde, auch die Täter selbst, ihre Motive sowie der genaue Tathintergrund in den Fokus der Präventionsarbeit rücken. Als denkbare Maßnahmen gelten hier schon die Anzeige oder Aussage des Opfers, die zur Ergreifung des Täters führen können.

Inwieweit die getroffenen Maßnahmen tatsächlich zur Verminderung des Problems beitragen, bleibt allerdings offen. Trotz der vielversprechenden Ansatzpunkte, gilt die Wirksamkeit der Maßnahmen aus wissenschaftlicher Sicht noch nicht als bewiesen.

Anzeichen für Cybergrooming

Kinder sollten besonders vorsichtig sein, wenn:

- ein Chatpartner unbedingt privat schreiben will, etwa über einen Messenger- Dienst
- er sein Opfer unter Druck setzt und das Senden von intimen Bildern fordert
- er mit Geschenken oder mit Geld lockt
- er Nachrichten mit sexuellem Inhalt versendet
- er persönliche Daten fordert (Adresse, Telefon-Nummer, Bilder mit GPS-Koordinaten, ...)
- der Chatpartner oder Täter kein »NEIN« akzeptiert
- er die Anweisung gibt, es soll alles geheim bleiben
- er auf ein persönliches Treffen drängt mit dem Ziel, sein Opfer zu missbrauchen

Hinweis: Einige soziale Netzwerke und Plattformen haben

mittlerweile Sicherheitsvorkehrungen eingerichtet, um Cybergrooming zu erkennen und verdächtige Nutzerinnen und Nutzer auszuschließen. Bei den Messengerdiensten sind die Nachrichten in der Regel verschlüsselt - der Täter kann dadurch sicher sein, dass er mit seinem Opfer »allein« ist, um das Opfer zum Austausch intimer Nachrichten überreden zu können.

Opfer verlieren die Kontrolle

In manchen Fällen erpressen Täterinnen und Täter ihre Opfer mit der Veröffentlichung oder Weiterleitung bereits übersandter Nacktfotos oder -Videos und fordern ein Treffen in der realen Welt zum Zwecke des sexuellen Missbrauchs oder zur Übersendung weiterer Fotos und Videos. Einmal auf diese Weise im Internet veröffentlichtes sexualisiertes Bild- oder Videomaterial bleibt weiter im Umlauf. Es wird in der Regel getauscht, an Dritte weitergegeben oder auf andere Weise verbreitet. Die Gründe hierfür sind vielfältig. Neue und unbekannte Aufnahmen ermöglichen den Tätern oft, an weiteres, wenig verbreitetes kinder- und jugendpornografisches Material zu gelangen.

Was ist zu tun, wenn man auf diese Art »angemacht« wird?

- Das Gespräch mit einer Vertrauensperson ist wichtig. Dies können zum Beispiel Freunde/Freundinnen, eine Lehrkraft oder die Eltern sein.
- Für Kinder und Jugendliche gilt: Triff dich nie allein mit einem dir nicht persönlich bekannten Chatpartner - auch nicht aus Neugier.
- Erwachsene sollten solche Treffen ebenfalls vermeiden oder zumindest auf ein Treffen in der Öffentlichkeit bestehen.
- Bilder, insbesondere freizügige Bilder, nie an unbekannte Personen, die man nur aus der virtuellen Welt kennt, versenden.

Bei beweisbaren Cybergrooming (Screenshots, Bilder, Texte, ...), kann man Strafanzeige erstatten oder ein Termin für ein ausführliches Beratungsgespräch bei der Polizei vor Ort vereinbaren.

Hinweis: Es gibt Opferberatungsstellen für Kinder und Eltern, die dabei helfen, das Erlebte zu verarbeiten.

In der polizeilichen Kriminalstatistik (Jahr: 2022) wurden 2.878 Fälle von sexuellem Missbrauch von Kindern ohne Körperkontakt mit dem Kind erfasst. Allerdings spiegelt sich nicht die tatsächliche Verbreitung von Cybergrooming in der Statistik wider. Dies liegt zum einen an der **hohen Dunkelziffer**, denn viele (versuchte) Fälle von Cybergrooming werden der Polizei gar nicht gemeldet. Zum anderen sind die Grenzen zu anderen Tatbeständen wie etwa Kinderpornografie mitunter fließend.

Wie können Eltern zur Verhinderung der Straftat beitragen?

- Sprechen Sie mit Ihren Kindern über die Problematik und achten Sie darauf, dass Ihre Kinder in Chats und sozialen Netzwerken keine persönlichen Angaben wie Adresse und Telefonnummer machen.
- Wirken Sie darauf hin, dass Kinder und Jugendliche verantwortungsvoll mit ihren Fotos und Videos umgehen und nicht alles posten, insbesondere keine Aufnahmen aus dem intimen Lebensbereich.
- Eltern und Pädagogen sind gefragt, sich mit dem Internet auseinanderzusetzen und sich gemeinsam mit den Kindern über mögliche Gefahren, aber auch den Nutzen des Internets auszutauschen.
- Besprechen Sie mit Ihren Kindern den Unterschied zwischen einem »Freund« im realen Leben und einem »Freund« in der virtuellen Welt.

- Helfen Sie Ihren Kindern bei den Einstellungen für die Privatsphäre in sozialen Netzwerken, um private Informationen auf ein Mindestmaß zu reduzieren und nur einem engen Personenkreis sichtbar zu machen.

Rechtslage

In Deutschland ist Cyber-Grooming seit dem 1. April 2004 (Verschärfung des Gesetzes: 26. Januar 2015) bei unter 14-jährigen Personen verboten. Dafür wurde der damals neue § 176 Absatz 4 Nr. 3 (Strafgesetzbuch (StGB)) geschaffen:

[...] Mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren wird bestraft, wer [...] auf ein Kind durch Schriften (§ 11 Abs. 3) oder mittels Informations- und Kommunikationstechnologie einwirkt, um es zu sexuellen Handlungen zu bringen, die es an oder vor dem Täter oder einem Dritten vornehmen oder von dem Täter oder einem Dritten an sich vornehmen lassen soll [...].

Hinweis: In der am 17. Dezember 2011 in Kraft getretenen EU-Richtlinie 2011/93/EU ist vorgesehen, in den Mitgliedstaaten der Europäischen Union auch den Versuch der »Kontaktaufnahme zu Kindern für sexuelle Zwecke« (auch im realen Raum) unter Strafe zu stellen. Während Österreich diesen Teil der Richtlinie bereits 2012 umgesetzt hat, kam Deutschland dem erst 2015 nach.

Der Kontakt muss dabei nicht zwingend sexuell geprägt sein. Bereits die Anbahnung solcher Gespräche fallen unter den Tatbestand des Cybergrooming. Strafbar ist die Kontaktaufnahme, die mit der Absicht erfolgt, das Kind zu sexuellen Handlungen zu bringen. Zu »tatsächlichen« sexuellen Handlungen muss es nicht kommen - allein die Absicht genügt. Auch muss das Kind nicht auf die Nachrichten reagiert haben: Für eine Strafbarkeit reicht es aus, dass das Kind eine solche Nachricht zur Kenntnis genommen hat.

IT-Sicherheit beim Umgang mit smarten Haushaltshelfern

Datenschutz im Smart Home hat in den vergangenen zwei Jahren massiv an Bedeutung gewonnen.

Die smarten Haushelfer, z.B. die Saugroboter, sind dann für den persönlichen Datenschutz problematisch und können zu einer Gefahrenquelle werden, wenn sie Informationen unkontrolliert und unverschlüsselt weiterleiten.

Damit der Saugroboter die Wohnung möglichst klug und effizient reinigen kann, setzen viele Hersteller auf smarte Funktionen und auf eine Internet-Anbindung an einer Daten-Cloud.

Manche Saugroboter können heimlich Bilder und Audiodateien per WLAN oder Bluetooth an das Smartphone des Besitzers des Saugroboter senden. Der Saugroboter zeigt den beobachteten Personen aber nicht an, wenn entsprechende Aufnahmen gemacht werden. Diese Funktion ist als problematisch zu betrachten.

Ein Saugroboter ist ein nützliches technisches Haushaltsgerät, das in der eigenen Wohnung jeden einzelnen Raum kennt. Er kennt jede Ecke, jeden Winkel und jeden Kasten. Damit ihm das gelingt und er effizient reinigen kann, ist er mit zahlreichen Sensoren und Kameras ausgestattet. Sie helfen ihm dabei Karten von seiner Umgebung zu erstellen, um sich zu orientieren und Hindernissen geschickt auszuweichen.

Die dabei entstandenen Daten müssen im Anschluss verarbeitet und zum Teil gespeichert werden. Dies kann in einer Daten-Cloud des Herstellers erfolgen. Dafür und für eine bequeme Steuerung - auch von unterwegs - sind die allermeisten Saugroboter internetfähig und per App oder Sprache steuerbar.



Was auf den ersten Blick sehr praktisch klingt, lässt bei einigen Menschen die Alarmglocken schrillen. Denn der Roboter ist die ganze Zeit über mit dem Internet verbunden.

Saugroboter, die Daten über die Wohnung sammeln, könnten Informationen über die komplette Einrichtung, die Gewohnheiten der Wohnungsinhaber und sogar die Struktur des Hauses sammeln. Dies sind sensible Informationen, die geschützt werden müssen.

Wenn die Daten, die der Saugroboter sammelt, in falsche Hände geraten, könnten Unbefugte Zugang zu Informationen über die Wohnung erlangen. Das kann zu Sicherheitsrisiken führen, zum Beispiel, wenn Einbrecher wissen, wie die Wohnung oder das Haus aussieht und wann die Wohnungsinhaber normalerweise nicht anwesend sind.

Hinweis: Das eigene Zuhause ist ein sehr persönlicher Raum und niemand sollte ungefragt Einblick in dessen Details haben.

Datenschutz & Privatsphäre

Smart-Home-Geräte verschaffen Hausbewohnern ein sicheres Gefühl, unabhängig davon, wo sie sich gerade aufhalten. Doch wie lässt sich der Datenschutz dieser Geräte optimal an die eigenen Bedürfnisse anpassen?

- Die Ende-zu-Ende-Videoverschlüsselung schützt auf Wunsch Video- und Audioaufnahmen die von den smarten Haushaltshelfern erstellt werden.
- Mit der Funktion für Privatsphärenbereiche lassen sich Tabu-Bereiche, wie die Haustür des Nachbarn, festlegen. Sie werden dann nicht vom Blickwinkel der Kamera erfasst und sind nicht im Live-Video zu sehen und werden dann auch nicht aufgezeichnet.
- Nutzer und Nutzerinnen können die Bewegungserfassung auf einen bestimmten Bereich beschränken. Stark frequentierte Bereiche wie eine belebte Straße sind damit aus den Bewegungszonen ausgeschlossen. Das reduziert die Anzahl falsch-positiver Bewegungsbenachrichtigungen, sowohl für kabelgebundene als auch für akkubetriebene Geräte.
- Der Audio-Umschalter ermöglicht das einfache Ein- und Ausschalten der Audioübertragung und -aufzeichnung der Videotürklingel oder der Kameras der smarten Geräte.

Vor dem Kauf eines Saugroboters

Kaufinteressierte sollten sich die Frage stellen: Welche Funktionen neben einer zufriedenstellenden Saugleistung sind mir wichtig?

Durch einige Zusatzfunktionen, etwa weitere Sensoren, werden auch zusätzliche Daten generiert.

Wer letzteres gänzlich vermeiden möchte, kann das Gerät

ausschließlich offline nutzen. In diesem Fall baut es keine Verbindung zum Internet auf und überträgt demnach auch keine Daten. Wer darauf nicht verzichten möchte, sollte sich vorab informieren, um ein möglichst sicheres Gerät auszuwählen.

Diese Fragen können bei der Entscheidung für ein sicheres Gerät behilflich sein:

- Wie lange sind Softwareupdates für das Gerät verfügbar?
- Sind Zusatzkomponenten, wie zum Beispiel eine begleitende Smartphone-App für die Steuerung bzw. Installation notwendig?
- Welche Zugriffsrechte fordern diese Apps von den Nutzenden ein?
- Auf welche Rechte verzichte ich, wenn ich eine begleitende App installiere und nutze?
- Welche Daten erhebt die App?
- Welche Informationen werden davon abgeleitet?
- Was passiert mit den generierten Daten?
- Wohin sendet die App diese Daten oder werden sie mit anderen Anwendungen geteilt?
- Wo werden sie gespeichert bzw. weiterverarbeitet - innerhalb oder außerhalb der Europäischen Union (EU)?
- Bei Cloud-Speicherung: Wo stehen die Server des Cloud-Betreibers? An welche Rechtsgrundlage ist er dadurch gebunden?
- Will ich den Saugroboter lediglich offline verwenden?

Saugroboter - Sicherheitseinstellungen

Auch wenn einige Hersteller gute Sicherheitsfeatures verbauen, sind Nutzer und Nutzerinnen selbst für die korrekten Einstellungen der eigenen internetfähigen Geräte verantwortlich. Denn: Ein noch so hochwertiger Saugroboter von einem seriösen Hersteller schützt

nicht davor, wenn z.B. das Heimnetzwerk oder der WLAN-Router unzureichend abgesichert sind.

Wird eine begleitende Smartphone-App für den Saugroboter genutzt, sollte diese stets auf dem aktuellsten Stand sein (**Hinweis:** Basisfunktionen funktionieren häufig auch ohne App). Ein vernetztes Gerät, das eine 3D-Umgebungskartierung vornehmen kann, Kamera- und Mikrofondaten sammelt und diese verarbeitet, kann mitunter unbeabsichtigt Daten übertragen oder von außen kompromittiert und anschließend fremdgesteuert werden. Saugroboter, die über eine ständige Internetverbindung verfügen, bieten hierüber eine stetige potenzielle Angriffsfläche.

Man sollte auch immer darauf achten, wo die Anbieter der Saugroboter-App ihren Hauptsitz haben. Ist es eine ausländische Firma, werden vermutlich auch die Daten nicht auf deutschen Servern abgespeichert. Besonders ausländische Hersteller sind immer mit Vorsicht zu genießen. Denn ihre Datenschutzregelungen entsprechen nicht dem deutschen und europäischen Standard.

Hinweis: Datenschutzregeln existieren, um sicherzustellen, dass die persönlichen Daten geschützt sind und nicht missbraucht werden.

Nutzt der Hersteller eine veraltete Software und vernachlässigt regelmäßige Updates, bekommen Hacker ein leichtes Spiel, sich im heimischen WLAN-Netz und in den angeschlossenen Computer einzuhacken. Schnell können Kriminelle dadurch sensible Daten wie Bankinformationen abrufen. Dabei benötigen Staubsauger-Roboter häufig mehr als nur **eine** Internetverbindung. Die gemessenen Daten speichern einige Hersteller in ihrer Cloud ab.

Außerdem ist es dem Datenschutz nicht dienlich, wenn Hersteller

die gesammelten Daten an Drittanbieter weitergeben. Auch diese erfreuen sich an den Informationen, um z.B. passgenaue Werbeanzeigen zu senden. Erkennt die Kamera etwa einen bestimmten Einrichtungsstil oder haben die Bewohner ein Kind, Katze oder einen Hund, so fallen die Personen schnell in bestimmte Werbekategorien.

Hinweis: Saugroboter müssen nicht zwingend mit dem Internet verbunden sein, jedoch geht die Offline-Nutzung oftmals mit einer Einschränkung von Funktion und Komfort einher.

Saugroboter sicher einrichten

- Ist eine Offline-Nutzung des Saugroboters nicht gewünscht oder die Vernetzung des Gerätes unabdingbar, sollte für das Gerät ein Gastnetzwerk im heimischen WLAN eingerichtet werden.
- Die Datenschutzeinstellungen sollte man kontrollieren und - falls möglich - gemäß der persönlichen Bedürfnisse ändern.
- Bei Nicht-Nutzung oder längerer Abwesenheit ist der Saugroboter auszuschalten und vom Netz zu trennen.
- Verlangt die entsprechende Smartphone-App nach einem Passwort, sollten die Passwortregeln eingehalten werden.
- Auf den verwendeten Peripherie-Geräten wie z.B. dem WLAN-Router sollten entsprechende Sicherheitseinstellungen gesetzt oder das Smartphone oder Tablet-Computer durch regelmäßige Updates immer auf dem neuesten Stand gebracht werden.

Hinweis: Bei Saugrobotern, die nach dem Zufalls- oder Chaos-Prinzip navigieren, gibt es nahezu kein Risiko für Spionage. Sie fahren so lange in eine zufällige Richtung, bis sie an ein Hindernis stoßen. Anschließend drehen sie um ein paar Grad ab und fahren in eine zufällige Richtung weiter. Solche Roboter sind allerdings sehr ineffektiv, da sie nicht wissen, wo sie bereits geputzt haben und wo nicht.

IT-Sicherheitskennzeichen checken

Beim Kauf neuer Technik und bei der Auswahl von digitalen Diensten sollte man nicht nur auf die neuesten Features und beste Ausstattung achten. Für mehr Durchblick bei der IT-Sicherheit kann man den QR-Code des IT-Sicherheitskennzeichens scannen.

Mit dem IT-Sicherheitskennzeichen des BSI (Bundesamt für Sicherheit in der Informationstechnik) ist es schnell und einfach möglich, mehr über die IT- Sicherheit von digitalen Produkten zu erfahren. Einfach den QR-Code im Onlineshop oder direkt auf der Verpackung scannen, um die Produktinformationsseite des BSI aufzurufen.

Dort sind die **wesentlichen** Sicherheitseigenschaften des Produkts übersichtlich aufbereitet. Auf der Seite findet man die aktuellen Informationen zu den bekannten Schwachstellen und zugehörigen Updates (dem BSI **bekannten** Schwachstellen und Updates). Und zwar nicht nur beim Kauf, sondern über die gesamte Laufzeit des IT-Sicherheitskennzeichens.

Während der Laufzeit des IT-Sicherheitskennzeichens prüft die BSI-Marktaufsicht stichprobenartig oder anlassbezogen, ob die gekennzeichneten Produkte die Anforderungen des BSI noch einhalten. Das IT- Sicherheitskennzeichen ist keine Zertifizierung. Im Unterschied zur Zertifizierung, wird das Produkt bei der Erteilung nicht durch das BSI, sondern vom Hersteller geprüft.

Hinweis: Durch die Unterstützung von Herstellern und Anbietern, die sich der IT- Sicherheit verpflichtet haben, wird ein verantwortungsvoller Umgang mit Technologien gefördert. Damit wird dazu beigetragen, Nutzer und Nutzerinnen von smarten Geräten vor Cyberbedrohungen zu schützen.



Hinweise zum Mähroboter

Die vorhergehenden Hinweise gelten analog auch für den Mähroboter als hilfreichen Gartenhelfer.

Der Mähroboter ist mit scharfen Messern ausgestattet und diese Messer können langsamen Haus- und Wildtieren (Schildkröte, Igel, ...) schwerwiegende Verletzungen zufügen.

Um dies zu vermeiden, sollten die Mähroboter am Tage nur unter Aufsicht ihre Arbeit nachkommen und in der Dämmerung und in der Nacht sollten Mähroboter automatisch deaktiviert werden.

Warnung zum Schluss: Man muss sich immer bewusst sein, dass alle smarten Haushalts-Geräte, die per WLAN kommunizieren, Hackern zum Opfer fallen können. Also man sollte immer ein wachsames Auge haben, für die smarten »Haushaltshelfer«.

Biometrische Zutrittskontrolle zu Serverräumen: Für den Zutritt mit erhöhter Sicherheitsstufe stehen biometrische Kontrollsysteme zur Verfügung, die Personen anhand von physischen Eigenschaften, wie z. B. durch Gesichtserkennung, überprüfen. Diese Technologie scannt ein oder mehrere physische Attribute von Personen, um den Zutritt zu den Einrichtungen und den sensiblen Bereichen zuverlässig und effektiv einzuschränken.

Black-Building-Test (BBT): In der Literatur wird der »Black-Building-Test« auch als »Schwarzschtaltung« und »black building procedure« oder auch als »Blackout-Test« bezeichnet. Sofern ein BBT schon seit Längerem nicht mehr durchgeführt worden ist oder noch nie, sollte man nicht mit einem BBT unter Volllast beginnen, sondern sich durch eine Reihe geeigneter Übungsszenarien einem scharfen BBT unter Volllast annähern.

Blade-Server: Blade-Server sind konzipiert, um noch mehr Platz zu sparen. Jedes Blade enthält Prozessoren, Netzwerk-Controller, Arbeitsspeicher und teilweise auch Speicher. Sie sind so konzipiert, dass sie in ein Gehäuse passen, das mehrere Blades aufnimmt und die Stromversorgung, das Netzwerkmanagement und andere Ressourcen für alle Blades im Gehäuse enthält.

CRAC: Die Computerraumklimatisierung (CRAC) ist eine Art von Kühlsystem, das speziell für die IT-Ausrüstung und Computerräume entwickelt wurde. Eine CRAC-Einheit (CRAC = Computer Room Air Conditioning) ist ein Gerät, das die Temperatur, Luftverteilung und Luftfeuchtigkeit in einem Server-Raum oder Datacenter überwacht und am Laufen erhält. Die Klimatisierung von Computerräumen (CRAC) ist ein wichtiger Aspekt der IT-Infrastruktur, der dafür sorgt, dass Computerhardware und andere Geräte bei optimalen Temperaturen bleiben. Sie ist für die Aufrechterhaltung der Effizienz und Zuverlässigkeit von Computersystemen und Netzwerken unerlässlich.

Cybermobbing und Cybergrooming: Sowohl beim Cybermobbing als auch beim Cybergrooming handelt es sich um Formen der Belästigung, die über das Internet begangen werden. Allerdings zeichnen sich diese durch unterschiedliche Absichten aus. So geht es beim Cybermobbing darum, dass Opfer durch Beleidigungen und Drohungen in seinem Selbstwertgefühl zu beeinträchtigen, damit ein Machtungleichgewicht entsteht. Beim Cybergrooming können unter Umständen auch Drohungen verwendet werden, Ziel ist hingegen die Anbahnung von Missbrauchshandlungen an Minderjährigen.

Dark Web: Es gilt als die dunkelste Seite des Internets: das Dark Web - ein digitaler Ort ohne Regeln und Gesetze. Doch was genau verbirgt sich eigentlich in dieser vermeintlichen Schattenwelt, in der Kriminelle ihre Deals abwickeln oder politisch Verfolgte einen geschützten Raum finden, »ohne Spuren« zu hinterlassen? Hinweis: Es kann davon ausgegangen werden, dass etwa 25% der Server im Dark Web durch verschiedenste Organisationen - deren Kürzel häufig aus 3 Buchstaben bestehen - kompromittiert wurden und werden.

Deep Web: Das Internet ist um ein Vielfaches größer, als die meisten Menschen wahrnehmen. Gerade, wenn man über Google nach bestimmten Inhalten sucht, findet man nur einen Bruchteil von dem, was wirklich da ist - die Inhalte im sogenannten »Deep Web« sind nämlich zugangsbeschränkt.

EMV: Der Begriff Elektromagnetische Verträglichkeit (EMV) beschreibt einen Systemzustand, in dem sich elektrische Einrichtungen gegenseitig nicht stören und in dem die Funktion elektrischer Einrichtungen auch durch externen Quelle, z. B. Blitze, nicht nachteilig beeinflusst wird.

Harmonische Verzerrung: Die harmonische Verzerrung ist die Abweichung der tatsächlichen Kurvenform der Spannung oder des Stroms von der reinen Sinusform. Verursacht wird diese Verzerrung durch nicht lineare Verbraucher wie z. B. Schaltnetzteile oder Frequenzumrichter. Physikalisch sind solche Verzerrungen nichts Anderes als Frequenzanteile (Oberwellen) in Spannung und Strom, die teils weit über die Grundfrequenz von 50 Hz hinausgehen und durchaus bis deutlich in den dreistelligen kHz-Bereich hineinreichen. Da diese Oberwellen sowohl auf die ordnungsgemäße Funktion als auch auf die Lebensdauer von Geräten nachteilige Wirkung haben, muss der Wert der Oberwellen in Grenzen gehalten werden.

Hoax (Falschmeldung) im Internet: Hoax bedeutet im Englischen so viel wie »Zeitungssente« oder »schlechter Scherz«. Im Internet steht der Begriff für Falschmeldungen. Früher handelte es sich meist nur um scherzhafte Warnungen vor vermeintlichen Computerviren, die auf befallenen Systemen zum Beispiel die Festplatte löschen. Heute spielen Hoaxes aber auch zur politischen Desinformation eine Rolle. Zudem zielen Falschmeldungen oft darauf ab, den Ruf bestimmter Firmen oder Organisationen zu diskreditieren. Auch E-Mail-Kettenbriefe zählen zur Hoax-Kategorie - zum Beispiel E-Mails von vermeintlichen Redakteuren eines Messenger-Dienstes. In der Hoax-Mail steht in aller Regel die Aufforderung, sie an möglichst viele Empfänger weiterzuleiten. Nur so könne der Account auch künftig gratis angeboten werden.

Hub-and-Spoke-Architektur: Die Hub-and-Spoke-Architektur eines Netzwerks hat die Form eines Sterns. Die verschiedenen Kommunikationsendpunkte (Spokes) sind jeweils mit einer Netzwerkverbindung mit dem zentralen Netzwerkknoten, dem Hub, verbunden. Sämtlicher Netzwerkverkehr fließt über den Hub.

Die Hub-and-Spoke-Architektur eines Netzwerks erinnert an den Aufbau eines Rads mit Speichen (Spokes) und Nabe (Hub). Die einzelnen Endpunkte des Netzes sind sternförmig über jeweils genau eine Netzwerkverbindung mit dem zentralen Netzwerkknoten verbunden. Möchten einzelne Endpunkte miteinander kommunizieren, werden die Daten zunächst an den zentralen Knoten und dann weiter zum Endpunkt übermittelt. Es existieren keine direkten Verbindungen zwischen den einzelnen Endpunkten. Der Hub ist zentraler Knoten im Netzwerk und an jeglicher Kommunikation beteiligt. Ohne den Hub ist kein Datenaustausch möglich. Die Anzahl benötigter Leitungen lässt sich in einem Hub-and-Spoke-Netz sehr einfach bestimmen. Sie entspricht der Anzahl der zu verbindenden Endpunkte (ohne den zentralen Hub).

HVAC: HVAC steht für - Heating, Ventilation and Air Conditioning (dt. Heizung, Lüftung, Klimatechnik) Die absolute Kontrolle der Umgebungstemperatur im Rechenzentrum ist ein wichtiger Faktor für die allgemeine Leistung der darin enthaltenen Technik.

ISB - Zuständigkeiten und Aufgaben: Der Informationssicherheitsbeauftragter (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden.

Ein Informationssicherheitsbeauftragter ist für alle Fragen rund um die Informationssicherheit in der Institution zuständig. Zu seinen Aufgaben gehört es,

- den Sicherheitsprozess zu steuern und zu koordinieren,
- die Leitung bei der Erstellung der Sicherheitsleitlinie zu unterstützen,
- die Erstellung des Sicherheitskonzepts und zugehöriger Teilkonzepte und Richtlinien zu koordinieren,
- Realisierungspläne für Sicherheitsmaßnahmen anzufertigen sowie ihre Umsetzung zu initiieren und zu überprüfen,
- der Leitungsebene und anderen Sicherheitsverantwortlichen über den Status der Informationssicherheit zu berichten, sicherheitsrelevante Projekte zu koordinieren,
- sicherheitsrelevante Vorfälle zu untersuchen sowie
- Sensibilisierungen und Schulungen zur Informationssicherheit zu initiieren und zu koordinieren.

Ein ISB sollte Erfahrung und Wissen sowohl auf den Gebieten der Informationssicherheit als auch der IT besitzen. Darüber hinaus sollte er die Geschäftsprozesse der Institution kennen.

Zur Wahrung der Unabhängigkeit sollte der ISB direkt der obersten Leitung zugeordnet sein. Eine Integration in die IT-Abteilung kann zu Rollenkonflikten führen, da der ISB seine Verpflichtung zur Kontrolle der Sicherheitsmaßnahmen nicht frei von Beeinflussung wahrnehmen kann. Auch eine Personalunion mit dem Datenschutzbeauftragten ist nicht unkritisch. Sollte dies der Fall sein, müssen die Schnittstellen dieser beiden Aufgaben klar definiert werden, um Rollenkonflikte zu vermeiden.

Ein ISB benötigt darüber hinaus ausreichend Ressourcen und Zeit für erforderliche Fortbildungen. Es muss einen direkten Berichtsweg zur Leitung geben, um in Konfliktfällen schnell entscheiden zu können.

Je nach Größe des Unternehmens oder der Behörde kann es auch weitere ISB etwa für verschiedene Bereiche, Standorte oder auch große Projektvorhaben der Institution geben.

LNB: Die Abkürzung LNB steht für Low Noise Block, einen Signalumsetzer. Sinngemäß lässt sich die Bezeichnung mit »rauscharmer Signalumsetzer« übersetzen. Die Hauptaufgabe des LNBs in einer SAT-Anlage ist die Umsetzung hochfrequente Satellitensignale im Gigahertz-Bereich in niedrige Frequenzen. Das LNB-Modul befindet sich im Brennpunkt einer Sat-Schüssel, die Hochfrequenzsignale von einem Satelliten bündelt und zum LNB reflektiert. Die verschiedenen LNB-Typen unterscheiden sich durch die Anzahl der anschließbaren Receiver. Für den privaten Gebrauch werden meist Single- oder Quad-LNB (quad ... vier) verwendet. Größere Sat-Anlagen werden in der Regel mit einem Octo-LNBs (octo ... acht) realisiert.

Der LNB-Aufbau ist auf die Polarisationen von Satellitensignalen abgestimmt. Die Sat-Schüssel empfängt sowohl Signale mit horizontaler als auch mit vertikaler Polarisation. Diese werden gebündelt und auf den LNB reflektiert. Durch die zwei Polarisierungen können über dieselben Frequenzen mehr Signale übertragen und damit auch mehr Sender empfangen werden. Der LNB-Aufbau spiegelt genau das wider. Denn im Hohlleiter eines modernen LNBs sitzen zwei Rillenhornantennen: eine oben und eine links. Dort werden die Signale empfangen und an Verstärkertransistoren weitergegeben. Diese wiederum übernehmen die hauptsächliche Funktion bei allen LNB-Typen, nämlich die Umsetzung des Hochfrequenzsignals in niedrigere Frequenzen. Der nötige Strom wird über das angeschlossene Koaxialkabel am LNB-Anschluss bereitgestellt, über das auch die umgesetzten Signale übertragen werden.

Für den Empfang des Satellitenfernsehen braucht man im LNB keine Frequenzen einstellen. Wichtig hingegen, ist die Ausrichtung der Satellitenschüssel um die gewünschten Frequenzbereiche des Satelliten optimal zu empfangen. Die Sender sind meist bereits programmiert und werden über eine bestimmte Frequenz und Polarisation im Bereich von 10,7 bis 12,75 Gigahertz (Low-Band : 10,7 – 11,7 GHz, High-Band: 11,7 – 12,75 GHz) übertragen. Welche LNB-Frequenz die einzelnen Sender haben, hängt nicht von den einzelnen LNB-Typen ab, sondern von den Satelliten-Betreibern.

Nach einem Sendersuchlauf und korrekter Ausrichtung der Sat-Schüssel findet man automatisch alle Sender, die im Fernseher oder Sat-Receiver dann auch gespeichert werden.

Um die Signale in ausreichender Stärke oder Intensität (man spricht von »Pegel« oder »Signalpegel«) an den Receiver zu übertragen, wird das Signal im LNB verstärkt. Der Pegel wird dabei in Dezibel (dB) angegeben. Die meisten Receiver haben eine Anzeige des Signalpegels (meist in Prozent) in ihre Software integriert, so dass man diesen Wert sehr gut selbst kontrollieren kann.

Über die möglichen 4 Schaltungen bzw. Kombinationen aus Polarisation und Frequenzband werden die unterschiedlichen Sender übertragen. Der Receiver ruft dabei einen bestimmten Schaltzustand auf, je nach gewünschtem TV-Programm. Beispiel: ZDF HD - Polarisation: horizontal, Frequenz: 11,362 (Low-Band). Zur Umschaltung der Polarisation wird vom Receiver eine bestimmte Spannung (zwischen Innenleiter und Schirm im Koaxialkabel) angelegt. Das Frequenzband wird umgeschaltet durch das Aussenden einer bestimmten Frequenz durch den Receiver.

LPZ: Lightning Protection Zone (Blitzschutzzone); Die Werte laufen von »0« für den freien Raum außerhalb von Gebäuden ohne irgendwelche schützenden Einrichtungen bis »2« oder mehr für geschützte Bereiche z. B. innerhalb von Gebäuden.

Mainframes: Mainframes sind Hochleistungscomputer mit mehreren Prozessoren, die deutlich leistungsfähiger sind als viele zusammengeschaltete Server (z.B. Blade-Server). Mainframes, als erste virtualisierbare Computer, können Milliarden von Berechnungen und Transaktionen in Echtzeit verarbeiten.

Perimeterschutz: Rechenzentren finden sich in einer Vielzahl von Gebäuden, wobei der Schutz der Umgebung immer die erste Abwehrlinie darstellt. Unter Perimeter versteht man das Umfeld eines Gebäudes und die Abgrenzung des Umfelds nach außen sowie für die besonders gefährdeten Bereiche auf dieser Fläche. Der Perimeterschutz umfasst dementsprechend alle mechanischen, baulichen, personellen und organisatorischen Maßnahmen zum Schutz eines Objekts.

PE-System (Schutzleiter-System): Die Begrenzung des Schutzleiterstroms hat neben dem Personenschutz in Rechenzentren (RZ) einen weiteren wichtigen Grund. Die harmonischen Verzerrungen breiten sich auf allen stromdurchflossenen Leitern aus, also auch auf dem PE-System. Ist der Strom auf dem PE-System hoch, ist auch der Pegel des harmonischen Anteils hoch. Da alle PE-Ströme anteilig auch über die Schirmungen von Datenleitungen fließen, können die harmonischen Frequenzanteile dort Störungen der Datenübertragung bewirken, die bis zum Abbruch der Kommunikation führen können. In jedem Fall ist zu verhindern, dass auch von außerhalb zusätzliche Ströme auf das PE-System gelangen. Eine sehr häufige Quelle für störende PE-Ströme ist die Erdung der Schirmung von Mittelspannungskabeln an Trafos.

PUE-Wert: PUE .. Power Usage Effectiveness; Verhältnis des Energieverbrauchs des kompletten Rechenzentrums zu dem der reinen IT-Systeme. Selbstverständlich ist ein möglichst guter PUE-Wert anzustreben. Dieses Ziel steht aber in unauflösbarem Widerspruch zur den angesichts der hohen oder sehr hohen Verfügbarkeits-Anforderung erforderlichen Redundanzen.

PVC-Vermeidung: Der Grund, alle Gewerke so PCV-frei wie möglich auszuführen, liegt darin, dass PVC beim Verbrennen zahlreiche, für Mensch und IT schädliche Substanzen freisetzt. Diese reichen von CO (Kohlenmonoxid) über HCN (Blausäure), HCl (Salzsäure) und Acrolein, einem sehr starken Umweltgift bis zu polyzyklischen aromatischen Kohlenwasserstoffen (PAK). Des Weiteren führt PVC bei der Verbrennung zu einer sehr starken Schwarzaufbildung, dessen Rauchpartikel zu elektrisch leitenden Ruß-Brücken und damit zum Ausfall von elektrischen Einrichtungen führen können, selbst wenn diese durch den eigentlichen Brand gar nicht betroffen sind.

Rackmount-Server: Rackmount-Server sind breite, flache Standalone-Server - in der Größe eines kleinen Pizzakartons - die dafür konzipiert sind, in einem Rack platzsparend übereinander gestapelt zu werden (im Gegensatz zu einem Tower- oder Desktop-Server). Jeder Rackmount-Server verfügt über eine eigene Stromversorgung, Lüfter, Netzwerk-Switches und Ports sowie den üblichen Prozessor, Arbeitsspeicher und Speicher.

Server: Server sind leistungsfähige Computer, die Anwendungen, Dienste und Daten für Endbenutzergeräte bereitstellen.

Spine-Leaf-Architektur: Eine Spine-Leaf-Architektur ist eine Topologie bei Netzwerken für Rechenzentren, die aus zwei wechselnden Ebenen besteht, nämlich Spine und Leaf. Die Leaf-Ebene besteht aus Access-Switches, die den Verkehr der Server sammeln und direkt mit der Spine-Ebene oder dem Kernbereich verbunden sind. Spine-Switches sind mit allen Leaf-Switches in einer vollvermaschten Topologie verbunden.

SPOF: Single Point of Failure; Die Vermeidung von Einzel-Fehler-Stellen (SPOF) ist ein wichtiges Konstruktionsprinzip für die Verfügbarkeit von Rechenzentren.

TK-Systeme: Telekommunikationssysteme (TK-Systeme) oder Telekommunikationsanlagen (TK-Anlagen) sind Systeme, an denen Endgeräte für TK-Dienste angeschlossen werden. Die Endgeräte haben Zugriff auf die System-Leistungsmerkmale und können interne und externe Verbindungen über die Amtsleitungen der öffentlichen Kommunikationsnetze zu anderen Endgeräten aufbauen.

Transferschalter (TS): Transferschalter haben den Zweck, zur Erhöhung der Versorgungssicherheit von Rechenzentren zwischen zwei alternativen Stromversorgungspfaden umschalten zu können. Erfolgt diese Umschaltung kontaktbehaftet spricht man von einem »Automatischem Transferschalter – ATS«. Erfolgt die Umschaltung vollelektronisch, also kontaktfrei, spricht man von »Statischen Transferschaltern - STS«. Grundsätzlich erfolgt beim ATS wie beim STS die Umschaltung in weniger als 20 ms. Mechanisch arbeitenden ATS haben gegenüber den rein elektronisch arbeitenden STS den Nachteil, dass die Kontakte durch Alterung (Abreißfunken, Wärmebeanspruchung etc.) ihre Schaltcharakteristik so ändern können, dass die Umschaltzeit auch über 20 ms hinausgehen kann.

ZEP: Zentraler Erdungspunkt

ZKA: Zutrittskontrollanlage

