

# Inhaltsverzeichnis

Prinzipien der IT-Sicherheit .....	02	Hunk - Splunk Analytics für Hadoop .....	84
Vereinfachte Grundprinzipien der IT-Sicherheit .....	05	Windows-Features .....	85
Härtung von IT-Systeme .....	09	Datenträgerbereinigung unter Windows .....	86
Härtung mit Windows-Werkzeuge .....	13	Festplatten-Partitionen - MBR oder GPT? .....	87
Penetrationstest (Pentest) .....	15	Speichermedien sicher löschen .....	89
KRITIS - Kritische Infrastrukturen .....	20	Wiederherstellung mit Recuva .....	93
Ablauf eines Ransomware-Angriffs .....	21	Windows 11 und 10: Bootfähigen USB-Stick erstellen .....	94
Demilitarisierte Zone (DMZ) .....	23	Boot-Menü reparieren .....	97
SOC - Security Operations Center .....	27	Abgesicherten Modus zum Boot-Menü hinzufügen .....	100
SIEM - Security Information and Event Management .....	28	Was ist ein Wasserloch-Angriff? .....	101
SOAR - Security Orchestration Automation and Response .....	31	Lieferketten-Angriffe .....	103
Cisco Meraki - Netzwerk .....	32	APT-Blocker .....	106
Firewall .....	35	IPsec - Verschlüsselung und Paketfilter .....	109
Palo Alto Networks - Next-Generation Firewall .....	37	Syntaxparameter für Netsh – was bedeuten sie? .....	110
HP Wolf Security .....	38	Was ist MPLS? .....	114
Open-Source-Firewall pfSense .....	39	PowerShell-Kommandos .....	115
Open-Source-Firewall OPNsense .....	41	PowerShell-Skript .....	116
Was ist Packet Sniffing? .....	43	CMD-Skript (Batch-Datei) .....	117
Pegasus .....	45	IPv6 Netzwerk-Adressbereiche .....	121
Portknocking .....	46	Open Systems Interconnection (OSI) .....	122
Was macht der TPM-Chip? .....	47	Probleme und Lösungen .....	123
Was ist unter Windows 11 anders? .....	49	Glossar .....	125
Tastatur-Kurzbefehle W10 und W11 .....	54	Internet-Links .....	151
System-Programme .....	55	Literatur-Tipps .....	153
Dienste unter Windows 10 beenden .....	56	Index .....	154
Browser im privaten Modus .....	62		
Wie funktioniert TLS - Transport Layer Security? .....	65		
VPN-Kaskaden oder Multi-Hop VPN .....	72		
VPN-Dienst Surfshark .....	77		
Mesh-Network .....	78		
Verschlüsselung mit VeraCrypt .....	80		
Was ist Splunk? .....	82		
Hadoop und Big Data .....	83		

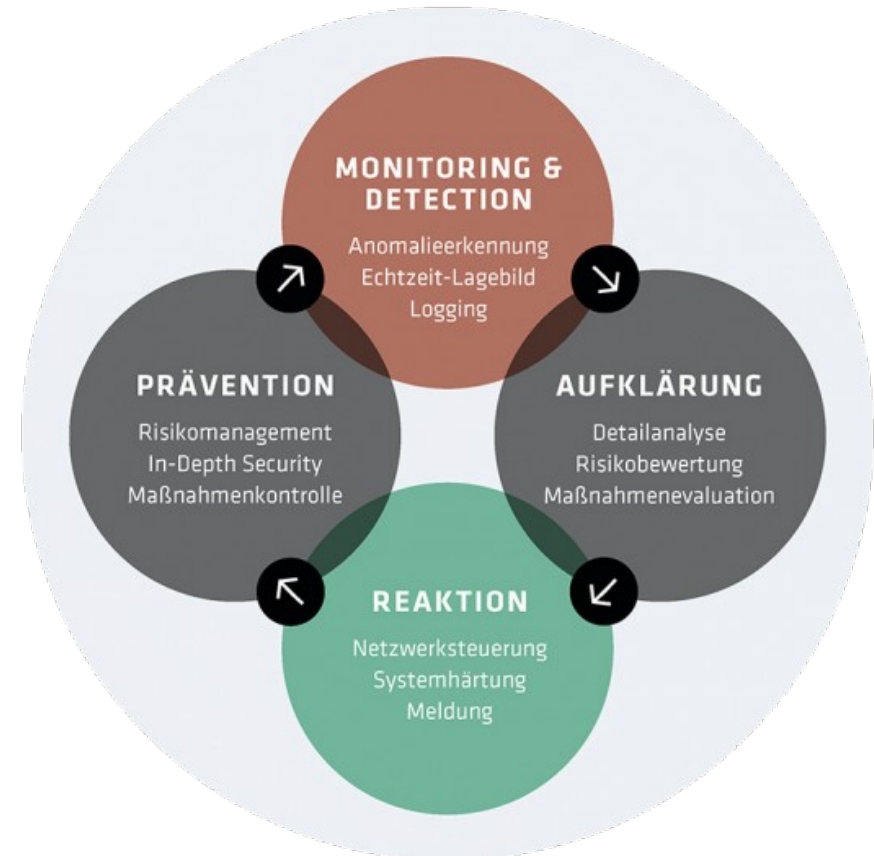
# Prinzipien der IT-Sicherheit 1/3

## Grundsätze der IT-Sicherheit

Informationen bzw. Daten sind schützenswerte Güter. Der Zugriff auf diese sollte daher im Unternehmen beschränkt und kontrolliert sein. Nur autorisierte Benutzer oder Programme sollen die Möglichkeit haben, auf die Information zuzugreifen. Folgende allgemeinen Schutzziele bilden die Basis für jede Strategie zur IT-Sicherheit:

- **Vertraulichkeit:** Daten dürfen lediglich von autorisierten Benutzern gelesen bzw. verändert werden. Dies gilt sowohl beim Zugriff auf gespeicherte Daten, als auch während der Datenübertragung.
- **Integrität:** Daten dürfen nicht unbemerkt verändert werden. Alle Änderungen müssen nachvollziehbar sein.
- **Verfügbarkeit:** Systemausfälle müssen verhindert werden. Der Zugriff auf Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet sein.
- **Authentizität:** Diese bezeichnet die Eigenschaften der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit eines Objekts.
- **Verbindlichkeit / Nichtabstreitbarkeit:** Dies bedeutet, dass »kein unzulässiges Abstreiten durchgeführter Handlungen« möglich ist. Das ist unter anderem wichtig beim elektronischen Abschluss von Verträgen. Eine Lösung hierfür sind elektronische Signaturen.
- **Zurechenbarkeit:** Eine durchgeführte Handlung kann einem Kommunikationspartner eindeutig zugeordnet werden.
- Und in bestimmtem Kontext auch **Anonymität**.

Die vorstehende Aufzählung zeigt, dass eine allgemeingültige Lösung für die IT-Sicherheit nicht existiert, sondern auf jedes Unternehmen individuell angepasst werden sollte. Ein Abgleich des eigenen Geschäftsmodells liefert mit den oben genannten Zielen jedoch wichtige Eckpunkte für die Anforderungen an eine IT-Sicherheitslösung. Damit sollte eine Kosten-Nutzen-Analyse einhergehen.



Ausgerüstet mit diesen übergeordneten Prinzipien haben IT-Sicherheitsspezialisten »Best Practices« für Unternehmen entwickelt. Diese bewährten Methoden sollen verschiedenste Firmen dabei unterstützen, die Sicherheit ihrer Informationen zu gewährleisten.

## Best Practices für die IT-Sicherheit

Es gibt zahlreiche »Best Practices« innerhalb der IT-Sicherheit, die auf bestimmte Branchen oder Unternehmen zugeschnitten sind, einige gelten jedoch allgemein.

## 1. Ausgewogener Schutz

Eine der größten Herausforderungen bei der IT-Sicherheit besteht darin, ein Gleichgewicht zwischen Ressourcen-Verfügbarkeit und der Vertraulichkeit, sowie der Integrität der Ressourcen zu finden.

Anstatt zu versuchen, sich vor allen Arten von Bedrohungen zu schützen, konzentrieren sich die meisten IT-Abteilungen darauf, zuerst die wichtigsten Systeme zu isolieren. Im nächsten Schritt werden dann akzeptable Wege gefunden, um den Rest zu schützen, ohne die Hardware unbrauchbar zu machen. Systeme mit niedrigerer Priorität können beispielsweise Kandidaten für eine automatisierte Analyse sein, sodass die wichtigsten Systeme weiterhin im Mittelpunkt stehen.

## 2. Benutzer und Ressourcen aufteilen

Damit ein Informationssicherheitssystem funktioniert, muss es wissen, wer bestimmte Dinge sehen und tun darf. Jemand in der Buchhaltung muss beispielsweise nicht alle Namen in einer Kundendatenbank sehen, aber er braucht möglicherweise die Zahlen aus dem Verkauf.

Dies bedeutet, dass ein Systemadministrator den Zugriff nach den Arbeitsaufgaben einer Person zuweisen und diese Grenzwerte entsprechend der organisatorischen Trennung weiter verfeinern muss. Dies stellt sicher, dass der Chief Financial Officer im Idealfall auf mehr Daten und Ressourcen zugreifen kann als ein Junior Accountant.

Der Rang garantiert jedoch nicht den vollständigen Zugriff. Der CEO eines Unternehmens braucht eventuell mehr Daten als seine Kollegen, muss jedoch nicht automatisch uneingeschränkt auf das System zugreifen können. Dies bringt uns zum nächsten Punkt.



### 3. Mindestberechtigungen zuweisen

Jedem Mitarbeiter sollten die Mindestrechte zugewiesen werden, die er zur Wahrnehmung seiner Aufgaben benötigt.

Wenn sich die Verantwortlichkeiten einer Person ändern, verschieben sich auch die Berechtigungen. Das Zuweisen von Mindestberechtigungen verringert die Wahrscheinlichkeit, dass Joe vom Design mit allen Marketingdaten aus der Tür geht.

# Prinzipien der IT-Sicherheit 3/3

## 4. Unabhängige Abwehr

Dies ist sowohl ein bekanntes militärisches als auch ein IT-Prinzip. Die Verwendung einer wirklich guten Verteidigung wie Authentifizierungsprotokollen sind nur dann sinnvoll, wenn jemand dagegen verstößt.

Wenn mehrere unabhängige Verteidigungen eingesetzt werden, muss ein Angreifer verschiedene Strategien anwenden, um diese zu überwinden.

Die Einführung dieser Art von Komplexität bietet keinen hundertprozentigen Schutz vor Hackern, verringert jedoch die Wahrscheinlichkeit eines erfolgreichen Angriffs.

## 5. Ausfälle einplanen

Wenn Unternehmen Ausfälle einplanen, können sie die tatsächlichen Konsequenzen für den Fall minimieren.

Durch die Einrichtung von Backup-Systemen im Vorfeld kann die IT-Abteilung die Sicherheitsmaßnahmen ständig überwachen und schnell auf Sicherheitslücken reagieren. Ist der Verstoß gegen die allgemeinen Prinzipien der IT-Sicherheit nicht schwerwiegend, so kann das Unternehmen die Sicherung fortsetzen, während das Problem zur selben Zeit behoben wird.

Bei der IT-Sicherheit geht es also nicht nur darum, den Schaden durch Sicherheitsverletzungen zu begrenzen, sondern ihn auch zu verhindern.

## 6. Protokollieren

Im Idealfall wird ein Sicherheitssystem niemals verletzt. Wenn jedoch ein Sicherheitsverstoß auftritt, sollte das Ereignis aufgezeichnet werden. Tatsächlich zeichnen IT-Mitarbeiter in der Regel sehr viel

auf, auch wenn kein Verstoß vorliegt. Manchmal sind die Ursachen von Verstößen nachträglich nicht erkennbar. Daher ist es wichtig, Daten zu haben, die rückwärts verfolgt werden können. Informationen von Sicherheitsverletzungen können dazu beitragen, das System zu verbessern und zukünftige Angriffe zu verhindern.

## 7. Häufige Tests

Hacker verbessern ständig ihr Handwerk, was bedeutet, dass die Informationssicherheit Schritt halten muss.

IT-Experten kümmern sich dabei nicht nur um Tests, sondern führen auch Risikobewertungen durch, lesen den Disaster Recovery-Plan erneut, überprüfen den Business Continuity-Plan im Falle eines Angriffs und wiederholen die Tests und Risikobewertungen.

## Fazit

IT-Sicherheit ist eine herausfordernde Aufgabe, bei der gleichzeitig die Aufmerksamkeit für Details und ein neues Level der Wahrnehmung gefragt sind.

Wie viele andere komplexe Aufgaben kann auch die IT-Sicherheit in grundlegende Schritte unterteilt werden, die den Prozess wesentlich vereinfachen können.

# Vereinfachte Grundprinzipien der IT-Sicherheit 1/4

IT-Sicherheit ist heute ein riesiges Betätigungsfeld. Menschen, die im ITSec-Umfeld tätig sind, werden mit Begriffen überschwemmt. Der Markt hält eine unüberschaubare Menge an Sicherheits-Produkten bereit. Kaum jemand, der sich mit »Cybersecurity« beschäftigt, kann der »Werbung für Sicherheitsprodukte« entkommen. Dabei wird der Eindruck erweckt, es ginge ohne diese neuen Produkte nicht mehr. Dabei verwendet die ITSec-Industrie oft die Strategie der Angst- und Panikmache. Doch Angst ist nicht nur in der ITSec-Branche ein schlechter Ratgeber.

Das soll nicht heißen, dass alle ITSec-Produkte schlecht sind. Viele sind allerdings sehr komplex und verstecken diese Komplexität hinter vereinfachten Oberflächen. Viel zu oft werden auch Produkte verkauft, die schlicht nicht nötig sind. Dann werden Produkte ohne Plan und ohne Konzept eingesetzt, nur weil gesagt wurde, dass man heutzutage so etwas haben müsse.

Es ist Zeit, sich von der Begriffsverwirrung und der Produktschwemme zu befreien. Zeit, einen Schritt zurückzutreten und sich darüber Gedanken zu machen, welche Grundprinzipien IT-Sicherheit ausmachen.

## 1. Kenne deine Systeme und die Bedrohungen

»Wenn du dich und den Feind kennst, brauchst du den Ausgang von hundert Schlachten nicht zu fürchten.« - Die Kunst des Krieges - Sunzi

- Man kann nichts verteidigen, wenn man nicht weiß, was man verteidigt oder wogegen man es verteidigt.
- Lerne dein System so gut wie möglich kennen. Verstehe, welche Komponenten und Dienste dein System benutzt. Dazu gehören auch Dienstleister (Stichwort: Lieferketten-Angriff oder Supply-Chain-Angriff), von denen die Systeme abhängig sind. Läuft dein System bei einem anderen Anbieter in der »Cloud«, sind dessen Probleme auch deine Probleme.

- Stellst du einen unnötigen Dienst fest, stelle ihn ab.
- Stelle fest, welche Risiken durch die laufenden Dienste entstehen können. Denke, wie der Angreifer - welches ist die Schwachstelle bei der du angreifen würdest?
- Verlasse dich nicht nur auf externen Support (z.B. des Herstellers). Dies macht dich abhängig vom Supporter und kann schnell zur Katastrophe führen, wenn er nicht reagiert oder das Problem nicht beheben kann. Open Source Software zu verwenden ist hier sehr hilfreich, weil diese meist sehr gut dokumentiert und ihre Funktionsweise daher gut erlernbar ist.
- Dokumentiere deine Systeme und Komponenten. Ein guter Überblick ist wichtig, um zu sehen, wo Schwachstellen entstehen können. Kümmere dich dann zunächst um die schwächsten Stellen in deinem System, denn das ist die Stelle, die sich Angreifer gezielt aussuchen, um dann zuzuschlagen.
- Verhindere, dass Angreifer dein System besser kennen als du. Verwende Verschlüsselung bei der Kommunikation und dort wo es nötig ist, auch bei der Speicherung von Daten. Halte Einzelheiten über deine Systeme geheim. »Der General ist ein weiser Verteidiger, wenn sein Gegner nicht weiß, was er angreifen soll.« (Sunzi, die Kunst des Krieges)
- Beobachte Systemmeldungen und Protokolle (Log-Dateien). Oft beinhalten sie wertvolle Hinweise. Auch darüber, wo noch Maßnahmen nötig sein könnten.

## 2. Verwende Ressourcen und Informationen und nutze Informationsaustausch

Allzu leicht zieht man sich in eine Filterblase zurück und bekommt kaum noch Informationen von der Welt da draußen, während Angreifer sich ständig über neue Möglichkeiten informieren.



# Vereinfachte Grundprinzipien der IT-Sicherheit 2/4

- Vernetze dich mit der Community, also mit Leuten denen es ähnlich geht wie dir. Tausch dich mit Ihnen aus, z. B. über Mailinglisten. Gehe zu Community-Veranstaltungen mit Schwerpunkt Security (nicht aber zu reinen Produkt-Werbeveranstaltungen von Herstellern). Gute Adressen vor Ort sind oft der »Computer Chaos Club« (CCC) oder die »Linux User Group« (LUG). Verwende auch Ressourcen der Community, z. B. Blocklisten (z.B. Zusammenstellungen von unliebsame Accounts).
- Informiere dich bei CERTs (Computer Emergency Response Team) und Security-Mailinglisten über neue Sicherheitslücken. Dies ist Voraussetzung dafür, dein System zu kennen.
- Verwende gut dokumentierte, offene und gebräuchliche Systeme. Dies ist Voraussetzung dafür, zu wissen was man einsetzt. Vermeide den Einsatz von »Blackboxen«, deren Inhalt du nicht kennst. Wieder ist es von Vorteil, Open Source Software zu benutzen. Gebräuchliche und verbreitete Open Source Software ist gut dokumentiert und der Quellcode liegt offen. Vermeide jedoch Exoten, die kaum jemand einsetzt und schlecht dokumentiert sind. Vermeide auch, das Rad neu zu erfinden. Nutze die Community. Verwende robuste und stabile Systeme, die gut geprüft sind.

## 3. Lege Richtlinien und Parameter fest und überprüfe diese

Um zu wissen, ob deine Systeme korrekt und sicher laufen, müssen sie überprüft werden. Dazu ist es nötig, Richtlinien und Parameter festzulegen innerhalb der die Systeme laufen sollen.

- Verwende Monitoring, um deine Systeme zu überprüfen. Falls ein System außerhalb diese Parameter läuft, sollte es Alarmmeldungen geben.
- Beobachte Systemprotokolle. Halte Logs einfach (im Textformat) und zentralisiere das Logging. Verwende Filter für Logmeldungen, um nicht von der Flut der Meldungen erschlagen zu werden.

- Verwende Informationen, um zu überprüfen, ob deine Systeme Sicherheitslücken aufweisen. Patche die Systeme schnell, denn Angreifer wissen spätestens mit der Veröffentlichung des Patches über die Angreifbarkeit von Systemen Bescheid.
- Auch für die Benutzung der Systeme müssen Richtlinien festgelegt werden. Diese müssen kommuniziert werden (Mitarbeiter, Community). Security-Awareness-Schulungen (awareness .. ins Bewusstsein rufen) können ebenfalls dabei helfen. Es muss überprüft werden, ob die festgelegten Richtlinien auch umgesetzt und eingehalten werden.

## 4. Halte dein System klein und einfach

Systeme und Applikationen sollen so klein und einfach wie möglich sein. Komplexität ist der Feind der Sicherheit. Verwende immer ein möglichst einfach aufgebautes System. Zum einen vermeidet man so Komplexität, zum anderen schont man die vorhandenen Ressourcen.

- Füge einem System nicht mehr Komponenten oder Features hinzu als unbedingt benötigt werden. Lass nicht mehr Dienste laufen als unbedingt nötig. Verzichte auf alle unnötige Software. So wird die Angriffsfläche verkleinert, ebenso wie die Wahrscheinlichkeit, dass etwas schiefgehen kann. Falls das System schon bei Lieferung zu komplex ist, passe es an. Hilfreich ist es in dieser Hinsicht Open Source Software zu verwenden.

**Beispiel:** Verzichte auf Web-Interfaces zur Administration einer Firewall. Das Webinterface benötigt einen HTTP-Server und implementiert eine Schnittstelle zur Umsetzung der Eingaben im Webinterface in Kommandozeilen-Befehle für die Firewall. Dies sind zwei zusätzliche, aber unnötige Angriffsvektoren. Lerne stattdessen, die Kommandozeile direkt zu benutzen.

- Fast das Gleiche gilt für Daten: Lösche sensitive Daten, wenn sie nicht mehr gebraucht werden. Speicher sie erst gar nicht, wenn sie nicht benötigt werden.

# Vereinfachte Grundprinzipien der IT-Sicherheit 3/4

- Auch bei der Rechtevergabe sollte Minimalismus vorherrschen. Gib jeder Person und jedem Prozess nur die Rechte, die unbedingt benötigt werden (Prinzip des geringsten Privilegs).

## 5. Isoliere deine Systeme

Große All-in-One-Systeme sind oft bequem und komfortabel zu nutzen. Leider sind sie auch überaus komplex und bieten daher eine große Angriffsfläche.

- Systeme und Funktionen sollten daher so weit wie möglich voneinander getrennt werden. Bei Problemen ist so immer nur eine Komponente betroffen. Separiere Systeme voneinander, auf möglichst unterschiedlichen Ebenen. Verwende verschiedene Netzwerksegmente, da wo es angebracht ist. Verwende unterschiedliche Hosts für einzelne Dienste. Nutze dabei Virtualisierung, keine Containerisierung, denn Virtualisierung bietet eine bessere Isolation.
- Separiere auch Daten. Wichtige Daten sollten woanders gehalten (und besser abgesichert werden) als unwichtige Daten. Verwende nicht das gleiche Passwort für alle Systeme und Dienste.
- Verwende Schnittstellen, um die Kommunikation zwischen den isolierten Systemen herzustellen und kontrolliere diese.
- Jede Komponente sollte immer genau eine Aufgabe erfüllen, und diesen Aufgabenbereich auch gut erfüllen. Verwende daher keine Universalisten, sondern Spezialisten. Vergiss aber nicht, dass diese einfach und klein sein sollen. Die Prinzipien des Minimalismus und der Isolierung haben viele Gemeinsamkeiten und beide ergänzen sich.

## 6. Gestalte deine Systeme fehlertolerant

Frage dich bei jedem System: »Was passiert, wenn es ausfällt?« Ist dann das gesamte Gefüge betroffen oder kann es auch ohne das System weiterhin funktionieren?

Erstelle einen Notfall-Plan, der sagt, was bei Ausfällen zu tun ist. Denn früher oder später wird jedes System gestört sein oder ausfallen.

- Sorge bei kritischen Systemen dafür, dass ein Reservesystem zeitnah bereit steht (gestalte es z. B. als hochverfügbares System). Aktuelle Daten benötigen aktuelle Backups und sollten zeitnah wieder eingespielt werden können.
- Je kleiner und einfacher die Systeme sind, desto besser sind sie fehlertolerant zu gestalten. Auch die Isolierung unterstützt dabei, fehlertolerante Systeme einfach aufbauen zu können.
- Sicherheitsmaßnahmen können ebenfalls ausfallen oder fehlschlagen. Wenn ein Account oder ein Zertifikat kompromittiert wird, muss es Maßnahmen geben, die den damit eingehenden Risiken entgegenwirken. Es ist daher eine gute Idee, mehrere Sicherheitsmaßnahmen auf mehreren Ebenen einzuführen.
- Und es geht nicht nur um technische Systeme. Auch Personen können ausfallen. Es sollte daher vermieden werden, dass der Ausfall einer Person (z. B. des einzigen Sysadmins) zu einem Problem werden kann.

## 7. Beachte die Verhältnismäßigkeit

Sicherheit kostet Zeit, Geld und Aufwand. Bei jedem vorangegangenen Punkt sollte man sich daher fragen: Ist das auch verhältnismäßig?

- Man kauft sich schließlich auch keinen 1000-Euro-Safe, um darin 100 Euro zu lagern. Daher sollte geprüft werden, was man mit der Sicherheitsmaßnahme eigentlich schützen will und welche Auswirkungen die Maßnahme auf den Betrieb hat. Die Datenbank mit den Ergebnissen der Betriebs-Fußballmannschaft braucht sicher weniger Schutz, als die Datenbank mit den Firmenpatenten. Auch die Wahrscheinlichkeit eines Sicherheitsrisikos spielt eine Rolle, es ist wenig sinnvoll teure Sicherheitsmaßnahmen für sehr unwahrscheinliche Risiken einzuführen.



# Vereinfachte Grundprinzipien der IT-Sicherheit 4/4

Ein guter Weg, um die Verhältnismäßigkeit festzustellen, sind daher folgende Fragen:

- Muss das System geschützt werden und inwieweit?
- Welche Sicherungsmaßnahme hat die geringste Auswirkung auf den laufenden Betrieb?
- Wie hoch bzw. wahrscheinlich ist das Sicherheitsrisiko?
- Welches ist die einfachste und kostengünstigste Lösung für die Sicherungsmaßnahme? (**Hinweis:** oft lautet die Antwort »Open Source Software«)

## Schlusswort

Jedes einzelne dieser Grundprinzipien ist ein wichtiger Baustein. Jedoch sind sie um so wirksamer, wenn sie zusammen arbeiten. Wenn man sich diese Grundprinzipien vor Augen führt, kann man dabei helfen, Ordnung im Gewirr der Fachwörter der ITSec-Industrie zu bekommen und auch im eigenen Netz die Übersicht zu behalten.

Die Systeme zu kennen, zu separieren, klein und einfach zu halten und zu überprüfen kann so manches »Cybersecurity-Produkt« überflüssig machen. Wenn man die Prinzipien kennt, muss man nicht unbedingt die ISO 27001 im Detail kennen – vieles von dem, was dort steht, wird sich daraus automatisch ergeben.

Dieser Artikel basiert auf der Arbeit »The Information Security Practice Principles« von Craig Jackson, Scott Russell und Susan Sons vom »Center for Applied Cybersecurity Research« der Universität Indiana. The Information Security Practice Principles, Craig Jackson, Scott Russell, and Susan Sons, University Center for Applied Cybersecurity Research

**Hinweis:** Die internationale Norm ISO/IEC 27001 »Information technology – Security techniques – Information security management systems – Requirements« spezifiziert die Anforderungen für geeignete Sicherheitsmechanismen zum Schutz sämtlicher Werte in der IT. Sie berücksichtigt dabei die Sicherheitsrisiken innerhalb der einzelnen Organisation (Unternehmen, staatliche Organisationen, Non-Profit-Organisationen) und formuliert Grundsätze zu Implementierung, Betrieb, Überwachung, Wartung und Verbesserung eines Information-Security-Management-Systems.

# Härtung von IT-Systeme 1/4

## Was bedeutet Systemhärtung?

Der Begriff »Systemhärtung« ist die Übersetzung des Englischen »System Hardening«. Im IT-Sprachgebrauch wird vereinfacht auch nur von der »Härtung« gesprochen.

Da auf IT-Systemen unter anderem auch höchst sensible Informationen eines Unternehmens sowie personenbezogene Daten verarbeitet und gespeichert werden, müssen die verwendeten Systeme besonderen Schutzmaßnahmen unterzogen werden. Eine sehr wirkungsvolle Maßnahme zur Absicherung stellt die Systemhärtung dar. Sie sichert das Betriebssystem ab, unabhängig davon, ob es sich um ein physikalisches, virtuelles oder cloud-basiertes System handelt.

## Warum IT-Systeme speziell konfiguriert werden?

Gängige IT-Systeme mit Betriebssystemen wie z.B. Microsoft Windows oder Linux werden von den Herstellern auf die größtmögliche Kompatibilität und den breitesten Feature-Umfang vorkonfiguriert. Die Systeme sind daher mit potentiell angreifbaren, aber oftmals ungenutzten Komponenten ausgestattet.

Das bedeutet: Standardmäßig werden bei Betriebssystemen keine restriktiven Sicherheitskonfigurationen angewendet. Gerade diese oft ungenutzten und nicht konfigurierten Funktionalitäten nutzen Angreifer wie Hacker häufig als Angriffsvektor aus.

Ziel der technischen Maßnahme »Härtung«: Diese Funktionalitäten, sowie deren exponierten Schnittstellen, werden deaktiviert oder sogar deinstalliert.

## Welche Bedrohungen existieren?

Die wesentlichen Bedrohungen bei nicht gehärteten IT-Systemen sind unter anderem:

- Identitätsdiebstahl, z.B. bei Angriffen auf die zentrale Identitäts-Management-Struktur
- Daten-Manipulation von personenbezogenen Daten und sensiblen Unternehmensdaten

- Datenabfluss durch Kopieren gesamter Datenbanken
- Manipulation von Anwendungen oder damit verbundener Systeme
- Sabotage oder Spionage bei Betriebs- und Produktionsabläufen
- Einschleusen und Verbreitung von Malware

Viele Unternehmen sind von Hacker-Angriffen, Datendiebstahl und Spionage betroffen. Aus diesem Grund sind die Informationssicherheit und die Härtung von Systemen mehr als wichtig.

## Maßnahmen zur Systemhärtung

Systemhärtung ist ein technischer Baustein, um mögliche Schwachstellen (Vulnerabilities) von IT-Systemen und IT-Infrastrukturen zu verringern.

### Maßnahmen:

- Regelmäßige Überprüfung der Notwendigkeit von aktivierten Diensten
- Laufende Dienste nur mit minimalen Rechten betreiben
- Wenn möglich: Betrieb der laufenden Dienste in einer isolierten Umgebung
- Minimale Rechtevergabe für Wartungsschnittstellen und -zugänge
- Einschränkung des Zugriffs auf die Konfigurationsdateien des Betriebssystems
- Änderung aller vorhandenen Standard-Kennwörter durch Passwörter einer entsprechenden unternehmensinternen Kennwort-Richtlinie
- **Deaktivierung** von Fehler- oder Debug-Meldungen für Endbenutzer
- **Deaktivierung** von unsicheren, veralteten und/oder nicht benötigten Schnittstellen
- **Deaktivierung** von nicht benötigten Autostart-Mechanismen
- **Deaktivierung** von unnötigen Betriebssystem-Komponenten, inklusive aller unnötigen Hintergrund-Dienste

# Härtung von IT-Systeme 2/4

- Aktivierung eines Bildschirmschoners mit Kennwort-Schutz
- Aktivierung starker Benutzerkontensteuerung (User Account Control)
- Aktivierung des Antiviren-Programms beim Bootvorgang
- Aktivierung der Protokollierung
- Aktivierung der CPU-Sicherheitsfunktionen
- Aktivierung des BIOS-Zugriffspasswortes
- Aktivierung einer festgelegten Boot-Reihenfolge

Ein großer Teil der oben aufgeführten Härtungsmaßnahmen ist durch technische Einstellungen machbar. Diese Einstellungen lassen sich über ein Härtungspaket (z.B. mittels Skripte) automatisiert auf alle Server-Systeme des Unternehmens verteilen.

Zudem gilt: Neue Server-Systeme sollten direkt nach Abschluss der Installation mit der entsprechenden standardisierten Konfiguration versorgt und Ausnahmen von der Härtung sollten zentral verwaltet werden.

## Drei grundlegende Konfigurationsänderungen

Ziel ist es, durch drei grundlegende Konfigurationsänderungen die Kontrolle über das Betriebssystem zu erlangen:

**1. Versiegeln:** Das Starten von Programmen ist standardmäßig verboten und wird nur für zugelassene Programme erlaubt. Programme können nur starten, wenn sie auf einer »Whitelist« stehen. Unbekannte Programme sind nicht vertrauenswürdig und dürfen nicht starten.

**2. Isolieren:** Ausgehender und eingehender Netzwerkverkehr ist grundsätzlich verboten und nur für festgelegte Ausnahmen erlaubt. Unbekannter ausgehender und eingehender Netzwerkverkehr ist nicht vertrauenswürdig und wird unterbunden.

**3. Herabstufen:** Die automatische Nutzung von administrativen Rechten für administrative Konten ist deaktiviert. Administrative Rechte werden immer erst nach einer Zustimmungsabfrage gewährt. Dies verhindert ungewollte Änderungen am System, wie z.B. Installation von Malware oder Fehlkonfigurationen.

Diese drei einfachen Konfigurationsänderungen unterbinden wirksam diverse Angriffsszenarien auf standardmäßig eingerichtete Betriebssysteme. Vor allem und zuerst profitieren alle Internetanwendungen von der Versiegelung des Systems, welche das unerwünschte Starten von unbekannten Programmen unterbindet.

## Vier Konfigurationsprinzipien

Einen umfassenderen Schutz bietet diese Anleitung, vor allem für Server-Systeme an denen als Administrator gearbeitet werden muss. Ein System das nach dieser Anleitung konfiguriert wurde, ist weniger für 0-Day-Exploits anfällig.

Diese Anleitung beruht auf folgenden grundlegenden Prinzipien:

1. Beschränke die Zugriffsrechte auf das erforderliche Maß. Arbeite als Administrator, root oder Supervisor nur wenn es unbedingt notwendig ist und dann nicht mit automatischer Rechtegewährung.
  2. Beschränke die beliebige Ausführung von Programmen. Erlaube nur Programme, die benötigt werden. »Software-Whitelisting« ist einfach der bessere Anti-Virus-Schutz.
  3. Beschränke zufälligen Netzwerkverkehr. Erlaube nur notwendigen ausgehenden und eingehenden Netzwerkverkehr.
  4. Benutze möglichst wenige Programme und vermeide die Duplizierung von Funktionalitäten. Konzentriere Dich auf das zu erreichende Ergebnis.
- Hinweis:** Je mehr Programme, je mehr potentielle Sicherheitsprobleme.

# Härtung von IT-Systeme 3/4

## Vorteile der angepassten Konfiguration

- Systeme funktionieren langfristig zuverlässiger und vorhersehbarer, verglichen mit den Standardkonfigurationen.
- Patches können nach dem Rhythmus der jeweiligen Organisation eingespielt werden und müssen nicht immer sofort installiert und aktiviert werden.
- Die Reichweite von administrativen Konten ist auf vertrauenswürdige IP-Adressen beschränkt, so dass möglichst lange und komplexe Passwörter durch kürzere praktikablere Passwörter ersetzt werden können.
- Die PC-Hardware kann wieder vorrangig für ihre ursprüngliche Aufgabe genutzt werden: erwünschte Software auszuführen. Die Nutzung von Software Whitelisting ermöglicht die Deaktivierung von Software Blacklisting (Viren- und Malwarescanner), so dass mehr Hardware-Ressourcen für erwünschte Anwendungen zur Verfügung stehen.
- Durch die Akzeptanz von UAC (User Account Control, Benutzerkontensteuerung) wird das Arbeiten als eingeschränkter Administrator unter UAC selbstverständlicher..

## Nachteile der angepassten Konfiguration

- Für die Installation von neuer Software, einschließlich von Updates, muss das Software Whitelisting rekonfiguriert werden.
- Diverse Netzwerkprotolle, welche sich nicht über einen lokalen Proxy-Server lenken lassen, z.B. Multimedistreaming-Protokolle, erfordern eine Anpassung der Isolierung vom Internet durch die Firewall und/oder von verschiedenen weiteren Filtern (z.B. IPSec-Filter).
- Die strikte Durchsetzung von UAC (User Account Control, Benutzerkontensteuerung) verringert die Produktivität durch mehr GUI-Arbeit (GUI .. Graphical User Interface), dies wird aber deutlich kompensiert durch den Mehrgewinn an Sicherheit und nicht zuletzt auch durch den erhöhten Schutz vor Fehlern, z.B. versehentliches Löschen von Daten.

## Wie kann eine IT-Abteilung ihren Zeitaufwand für die Systemhärtung reduzieren?

Über Automatisierung. Selbst programmierte Skripte sorgen dafür, dass viele Abläufe des System-Hardenings eigenständig ablaufen. Doch das Entwickeln und Anpassen des Codes erfordert ebenfalls viel Zeit.

## Die Lösung für automatisierte Systemhärtung

Das Härten von IT-Systemen ist sehr kompliziert und bei großen Unternehmen auch sehr komplex. Im Normalfall müssen die Verantwortlichen manuell tausende Einstellungen vornehmen - das kostet viel Zeit. Und bindet damit viele Ressourcen, die an anderer Stelle benötigt werden.

Trotzdem darf die Systemhärtung auf keinen Fall vernachlässigt werden. Ansonsten steigt die Wahrscheinlichkeit, dass »Cyber-Gangster« mit ihren »Cyber-Attacken« Erfolg haben.

## Strategie der umfassenden Verteidigung

Angeichts der Angriffe auf Informationen reicht es nicht aus, sich auf einen einzigen Mechanismus für Netzwerk- und Hostsicherheit zu verlassen:

- Ein einziger Konfigurationsfehler ermöglicht einem Eindringling kompletten Zugriff auf das Netzwerk.
- Eine einzige Abwehrebene bietet nur geringen Widerstand gegen Angriffe und einem Eingreifteam bleibt zu wenig Zeit zum Reagieren.
- Wenn versucht wird, alle Sicherheitsrichtlinien auf einer einzigen Ebene unterzubringen, kann dies zu unhandlichen Regelsätzen führen, die sich immer schwieriger verwalten lassen.

# Härtung von IT-Systeme 4/4

Wenn die Verantwortlichkeit für den Schutz auf mehrere Ebenen aufgeteilt wird, werden einige Aspekte automatisch berücksichtigt:

- Ein Konfigurationsfehler auf einer Ebene wird höchstwahrscheinlich auf einer anderen Ebene ausgeglichen.
- Mehrere Abwehrebene verursachen einem Angreifer mehr Arbeitsaufwand - allein diese Tatsache wird von gelegentlichen Angriffen abschrecken. Außerdem bieten solche Abwehrebene dem Eingreifteam die wertvollste Ressource: Zeit.
- Mehrere Sicherheitsstufen ermöglicht das Erstellen von Richtlinien, die für jede Stufe geeignet sind. Dies vereinfacht den Konfigurationsaufwand.

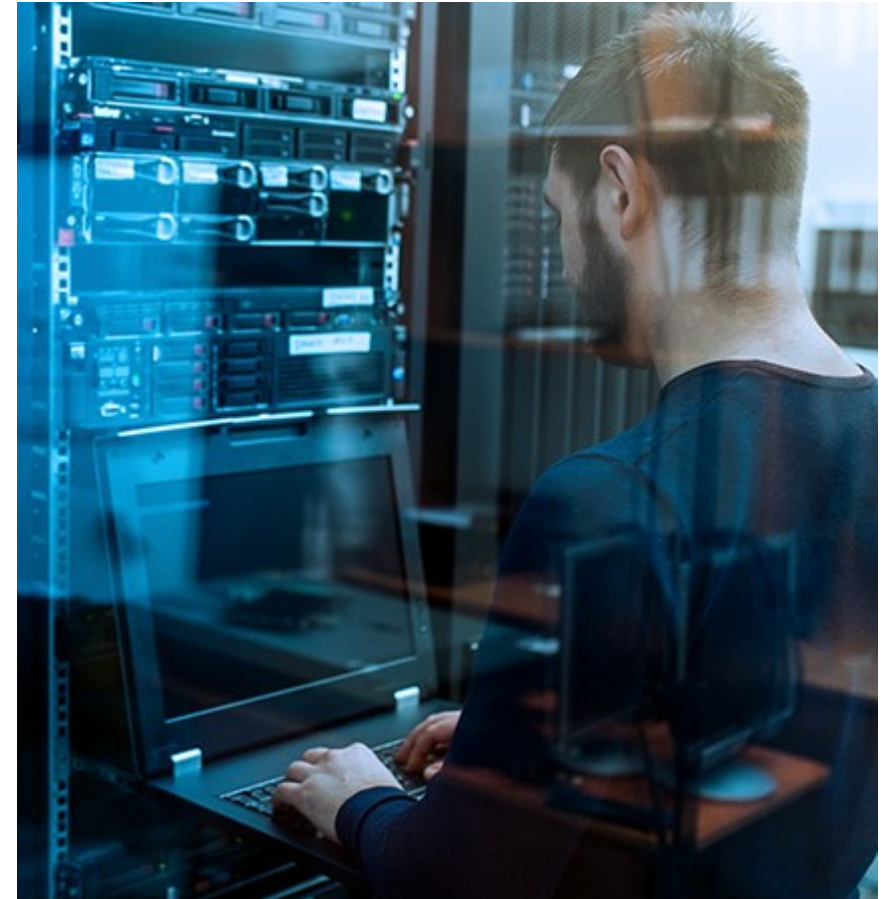
Durch die umfassende Verteidigung können Änderungen auf flexible Weise berücksichtigt werden.

## Langfristige Sicherheitsstrategie

Es ist langfristig sinnvoller, Zeit in die Sicherheit der Endsysteme zu investieren, als sich allein auf Netzwerkfirewalls zu verlassen. Netzwerkfirewalls können allgemein die Sicherheit erhöhen, aber letztendlich viele Angriffsszenarien nicht verhindern.

Es ist von grundlegender Bedeutung zu verstehen, dass jedes System in der Lage sein muss, sich selbst zu schützen. Ein isolierter Einsatz von Netzwerkfirewalls zum Schutz vor Sicherheitsproblemen ohne Beachtung der Konfiguration der Endsysteme ist langfristig nicht erfolgversprechend.

Netzwerkfirewalls sind lediglich ein Baustein einer Sicherheitsstrategie, die darauf abzielt einen störungsfreien Betrieb der Endsysteme zu gewährleisten. Das Hauptaugenmerk muss auf der sicheren Konfiguration der Endsysteme liegen.



*»Alles was hier möglich ist, ist meistens auch erlaubt.«*

Diesen Satz sollte man sich vom Standpunkt eines Admins, wie auch vom Standpunkt eines Angreifers sehr langsam über die Zunge rollen lassen. Die Härtung von IT-Systemen erfordert immer eine durchdachte und strukturierte Vorgehensweise.



# Härtung mit Windows-Werkzeuge 1/2

## Whitelisting-Regeln mittels Bordmitteln

Die Konfiguration der Software-Whitelist können unter Windows entweder manuell per Gruppenrichtlinien-Snap-In »gpedit.msc« realisiert werden oder direkt unter Umgehung der Gruppenrichtlinien in die Registry geschrieben werden. Dabei sind die gesetzten Regeln per Gruppenrichtlinien-Snap-In »gpedit.msc« nicht sichtbar, werden jedoch trotzdem vom System beachtet.

Alternativ ist es möglich, die gruppenrichtlinienbasierte Software Restrictions per Powershell-Skripts mit der kostenpflichtigen Zusatzsoftware GPEXpert Software Group Policy Automation Engine (GPAE) auf allen Windows Systemen ab Windows XP umzusetzen.

## Windows Defender Application Guard

Windows Defender Application Guard (WDAG) kann Sitzungen im Webbrowser über Hyper-V virtualisieren und dadurch sicherstellen, dass Malware nicht über das Internet auf einen PC übertragen werden kann. Bislang steht die Funktionalität nur unter den Windows Enterprise- und Pro-Versionen zur Verfügung.

WDAG erstellt eine Art Sandbox und nutzt hierfür integrierte Virtualisierungs-Technologien. Die Funktionalität von Windows Defender Application Guard wird kontinuierlich erweitert.

**Hinweis:** Die Sicherheitstechnologie arbeitet derzeit nicht mit allen Webbrowsern zusammen.

## Windows Device Guard

Microsoft bietet mit Windows Device Guard die Möglichkeit Arbeitsstationen so abzusichern, dass nur definierte Anwendungen (Whitelist) gestartet werden können. Windows Device Guard stellt gewisse Anforderungen an das verwendete System und die Hardware, die unterstützt werden müssen.

## Windows Defender Exploit Guard

Der Windows Defender Exploit Guard wurde ins Betriebssystem integriert. Hier kann man die Angriffsfläche, die ein System bietet, deutlich reduzieren. Anwendungen lassen sich gegen typische Sicherheitslücken, wie etwa Buffer Overflows, härten. Administratoren können so mehr Kontrolle darüber erhalten, wie Code auf den Systemen ausgeführt wird. Auf Einzelsystemen finden sich die Einstellungen zum Exploit-Schutz im Windows Defender Security Center (siehe auch: regedit) im Bereich App- & Browsersteuerung (Systemsteuerung -> Suchenfeld) unter Exploit-Schutz.

Zur Funktionalität des Windows Defender Exploit Guard gehört auch der überwachte Zugriff auf Ordner.

## User Account Control (UAC)

Mit Hilfe der UAC (User Account Control, Benutzerkontensteuerung), kann ein striktes Herabstufen jeder administrativen Handlung mittels Mandatory Integrity Control (MIC) und der Deaktivierung der automatischer Rechtegewährung für administrative Konten durchgeführt werden.

Für das Herabstufen und der Deaktivierung der automatischer Rechtegewährung sind in der Registry über die Kommandozeile (CMD, Powershell) einige Änderungen einzutragen:

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\
Policies\System/v EnableLUA /t REG_DWORD /d 0x1 /f
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\
Policies\System/v FilterAdministratorToken /t REG_DWORD /d 0x1 /f
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\
Policies\System/v ConsentPromptBehaviorAdmin /t REG_DWORD /d
0x2 /f
```



# Härtung mit Windows-Werkzeuge 2/2

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\
Policies\System/v PromptOnSecureDesktop /t REG_DWORD /d
0x1 /f
```

## Windows-Firewall ein- und ausschalten

Wenn man die Windows-Firewall aktivieren oder deaktivieren will, reicht eine einfache Netsh-Befehlssyntax aus.

Eine Firewall aktiviert man über die Kommandozeile (Powershell) wie folgt:

```
netsh -> firewall -> set opmode enable
```

Die Deaktivierung der Firewall geschieht mit folgender Befehlszeile:

```
netsh -> firewall -> set opmode disable
```

**Hinweis:** Kommandos nacheinander eingeben.

## Windows-Firewall-Protokollierung einschalten

Zur Härtung eines Systems gehört auch immer die Protokollierung aller wesentlichen Aktivitäten.

### Protokollierung einschalten:

Windows Einstellungen aufrufen [Win] + [I] -> Netzwerk und Internet -> Ethernet -> Windows Firewall -> Erweiterte Einstellungen  
Öffentliches Profil -> Windows Defender Firewall-Eigenschaften -> Tab: Privates Profil -> Protokollierung -> Anpassen und Verworfen Pakete und erfolgreiche Verbindungen protokollieren -> auf **JA** einstellen und bestätigen

oder

Windows Einstellungen aufrufen [Win] + [I] -> Begriff suchen: Firewall  
-> Firewall- & Netzwerkschutz -> Erweiterte Einstellungen [...]

### Protokoll ansehen:

Windows Einstellungen aufrufen [Win] + [I] -> Netzwerk und Internet -> Ethernet -> Windows Firewall -> Erweiterte Einstellungen -> Überwachung -> Protokollierungseinstellungen und den Link zur Protokolldatei anklicken

# Penetrationstest (Pentest) 1/5

## Was ist ein Pentest?

Die Penetrationstests werden häufig von ethischen Hackern (Penetrationstester, auch Red Teams genannt) durchgeführt. Das können interne Mitarbeiter oder aber auch Dienstleister sein. Diese ahmen die Strategien und Aktionen eines Angreifers nach, um die Angreifbarkeit der Computersysteme, des Netzwerks oder den Webanwendungen einer Organisation zu bewerten. Organisationen verwenden Pentests auch, um die Einhaltung von Compliance-Vorschriften zu testen.



Durch den Einsatz verschiedener Methoden und Tools können Unternehmen simulierte Cyberangriffe durchführen, um die Stärken und Schwächen ihrer bestehenden IT-Sicherheitssysteme zu testen.

Penetration bezieht sich in diesem Fall auf den Grad, in dem ein hypothetischer Bedrohungsakteur oder Hacker an den Sicherheitsmaßnahmen vorbei, in ein Unternehmen eindringen kann.

Es existieren drei wesentliche Strategien für Pentests:

- Bei **Whitebox**-Penetrationstests erhält der Tester beispielsweise alle Details über das System oder das Zielnetzwerk einer Organisation.
- Bei **Blackbox**-Tests hat der Tester keinerlei Kenntnisse über das System.
- Beim **Graybox**-Ansatz erhält der Testende Teilkenntnisse über das System.

Pentests werden oft mit einem bestimmten Ziel durchgeführt. Ganz typisch sind hierfür die drei folgenden Ziele:

- angreifbare Systeme zu identifizieren,
- versuchen, ein bestimmtes System anzugreifen oder
- einen Datendiebstahl durchzuführen.

Jedes dieser Ziele konzentriert sich dabei auf bestimmte Ergebnisse, die IT-Leiter im richtigen Leben zu vermeiden versuchen.

1. **Kick-off:** Vorbesprechung des Projekts (Testzeitpunkt, Testumfang, ...)
2. **Penetration, Test:** Sicherheits- oder Penetrationstests als aktive Qualitätskontrolle der IT-Sicherheit
3. **Dokumentation:** Alle Testergebnisse werden am Ende des Projekts in einem Bericht (Schwachstellen mit Risikoeinschätzung, Maßnahmen zur Behebung) zusammengefasst.
4. **Workshop:** Präsentation mit Workshopcharakter und/oder technischer Workshop für Systemverantwortliche und Administratoren
5. **Maßnahmenplan:** Behebung der Schwachstellen
6. **Nachüberprüfung:** der Nachtest oder Nachüberprüfung hat die Aufgabe, die Wirksamkeit der Maßnahmen zur Behebung von Sicherheitsschwächen zu prüfen

# Penetrationstest (Pentest) 2/5

## Ablauf eines Penetrationstests

Ein Penetrationstest ist ein simulierter Cyberangriff, um Sicherheitslücken in Systemen, Anwendungen oder Organisationen zu identifizieren und dem Kunden detaillierte Informationen über den Sicherheitszustand zu liefern.

Beim Penetrationstest geht es in erster Linie um die Sammlung von möglichst vielen Informationen (IT-Infrastruktur, Personen, Social Engineering) und deren Nutzung in einem mehrstufigen Angriffsplan.



## Externe Penetrationstests

In einem externen Penetrationstest analysiert man die im Internet exponierte Infrastruktur und sucht nach Schwachstellen. Üblicherweise prüft man als erstes die Systeme und Dienste mit automatisierten Tools. Danach wird die Analyse mit manuellen Tests verfeinert. Die identifizierten Schwachstellen werden verifiziert und allenfalls ausgenutzt, um die effektiven Risiken zu quantifizieren.

Typische Aktivitäten bei externen Penetrationstests:

- Identifikation von Systemen und Diensten
- Identifikation von virtuellen Hosts mittels Namen
- Schwachstellenanalyse und Plausibilisierung
- Ausnutzung der entdeckten Schwachstellen
- Angriffe von infizierten Systemen auf benachbarte Dienste ausweiten (pivoting)

## Interne Penetrationstests

Ein unerlaubter Zugriff auf ein Netzwerk kann auch durch Schadcodes, frustrierte Mitarbeiter oder durch angebundene Partnerfirmen erfolgen. In einem internen Penetrationstest besucht man einige Mitarbeiter, Partnerfirmen und simuliert einen Angriff aus interner Sicht. Danach analysiert man die interne Infrastruktur und sucht nach Schwachstellen und möglichen Angriffsvektoren. Die entdeckten Angriffsvektoren werden ausgenutzt, um zusätzliche Privilegien im Netz zu erlangen, kritische Systeme zu kompromittieren und Zugriff auf sensible Daten zu erhalten.

Typische Aktivitäten bei internen Penetrationstests:

- Schwachstellenanalyse
- Ausnutzung der entdeckten Schwachstellen
- Privilegien eskalieren (auf dem Computer und innerhalb der Domäne)
- Suche nach Passwörtern und Schlüsselmaterial (Dateien, Konfiguration, Software, Repositorien, Firmen-Wiki)
- Überprüfen der internen Netzwerktrennung
- Identifizierung und Ausnutzung von Active Directory Fehlkonfigurationen (Bloodhound, Pingcastle, etc.)
- Angriffe mittels Windows-Netzwerk Mechanismen (NTLM Relay, Pass-the-Hash, Kerberoasting, Delegation, etc.)

# Penetrationstest (Pentest) 3/5

## Tools für Penetrationstests

Penetrationstester, auch Red Teams genannt, werden seit Jahren eingesetzt, um Default-Passwörter in Active-Directory-Umgebungen (AD) aufzuspüren, mit denen die Netzwerke infiltriert werden können. Von dort aus dringen sie weiter vor und versuchen, sich administrative Rechte zu verschaffen. Diese Entwicklung hat zu einer Reihe in vielerlei Hinsicht nützlicher Open-Source-Tools geführt, mit denen sich zum Beispiel ein komplettes Verzeichnis eines Active Directory erstellen lässt. So können die Tester schneller geeignete Ziele identifizieren und ganze Angriffsketten aufbauen. Diese Angriffsketten ähneln in der Regel den Attacken, die Ransomware ausführt, um sich in Netzwerken festzusetzen und um sich weiter zu verbreiten. Die Tools, die ursprünglich für Penetrationstester geschrieben wurden, sind auch für alle IT-Admins interessant, die ihre Netzwerke gegen Angriffe durch Ransomware verteidigen wollen.

### Das BloodHound-Tool

Ein für das Auditing (Prüfung) von Active Directory besonders nützliches Werkzeug ist BloodHound. Das Tool wurde erstmals auf der DefCon 24 im Jahr 2016 vorgestellt. Es dient dazu, große Active-Directory-Netze mit einer erheblichen Zahl von Trusted Domains zu mappen. Um die Ergebnisse grafisch darzustellen, nutzt die Software eine kostenlose Version der Neo4j Graph Plattform. Damit lassen sich etwa Schaubilder erstellen, die alle Datenpunkte im Active Directory miteinander in Beziehung setzen. BloodHound verwendet entweder eine herkömmliche ausführbare Datei oder aber auch ein Ingestor-Skript (Aufnahme, Einsammlung von Daten) für die PowerShell, um die benötigten Informationen aus dem Active Directory zu sammeln. Es kann im Prinzip auch mit normalen User-Rechten laufen. Mit Admin-Rechten ist es aber möglich, weit mehr Daten einzusammeln. Mit BloodHound lässt sich auch herausfinden, welche Informationen ein Standardnutzer im Active Directory zu sehen bekommt.

Nachdem die Daten durch den Ingestor eingesammelt wurden, können sie in Neo4j importiert werden. BloodHound gibt es für Windows, MacOS und Linux.



### PingCastle

Ping Castle ist ein kommerzielles Produkt unter der »Non-Profit Open Software License (Non-Profit OSL)«. PingCastle ist ein Tool für die Kommandozeile, das zahlreiche Schalter und Optionen bietet. Für den Einstieg reicht aber der interaktive Modus aus, der automatisch gestartet wird, wenn man das Programm ohne Parameter aufruft. Dieser schlägt dann die aktuelle Domäne vor, bevor er die Prüfroutine startet. Gibt man bei der Auswahl der Domäne das Stern-Wildcard (\*) ein, dann durchleuchtet das Tool alle erreichbaren Domänen und konsolidiert anschließend die Ergebnisse in einem Gesamtbericht.

Dem Entwickler Vincent le Toux zufolge entstand PingCastle aus einem Projekt für einen internationalen Konzern, dessen Verzeichnisdienst mehr als 300 Domänen umfasst.

## Penetrationstest (Pentest) 4/5

Das Tool kann daher nicht nur einzelne Domänen unter zahlreichen Kriterien durchleuchten, sondern skaliert auch für Umgebungen mit komplexen AD-Forests und Vertrauensbeziehungen. Der Healthcheck von PingCastle prüft das Active Directory anhand von mehr als 70 Regeln. Sie sollen Verstöße gegen unterschiedlichste Empfehlungen und Sicherheitsrichtlinien aufspüren. Dazu zählt beispielsweise die Existenz inaktiver Objekte (User, Computer, Betriebssysteme) und veralteter Protokolle.

**Hinweis:** Ein Active Directory Forest (AD Forest) ist ein Container auf der höchsten Organisationsebene einer Active Directory-Konfiguration, in der Domänen, Benutzer, Computer und Gruppen-Richtlinien enthalten sind.

Weitere Prüfkriterien sind unter anderem ACLs (Access Control List oder Zugriffssteuerungsliste) und Delegierungen, in GPOs (Group Policy) enthaltene Passwörter, Passwortregeln, Mitglieder in administrativen Gruppen oder AdminSDHolder. Entdeckt werden auch Accounts, deren Passwort nie abläuft oder wo dieses leer sein darf.

**Hinweis:** Der AdminSDHolder, frei übersetzt der »Bewahrer des Security Descriptors für Administratoren«, dient dem Schutz administrativer Accounts vor Rechteänderungen von ACLs (Access Control List oder Zugriffssteuerungsliste).

### Open-Source-Graphdatenbank Neo4j

Die sehr populäre Graphdatenbank Neo4j (wird in Verbindung mit dem BloodHound-Tool genutzt) ist eine in Java implementierte Open-Source-Graphdatenbank. Neo4j wurde von Neo Technology entwickelt, einem Startup-Unternehmen mit Sitz in Malmö/Schweden und San Francisco Bay/USA.

Die Entwickler beschreiben Neo4j als eine eingebettete, disk-basierte, transaktionale Datenbank-Engine, die Daten anstatt in Tabellen in Graphen strukturiert speichert. Neo4j Version 1.0 wurde im Februar 2010 freigegeben. Die Community-Edition der Datenbank ist unter der GNU General Public License (GPL) v3 lizenziert. Zusatzmodule wie Online-Backup und Hochverfügbarkeit sind unter der GNU Affero General Public License (AGPL) v3 lizenziert. Die Datenbank sowie die Zusatzmodule sind in einem dualen Lizenzmodell auch unter einer kommerziellen Lizenz erhältlich.

### Purple Knight

Mit dem Tool Purple Knight kann die Active-Directory-Umgebung (AD) untersucht werden. Das kostenlose Sicherheitsanalyse-Tool kann Fehlkonfigurationen und Schwachstellen aufdecken, über die Angreifer in der Lage versetzt werden, Daten zu stehlen und Malware-Kampagnen zu starten.





# Penetrationstest (Pentest) 5/5

Einige typische Szenarien, die durch Purple Knight aufgedeckt wurden und zu AD-Schwachstellen führen:

- Passwortrichtlinien, die für einen zeitgemäßen Schutz von Konten unzureichend sind,
- Konten mit erhöhten Rechten, die nicht ausreichend revidiert wurden,
- über die Zeit entstandene Konten mit delegierten Rechten über Active Directory, die unerwünschte Auswirkungen auf die AD-Sicherheit haben,
- Unzulänglichkeiten bei der Kerberos-Nutzung, die zunehmend ausgenutzt werden, um privilegierten Zugriff zu erhalten,
- Schwachstellen in der Konfiguration von Group-Policies, die massive und ausnutzbare Lücken schaffen.

## Specops Password Auditor

Passwörter sind nach wie vor die wichtigste Methode zur Authentifizierung von Benutzern im Active Directory. Man kann standardmäßig nicht verhindern, dass Benutzer schlechte Passwort-Entscheidungen treffen. Da viele Sicherheitsverletzungen auf kompromittierte Passwörter zurückzuführen sind, sind Konten mit kompromittierten Passwörtern häufig der erste Einstiegspunkt für Angreifer. Durch das Scannen des Active Directory sammelt und zeigt das kostenlose Passwort-Audit-Tool »Specops Password Auditor« mehrere interaktive Berichte mit Informationen zu Benutzer- und Passwortrichtlinien an.

Leistungsumfang des Specops Password Auditor:

- Überblick über Passwort-Richtlinien und deren Einstellungen
- Identifikation von Konten mit kompromittierten Passwörtern
- Identifikation von Benutzerkonten ohne Anforderung an ein Passwort
- Identifikation ruhender Benutzerkonten

- Interaktives Dashboard über das Ablufen von Passwörtern, um passwortbezogene Helpdesk-Anrufe zu reduzieren
- Berichtsdaten zur weiteren Verarbeitung in CSV-Dateien exportieren
- Erstellen von PDF-Berichten mit einer Management Summary, um Ihre Ergebnisse mit Entscheidungsträgern zu teilen.





# KRITIS - Kritische Infrastrukturen

## Was sind Kritische Infrastrukturen?

Wasser, Strom, Telekommunikation, Lebensmittel oder der öffentliche Nahverkehr sind für uns alltägliche Dinge, die jedoch lebensnotwendig sind. Die Versorgung mit diesen und weiteren unentbehrlichen Gütern und Dienstleistungen übernehmen in Deutschland sogenannte Kritische Infrastrukturen (KRITIS). Dazu gehören beispielsweise die Energie- und Wasserversorgung, der Verkehr, aber auch die medizinische Versorgung.

Wie bedeutsam Kritische Infrastrukturen sind, erkennt man erst, wenn es zu Störungen kommt. Denn sie bilden die Grundlage für das Funktionieren unserer Gesellschaft.

Die Gewährleistung des Schutzes Kritischer Infrastrukturen ist eine Kernaufgabe staatlicher und unternehmerischer Sicherheitsvorsorge.

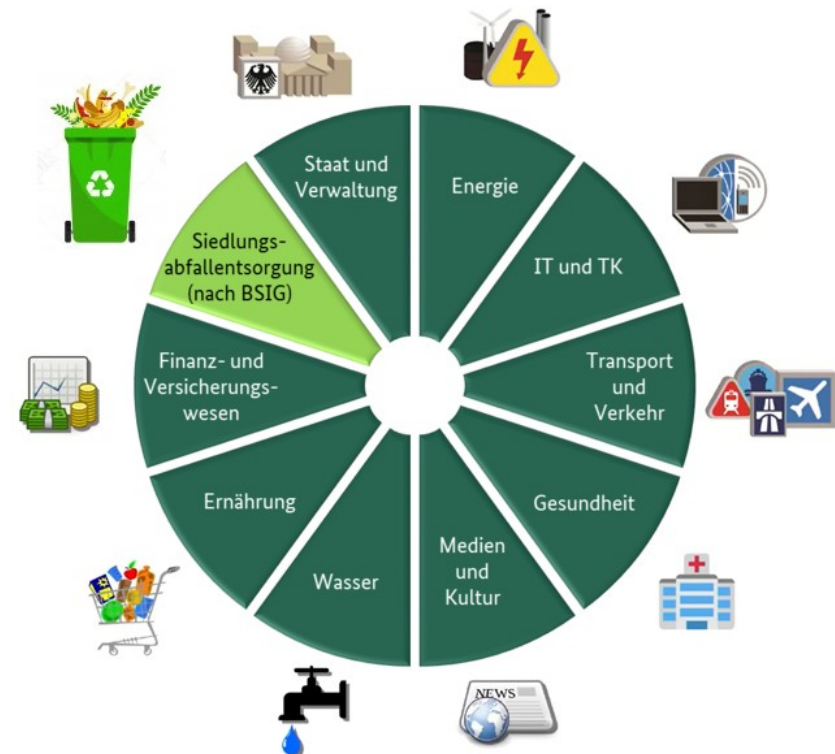
## Gefahren für die Kritische Infrastrukturen

Für die meisten »analogen Gefahren« gibt es – nicht zuletzt durch die jahrelange Erfahrung und der daraus resultierenden Lernkurven – eine Vielzahl an Katastrophenplänen und Notfallteams, die nach Katastrophen aller Art helfen, die Lage in den Griff zu bekommen. Bei Cyber-Angriffen besteht diese Routine (noch) nicht, erst recht nicht, wenn es sich bei dem Ziel um eine Kritische Infrastruktur handelt.

Grundsätzlich haben sich im KRITIS-Umfeld zwei Typen von Cyber-Angriffen herauskristallisiert:

- Diejenigen, die darauf aus sind zu zerstören
- und diejenigen, denen es darum geht, zu spionieren.

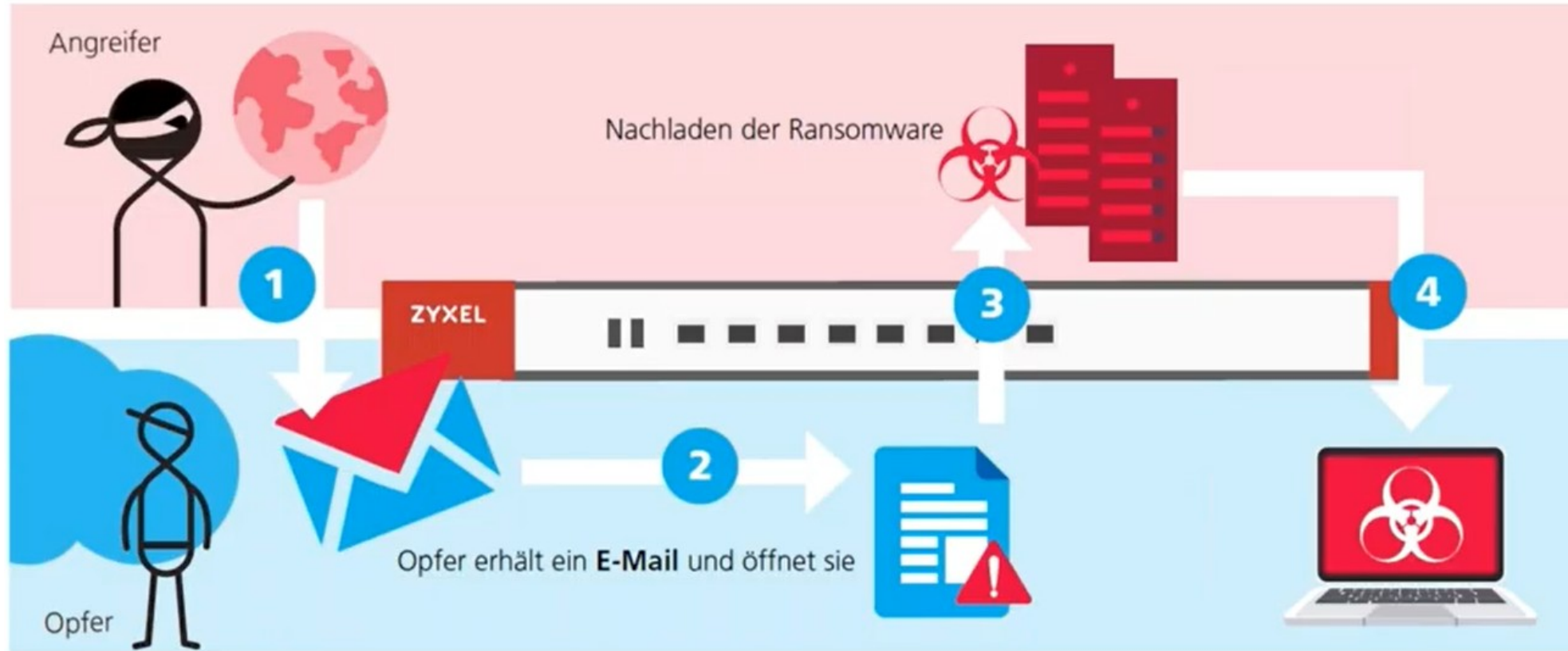
Gerade Letztere haben ein großes Interesse daran, möglichst lange unentdeckt zu bleiben. aufgrund diverser Erfahrungen kann davon ausgegangen werden, dass - gerade im KRITIS-Bereich - bereits vielerorts unentdeckt Trojaner eingeschleust wurden, die im Angriffsfall aktiviert werden.



In der Vergangenheit waren fortschrittliche Angriffe in ihrer Planung und Durchführung sehr aufwendig, so dass meist staatliche Organisationen hinter den Akteuren vermutet wurden.

Inzwischen ist die Planung und Durchführung von Cyber-Angriffen allerdings bei weitem keine staatliche Domäne mehr. Sogenannte Exploit Kits machen es quasi für jedermann möglich, Schwachstellen in den Sicherheitsmaßnahmen auszunutzen. Professionelle Software-Entwickler, denen Informationen über Schwachstellen in IT-Anwendungen bekannt sind, haben hier mitunter eine lukrative Einnahmequelle gefunden.

# Ablauf eines Ransomware-Angriffs



1 Opfer erhält ein E-Mail mit einem Link oder Attachment

2 Der Link oder das Attachment wird geöffnet

3 Ransomware wird von einer kompromittierten Website nachgeladen

4 Ransomware wird auf dem Rechner installiert und versucht sich im Netzwerk zu verbreiten

# Ablauf eines Ransomware-Angriffs

## Ablauf eines Ransomware-Angriffes

Meistens beginnt es mit einer klassischen Phishing E-Mail, die als Köder zum Download einer infizierten Datei dient. Häufig geschieht die Infizierung mit der Ransomware durch eine verseuchte PDF-, DOC- oder XLS-Datei.

Durch Öffnen der schädlichen Datei, hat der Täter die größte Hürde überwunden. Die Installation auf dem jeweiligen System erfolgt. Dabei bleibt zu erwähnen, dass die Installation unabhängig von der Aktivierung der Ransomware ablaufen kann.

Sobald die Ransomware aktiviert wird, beginnt der eigentliche Schaden: die Verschlüsselung beginnt. Dabei können einzelne Dateien auf einem System oder sogar mehrere Systeme innerhalb eines Unternehmensnetzwerkes verschlüsselt werden.

Von nun an hat der Benutzer keinen Zugriff mehr auf bestimmte Dateien oder seinen gesamten Rechner. Seine Admin-Rechte hat er komplett verloren. Die Kontrolle liegt in den Händen des Hackers. Sobald alles verschlüsselt ist, erscheint eine Benachrichtigung auf dem Bildschirm des Opfers. Hier fordert der Hacker ein Lösegeld (meistens in Bitcoins), um die Ransomware wieder zu entfernen.

Die Kopplung der Lösegeldforderung an eine Deadline ist ein probates Mittel der Cyberkriminellen, um den Druck auf die Betroffenen zu erhöhen.

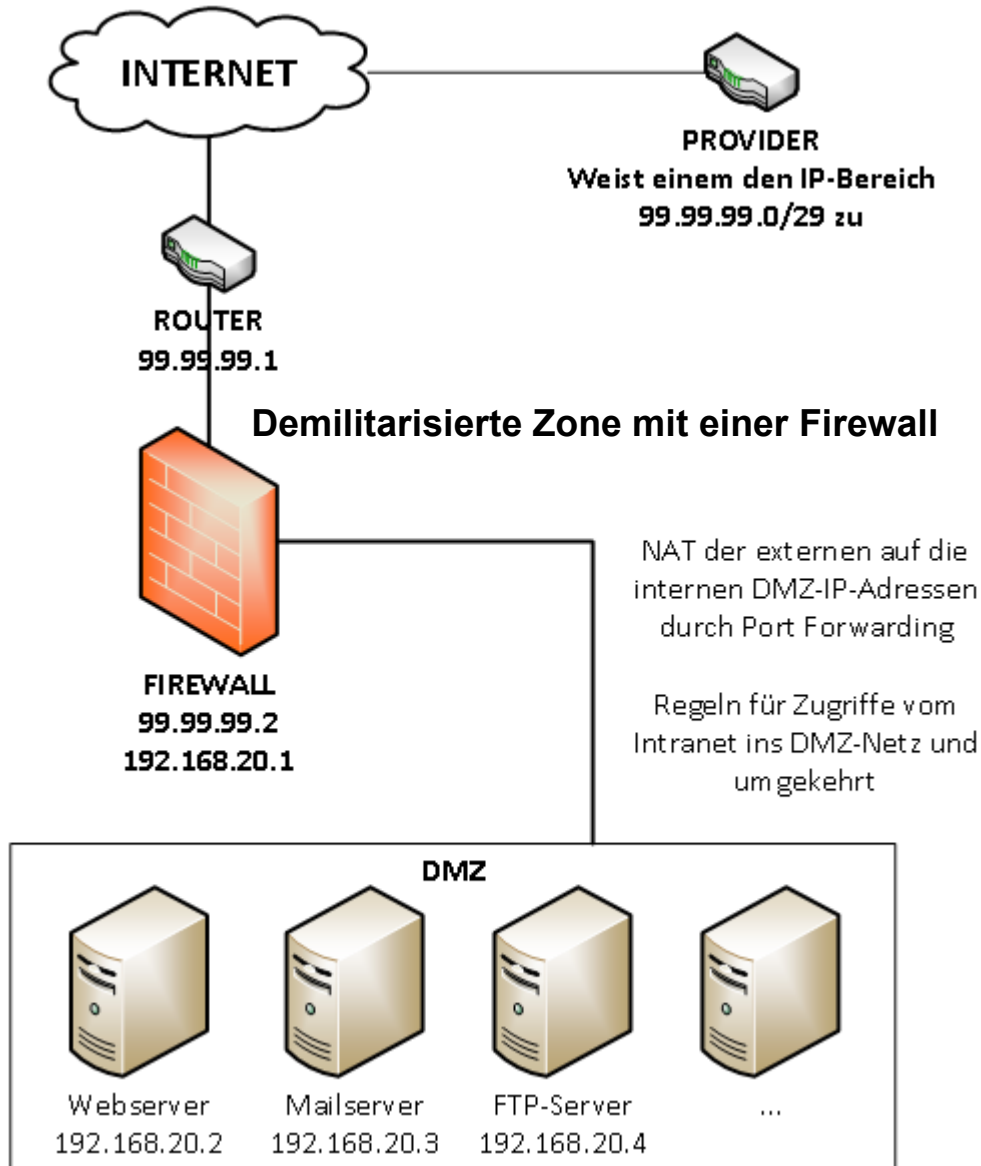
Sollten die Inhaber der Systeme bis zum Zeitpunkt der Deadline keine Zahlung getätigt haben, erhöht sich entweder die Lösegeldforderung oder es wird mit dem Löschvorgang von Daten begonnen.

Waren es 2020 noch 26 Prozent, zahlten 2021 schon 32 Prozent der Betroffenen Lösegeld, um wieder an ihre Daten zu kommen. Dabei geht es nicht um Kleckerbeträge, sondern um enorme Summen: Der Erhebung zufolge überwiesen deutsche Unternehmen Hackern im Schnitt 1 Million Euro, um den Schaden nach einem Angriff wieder zu beheben. Noch schlimmer ist, dass sich das Problem damit häufig nicht aus der Welt schaffen lässt. Vielmehr ist die Wahrscheinlichkeit, nach einer Lösegeldzahlung wieder auf alle Daten komplett zugreifen zu können, laut der Sophos-Studie eher gering. So erhielten Unternehmen, die Lösegeld bezahlt hatten, im Durchschnitt nur 65 Prozent ihrer Daten zurück. Gerade mal acht Prozent der Opfer konnten ihre Daten danach komplett entschlüsseln. Eine Garantie, dass die Daten wieder vollständig zur Verfügung stehen, gibt es demnach nicht.

2020 2021

26 %	32 %	zahlten Lösegeld, um Daten wieder zurückzubekommen
56 %	57 %	stellten Daten über Backups wieder her
12 %	8 %	stellten Daten mit anderen Mitteln wieder her
94 %	96 %	konnten Daten zumindest teilweise wiederherstellen

## Demilitarisierte Zone (DMZ) 1/4



Die ursprüngliche Wortbildung »demilitarized zone« ist ein militärischer Begriff. Um Irritationen zwischen zwei sich direkt gegenüberstehenden Armeen zu vermeiden, wurde ein neutraler Zwischenbereich festgelegt, eben diese demilitarisierte Zone.

Im technischen Sinne, bezeichnet eine Demilitarisierte Zone (DMZ, auch Demilitarized Zone, ist ein abgeschotteter Bereich) ein Computernetz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Server.

Die in der DMZ aufgestellten Systeme werden durch eine oder mehrere Firewalls gegen andere Netze (z. B. Internet, LAN) abgeschirmt. Durch diese Trennung kann der Zugriff auf öffentlich erreichbare Dienste gestattet und gleichzeitig das interne Netz (LAN) vor unberechtigten Zugriffen von außen geschützt werden.

Der Sinn besteht darin, auf möglichst sicherer Basis Dienste des Rechnerverbundes sowohl dem WAN (Internet) als auch dem LAN (Intranet) zur Verfügung zu stellen.

Ihre Schutzwirkung entfaltet eine DMZ durch die Isolation eines Systems gegenüber zwei oder mehr Netzen.

LAN und DMZ sollten über separate Switches (LAN <-> Switch <-> Firewall, DMZ <-> Switch <-> Firewall) angeschlossen werden, so dass bei Überwindung eines Switches nicht gleich beide Zonen kompromittiert werden.

## Demilitarisierte Zone (DMZ) 2/4

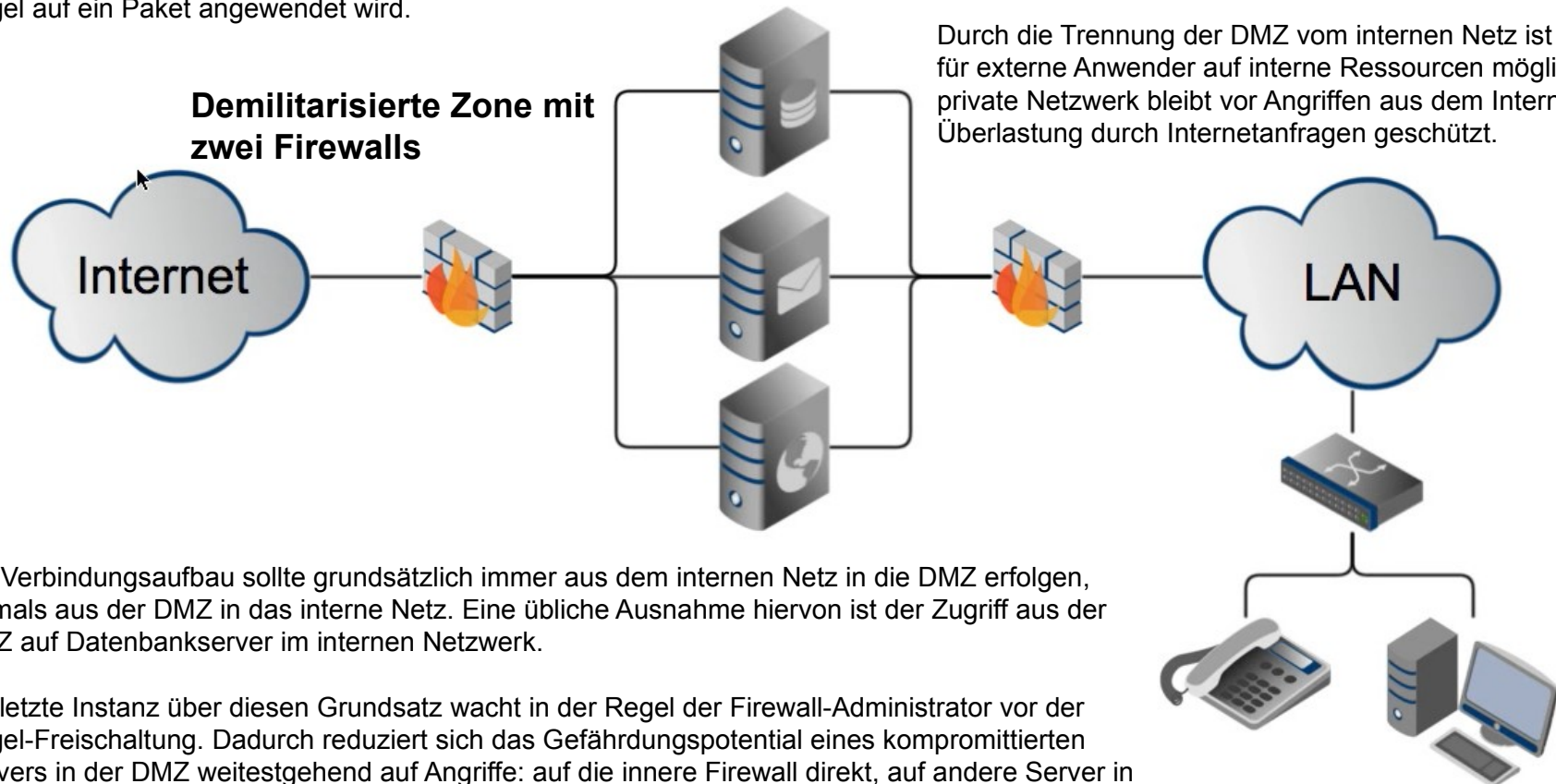
Eine Firewall muss mindestens 2 Netzbereiche voneinander trennen und die kontrollierte Weiterleitung (Anwendung von Regeln) von Paketen bewerkstelligen.

Die Firewall ist fest mit dem Internet verbunden. Bei der Erstellung der Firewall-Regel sollten die wichtigsten Regeln am Anfang stehen, da die erste zutreffende Regel auf ein Paket angewendet wird.

Die DMZ stellt eine Art Pufferzone dar, die die Netze durch strenge Kommunikationsregeln und Firewalls voneinander trennt.

In der DMZ befinden sich Server wie Webserver, Mailserver, Authentication-Server oder Anwendungs-Gateways. Nur diese sind für die Benutzer aus dem Internet erreichbar.

Durch die Trennung der DMZ vom internen Netz ist kein Zugriff für externe Anwender auf interne Ressourcen möglich. Das private Netzwerk bleibt vor Angriffen aus dem Internet oder vor Überlastung durch Internetanfragen geschützt.

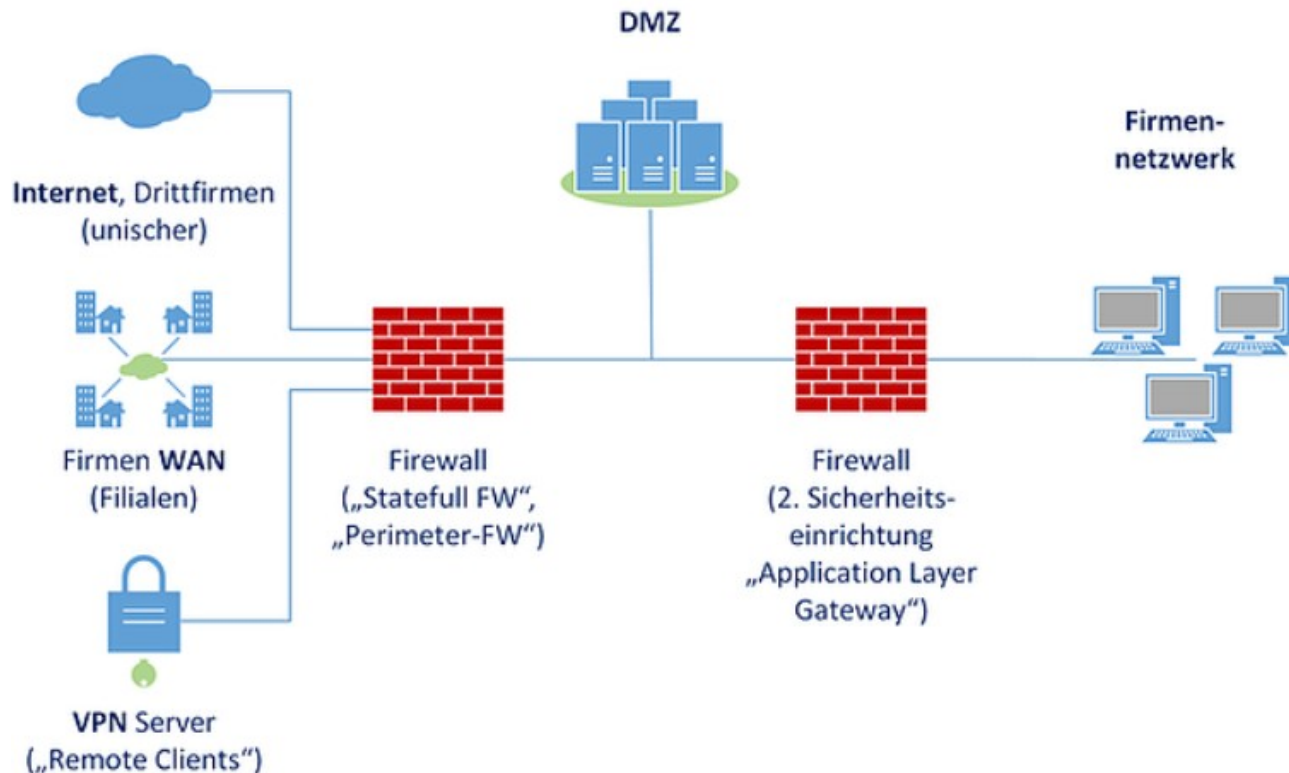


Ein Verbindungsaufbau sollte grundsätzlich immer aus dem internen Netz in die DMZ erfolgen, niemals aus der DMZ in das interne Netz. Eine übliche Ausnahme hiervon ist der Zugriff aus der DMZ auf Datenbankserver im internen Netzwerk.

Als letzte Instanz über diesen Grundsatz wacht in der Regel der Firewall-Administrator vor der Regel-Freischaltung. Dadurch reduziert sich das Gefährdungspotential eines kompromittierten Servers in der DMZ weitestgehend auf Angriffe: auf die innere Firewall direkt, auf andere Server in derselben DMZ, über Sicherheitslücken in Administrations-Werkzeugen wie Telnet oder SSH und auf Verbindungen, die regulär in die DMZ aufgebaut wurden.



## Demilitarisierte Zone (DMZ) 3/4



Eine Zusammenlegung von Firewalls kann je nach Unternehmensgröße üblich sein. Aus Security-Sicht muss dann ein potenzieller Angreifer nur ein Gerät überwinden, um im schlimmsten Fall Zugang zu allen Bereichen zu erlangen.

**Hinweis:** Mehrere unterschiedliche Sicherheitslinien sorgen hingegen für einen ungleich höheren IT-Schutz.

Bei sicherheitsbewussten Unternehmen werden die einzelnen DMZ-Firewalls durch Firewalls von zwei verschiedene Hersteller realisiert, die so genannte »multi vendor strategy«. Dadurch bleibt das Unternehmensnetzwerk geschützt, auch wenn bei einer Firewall eine Sicherheitslücke ausgenutzt wird oder vorhanden ist.

### Demilitarisierte Zone mit zwei Firewalls

Eine DMZ ist in der Praxis der Bereich zwischen einer Internet-Firewall und einer zweiten internen Firewall zum Schutz des nachfolgenden Unternehmensnetzwerkes.

Erst hinter einer zweiten internen Firewall (second line of defence), befindet sich dann das eigentliche Unternehmensnetzwerk.

Alternativ oder auch zusätzlich kann sich in der DMZ ein so genanntes ALG (Application Layer Gateway) befinden, welches den Netzwerktraffic komplett auffrennt und sich zu beiden Seiten hin als Kommunikationspartner ausgibt.

Zu schützende kritische interne Unternehmensserver befinden sich hingegen nicht in einer DMZ. Diese Server werden üblicherweise durch eine dritte Datacenter-Firewall vom Unternehmensnetzwerk getrennt, ein Zugriff von außen, wie es bei den DMZ Servern geregelt möglich ist, wird bei den internen Servern ausgeschlossen.

Dadurch entstehen eine oder mehrere zusätzliche Servernetze oder eine Datacenter-Umgebungen, aber eben keine neue »demilitarisierte Zone«.



## Demilitarisierte Zone (DMZ) 4/4

### Firewall-Regeln für die Verbindung zur Demilitarized Zone

Die Regeln der Firewall sorgen im Zusammenspiel mit der Demilitarized Zone für folgende Kommunikationsmöglichkeiten:

- Anwender aus dem Internet dürfen lediglich auf Server in der Demilitarized Zone und nicht auf Ressourcen des internen Netzwerks zugreifen.
- Anwender aus dem internen Netz kommunizieren in der Regel nicht direkt mit Ressourcen aus dem Internet. Sie greifen beispielsweise über einen Proxy-Server, der als Stellvertreter die Kommunikation in das Internet für sie abwickelt, auf externe Ressourcen zu.
- Pakete aus der Demilitarized Zone heraus, für die es keine korrespondierenden Eingangspakete gibt, werden von der Firewall in Richtung Internet und internes Netz verworfen.
- Es existieren Ausnahmen von diesen grundlegenden Kommunikationsregeln, um beispielsweise Anwendungsserver an interne Datenbanken anzubinden. Diese Ausnahmen konfiguriert der Administrator der Firewall.

### Die DMZ mit einer oder zwei Firewalls

Eine Demilitarized Zone lässt sich mit einer oder mit zwei Firewalls realisieren. Kommen zwei Firewalls zum Einsatz, befindet sich jeweils eine zwischen DMZ und internem Netz (innere Firewall) sowie zwischen DMZ und externem Netz (äußere Firewall).

Im Optimalfall handelt es sich um Firewalls von verschiedenen Herstellern. Dies verhindert, dass Sicherheitslücken es erlauben, beide Firewalls gleichzeitig zu überwinden.

Eine kostengünstigere Lösung stellt die Realisierung der Demilitarized Zone mit nur einer Firewall dar. Diese besitzt mindestens drei Netzwerkanschlüsse, mit denen das interne Netz, das externe Netz und die Demilitarized Zone verbunden sind. Die komplette Kommunikation überwacht in diesem Fall nur eine einzige Firewall.

### Der Exposed Host (Pseudo-DMZ) als günstige Alternative zu einer Demilitarized Zone

Günstige Router, wie sie beispielsweise für den privaten Internetzugang zum Einsatz kommen, werben oft mit einer DMZ-Unterstützung. In der Regel handelt es sich jedoch nicht um eine echte Demilitarized Zone, sondern um einen »Exposed Host«.

Durch die Konfiguration eines »Exposed Host« kann man die IP-Adresse eines Rechners im internen Netz angeben, an den alle Pakete aus dem Internet weitergeleitet werden, die nicht über die NAT-Tabelle einem anderen Empfänger zugeordnet werden können.

Damit wird der »Exposed Host«, neben den Nutzern, auch für potenzielle Angreifer aus dem Internet erreichbar. Eine Portweiterleitung der tatsächlich benutzten Ports ist dem - falls möglich - vorzuziehen.

**Fazit:** Ein »Exposed Host« ist nicht vom LAN separiert und bietet damit keine vergleichbare Schutzwirkung wie eine DMZ.

# SOC - Security Operations Center

## Was ist ein Security Operations Center (SOC)?

Die SOC, versteht sich als Zentrale für alle sicherheitsrelevanten Services im IT-Umfeld von Organisationen oder Unternehmen. Es schützt die IT-Infrastruktur und Daten vor internen und externen Gefahren.

Beim Security Operations Center handelt es sich um eine Sicherheitsleitstelle, die sich um den Schutz der IT-Infrastruktur eines Unternehmens oder einer Organisation kümmert. Um diese Aufgabe leisten zu können, integriert, überwacht und analysiert das SOC alle sicherheitsrelevanten Systeme wie Unternehmensnetzwerke, Server, Arbeitsplatzrechner oder Internetservices. Unter anderem werden die Log-Dateien der einzelnen Systeme gesammelt, analysiert und nach Auffälligkeiten untersucht. Neben der Analyse der verschiedenen Systeme und Log-Dateien sind das Alarmieren und Ergreifen von Maßnahmen zum Schutz von Daten und Anwendungen zentrale Aufgabe des Security Operations Centers.

## Aufbau eines SOC

Meist ist das SOC als eine Art zentraler Kommandostand aufgebaut, an dem alle Mitarbeiter an einem Ort versammelt sind. Dort zeigen Monitore Informationen über den aktuellen Zustand der IT, die Bedrohungslage und über die eventuell ergriffenen Maßnahmen. Die Maßnahmen können sowohl auf physikalischer Ebene als auch auf Anwendungsebene greifen. Physikalische Sicherheitsmaßnahmen lassen sich beispielsweise auf Firewalls oder Intrusion Detection Systemen realisieren und sorgen für den direkte Schutz des Unternehmensnetzwerks. Schutzmaßnahmen auf Anwendungsebene sind spezielle Lösungen zur Autorisierung und Authentifizierung von Anwendern oder Antimalware-Software zur Erkennung von Schadprogrammen.

Das SOC arbeitet zum einen proaktiv und versucht Schwachstellen der IT-Infrastruktur frühzeitig zu erkennen und zu beseitigen und zum

anderen reaktiv über direkte Schutzmaßnahmen bei aktuellen Angriffen wie DoS-Attacken. Das Management des Unternehmens oder der Organisation wird in regelmäßigen Abständen durch Reports über die Arbeit des SOC und die Sicherheit der IT-Systeme informiert.

## Zentrale Services des SOC

Um für einen wirkungsvollen Schutz der Daten und IT-Systeme zu sorgen, leistet das Security Operations Center folgende zentralen Services:

- Proaktive Überwachung der IT-Systeme und laufende Analysen zur aktuellen Bedrohungslage
  - Erkennen von Schwachstellen der IT-Sicherheit und deren Beseitigung
  - Zentrales Sicherheitsmanagement für die unterschiedlichen Devices
  - Alarmierung bei erkannten Angriffen und Bedrohungen
  - Direkte Abwehrmaßnahmen zur Schadensbegrenzung von Cyber-Attacken
  - Durchführung von Security-Assessments
- Hinweis:** Unter einem Security-Assessment versteht man die systematische Erfassung und Bewertung von Zuständen (IT-Sicherheitslücken und -risiken).
- Technische Unterstützung bei allen sicherheitsrelevanten Fragestellungen
  - Reporting zur Arbeit des Security Operations Centers und über alle sicherheitsrelevanten Systeme

Durch ein SOC können Cyber-Attacken schnell erkannt, analysiert und abgewehrt werden, bevor größere negative Auswirkungen entstehen können. Durch die dynamische Anpassung der Security-Maßnahmen des SOC an die aktuelle Bedrohungslage sind die zu schützenden Systeme zu jeder Zeit optimal geschützt.

# SIEM - Security Information and Event Management 1/3

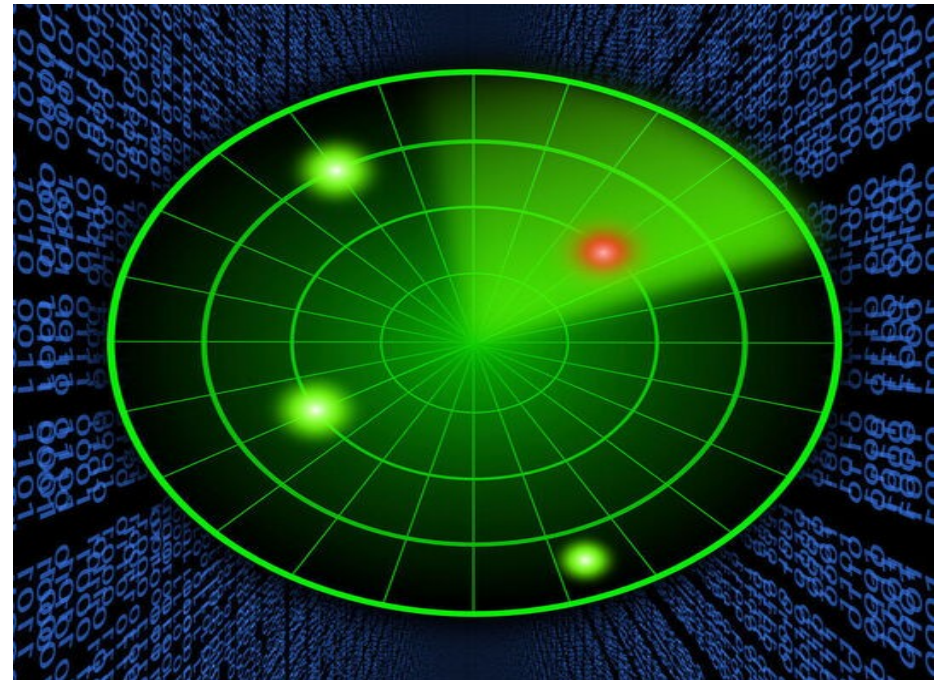
## Was ist ein Security Information and Event Management (SIEM)?

Das Security Information and Event Management (SIEM) ermöglicht einen ganzheitlichen Blick auf die IT-Sicherheit, indem Meldungen und Logfiles verschiedener Systeme gesammelt und ausgewertet werden. Verdächtige Ereignisse oder gefährliche Trends lassen sich in Echtzeit erkennen. Bei SIEM handelt sich um ein softwarebasiertes Technologiekonzept aus dem Bereich des Sicherheits-Managements, mit dem ein ganzheitlicher Blick auf die IT-Sicherheit möglich wird. SIEM stellt eine Kombination aus Security Information Management (SIM) und Security Event Management (SEM) dar. Auf verschiedene Geräte (Server) und Netzkomponenten werden Sensoren installiert. Die gesammelten Daten werden an einen SIEM-Rechner geschickt und dort ausgewertet wurden. Durch das Sammeln, Korrelieren und Auswerten von Meldungen, Alarmen und Logfiles können Anwendungen und Security-Systeme (SIEM, SOAR, SOC) in Echtzeit Angriffe, außergewöhnliche Muster oder gefährliche Trends sichtbar machen. Auf Basis der gewonnenen Erkenntnisse werden Unternehmen oder Organisationen in die Lage versetzt schnell und präzise auf Bedrohungen reagieren. Das Security Information and Event Management nutzt Verfahren des maschinellen Lernens und der Künstlichen Intelligenz (KI). SIEM-Lösungen sind auch als Services aus der Cloud verfügbar.

## Funktionsprinzip und Arbeitsweise eines SIEM

Die Grundidee eines SIEM ist alle für die IT-Sicherheit relevanten Daten an einer zentralen Stelle zu sammeln und durch Analysen Muster und Trends zu erkennen, die auf gefährliche Aktivitäten schließen lassen. Das Sammeln und die Interpretation der Daten erfolgen in Echtzeit. Sämtliche Informationen sind manipulations- und revisionssicher gespeichert. Typische Quellen für das SIEM sind Firewalls, Server, Router, IDS, IPS und Anwendungen. Das Security Information and Event Management sorgt für die Normalisierung und Strukturierung aller gesammelten Daten. Durch das Korrelieren der Datensätze ist es beispielsweise möglich, Einbruchversuche

durch fehlerhafte Anmeldeversuche und/oder unerlaubte Zugriffe auf Systeme zu erkennen. Für das Sammeln der Daten sind in der Regel Software-Agenten (Sensoren) zuständig. Diese leiten die Informationen an eine zentrale Management-Station weiter. Die zentrale Station ist für die Speicherung, Normalisierung, Strukturierung und Auswertung der Daten zuständig. Die Analysen verwenden Regeln, Korrelations-Modelle, maschinelles Lernen und Künstliche Intelligenz, um Beziehungen zwischen den Einträgen herzustellen und Auffälligkeiten zu identifizieren. Einige Systeme führen eine Vorverarbeitung der Daten in den Software-Agenten durch, um die Menge an zu übertragenden Informationen zu reduzieren.



Ein SIEM-System ermöglicht eine ganzheitliche Sicht auf die IT-Sicherheit durch sammeln und auswerten von Logfiles und Meldungen.

# SIEM - Security Information and Event Management 2/3

## Die Ziele des Security Information and Event Managements

Das SIEM bietet einen Überblick über sicherheitsrelevante Ereignisse in IT-Umgebungen und hilft, gesetzliche Vorgaben oder Richtlinien und Compliance-Regularien der IT-Sicherheit zu erfüllen. Sowohl die Echtzeit-Reaktion auf Bedrohungen als auch der nachträgliche Nachweis von Sicherheitsereignissen sind möglich. Automatisierte Berichte und gezielte Alarmierungen erlauben dem IT-Sicherheitspersonal angemessen auf die unterschiedlichen Bedrohungen zu reagieren.

## Vorteile durch den Einsatz eines SIEM

Durch den Einsatz des Security Information and Event Managements ergeben sich zahlreiche Vorteile. Zu diesen Vorteilen zählen:

- schnelle und zuverlässige Erkennung von Bedrohungen
- schnelle und angemessene Reaktion auf sicherheitsrelevante Ereignisse
- Einhaltung von gesetzlichen Vorgaben und Compliance-Regularien
- Einsparung von Personal im IT-Security-Umfeld durch Automatisierung
- nachträglicher Nachweis von Sicherheitsereignissen
- manipulations- und revisionssichere Speicherung aller sicherheitsrelevanten Ereignisse

## SIEM Use Cases – Was ist das?

Um verschiedene Arten von Cyber-Angriffen im Unternehmen zeitnah zu erkennen, nutzt man SIEM Use Cases. Damit man Cyber-Angriffe erkennen kann, muss man wissen was in der IT-Infrastruktur überhaupt passiert. Hierzu ist es wichtig zu wissen, welche Netzwerkkomponenten (Router, Gateways, Switches, ...) sich im Firmennetzwerk befinden. Wenn man weiß, welche IT-Geräte sich im Netzwerk befinden, kann man auch leichter herausfinden, welche IT-Geräte möglicherweise entbehrlich sind. Ein Gerät, dass nicht installiert wurde, kann auch kein Sicherheitsrisiko mehr darstellen.

Unter einem SIEM Use Case versteht man eine bestimmtes Szenario, welches mit einem SIEM beobachtet wird. Das Szenario beschreibt hierbei ein ungewöhnliches oder auffälliges Verhalten, welches näher analysiert werden sollte, sobald es auftritt (Erzeugung eines Alarms). Ein Beispiel wäre das Hinzufügen von neuen Benutzern in eine Admin-Gruppe oder die Verwendung eines Ports, der nicht durch einen Service benutzt wird. Solche Aktivitäten sind ungewöhnlich und sollte i.d.R. nur sehr selten auftreten. Wenn sie dennoch vorkommen, so muss geprüft werden, ob eine legitime Handlung vorliegt oder ob Hinweise auf einen Cyber-Angriff vorliegen.

## Welche SIEM Use Cases werden benötigt?

SIEM Use Cases kann man sich als eine Art von Datenbank vorstellen, in denen sich Anwendungen oder Algorithmen befinden, die für ein bestimmtes Szenario optimiert wurden. SIEM Use Case ist also ein bestimmtes Szenario, welches mit SIEM beobachtet wird.

Alle bekannten SIEM Use Cases zu implementieren macht keinen Sinn, bedingt durch fehlende Ressourcen und den unnötigen Arbeitsaufwand. Man muss also einen Weg finden, für die Auswahl der wichtigsten SIEM Use Cases.

- Eine Möglichkeit ist risikobasiert vorzugehen. Das IT-Risikomanagement analysiert die Angriffsvektoren, denen ein Unternehmen ausgesetzt ist. Aus dieser Analyse ergeben sich Gefahren und das Schadenspotenzial, welches beim Eintreten der Gefahren entsteht. Auf Basis der identifizierten Risiken können nun SIEM Use Cases ausgewählt werden, die zur Reduktion von Risiko beitragen.
- Nun hat nicht jedes Unternehmen ein IT-Risikomanagement, welches eindeutige Informationen liefern kann. In diesem Fall ist man auf die Verwendung von Best-Practices und Meinungen von Experten angewiesen.

# SIEM - Security Information and Event Management 3/3

Durch die Entscheidung für eines der zwei vorgenannten Arten, lassen sich aus der großen Menge an SIEM Use Cases die SIEM Use Cases auswählen, die den größten Nutzen bieten und damit auch wirtschaftlich vertretbar sind.

Es muss immer klar sein, wann eine Überwachung durchgeführt wird und welche Personen unter welchen Voraussetzungen dazu berechtigt sind.

## Wie geht es jetzt weiter?

Nach dem die passenden SIEM Use Cases implementiert wurden, müssen noch eine Reihe von Einstellungen vorgenommen werden. Dies ist notwendig, um die Anzahl von vermeidbaren Fehlalarme zu reduzieren. Fehlalarme erzeugen immer einen hohen Arbeitsaufwand, da die Security Analysten vor der Analyse eines Alarms nie wissen, ob es sich um einen echten Sicherheitsvorfall handelt oder nur um einen Fehlalarm. Außerdem erhöhen Fehlalarme das Sicherheitsrisiko. Durch eine große Anzahl von Fehlalarmen steigt auch immer die Wahrscheinlichkeit, dass echte Sicherheitsvorfälle nicht oder erst verspätet bearbeitet werden. Daher ist es wichtig die SIEM Use Cases ausreichend zu testen und kontinuierlich zu verbessern, um die Anzahl der Fehlalarme klein zu halten.

## Wie reagiert man auf Alarme?

Hier kommt das Security Incident Management und Incident Response ins Spiel. Das Security Incident Management regelt, wie man mit Sicherheitsvorfällen umgehen sollte. Es beschreibt die Abläufe, von der Erkennung eines Sicherheitsvorfalles bis zu dessen vollständigen Beseitigung. Es regelt außerdem, welche Personen die entsprechenden Tätigkeiten durchführen müssen und welche Personen mit welchen Informationen versorgt werden müssen.

## Betriebsrat und Datenschutz

SIEM Use Cases kann auch einen starken Einfluss auf das Betriebsklima in einem Unternehmen haben. Da SIEM nicht nur für die Erkennung von Cyber-Angriffen verwendet werden kann, sondern auch für die Überwachung von Mitarbeitern. Daher ist es wichtig, frühzeitig den Betriebsrat und den Datenschutzverantwortlichen bei der Planung und Umsetzung der SIEM Use Cases mit einzubinden.



# SOAR - Security Orchestration Automation and Response

SOAR (Security Orchestration, Automation and Response) ist eine Kombination aus kompatiblen Programmen, die es einem Unternehmen ermöglicht, aus unterschiedlichsten Quellen Daten über Sicherheitsbedrohungen einzusammeln. Zudem wird mit SOAR eine automatische Reaktion ohne menschliche Eingriffe auf bestimmte Sicherheitsereignisse möglich. Der Einsatz von SOAR soll Unternehmen dabei unterstützen, die Effizienz aller Sicherheitsoperationen zu verbessern. Der von Gartner geprägte Begriff lässt sich auf Produkte und Dienstleistungen anwenden, die dabei helfen, Vorfallsreaktionen zu priorisieren, zu standardisieren und zu automatisieren.

Nach Angaben von Gartner sind dies die drei wichtigsten Fähigkeiten von SOAR-Lösungen:

## Bedrohungs- und Schwachstellenmanagement

Die Lösungen unterstützen IT-Teams bei der Behebung von Schwachstellen. Darüber hinaus bieten sie standardisierte Workflow-, Berichts- und Kollaborationsfunktionen.

## Reaktion auf Sicherheitsvorfälle

Diese Technologien unterstützen IT-Abteilungen bei der Planung, Ablauforganisation, der Nachverfolgung und der Koordination der jeweiligen Reaktion auf einen Sicherheitsvorfall.

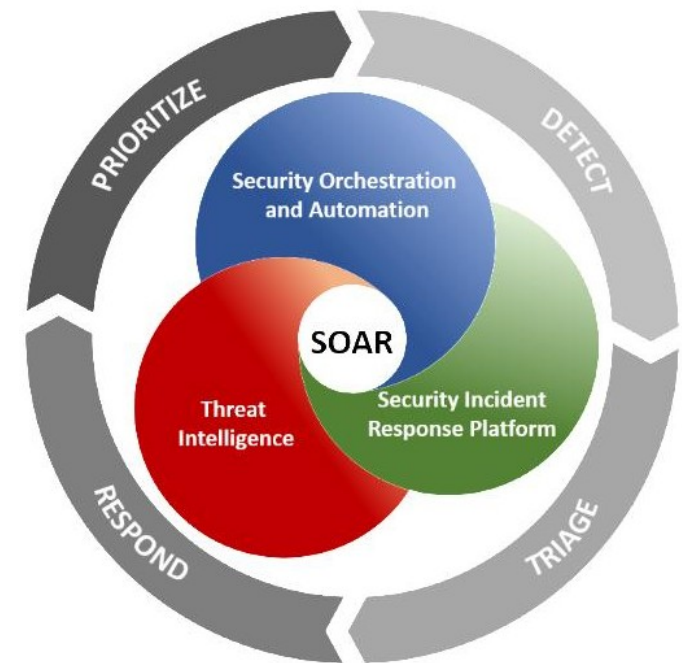
## Automatisierung von Sicherheitsoperationen

Diese Technologien unterstützen die Automatisierung und Orchestrierung von Abläufen, Prozessen, Richtlinienumsetzung sowie dem Berichtswesen.

Sowohl SIEM-Lösungen als auch SOAR-Produkte aggregieren Daten aus mehreren Quellen. SOAR -Dienste integrieren sich allerdings in eine breitere Palette interner und externer Anwendungen. Derzeit nutzen viele Unternehmen SOAR-Produkte, um die eigene SIEM-Software zu erweitern. Für die Zukunft ist zu erwarten, dass der Markt für die beiden Produktlinien zusammenwachsen wird. Insbesondere wenn SIEM-Anbieter beginnen ihre Lösungen, um SOAR-Funktionen zu erweitern.

**SIEM:** Als SIEM (Security Information and Event Management) bezeichnet man ein einzelnes Security-Management-System, das volle Sichtbarkeit und Transparenz zu Aktivitäten innerhalb Ihres Netzwerks bietet - dies versetzt Administratoren in die Lage in Echtzeit auf Bedrohungen zu reagieren.

**Gartner:** Gartner ist ein Anbieter, der Marktforschungsergebnisse und Analysen über die Entwicklungen in der IT anbietet. Das Unternehmen hat seinen Hauptsitz in Stamford, USA.



# Cisco Meraki – Netzwerk 1/3

## Meraki-Netzwerk

Meraki wurde 2006 gegründet und 2012 von Cisco übernommen. Seitdem hat sich Meraki zu einem Branchenführer entwickelt. Inzwischen sind weltweit fast 600.000 Kunden und 9,1 Millionen Netzwerkgeräte online (Stand: 2021).

Cisco Meraki ist eine vollständig über die Cloud verwaltete Netzwerklösung. Mit Hilfe von Cisco Meraki können Unternehmensnetzwerke drastisch vereinfacht werden.

Mit Meraki vereinfacht Cisco die Einrichtung, Verwaltung, Kontrolle und Erweiterung von Unternehmensnetzwerken durch eine einfache, zentrale Administration aller Komponenten über eine graphische Oberfläche. Dieses Dashboard umfasst neben Konfigurations- auch umfangreiche Monitoring-Funktionen.

Viele Aufgaben wie Upgrades, das Aufspielen von Patches, die Sicherung von Daten und Konfiguration erfolgen dabei weitgehend automatisch über die Cloud.

Cisco Meraki eignet sich besonders für Firmen mit verteilten Architekturen wie Hotelketten oder Unternehmen mit vielen Filialen und Standorten, die dieselbe Konfiguration mehrfach benötigen und diese einfach replizieren wollen.

**Hinweis:** Bei Verwendung von IT-Security-Systemen von US-Herstellern, werden Industrie-Netzwerke im Prinzip direkt mit Backdoors bestückt. Der »PATRIOT Act« schreibt den Zugriff durch Geheimdienste auf Systeme von amerikanischen IT-Security- und System-Herstellern vor. Der »PATRIOT Act« ist ein US-amerikanisches Bundesgesetz, das am 26. Oktober 2001 vom Kongress im Zuge des Krieges gegen den Terrorismus verabschiedet wurde. Es war eine direkte Reaktion auf die Terroranschläge am 11. September 2001.

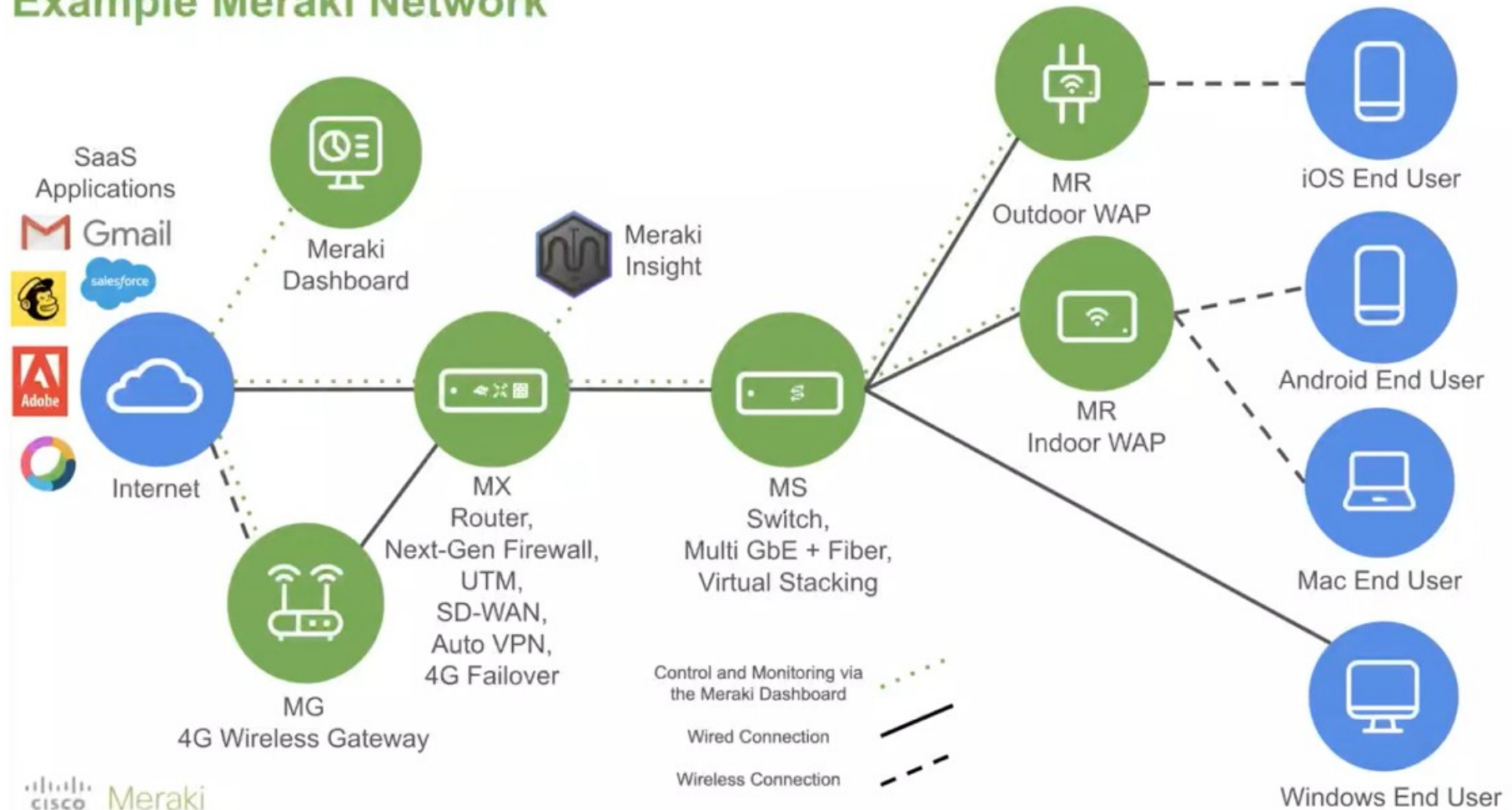
## Funktionsumfang

- Die Rechenzentren (Cloud) in Europa für die Verwaltung des Meraki-Netzwerkes befinden sich in Frankfurt/Main und München. In Dublin befindet sich noch ein weiteres Rechenzentrum für Backups.
- Der Hauptsitz von Cisco-Meraki befindet sich in San Francisco (USA).
- Cisco-Meraki betont das keine Benutzerdaten durch die Cloud geleitet werden.
- Die Kunden haben über ein geöffnetes Dashboard jederzeit Einblick in ihr eigenes Meraki-Netzwerk.
- Automatische Firmware und Security Updates (können auch benutzerdefiniert durchgeführt werden)
- Zusätzliche Geräte (auch mobile Geräte) können in das Meraki-Netzwerk integriert werden.
- Es gibt für die Kunden verschiedene Lizenzmodelle (Enterprise-Lizenz, Advanced Security-Lizenz) für die Dauer von 1, 3, 5, 7 oder 10 Jahre. **Hinweis:** Für die HA MX-Appliance ist keine Lizenz erforderlich.
- Mitarbeiter-Ortung, Überwachung und Blockierung (z.B. Internet) über das Dashboard ist möglich. Über die Gruppenrichtlinie (Einrichtung über das Dashboard) können die Zugriffsrechte der Mitarbeiter eingeschränkt werden.
- Über das Dashboard können auch Applikationen auf die Arbeitsrechner verteilt werden.
- Die Netzwerk-Topologie wird durch Meraki automatisch erstellt und aktualisiert.
- Kamera-Überwachung (Live und Aufzeichnungsmaterial, Meraki-Kameras haben einen eigenen Speicher) mit den Meraki-Überwachungskameras sind über das Dashboard möglich. Die Kameras können einzelne Personen zählen. Die Abrufenlaubnis der Daten erfolgt vom Dashboard aus, über ein Abrufen eines Zertifikats von der Kamera.

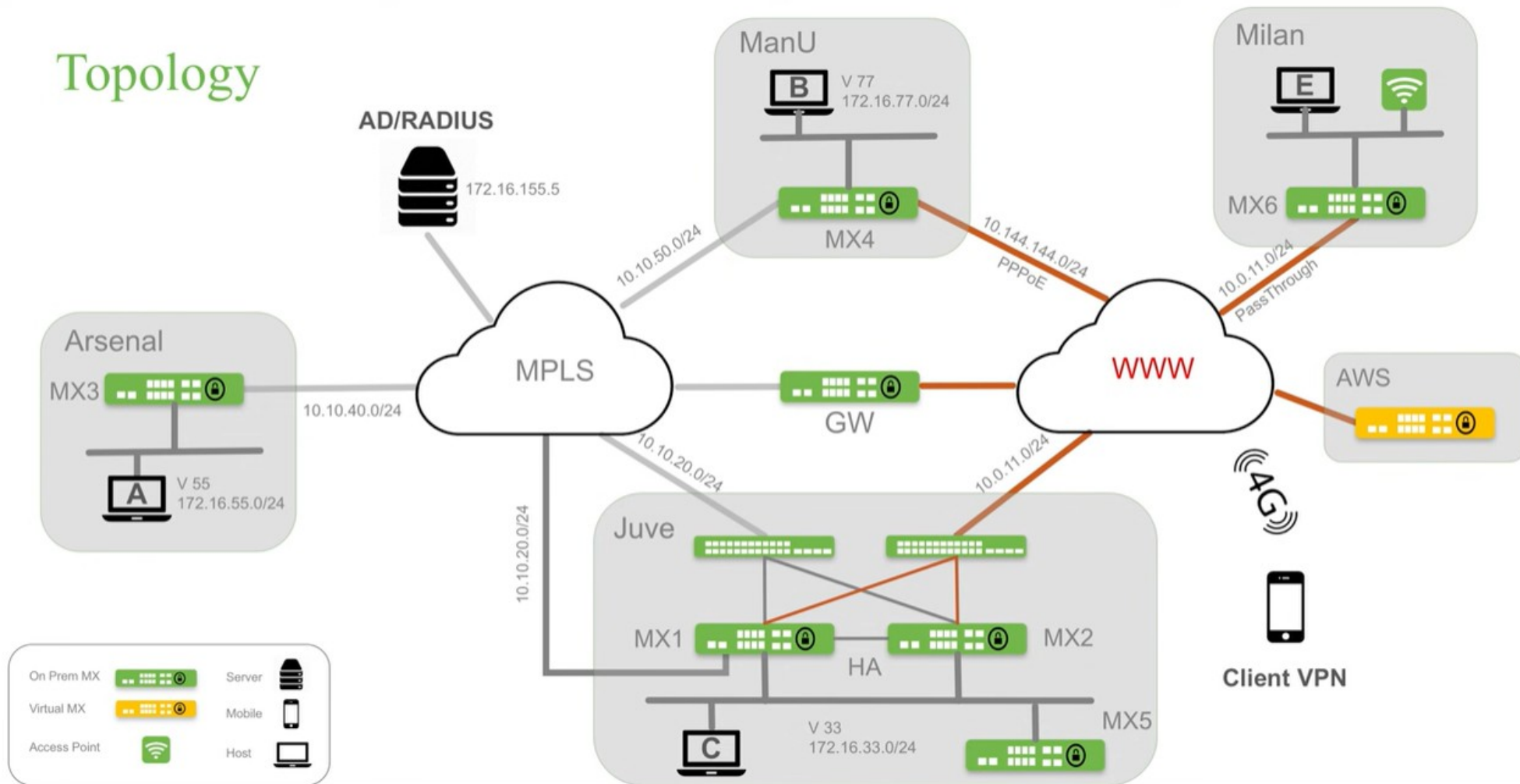
## Cisco Meraki – Netzwerk 2/3

**Hinweis:** Als Mitglied eines Meraki-Netzwerkes kann man sich bei Eingabe von <http://my.meraki.net/> einige Grunddaten (IP-Adresse, MAC-Adresse, Produktname, Netzwerkname) anschauen. Weiterhin hat man von dort Zugang zur Konfiguration und zum Dashboard. Zusätzlich kann man einen browser-basierten Geschwindigkeitstest zur Security Appliance starten. Bei einer vorhandenen Zugangsberechtigung bekommt man von dort auch Zugang zur Cloud.

### Example Meraki Network



## Topology



# Firewall 1/2

## Was ist eine Firewall?

Heute gibt es fünf Arten von Netzwerk-Firewalls: Paketfilter-Firewalls, Verbindungs-Gateways (Circuit Level Gateways), Stateful Inspection-Firewalls, Anwendungs- oder Proxy-Firewalls sowie Firewalls der nächsten Generation. Sie unterscheiden sich in der Art und Weise, wie sie den Datenverkehr bewerten und die Netzwerkleistung beeinflussen.

Eine Firewall muss mindestens 2 Netzbereiche voneinander trennen und die kontrollierte Weiterleitung (Anwendung von Regeln) von Paketen bewerkstelligen. Die Firewall sollte im Idealfall Open-Source-Software und aktuell wie in Zukunft anpassbar sein. Proprietäre Software ist keine verlässliche Software. Ein Firewall-Rechner sollte nur für die Aufgaben einer Firewall eingerichtet werden, d.h. zusätzliche Aufgaben haben auf diesen Rechner nichts zu suchen. Die Firewall ist fest mit dem Internet verbunden. Bei der Erstellung der Firewall-Regel sollten die wichtigsten Regeln am Anfang stehen, da die erste zutreffende Regel auf ein Paket angewendet wird.



## Was macht eine Firewall?

- Schützt ein Netzwerk vor unbefugten Zugriff
- Steuert eingehende und ausgehende Datenverbindungen
- Steuert Datenverkehr nach Regeln
- Verhindert, dass Anwendungsprogramme Zugriff ins Internet bekommen
- Regelt allgemeinen Datenverkehr

## Was sind Firewall-Regeln?

- Firewall-Regeln bestimmen, welche Verbindungen in ein Netzwerk oder aus einem Netzwerk heraus zugelassen oder blockiert werden
- Firewall-Regeln regeln den Netzverkehr
- Firewall-Regeln haben einen unterschiedlichen Aufbau, je nach verwendeter Applikation

## Welche Arten von Firewalls gibt es?

1. SPI – Stateful Inspection Firewall (statusbezogene Untersuchung)
  - untersucht Pakete nach ihren Status (Quell-IP, Ziel-IP, Quell-Port, Ziel-Port, Sequenznummer)
  - Pakete die als Antwort aus Anfragen des LANs zurückkommen, werden automatisch zugelassen
  - geringer Administrationsaufwand, aber es besteht die Gefahr der Einschleusung von gefälschten Paketen
2. Packetfilter-Firewall
  - Ein Packetfilter-Firewall verhält sich etwas vereinfacht dargestellt wie ein IP-Router, welcher alle ankommenden Pakete durch ein vorgegebenes Regelwerk filtert und erlaubte Pakete aufgrund seiner (normalerweise statisch) konfigurierten Routen an den Empfänger weiterleitet.



## Firewall 2/2

### 3. Application Layer Gateway, Application Level Gateway oder Application Level Proxy (Anwendungs- oder Proxy-Firewalls )

- tauscht Quelladressen der Clients gegen die des Proxy-Servers aus (verschleiern der LAN-Rechner)
- Pufferspeicherung, Zwischenspeicherung (Caching) von Webseiten
- Benutzersteuerung über Gruppenrichtlinien (GPO, Group Policy)
- erlaubt Anwendungen den Zugang zum Internet oder verhindert diese Anfragen (Filterung von Webseiten)

### 4. Verbindungs-Gateways (Circuit Level Gateways)

- Verbindungs-Gateways auf Leitungsebene überwachen die TCP-Daten zwischen Paketen im gesamten Netzwerk, um festzustellen, ob die gestartete Sitzung legitim ist und das vernetzte System als vertrauenswürdig angesehen werden kann. Der Datenverkehr wird auf der Grundlage von Richtlinien durchgelassen oder abgelehnt. Diese Gateways geben keine Daten über das zu inspizierende Netzwerk preis, können aber die Paketinhalte selbst nicht kontrollieren. Sie können daher leicht böartigen Datenverkehr übersehen.

### 5. Next-Generation Firewall

- Firewalls der nächsten Generation (Next-Generation Firewalls, NGFW) stellen die modernste und breiteste Klasse von Sicherheits-Gateways dar. Diese Firewalls kombinieren die traditionelle Paketfilterung und die Stateful-Inspection-Funktionen mit anspruchsvolleren Funktionen wie Deep Packet Inspection (DPI) und Inspektion von verschlüsseltem Traffic. Firewalls der nächsten Generation könnten auch andere Funktionalitäten außerhalb der Grenzen herkömmlicher Gateway-Systeme hinzufügen, wie Quality of Service (QoS), Bandbreitenmanagement und Identitätsmanagement.

### Welche Werkzeuge gibt es?

Folgende Werkzeuge dienen üblicherweise der Verteidigung am Netzwerkperimeter:

- Firewalls
- Überwachte Sub-Netze (Screened Subnets)
- Systeme zur Aufspürung von Eindringlingen (Intrusion Detection Systeme, IDS)
- Systeme zur Prävention unbefugten Eindringens (Intrusion Prevention Systeme, IPS)
- Web-Filter
- Border-Router, um Datenverkehr zu lenken

**Hinweis:** Perimeter ist die Stelle, wo ein Raum (lokale und öffentliche Netzwerke) endet und ein neuer anfängt.

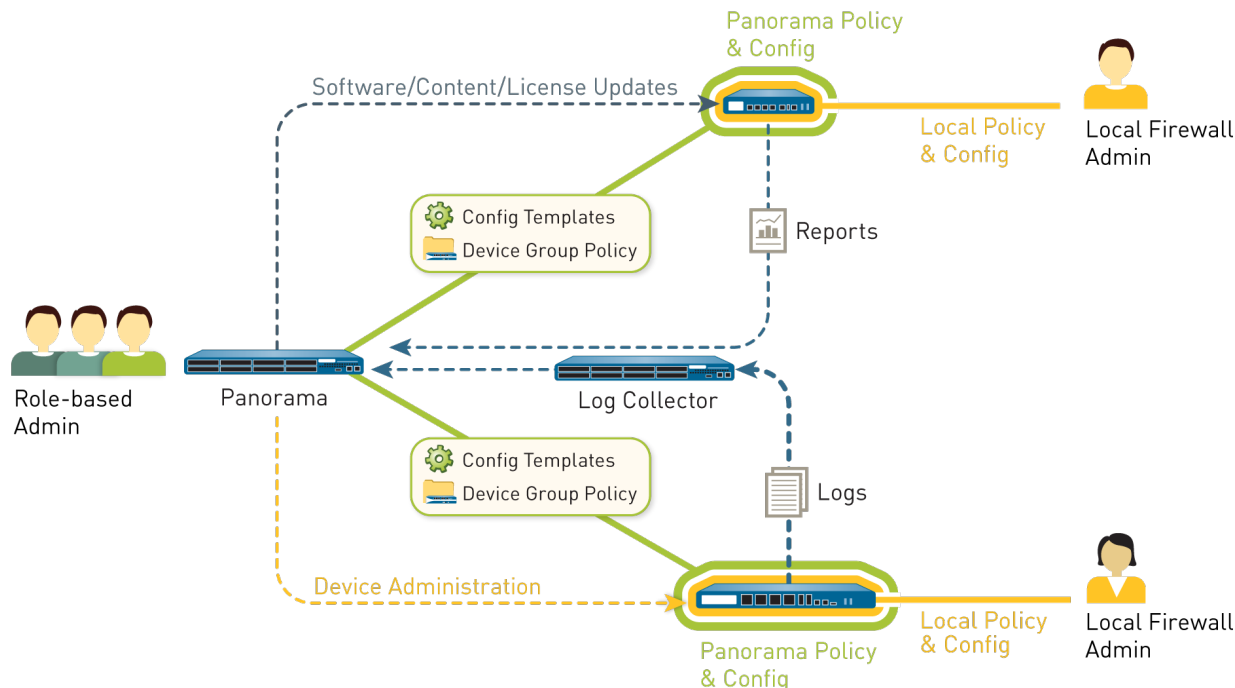
Nach Möglichkeit sollen diese Hindernisse (Grenze zwischen zwei Netzwerke) undurchdringlich sein. Praktisch ist dies jedoch nie der Fall, da sich die Angreifer an die Verteidigungsmaßnahmen anpassen. Deshalb gilt der Netzwerkperimeter nur als die erste Verteidigungslinie.

# Palo Alto Networks - Next-Generation Firewall

Palo Alto Networks, Inc. ist ein amerikanisches multinationales IT-Sicherheitsunternehmen mit Hauptsitz in Santa Clara, Kalifornien. Palo Alto Networks™ entwickelt, produziert und vermarktet leistungsstarke Next Generation Firewalls, welche Unternehmen und Organisationen jeder Größe zuverlässig vor Angriffen auf allen Netzwerkebenen schützen. Anders als klassische Stateful Inspection Firewalls, die lediglich Ports und IP-Adressen überwachen, sind die Plattformen von Palo Alto Networks in der Lage, sowohl Applikationen als auch Anwender zu kontrollieren. Mit Palo Alto Networks wurde die Idee des Perimeterschutzes völlig neu gedacht.

- Identifikation von Applikationen unabhängig von Port, Protokoll, Verschleierungsmethoden oder Verschlüsselung
- Identifikation von Benutzern unabhängig von der IP-Adresse
- Granulare Sicht und Kontrolle über Anwendungszugriffe und Funktionen
- Echtzeitschutz gegen in Anwendungen versteckte Bedrohungen
- Multi-Gigabit-Durchsatz, Inline Integration, minimale Latenzerhöhung

Palo Alto Networks verwendet drei einzigartige Technologien, um Applikationen exakt zu identifizieren, sie einem Benutzer zuzuweisen und den Traffic nach Content Policy-Verstößen zu kontrollieren: App-ID, User-ID und Content-ID.



Die Palette an Firewall-Modellen ist strukturiert nach Performance, Durchsatz, Unternehmensstrukturen und benötigten Funktionalitäten. Welches Modell als Physical Appliance (PA) oder Virtual Machine (VM) auch zum Einsatz kommt: die leistungsfähigen Next-Generation Firewalls ermöglichen immer maximale Transparenz und Kontrolle über Anwendungen, Benutzer und Inhalte.



# HP Wolf Security

Cyberkriminelle arbeiten auch nach Feierabend – also muss es ihre Sicherheitslösung auch (HP-Slogan). Cyberkriminelle haben es auf die Endpunkte in der sich weiter entwickelnden Arbeitsumgebung abgesehen. HP Wolf Security bietet den Mitarbeitern und Unternehmen rund um die Uhr hardwaregestützten Schutz. HP Wolf Security bleibt wachsam, damit man weiterarbeiten kann - immer und überall. Auf HP Elite PCs, Workstations und ausgewählten Pro PCs sind eine Reihe von hardwaregestützten Sicherheitsfunktionen vorinstalliert, die es den Mitarbeitern und Teams ermöglicht, von überall aus sicherer zu arbeiten, ohne Angst vor modernen Bedrohungen haben zu müssen.

## HP Wolf Security: Maximaler Schutz dank integriertem Security-Portfolio

Mit der Verlagerung des Lebens in die digitale Welt – Home-Office, Online-Shopping, Unterricht von zu Hause oder der rasanten Zunahme von Online-Freizeitbeschäftigungen haben viele Menschen unbemerkt ihre eigenen vier Wände mehr denn je für die neue Form von Angreifern geöffnet. Denn auch Cyber-Kriminelle haben sich den neuen Gewohnheiten angepasst und ihre Angriffsmuster umgestellt. Die zunehmende Verschmelzung von Privat- und Berufsleben bot eine zusätzliche Angriffsfläche: Schließlich sind Endgeräte im Heimnetzwerk häufig schlechter geschützt als hinter der Unternehmens-Firewall.

HP bietet daher mit dem integrierten Security-Portfolio Wolf Security umfassende Sicherheitslösungen für Privatpersonen, kleine und mittelständische Unternehmen ebenso wie für Behörden und Großkonzerne. Unternehmen mit eigener Cyber-Security Abteilung sind mit HP Wolf Security bestens geschützt, denn HP Wolf Enterprise Security bietet leistungsstarke Sicherheitslösungen für PCs und Drucker.

Besonders kleine und mittelständische Unternehmen stehen in Zeiten kleiner werdender IT-Teams vor der Herausforderung, eine umfassende und widerstandsfähige Endpoint-Infrastruktur für Drucker und PCs sowie Cyber-Abwehr zu ermöglichen. HP Wolf Security Pro setzt dort an. Dank HP Sure Click Pro werden potenzielle Bedrohungen vom restlichen System isoliert. Die Szenarien sind dabei unterschiedlich: Ob infizierter E-Mail Anhang oder Link auf eine manipulierte Webseite – die Isolierung sorgt dafür, dass Hardware, Software und Nutzerdaten zu keinem Zeitpunkt gefährdet sind. Das Konzept beruht auf einer hardwaregestützten Mikro-Virtualisierung. Gleichzeitig schützen KI-basierte Sicherheitsfeatures wie HP Sure Sense Pro vor Malware. Die neuen Features sind bereits in die HP Hardware-Security-Funktionen integriert.



## HP WOLF SECURITY

Das Prinzip der Virtualisierung schützt allerdings nicht nur den Anwender, sondern auch kritische Management-Applikationen der Administratoren, die in einem isolierten Browser betrieben werden. Diese Aufgabe übernimmt HP Sure Access Enterprise. Die Lösung setzt auf das Isolationsprinzip.

### Drucker die sich selber schützen

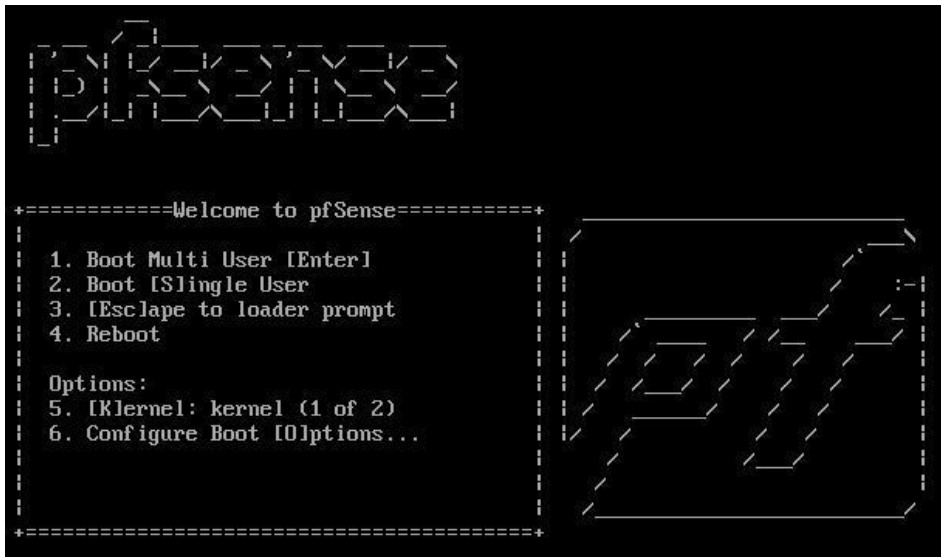
HP Wolf Security verteidigt das Netzwerk mit den weltweit sichersten Druckern, da es Cyberkriminelle auf die Druckinfrastruktur abgesehen haben. HP Wolf Security ermöglicht einen kontinuierlichen, hardwaregestützten Schutz und die Managed Services ermöglichen einen ausfallsicheren, grenzenlosen Arbeitsplatz.

# Open-Source-Firewall pfSense 1/2

Die Open-Source-Firewall pfSense (Firma: Netgate - USA/Texas) basiert auf FreeBSD und ist wie OPNSense, in wenigen Minuten einsatzbereit. pfSense setzt auf den Paketfilter »pf«. Die Verwaltung erfolgt über eine Weboberfläche.

Die grundlegende Installation der Systemdateien ist in wenigen Minuten abgeschlossen. Hier erfolgen nur die Partitionierung und die Auswahl der Sprache für die Tastatur. Die weiteren Einstellungen werden nach der Installation vorgenommen.

Die Firewall steht auch als Appliance mit dazu passender Hardware zur Verfügung.



Nach dem Start erscheint das Bootmenü. Hier kann die Installation gestartet werden.

## Einrichtung und weitere Einstellungen für den Erstbetrieb

Nach dem Start des installierten Systems werden grundlegende Einstellungen, wie die IP-Einstellungen definiert. Anschließend erfolgt die weitere Verwaltung über die Weboberfläche. Diese wird über die URL <https://<IP-Adresse>> erreicht. Die IP-Adresse ist beim Starten des Servers im Terminal zu sehen.

Der Standardbenutzername für die Anmeldung an der Oberfläche ist **admin** und das Standardkennwort ist **pfSense**. Die Anmeldedaten sollten schnellstmöglich geändert werden. Dazu blendet der Assistent nach der Anmeldung auch einen Hinweis ein.

Die ersten Schritte nach dem Aufrufen der Weboberfläche bestehen zunächst darin, die Anmeldedaten anzupassen. Danach wird der Hostname und die Domäne der Firewall konfiguriert und die DNS-Server, mit denen die Firewall arbeiten soll.

Anschließend werden Zeitserver und Einstellungen für das WAN-Interface konfiguriert. Im Assistenten kann man ebenfalls noch die IP-Adresse und die Subnetzmaske für das LAN-Interface anpassen. Diese Einstellungen stehen aber auch im Terminal zur Verfügung. Sollte man das Admin-Kennwort noch nicht angepasst haben, zeigt der Assistent eine entsprechende Information an. Sobald die Einrichtung abgeschlossen ist, sieht man die Weboberfläche (Dashboard) zur Verwaltung von pfSense.

## pfSense mit der Weboberfläche verwalten

Nachdem die Weboberfläche aufgerufen wurde, kann pfSense umfassend verwaltet werden. Standardmäßig wird das Dashboard der Firewall mit den wichtigsten Informationen geöffnet. Im oberen Bereich sind Menüs für die Verwaltung der Firewall-Funktionen zu finden. Die Firewall-Regeln sind über »Firewall\Rules« zu finden.

## Open-Source-Firewall pfSense 2/2

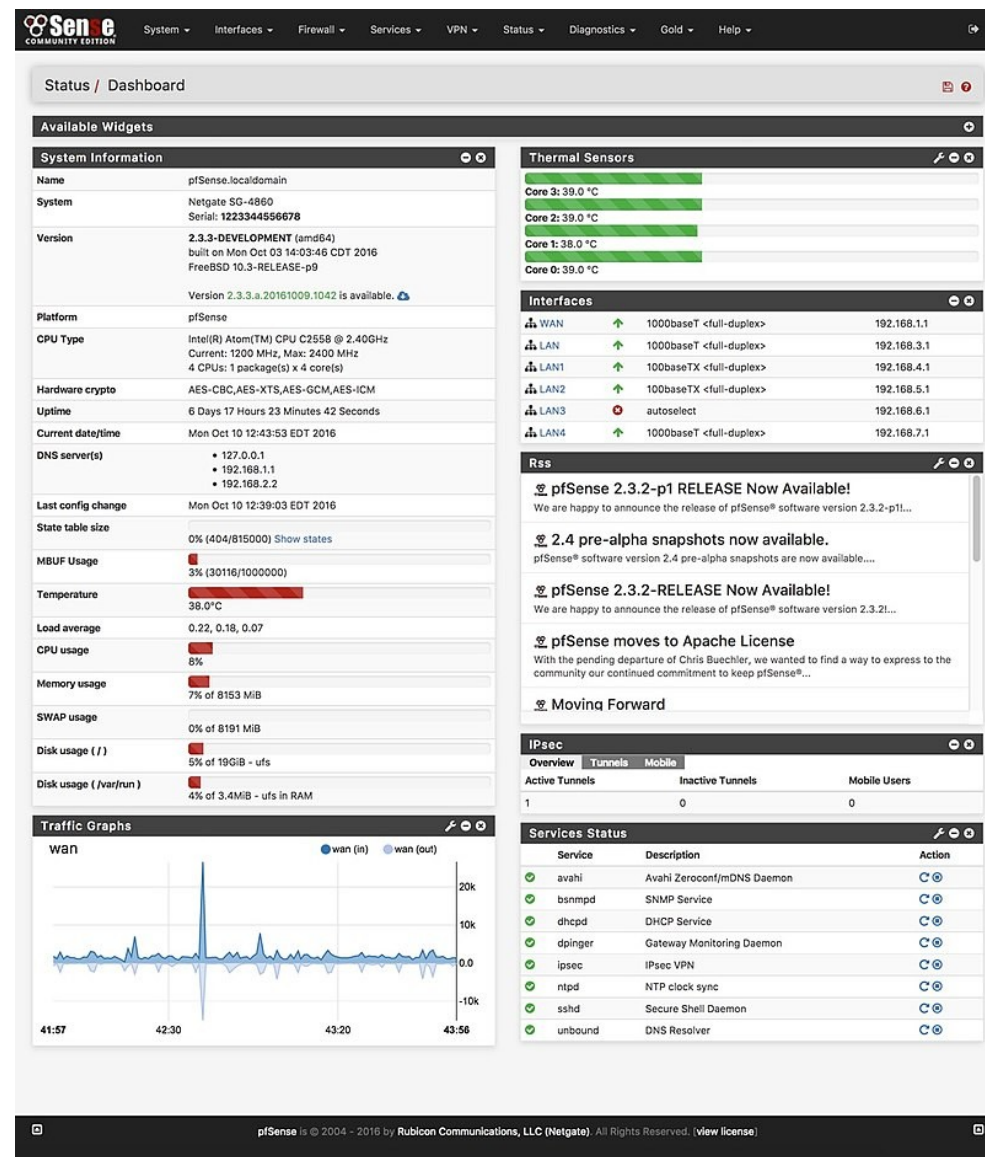
Hier stehen weitere Bereiche zur Verfügung, wie die NAT-Einstellungen und Virtual-IPs. Einstellungen zum Routing sind bei »System\Routing« zu finden. Über »Interfaces« werden die Systemeinstellungen der Netzwerkadapter konfiguriert. Hier können auch Adapter zeitweise deaktiviert werden.

Zeigt das Dashboard eine neue Version von pfSense an, kann über »System\Update« eine Aktualisierung der Firewall über die Weboberfläche stattfinden. Nach der Aktualisierung startet die Firewall auf Anforderung automatisch neu.

Über »Services« werden die Dienste verwaltet, die auf der Firewall aktiviert wurden. Dabei handelt es sich zum Beispiel um den DHCP-Server, den Load Balancer, NTP, DNS, SNMP oder PPPoE-Server. Im Bereich »Services« kann außerdem mit »Auto Configuration Backup« eingestellt werden, dass pfSense automatisch bei Änderungen der Konfiguration oder in regelmäßigen Abständen eine Datensicherung ablegt. Diese kann bei Problemen zur Wiederherstellung genutzt werden. Wenn Probleme mit der Firewall auftreten, lassen sich bei »Diagnostics« verschiedene Tools aufrufen, um zum Beispiel Systemdateien anzupassen, Computer zu pingen oder Protokolle aufzurufen.

### VPN mit pfSense

Über den Bereich »VPN« kann die pfSense-Firewall auch als VPN-Server betrieben werden. Hier steht neben IPSec, L2TP, auch OpenVPN zur Verfügung. Die Einrichtung des VPN-Servers erfolgt im Grunde genommen genauso, wie beim Einsatz anderer Appliances, wie OPNSense. Der virtuelle OpenVPN-Server wird in der Weboberfläche konfiguriert und anschließend wartet die Firewall auf dem entsprechenden Port auf Anfragen. Wenn pfSense hinter einer Firewall oder einem Router betrieben wird, müssen die entsprechenden Ports natürlich an die pfSense-Appliance weitergeleitet werden.



Dashboard von pfSense



# Open-Source-Firewall OPNsense 1/2

OPNsense ist eine einfach zu bedienende Open Source Firewall und Routing-Plattform. Basierend auf FreeBSD vereint OPNsense den reichhaltigen Funktionsumfang, den man sonst nur von kommerziellen Firewalls kennt, mit den Vorteilen offener und überprüfbarer Quellen.

OPNsense ist eine Abspaltung (Fork, 2015) von pfSense. Mittlerweile enthält die Firewall-Distribution nur noch wenige Prozent Code-Anteil von pfSense und gilt als neue, eigenständige Firewall-Distribution.

Für die Systemvoraussetzungen gibt OPNsense minimal eine 500 MHz Single-Core-CPU, 512 MByte RAM und mindestens 4 GByte verfügbarem Speicherplatz (Festplatte, CF-/SD-Card, USB-Stick) an. Für den optimalen Betrieb wird allerdings eine 1,5 GHz Multi-Core-CPU, 4 GByte RAM und eine SSD mit 120 GByte Kapazität empfohlen.

OPNsense sichert mit seinem reichhaltigen Funktionsumfang und mit seiner gut strukturierten Management-Oberfläche, sowohl kleine Netzwerke wie Home-Offices, Arztpraxen oder Steuerbüros als auch mittlere und große Umgebungen mit bis zu mehreren hundert Benutzern.

Die Funktionen reichen dabei von den bekannten Filtermöglichkeiten einer Stateful Firewall über Virtual Private Networks (VPNs) zur Einbindung von externen Benutzern oder Standorten bis hin zu Enterprise-Features wie Captive Portals für zugangsbeschränkte WLANs, hochverfügbare Firewall-Cluster oder Multi-WAN-Uplinks.

Bedient wird OPNsense über ein grafisches Webinterface mit Mehrsprachenunterstützung, integrierter Hilfe und schneller Navigation per Suchfunktion.

Die wöchentlich bereitgestellten Sicherheitsupdates lassen sich über sichere Update-Mechanismen einspielen. Zahlreiche Plugins der OPNsense Community erlauben darüber hinaus die modulare Erweiterung der Firewall.



Die Firewall steht auch als Appliance mit dazu passender Hardware zur Verfügung.

## Vorteile von OPNsense

- frei verfügbare Software - für kommerzielle oder private Zwecke einsetzbar
- einfach einspielbare, regelmäßige Sicherheitsupdates
- große Unterstützer-Community im Netz
- riesiger Funktionsumfang, vergleichbar mit vielen kommerziellen Produkten
- über Webinterface einfach bedienbar
- grafisches Dashboard zur Anzeige des Firewall-Status
- für kleine und große Installationen einsetzbar
- kontinuierliche Weiterentwicklung der Software
- beliebig erweiterbar und anpassbar über Plugins
- hohe Verfügbarkeit dank automatischen Hardware-Failover- und Backup-Mechanismen
- auf unterschiedlicher Hardware und auf virtuellen Maschinen oder eingebetteten Systemen ausführbar
- frei verfügbares, ausführliches Online-Benutzerhandbuch

# Open-Source-Firewall OPNSense 2/2

## Funktionsumfang der Open-Source-Firewall-Distribution

OPNSense bietet einen riesigen Funktionsumfang und ist für private wie für kommerzielle Anwendungen bis hin zu Enterprise-Installationen einsetzbar.

Die Feature-Liste von OPNSense enthält neben den klassischen Firewall-Funktionen Stateful Packetfiltering, ein auf Suricata basierendes Inline-Intrusion-Detection-System, Intrusion Prevention und automatische Backups auch einige regelrechte Enterprise-Features:

- **Hochverfügbarkeit** (HA .. High Availability): OPNSense unterstützt den Failover-Betrieb über das Common Address Redundancy Protocol (CARP). Damit lassen sich zwei Firewalls zu einer Failover-Gruppe zusammenfassen. Im Cluster ist immer nur ein System aktiv, Konfigurationsänderungen werden auf alle Systeme in einer Failover-Gruppe repliziert. Fällt das Produkktivsystem aus, übernimmt automatisch das zweite System aus der Failover-Gruppe den Produktivbetrieb.
- **Multi-WAN-Anbindung und Traffic Shaping**: OPNSense kann mehrere Internet-Uplinks verwalten und damit Failover, Loadbalancing oder eine Kombination beider realisieren.
- **Unterstützung für externe Authentifizierungsserver**: OPNSense bringt eine Benutzerdatenbank mit und bindet zusätzlich externe Authentifizierungsdienste wie LDAP inklusive Microsoft Active Directory und RADIUS ein.
- **2-Faktor-Authentifizierung**: Für die Dienste Web-GUI, Captive Portal, VPN (OpenVPN & IPsec) und den Caching Proxy unterstützt OPNSense 2-Faktor-Authentifizierung mit One-Time Passwords nach dem TOTP-Standard.
- **HTTP / HTTPS / Caching Web Proxy mit Blacklist Support**: Der auf Squid basierende Web-Proxy unterstützt auch den Transparent-Modus, bei dem für den Proxy-Betrieb keine Änderung an den Clients erforderlich ist.

- **VPN**: Unterstützte VPN-Technologien sind unter anderem SSL/TLS, IPsec, OpenVPN, L2TP und PPTP.
- **Captive Portal / Voucher Support**: Für den Betrieb von Gästenetzwerken (Ethernet oder WiFi) bietet OPNSense ein integriertes Captive Portal inklusive Voucher-Verwaltung. Das Captive Portal ist für Hotspots einsetzbar und erlaubt das Erzwingen einer Authentifizierung für den Zugang zum Netzwerk.
- **802.1Q VLAN Support**: Unterstützung für getaggte VLANs zur Verwaltung mehrerer virtueller Netzwerke.

Weiterhin bindet OPNSense auf Wunsch SSL-Blacklisten von abuse.ch (<https://abuse.ch/>) sowie die - ebenfalls kostenlose - GeoIP-Datenbank »Maxmind GeoLite2 Country« (<https://dev.maxmind.com/geoip/geolite2-free-geolocation-data?lang=en>) ein.

Ein weiteres Highlight ist der Netflow Analyzer »Insight«, mit dessen Hilfe Admins die Netzwerknutzung auf Benutzer- und Port-Ebene beziehungsweise Protokollebene grafisch und »on the fly« aufbereiten können.

OPNSense kann mit Hilfe des URL-Table-Alias regelmäßig die aktuellen (E)DROP-Listen von Spamhaus (<https://www.spamhaus.org/drop/>) beziehen und jegliche Kommunikation mit den darin enthaltenen Netzen per Firewall-Regel unterbinden.

Erwähnenswert ist die Tatsache, dass Administratoren bei OPNSense zwischen der Standard-Kryptobibliothek OpenSSL und der freien Alternative LibreSSL (Fork von OpenSSL) wählen können.

# Was ist Packet Sniffing? 1/2

Packet Sniffing ist das Sammeln und Protokollieren einiger oder aller Pakete, die durch ein Computer-Netzwerk gehen, unabhängig davon, wie das Paket adressiert ist. Auf diese Weise kann jedes Paket oder eine bestimmte Teilmenge von Paketen zur weiteren Analyse erfasst werden. Netzwerkadministratoren können diese gesammelten Daten für eine Vielzahl von Zwecken wie z. B. zur Überwachung von Bandbreite und Datenverkehr nutzen.

Ein Packet Sniffer, der manchmal auch als Packet Analyzer bezeichnet wird, besteht aus zwei Hauptteilen: erstens aus einem Netzwerkadapter, der den Sniffer mit dem bestehenden Netzwerk verbindet, und zweitens aus der Software, die die Protokollierung, Ansicht oder Analyse der gesammelten Daten ermöglicht.

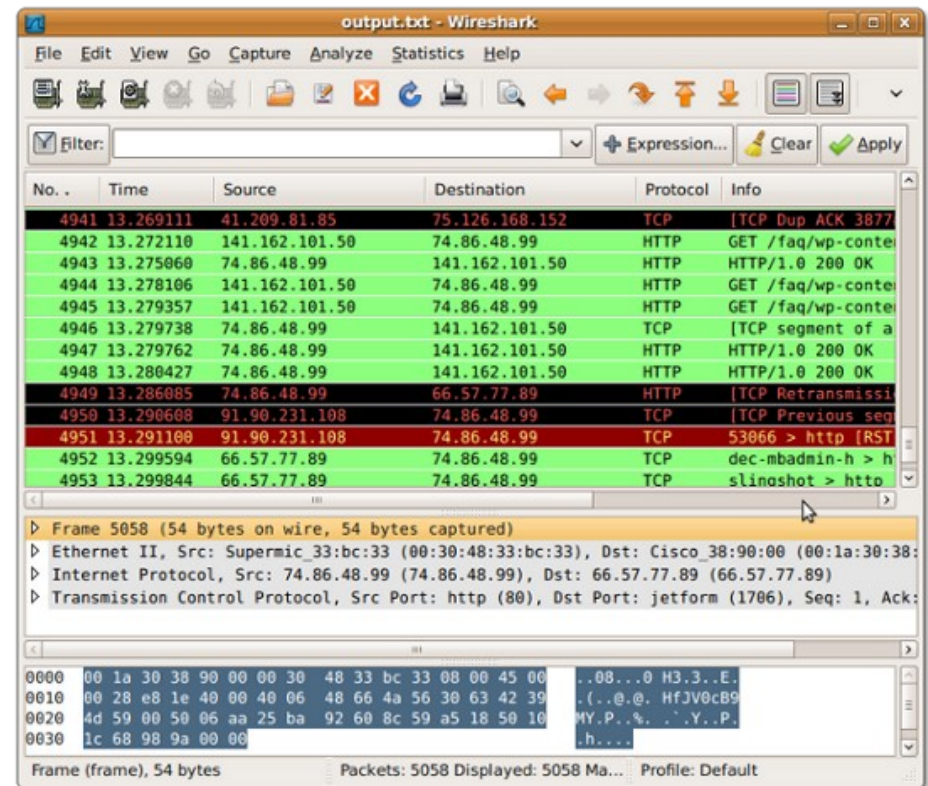
## Wie funktioniert Packet Sniffing?

Ein Netzwerk ist eine Ansammlung von untereinander verbundenen Knoten wie Personalcomputern, Servern und Netzwerkhardware. Die Netzwerkverbindung ermöglicht die Übertragung von Daten zwischen diesen Elementen. Die Verbindungen können physisch mit Kabeln oder drahtlos mit Funksignalen erfolgen. Netzwerke können auch eine Kombination aus beiden Typen sein.

Während die Knoten Daten durch das Netzwerk schicken, wird jede Übertragung in kleinere Einheiten unterteilt, die als Pakete bezeichnet werden. Dank ihrer festgelegten Länge und Form können die Datenpakete auf Vollständigkeit und Nutzbarkeit überprüft werden. Da die Infrastruktur eines Netzwerks vielen Knoten gemeinsam ist, werden Pakete, die für unterschiedliche Knoten bestimmt sind, auf dem Weg zu ihrem Ziel durch zahlreiche andere Knoten geleitet. Um sicherzustellen, dass keine Daten verwechselt werden, wird jedem Paket eine Adresse zugewiesen, die den vorgesehenen Zielort dieses Pakets darstellt.

Die Adresse eines Pakets wird von jedem Netzwerkadapter und verbundenen Gerät überprüft, um zu ermitteln, für welchen Knoten das Paket bestimmt ist. Wenn ein Knoten bei normalen Betriebsbedingungen ein Paket erkennt, das nicht an ihn adressiert ist, ignoriert er dieses Paket und seine Daten.

Beim Packet Sniffing wird diese Standardpraxis ignoriert und alle oder einige Pakete werden unabhängig von ihrer Adresse gesammelt.



## Was ist Packet Sniffing? 2/2

Es gibt zwei Haupttypen von Packet Sniffern:

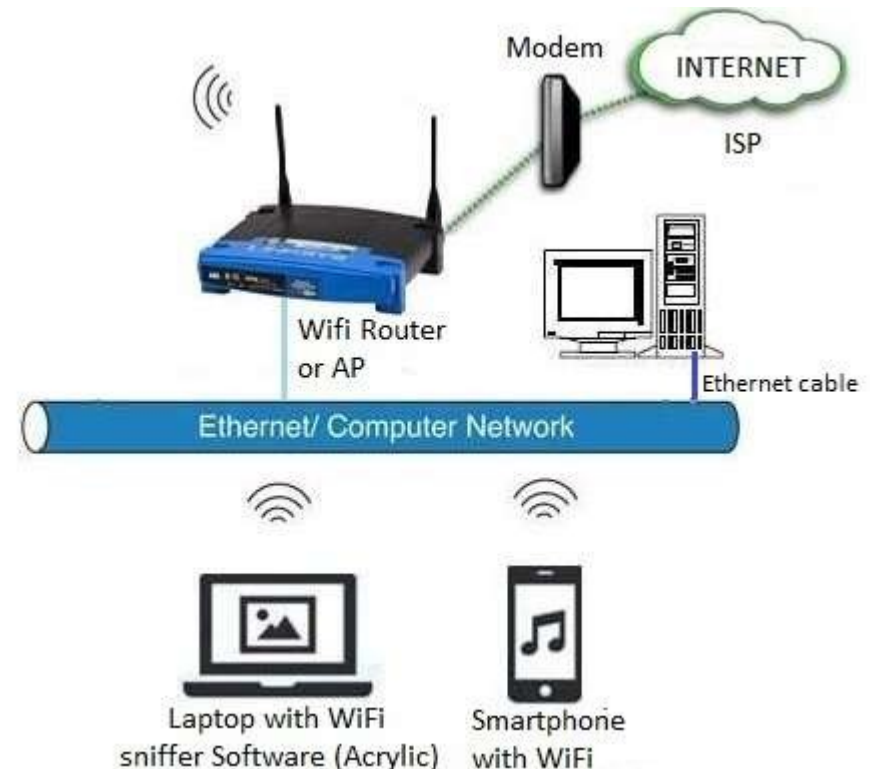
### Hardware Packet Sniffer

Ein Hardware Packet Sniffer ist dafür bestimmt, an ein Netzwerk angeschlossen zu werden und es zu überprüfen. Ein Hardware Packet Sniffer ist besonders nützlich, wenn versucht wird, den Datenverkehr eines bestimmten Netzwerksegments zu sehen. Durch direkten Anschluss an das physische Netzwerk an der passenden Stelle kann ein Hardware Packet Sniffer sicherstellen, dass keine Pakete durch Filterung, Routing oder andere beabsichtigte oder unbeabsichtigte Ursachen verloren gehen. Entweder speichert ein Hardware Packet Sniffer die gesammelten Pakete oder er leitet sie weiter an einen Sammler, der die gesammelten Daten zur weiteren Analyse protokolliert.

### Software Packet Sniffer

Heutzutage sind die meisten Packet Sniffer vom Software-Typ. Obwohl jede mit einem Netzwerk verbundene Netzwerkschnittstelle jedes Bit des durchgehenden Netzwerkverkehrs empfangen kann, sind die meisten Schnittstellen so konfiguriert, dass sie dies nicht tun. Ein Software Packet Sniffer ändert diese Konfiguration so, dass die Netzwerkschnittstelle den gesamten Netzwerkverkehr zum Stack weiterleitet. Diese Konfiguration ist für die meisten Netzwerkadapter als Promiscuous-Modus bekannt. Im Promiscuous-Modus besteht die Funktionalität eines Packet Sniffers darin, alle Software-Pakete, die durch die Schnittstelle gehen, unabhängig von ihrer Zieladresse zu zerlegen, wieder zusammenzusetzen und zu protokollieren. Software Packet Sniffer sammeln den gesamten Datenverkehr, der durch die physische Netzwerkschnittstelle fließt. Dieser Datenverkehr wird dann protokolliert und entsprechend den Packet-Sniffing-Anforderungen der Software genutzt.

Zur Erfassung der Daten in einem ganzen Netzwerk können mehrere Packet Sniffer nötig sein. Da jeder Sammler nur den Netzwerkverkehr sammeln kann, der vom Netzwerkadapter empfangen wird, kann er eventuell nicht den Datenverkehr sehen, der auf der anderen Seite von Routern oder Switchen existiert. In drahtlosen Netzwerken können sich die meisten Adapter nur mit jeweils einem Kanal verbinden. Um Daten in mehreren Netzwerksegmenten oder mehreren drahtlosen Kanälen zu erfassen, wird für jedes Segment des Netzwerks ein Packet Sniffer gebraucht. Die meisten Lösungen zur Netzwerküberwachung bieten Packet Sniffing als eine der Funktionen ihrer Überwachungs-Agenten an.





# Pegasus

Pegasus ist eine Spyware (Trojaner) des israelischen Unternehmens NSO Group zum Ausspähen von iOS- und Android-Geräten. Die Software kann unbemerkt auf sämtliche Daten zugreifen und sie über das Internet (WLAN) versenden. Pegasus wurde im August 2016 durch die Sicherheitsfirma Lookout und durch Citizen Lab entdeckt und analysiert. Pegasus wird ausschließlich an Regierungseinrichtungen, Strafermittler und Geheimdienste als **Softwaredienstleistung** angeboten. Journalisten, Menschenrechtler und Politiker wurden bisher mit Hilfe von Pegasus ausgespäht.

**Funktionsweise:** Nach dem Anklicken eines Links in einer gefälschten SMS (manuell) werden eine Reihe von Schwachstellen ausgenutzt und ein sogenannter »versteckter Jailbreak« durchgeführt. Heute können Schwachstellen direkt und automatisiert ausgenutzt werden. Die Spyware Pegasus prüft bei der Installation, ob bereits ein Jailbreak vorliegt, deaktiviert die Auto-Update-Funktion, um Sicherheitsupdates zu vermeiden und nistet sich mit Root-Rechten in das Betriebssystem ein.

**Hinweis:** Seit einiger Zeit, ist das Anklicken eines Links nicht mehr notwendig (Info-Stand: 2022).

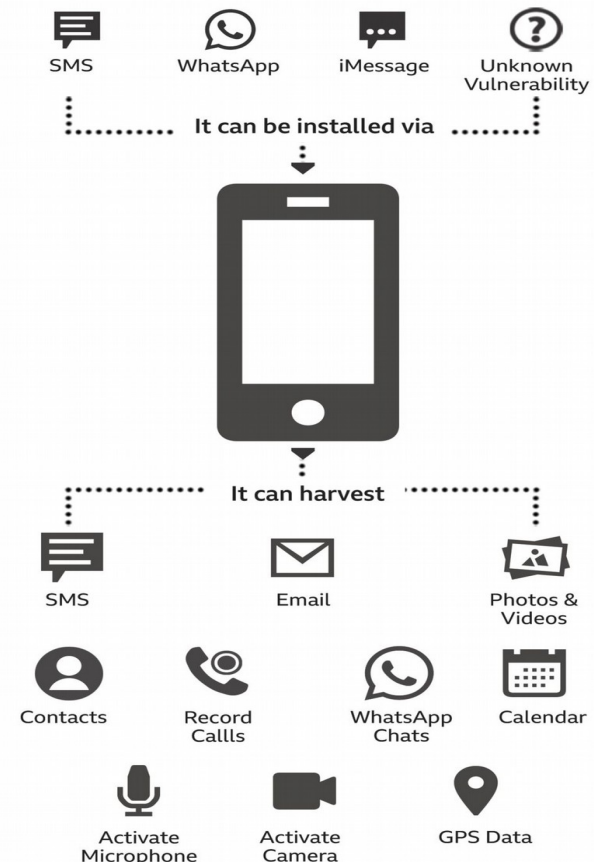
**Mögliche Abfolge einer automatischer Installation von Pegasus:** DNS-Umleitung und Sendung eines Datenfragments -> Datenfragment wird fälschlicherweise als Programmcode ausgeführt -> in Folge: Absturz einer Anwendung -> in Folge: wurden Administrator-Rechte erlangt -> Download und Installation der Pegasus-Software -> zusätzlich wird die Sendung des Fehlerberichts (Telemetrie) an den Hersteller unterdrückt

Bisher konnte folgendes ermittelt werden:

- Gesprächsaufzeichnung
- Kopieren des kompletten Adressbuches
- Abhören von Messengerkommunikation (SMS, iMessage, GMail, Viber, Facebook Messenger, Skype, Telegram, WhatsApp, Signal)
- Standortermittlung
- Batteriestatus
- Zugriff auf sämtliche Dokumente und Fotos
- Browserverlauf

- gespeicherte Passwörter
- gespeicherte WLAN-Passwörter und des Apple-Schlüsselbundes

## What Pegasus spyware can do



Source: Pegasus Project

BBC

Pegasus eröffnet damit alle Funktionen, die auch für staatliche Online-Durchsuchungen oder Quellen-Telekommunikationsüberwachung angewandt werden.



# Portknocking

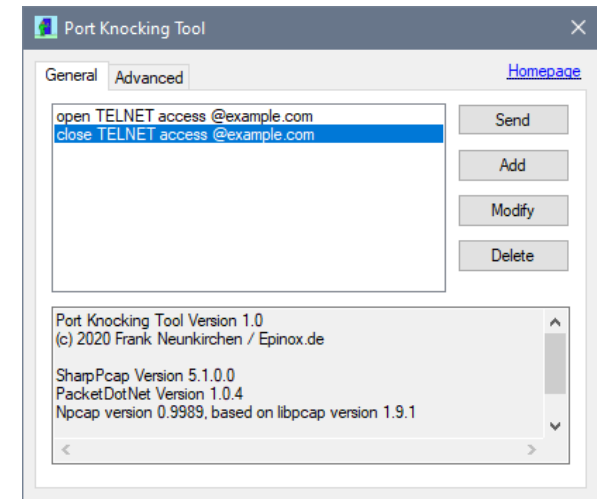
Portknocking (engl. to knock .. Klopfen; Port .. Anschluss) ist ein Verfahren, um Server bzw. Serverdienste in Netzwerken vor unbefugtem Zugriff zu schützen. Dabei werden die für die Kommunikation verwendeten Ports zunächst von der Firewall des Servers blockiert. Auf dem Server überwacht dabei ein Portknocking-Daemon ankommende SYN-Pakete, die bei korrekter zeitlicher Abfolge und Reihenfolge (der sogenannte »Knock«) den Daemon dazu veranlasst, den blockierten Port wieder zu öffnen. Sobald der Serverdienst nicht mehr benötigt wird, kann durch eine andere Reihenfolge der gesendeten SYN-Pakete der gewünschte Port wieder gesperrt werden.

Mit einem SYN-Paket wird im Transmission Control Protocol (TCP) normalerweise der Verbindungsaufbau eingeleitet, aber die Firewall blockiert diese Verbindungsversuche zunächst und antwortet nicht auf die Kommunikationsversuche oder sie sendet ein RST-Paket und weist damit die Verbindung zunächst ab. Ein Portknocking-Daemon hört aber mit, zum Beispiel indem er die Logdatei der Firewall auswertet und öffnet bei korrekter Abfolge und Inhalt der SYN-Pakete den gewünschten Port in der Firewall.

Der Vorteil dieses Verfahrens ist, dass man ohne Kenntnis der zuvor vereinbarten Abfolge von SYN-Paketen von außen nicht feststellen kann, ob an einem Port ein Serverdienst lauscht – **ein Portscan kann den Dienst nicht entdecken**. Eingesetzt wird Portknocking deshalb vor allem, um Zugriffsmöglichkeiten für die Fernwartung (z.B. SSH) zu verbergen. Gut implementierte Dienste für entfernte Administration bieten zwar selbst durch Verschlüsselung des Kommunikationsweges und Authentifizierung Sicherheit vor unbefugtem Zugriff, aber es könnten Fehler in der Server-Software existieren, über die man auch ohne Authentifizierung die Gewalt über den Server erlangen könnte. Der Portknocking-Daemon selbst kann allerdings auch Fehler enthalten, wodurch ein zuvor sicherer Server möglicherweise erst durch den Einsatz von Portknocking angreifbar wird.

Gegen Angreifer, die den Datenverkehr per Paket-Sniffer mitlesen, helfen verschlüsselte Hashwerte im Knock-Paket. Bei Man-in-the-middle-Angriffen bietet Portknocking prinzipiell keinen Schutz. Dienste, die für die Allgemeinheit im Internet angeboten werden, etwa ein Webserver, kann man mit Portknocking ebenfalls nicht absichern.

**Programm:** Die Windows-Anwendung **Port Knocking Tool Epinox** kann SYN-Pakete in die entsprechende Reihenfolge an geschützte Server senden. Dabei werden sowohl UDP als auch TCP-Pakete (benötigt: **Npcap**) unterstützt. Eine Konsolenanwendung ist zusätzlich vorhanden.



## Registerkarte: Allgemein

**Senden:** Die in der Liste ausgewählte Paketsequenz wird an den abgesicherten Server gesendet.

**Hinzufügen:** Zur Liste wird eine neue Paketsequenz hinzugefügt.

**Ändern:** Änderungen an der Sequenz durchführen.

**Entfernen:** Die Sequenz wird aus der Liste entfernt.

## Registerkarte: Erweitert

**Verzögerung:** Eingabe der Verzögerungszeit in Millisekunden zwischen zwei zu sendenden IP-Paketen.

**Verwende Pcap:** Um auch TCP-Pakete versenden zu können, muss diese Option aktiviert werden. Als Voraussetzung muss **Npcap** installiert sein.

# Was macht der TPM-Chip? 1/2

Mit der Ankündigung von Windows 11, ist es plötzlich zu einem der wichtigsten dreibuchstabigen Akronyme in der Computerwelt geworden. Dies liegt daran, dass Windows 11 ein Trusted Platform Module (TPM) in einem Computer benötigt, damit es überhaupt funktioniert. Insbesondere ist TPM 2.0 erforderlich, obwohl diese Anforderungen nach Ermessen von Microsoft geändert werden können.

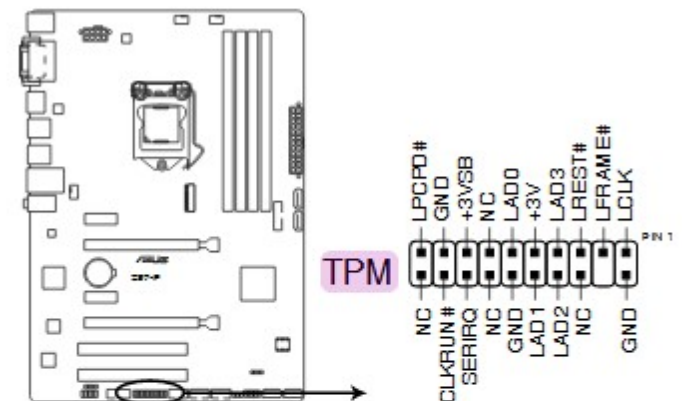
Das TPM ist eine physische Komponente (ein spezieller Chip), die normalerweise auf dem Motherboard eingebaut ist.

Das TPM speichert Passwörter, Sicherheitszertifikate und Schlüssel die für Verschlüsselung benötigt werden und verhindert unbefugte Manipulationen. Ein »Trusted Platform Module« (TPM) kann Verschlüsselungsschlüssel sicher generieren, sodass der Prozess nicht ausspioniert oder gestört werden kann. Das Ziel von Trusted Computing ist somit die Erhöhung der Sicherheit von Computern. Mittlerweile kommt Trusted Computing auch immer häufiger bei Handys und Tablets zum Einsatz.

- Unterstützt ein Computer das Trusted Computing, ist er mit einem zusätzlichen Chip ausgestattet, dem »Trusted Platform Module« (TPM). Der Chip sammelt Informationen über die angeschlossene Hardware sowie die genutzte Software auf dem PC und speichert diese Informationen verschlüsselt ab.
- Das Betriebssystem **kann** beim Start den Chip auslesen, um zu prüfen, ob eine Veränderung am PC vorgenommen wurde. Auch Programme können während des laufenden Betriebes die Informationen auslesen.
- Sorgt eine Malware für Veränderungen in der Hardware oder Software (kann Viren- oder auch Konkurrenzsoftware behindern) und wird diese durch das Trusted Computing erkannt, erhält der Nutzer mindestens eine Warnung. Je nach Bedarf kann das Trusted Computing auch das betroffene Programm sofort schließen oder die Verbindung zum Internet kappen, um das System zu schützen.

- Der TPM-Chip ist auf dem Mainboard des Computers platziert und bietet noch weitere Vorteile. Unter anderem sorgt er unter Windows dafür, dass die Dateien mit dem BitLocker verschlüsselt werden können.

TPM connector (20-1 pin TPM)



# Was macht der TPM-Chip? 2/2

## Wie arbeitet das Trusted Computing?

Ohne Trusted Computing wird ein PC per Software mit einem Anti-Viren-Schutz versehen. Dieser überwacht das laufende Geschehen und versucht Bedrohungen abzuwehren. Das Trusted Computing setzt bereits an einem viel früheren Zeitpunkt an.

**Hinweis:** Der Chip ist aktuell überwiegend passiv und kann weder den Bootvorgang noch den Betrieb direkt beeinflussen.

- Den Herstellern der Hardware und Software wird von Anfang an vertraut (»trust« ... »Vertrauen«). Der ursprüngliche Zustand von Hard- und Software wird im TPM-Chip gespeichert und beim Start des PCs Schritt für Schritt mit dem aktuellen Zustand abgeglichen.
- Als erstes wird geprüft, ob die Hardware sich verändert hat. Beispielsweise kann eine Festplatte fehlen oder gegen eine mit Malware infizierte Platte ausgetauscht worden sein. Wurde die unterste Ebene geprüft, kann sich die nächst höhere Ebene sicher sein, dass alles in Ordnung ist und den Betrieb starten.
- Nach der Hardware wird das BIOS geprüft, anschließend der Bootloader sowie alle Bestandteile des Betriebssystems und der installierten Software.
- Das TPM kann Schlüssel auch außerhalb des Trust Storage (z. B. auf der Festplatte) speichern. Diese werden ebenfalls in einem Schlüssel-Baum organisiert und deren Wurzel mit einem »Key« im TPM verschlüsselt. Somit ist die Anzahl der sicher gespeicherten Schlüssel nahezu unbegrenzt.

Neben diesen Funktionen enthält das TPM auch ein fest verdrahtetes, einzigartiges und einen unveränderlichen Verschlüsselungsschlüssel, der es wahrscheinlich unmöglich macht, ihn zu ersetzen oder zu manipulieren.

Kurz gesagt ist das TPM eine dedizierte Hardware auf dem Motherboard, die eine sichere Computernutzung und Authentifizierung ermöglicht. Außer wenn der Rechner nur **fTPM** oder **TPP** unterstützt.

## Firmware-TPM (fTPM) und Platform Trust Technology (PTT)

Firmware TPM (fTPM) und Platform Trust Technology (PTT) sind die jeweiligen Namen von AMD und Intel für Firmware-TPMs.

Anstelle eines dedizierten Chips auf dem Motherboard ist die Trusted Platform Module-Funktionalität in der Firmware der CPU vorhanden.

fTPM und TPP sind in den meisten modernen AMD-und Intel-Prozessoren integriert, die Funktion muss jedoch aktiviert werden, damit sie funktioniert.

Normalerweise deaktivieren Motherboard-Hersteller standardmäßig die Firmware-TPM-Funktionalität, erlauben es jedoch, diese im BIOS- oder UEFI-Menü zu aktivieren. Da jedes Motherboard-Modell unterschiedlich sein kann, sollte man im Motherboard-Handbuch nach spezifischen Anweisungen zur Aktivierung der Firmware-TPM suchen.

Ob das Motherboard über ein vorhandenes und funktionierendes Trusted Platform Module verfügt, kann man über das Programm tpm.msc in Erfahrung bringen.

Tastenkombination:

**[Win] + [R]** -> **tpm.msc** eingeben und mit der [Enter]-Taste bestätigen.

**Status:** Das TPM ist einsatzbereit.

**Spezifikationsversion:** 2.0 oder höher

## Was ist unter Windows 11 anders? 1/5

Seit dem 5. Oktober 2021 steht Windows 11 den Windows-Benutzern offiziell zur Verfügung. Die erkennbaren Änderungen betreffen im wesentlichen das Erscheinungsbild des Betriebssystems. Aber Erfahrungsgemäß wird die Redmonder Softwareschmiede mit jeder neuen Version neugieriger und man hat nur wenige Möglichkeiten den Abfluss der Daten zu reduzieren (Dienst deaktivieren, der die Telemetriedaten versendet). **Hinweis:** Sobald man den Windows Desktop sieht, hat man den Allgemeinen Geschäftsbedingungen der Redmonder Softwareschmiede zugestimmt.





# Was ist unter Windows 11 anders? 2/5

## Allgemeines

Seit dem 5. Oktober 2021 steht Windows 11 offiziell den Windows-Benutzern zur Verfügung. Für Privatbenutzer wird Windows 10 noch bis zum 14. Oktober 2025 vollständig mit Sicherheits- und Qualitäts-Updates versorgt. Im Herbst 2021 bekommt Windows 10 noch das Funktionsupdate - Windows 10 21H2.

## Änderungen unter Windows 11

- Windows 11 wurde mit einem neu gestalteten und aktualisierten Erscheinungsbild ausgestattet.
- Der Microsoft Edge Browser basiert nun auf dem von Google entwickelten Chromium Projekt. Alle gängigen Android-Anwendungen sollten, mithilfe einer Software des Chipherstellers Intel, direkt auf einem Windows 11 Rechner laufen.
- Windows-10-Rechner lassen sich direkt zu Windows 11 aktualisieren. **Für das Update muss mindestens Windows 10 Version 21H1 und der TPM-Chip in der Version 2.0 (Trusted Platform Module 2.0) auf dem Gerät installiert sein.**  
**Hinweis:** Mitunter ist der TPM-Chip standardmäßig im BIOS deaktiviert. Damit Windows 11 läuft muss der Chip im BIOS einfach nur aktiviert werden.
- Das Windows Terminal hat den Einzug in das neue Betriebssystem geschafft. Die Terminal-Anwendung vereint die Konsolen Eingabeaufforderung (Kommandozeile), PowerShell und Azure Cloud Shell. Die Software erreicht man per Rechtsklick auf den Desktop und im Windows-X-Menü. Tastenkombination: [Win] + [X]
- Windows 11 eignet sich nun auch für Geräte mit Touchscreen. Dabei kann es sich um reine Tablets oder um Hybrid-Geräte mit Tastatur und Touchscreen handeln.
- Windows 11 merkt sich nun die Anordnung der Fenster (Snap Groups), auch wenn man einen externen Monitor nutzt und stattet virtuelle Desktops nun auch mit eigenen Wallpapers aus.
- Tastenkombination für virtuelle Desktops:  
[Win] + [Strg] + [D] ... virtuellen Desktop neu erstellen  
[Win] + [TAB] ... virtuelle Desktops verwalten  
[Win] + [TAB] ... die ursprüngliche Bildschirmansicht wiederherstellen  
[Win] + [Strg] + [>] oder [<] ... virtuellen Desktop wechseln  
[Win] + [Strg] + [F4] ... aktuellen virtuellen Desktop schließen
- Die Mindestanforderungen für die **Taktfrequenz** von Prozessoren (Prozessoren von AMD, Intel und Qualcomm) bleibt mit **1 GHz** zwar unverändert. Allerdings benötigt man für Windows 11 einen **Prozessor mit mindestens 2 Kernen**. Darüber hinaus besteht für einige ältere Prozessoren mit Sicherheitslücken keine Unterstützung mehr. **Windows 11 unterstützt keine 32-Bit-Architekturen** mehr. Für den **Hauptspeicher** des Rechners sind **mindestens 4 GByte** erforderlich und **mindestens 64 GByte freier Speicherplatz**. Die Grafikkarte muss **mit DirectX 12** kompatibel sein. **Weiterhin sind nur Rechner die Secure Boot über die UEFI Firmware unterstützen, für Windows 11 geeignet.**
- Neue Tastenkombinationen unter Windows 11:  
[Win] + [W] ... Widgets öffnen  
[Win] + [Z] ... Fenster anordnen  
[Win] + [N] ... Benachrichtigungen und Kalender öffnen  
[Win] + [H] ... Spracheingabe starten  
[Win] + [A] ... Schnelleinstellungen öffnen  
[Win] + [Alt] + [Pfeiltaste links/rechts] ... heftet das im Vordergrund offene Fenster im dreigeteilten Layout an
- Geräte und Treiber, die unter Windows 10 laufen, sollten in der Regel auch mit Windows 11 funktionieren. Microsoft hat an dieser Stelle keine Änderungen vorgenommen.
- Für Administratoren wird die neue Update-Politik für Windows 11 von Interesse sein. Für das Betriebssystem wird nur noch ein Update im Jahr erscheinen.



# Was ist unter Windows 11 anders? 3/5

## Windows 11 Editionen

In der aktuellen Version Windows 11 gibt es die folgenden Editionen:

- Windows 11 Home
- Windows 11 Home N
- Windows 11 Pro
- Windows 11 Pro N
- Windows 11 Pro for Workstations
- Windows 11 Pro for Workstations N
- Windows 11 Enterprise
- Windows 11 Enterprise N
- Windows 11 Enterprise E3
- Windows 11 Enterprise E5
- Windows 11 Pro Education
- Windows 11 Pro Education N
- Windows 11 Education
- Windows 11 Education N

Auch eine Windows 11 Pro OEM Version wird wahrscheinlich wieder verfügbar sein.

In den N-Editionen von Windows fehlt der Media Player (Abspielen von Musik und Videos). Die Versionen mit den fehlenden Media Player beruhen auf eine Forderung der EU-Kommission an Microsoft, auch Editionen ohne Media Player anzubieten.

**Hinweis:** Die N-Editionen von Windows sind weniger gut getestet und damit wahrscheinlich auch fehleranfälliger.

## Aktivierung von Windows 11

Für die Aktivierung ist eine gültige Lizenz notwendig. In Geräten mit vorinstalliertem Windows ist die Seriennummer im Bios hinterlegt.

Diese Seriennummer, die hinterlegt ist oder die man gekauft hat, entscheidet welche Version von Windows 11 installiert wird.

**Mit diesen Schlüsseln kann man Windows 11 installieren und aktivieren:**

- Ein Windows 7 Key kann für die Installation und Aktivierung genutzt werden.
- Ein Windows 8.1 Key kann für die Installation und Aktivierung genutzt werden.
- Ein Windows 10 Key kann für die Installation und Aktivierung genutzt werden.
- Ist Windows 7, 8.1 oder Windows 10 installiert und aktiviert, reicht ein Inplace Upgrade, um auf Windows 11 umzusteigen.

Ist Windows 11 einmal aktiviert und man möchte Windows neu installieren, reicht es die Schlüsseleingabe zu überspringen. Die hinterlegte Hardware-ID aktiviert Windows 11 dann automatisch. Bei einer Neuinstallation kann die Aktivierung des neuen Systems bis zu einigen Stunden dauern. **Hinweis:** Als »In-Place- Upgrade« bezeichnet Microsoft eine Softwareaktualisierung, die frühere Versionen einer Anwendung überschreibt.

# Was ist unter Windows 11 anders? 4/5

## Mit einem generischen Key Windows 11 installieren

Die generischen Seriennummern sind von Microsoft bereitgestellt worden, um Windows 11 installieren zu können. Diese sind auch interessant, wenn man ein Versionswechsel, zum Beispiel von der Windows 11 Home auf die Pro macht.

Dann kann man diesen Key für den Wechsel nutzen und danach dann mit der vorhandenen Lizenz in den Einstellungen regulär aktivieren.

- Windows 11 Home: YTMG3-N6DKC-DKB77-7M9GH-8HVX7
- Windows 11 Home N: 4CPRK-NM3K3-X6XXQ-RXX86-WXCHW
- Windows 11 Pro: VK7JG-NPHTM-C97JM-9MPGT-3V66T
- Windows 11 Pro N: 2B87N-8KFHP-DKV6R-Y2C8J-PKCKT
- Windows 11 Pro for Workstations: DXG7C-N36C4-C4HTG-X4T3X-2YV77
- Windows 11 Pro N for Workstations: WYPNQ-8C467-V2W6J-TX4WX-WT2RQ
- Windows 11 Pro Education: 8PTT6-RNW4C-6V7J2-C2D3X-MHBPB
- Windows 11 Pro Education N: GJTYN-HDMQY-FRR76-HVGC7-QPF8P
- Windows 11 Education: YNMGQ-8RYV3-4PGQ3-C8XTP-7CFBY

- Windows 11 Education N: 84NGF-MHBT6-FXBX8-QWJK7-DRR8H
- Windows 11 Enterprise: XGVPP-NMH47-7TTHJ-W3FW7-8HV2C
- Windows 11 Enterprise N: WGGHN-J84D6-QYCPR-T7PJ7-X766F

## Windows 11 ohne Aktivierung nutzen

Windows 11 kann, wie schon Windows 10 mit dem generischen Key installiert und ohne eine Aktivierung genutzt werden. Eine 30-Tage Version, wie es im Netz immer wieder zu lesen ist, gibt es nicht. Windows 11 ist soweit voll nutzbar. Einige Einstellungen, wie unter Personalisation sind nicht möglich. Die kann man aber in der Registry vornehmen. Mit der Zeit wird dann ein Wasserzeichen auf dem Desktop erscheinen, dass Windows 11 aktiviert werden muss, was man dann auch machen sollte. Das man Windows 11 so installieren und nutzen kann ist dafür gedacht, wenn man noch nicht gleich an eine Windows 11 Lizenz kommt, aber schon installieren will.

## Aktivierung und Registrierung von Windows 11

Bei neuen Rechner sind die Geräte zentral auf Microsoft-Servern registriert, so dass bei einer Neuinstallation und einer bestehenden Internetverbindung kein Lizenzschlüssel eingegeben werden muss. Bei einer Neuinstallation kann die Aktivierung des neuen Systems bis zu einigen Stunden dauern.

Über den Windows-Product-Key-Viewer (winproductkey.exe, siehe Internet oder Verzeichnis: Windows-Product-Key-Viewer) kann man den Produkt-Key (Lizenzschlüssel) ermitteln und damit schon direkt bei einer notwendigen Neuinstallation eintragen.

# Was ist unter Windows 11 anders? 5/5

## Windows Enterprise E3

Für mittelgroße bis große Unternehmen, die erweiterte Sicherheit und umfassende Verwaltung benötigen.

### Windows 11 Enterprise E3 ist als Upgrade zu Windows 11 Pro erhältlich und bietet zusätzlich:

- vielseitige Optionen für die Bereitstellung des Betriebssystems und kontrollierte Updates
- umfassende Geräte- und App-Verwaltung
- universelles Drucken für serverlose Druckverwaltung
- erweiterten Schutz vor den neuesten Sicherheitsbedrohungen

#### Anforderungen:

- Berechtigtes Betriebssystem: Windows 11 Pro
- Pro Nutzer lizenziert, einschließlich Azure Virtual Desktop- und Windows 365-Instanzen.

## Windows Enterprise E5

Für Unternehmen, die eine ganzheitliche Lösung für Endpunktsicherheit nutzen möchten, die über die Cloud bereitgestellt wird.

### Windows 11 Enterprise E5 ist als Upgrade von Windows 10 Enterprise E3 erhältlich und bietet zusätzlich:

- Microsoft Defender für Endpunkt, eine Komplettlösung für Endpunktsicherheit

#### Anforderungen:

- Berechtigtes Betriebssystem: Windows 11 Enterprise E3
- Pro Nutzer lizenziert

## Windows Enterprise E3 in Microsoft 365 F3

Für mittelgroße bis große Unternehmen mit Mitarbeitern in Service und Produktion.

### Windows 11 Enterprise E3 ist in Microsoft 365 F3-Abonnements enthalten und bietet zusätzlich:

- vielseitige Optionen für die Bereitstellung des Betriebssystems und kontrollierte Updates
- umfassende Geräte- und App-Verwaltung
- universelles Drucken für serverlose Druckverwaltung
- erweiterten Schutz vor den neuesten Sicherheitsbedrohungen

#### Anforderungen:

- Berechtigtes Betriebssystem: Windows 11 Pro
- Pro Nutzer lizenziert, einschließlich Cloudverwaltung und Virtualisierung.

# Tastatur-Kurzbefehle W10 und W11

## Tastenkombinationen - Windows 11

- [Win] + [W]** ... Widgets öffnen
- [Win] + [Z]** ... Fenster anordnen
- [Win] + [N]** ... Benachrichtigungen und Kalender öffnen
- [Win] + [H]** ... Spracheingabe starten (funktioniert nicht mit jeder Systemversion)
- [Win] + [A]** ... Schnelleinstellungen öffnen
- [Win] + [Alt] + [Pfeiltaste links/rechts]** ... heftet das im Vordergrund offene Fenster im dreigeteilten Layout an

## Tastenkombinationen - Windows 10 und 11

- [Win] + [Q]** ... Suchfeld öffnen
- [Win] + [S]** ... Suchfeld öffnen
- [Win] + [X]** ... Expert-Modus, Schnellzugriff auf wichtige Windows-Einstellungen wie Datenträgerverwaltung, Taskmanager, Netzwerkverbindungen, Computerverwaltung, PowerShell, ...  
(**Alternativ:** Rechtsklick auf das Windows-Icon, unten links)
- [Win] + [D]** ... Desktop anzeigen und ausblenden
- [Win] + [Alt] + [D]** ... Datum und Uhrzeit auf dem Desktop anzeigen und ausblenden
- [Win] + [M]** ... alle Fenster minimieren
- [Win] + [Umschalt] + [M]** ... minimierte Fenster auf dem Desktop wiederherstellen
- [Win] + [L]** ... PC sperren oder Konto wechseln
- [Win] + [R]** ... Ausführen von Befehlen (cmd, regedit, calc, mspaint)
- [Win] + [I]** ... Windows-Einstellungen

**[Win] + [PAUSE]** ... Windows Systemsteuerung aufrufen -> auf Link »Startseite der Systemsteuerung« klicken;  
Aktivierung von Windows; Windows Aktivierung überprüfen;  
ProduktID -> ProduktKey ändern

- [Win] + [A]** ... öffnet das Infocenter; Zugriff auf Einstellungen, Hardware, Tablet, Bluetooth, Flugzeugmodus, ...
- [Win] + [Strg] + [O]** ... Bildschirmtastatur öffnen
- [Win] + [E]** ... Explorer (Dateimanager) aufrufen.

- [STRG] + [ESC]** ... Menü »Start« öffnen
- [STRG] + [UMSCHALT] + [ESC]** ... Task-Manager öffnen.
- [ESC]** ... aktuelle Aufgabe anhalten oder beenden
- [F6]** ... zwischen Bildschirmelementen in einem Programmfenster oder auf dem Desktop umschalten
- [ALT] + [ESC]** ... zwischen Elementen in der Reihenfolge, in der sie geöffnet wurden, umschalten
- [ALT] + [EINGABETASTE]** ... Eigenschaften für das ausgewählte Element anzeigen
- [ALT] + [LEERTASTE]** ... Kontextmenü für das aktive Fenster öffnen

## Tastenkombinationen - nur Windows 10

- [Win] + [V]**: Zwischenablagen-Verlauf einsehen, Zwischenablage öffnen
- [Win] + [UMSCHALT] + [S]** ... einen Screenshot von einem Teil des Bildschirms aufnehmen; **Hinweis:** Nach dem Kopieren des Schnappschusses in die Zwischenablage, kann das Bild in MSPAINT eingefügt werden.
- [Win] + [.]** ... Emoji-Bereich öffnen

# System-Programme

## System-Programme aufrufen

Über den Aufruf des Ausführen-Dialoges [Win] + [R] und der Eingabe der nachfolgenden Programmnamen, können diese Windows-Systemprogramme aufgerufen werden.

**appwiz.cpl** ... öffnet die Software-Verwaltung

**certmgr.msc** ... Zertifikate aktueller Benutzer

**cleanmgr.exe** ... Datenträgerbereinigung aufrufen

**cmd**... Shell für die Ausführung von Terminal-Befehle; [Win] + [R] -  
> **cmd** -> [Strg] + [Shift] + [ENTER] ... CMD mit Administrator-Rechten öffnen

**comexp.msc** ... Komponentendienste aufrufen; Ereignisanzeige, Dienste

**compmgmt.msc** ... Computerverwaltung aufrufen

**control** oder **control.exe**... Windows-Systemsteuerung aufrufen;  
Alternativ kann die Systemsteuerung auch über die Tastenkombination [Win] + [Pause] aufgerufen werden, anschließend auf den Link »Startseite der Systemsteuerung« klicken

**devmgmt.msc** ... Geräte-Manager aufrufen

**diskmgmt.msc** ... Datenträgerverwaltung

**displayswitch** ... Bildschirme konfigurieren, falls mehrere am Computer angeschlossen sind (Reihenfolge, Inhalt doppelt anzeigen, Anzeige auf Projektor)

**eventvwr.msc** ... Ereignisanzeige aufrufen

**fsmgmt.msc** ... Freigegebene Ordner

**gpedit.msc** ... Editor für die Gruppenrichtlinie aufrufen; Computerkonfiguration und Benutzerkonfiguration

**inetcpl.cpl** ... Internetoptionen aufrufen

**lusrmgr.msc** ... »Lokale Benutzer und Gruppen« aufrufen

**msconfig** oder **msconfig.exe** ... Systemkonfigurationsprogramm aufrufen; Abgesicherter Systemstart konfigurieren, Dienste anzeigen, System-Tools aufrufen

**msinfo32** oder **msinfo32.exe** ... Systeminformationen aufrufen

**msra.exe** ... Windows-Remoteunterstützung

**ms-settings** oder **ms-settings:start** ... Windows-Einstellungen aufrufen

**ms-settings:display** ... Bildschirm-Einstellungen aufrufen

**ms-settings:network-status** ... Netzwerk-Status aufrufen

**ms-settings:windowsupdate-history** ... Update-Verlauf anzeigen

**ms-settings:activation** ... Windows Aktivierung aufrufen

**netplwiz** oder **netplwiz.exe** ... Benutzerkonten aufrufen

**optionalfeatures.exe** ... Windows-Funktionen ein- oder ausschalten

**perfmon.msc** ... Zuverlässigkeits- und Leistungsüberwachung

**powershell** oder **powershell.exe** ... Shell für die Ausführung von Terminal-Befehle

**printmanagement.msc** ... Druckverwaltung aufrufen

**regedit** oder **regedt32.exe**... Editor für die Registry aufrufen

**rstrui.exe** ... Systemwiederherstellung aufrufen

**secpol.msc** ... Lokale Sicherheitsrichtlinie aufrufen

**services.msc** ... Konfigurationsprogramm für die System-Dienste aufrufen

**SystemPropertiesPerformance** ... Leistungsoptionen aufrufen

**taskmgr** ... Taskmanager öffnen

**tpm.msc** ... Trusted Module Management (TPM) aufrufen



# Dienste unter Windows 10 beenden 1/6

## Dienst für die Sendung der Telemetriedaten beenden (Enterprise Edition)

Die Telemetriedaten (Betriebsdaten) werden über ein System namens »Event Tracing for Windows« gesammelt. Verschickt werden die Daten im ETW-System über den Dienst »DiagTrack« (Diagnostics Tracking Service). Damit Windows keine Telemetriedaten mehr ins Internet sendet, muss man diesen Dienst beenden.

Tastenkombination: [Win] + [I] -> Suchfeld: Systemsteuerung -> System und Sicherheit -> Verwaltung -> Dienste -> Eintrag (Doppelklick): »Benutzererfahrung und Telemetrie im verbundenen Modus« -> Starttyp wechseln: Automatisch -> Deaktiviert  
Zusätzlich muss man in der Registry unter HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\AutoLogger-DiagTrack-Listener\Start den Wert von Start auf 0 setzen.

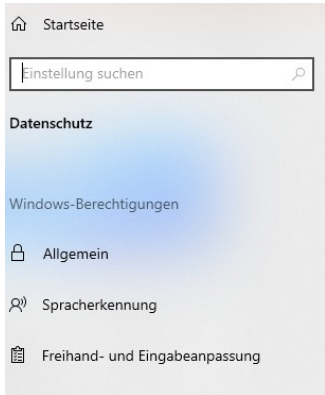
The screenshot shows the Windows Services console. The service 'Benutzererfahrung und Telemetrie im verbundenen Modus' is selected. The description on the left states: 'Durch den Dienst für Benutzererfahrung und Telemetrie im verbundenen Modus werden Features aktiviert, die Benutzerfreundlichkeit in Anwendungen und im verbundenen Modus unterstützen. Außerdem verwaltet dieser Dienst die ereignisgesteuerte Sammlung und Übertragung von Diagnose- und Nutzungsdaten (die zur Verbesserung der Benutzerfreundlichkeit und Qualität der Windows-Plattform eingesetzt werden). Dazu müssen die Diagnose- und Nutzungseinstellungen in der Datenschutzoption unter "Feedback und Diagnose" aktiviert sein.'

Name	Beschreibung
AppX-Bereitstellungsdienst (AppXSVC)	Stellt Infrastrukturunterstützung...
Arbeitsordner	Von diesem Dienst werden Da...
Arbeitsstationsdienst	Erstellt und wartet Clientnetz...
AssignedAccessManager-Dienst	AssignedAccessManager-Serv...
Aufgabenplanung	Ermöglicht einem Benutzer, a...
Autom. Setup von Geräten, die mit dem Netzwerk verbunden...	Der Dienst "Autom. Setup von...
Automatische Konfiguration (verkabelt)	Mit dem Dienst für die autom...
Automatische WLAN-Konfiguration	Der WLANSVC-Dienst bietet d...
Automatische Zeitonenaktualisierung	Legt die Systemzeitzone autor...
AVCTP-Dienst	Dies ist der AVCTP (Audio Video Control transport Protocol)-Dienst.
Basisfiltermodul	Das Basisfiltermodul ist ein Dienst, der Firewall- und IPsec-Richtlinien überwacht u...
Benachrichtigungsdienst für Systemereignisse	Überwacht Systemereignisse und benachrichtigt Abonnenten des COM+-Ereigniss...
Benutzerdatenspeicher_42104	Verarbeitet die Speicherung strukturierter Benutzerdaten, einschließlich Kontakinf...
Benutzerdatenzugriff_42104	Ermöglicht Apps den Zugriff auf strukturierte Benutzerdaten, einschließlich Kontak...
Benutzerdienst für die Plattform für verbundene Geräte_42104	Dieser Benutzerdienst wird für Szenarien in Verbindung mit der Plattform für verbu...
Benutzerdienst für GameDVR und Übertragungen_42104	Dieser Benutzerdienst wird für Spielaufzeichnungen und Liveübertragungen verwe...
<b>Benutzererfahrung und Telemetrie im verbundenen Modus</b>	<b>Durch den Dienst für Benutzererfahrung und Telemetrie im verbundenen Modus w...</b>
Benutzer-Manager	Der Benutzer-Manager stellt die Laufzeitkomponenten bereit, die für Interaktionen ...
Benutzerprofildienst	Dieser Dienst ist für das Laden und Entladen von Benutzerprofilen verantwortlich. ...
Bitdefender Endpoint Integration Service	Applies the security server settings to a managed client product.
Bitdefender Endpoint Protected Service	Provides protection against malware and other security threats.

Eigenschaften von Benutzererfahrung und Telemetrie im verbunde... X

The screenshot shows the 'Properties' dialog box for the service 'Benutzererfahrung und Telemetrie im verbundenen Modus'. The 'Allgemein' tab is selected. The service name is 'DiagTrack'. The display name is 'Benutzererfahrung und Telemetrie im verbundenen Modus'. The description is 'Durch den Dienst für Benutzererfahrung und Telemetrie im verbundenen Modus werden Features aktiviert, die Benutzerfreundlichkeit in Anwendungen...'. The path to the EXE file is 'C:\Windows\System32\svchost.exe -k utcsvc -p'. The start type is 'Automatisch'. The service status is 'Wird ausgeführt'. There are buttons for 'Starten', 'Beenden', 'Anhalten', and 'Fortsetzen'. A text box for 'Startparameter' is empty. At the bottom are 'OK', 'Abbrechen', and 'Übernehmen' buttons.

# Dienste unter Windows 10 beenden 2/6



## Allgemein

### Datenschutzoptionen ändern

Ermöglicht Apps die Verwendung der Werbe-ID, um Ihnen anhand Ihrer App-Aktivität interessantere Werbung anzuzeigen (bei Deaktivierung wird Ihre ID zurückgesetzt).

☐ Aus

Websites den Zugriff auf die eigene Sprachliste gestatten, um die Anzeige lokal relevanter Inhalte zu ermöglichen

☐ Aus

Windows erlauben, das Starten von Apps nachzuverfolgen, um Start und Suchergebnisse zu verbessern

☐ Aus

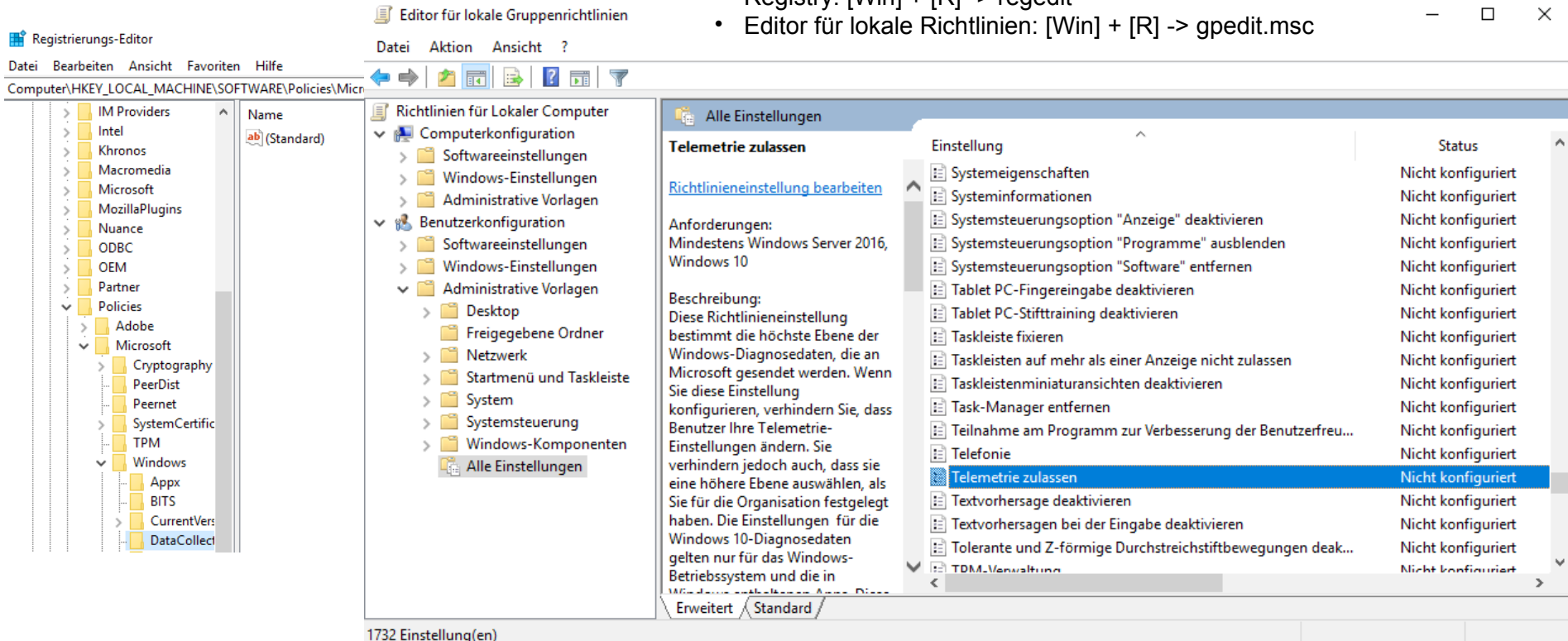
## Dienst »Telemetrie zulassen« deaktivieren

Um diesen Dienst zu deaktivieren, müssen an mehreren Orten Änderungen vorgenommen werden:

- Tastenkombination: [Win] + [I] -> Datenschutz -> Allgemein -> Verwendung der Werbe-ID ausschalten
- Tastenkombination: [Win] + [I] -> Datenschutz -> Diagnose und Feedback -> Senden der Diagnosedaten auf Einfach oder Standard stellen, Feedbackhäufigkeit auf »Nie« stellen

**Hinweis:** In der Enterprise-Version kann man das Senden der Diagnosedaten auch ganz abschalten.

- Registry: [Win] + [R] -> regedit
- Editor für lokale Richtlinien: [Win] + [R] -> gpedit.msc



# Dienste unter Windows 10 beenden 3/6

## Benutzererfahrung und Telemetrie nicht teilen (Windows Pro)

Standardmäßig sammelt die Redmonder Software-Schmiede viele Nutzungsdaten in Windows 10. Eine einfache Möglichkeit, diese abzuschalten, gibt es nicht. Man kann lediglich zwischen den Arten Einfach (Standard) und Vollständig wählen. Für alle, die den Datenschutz sehr ernst nehmen, bietet Microsoft keine direkte Möglichkeit an, die Datenweitergabe weiter einzuschränken. Glücklicherweise gibt es dennoch einen Weg, sie komplett zu deaktivieren. Nach jedem Funktionsupdate von Windows, sind die nachfolgenden Änderungen wieder einer Prüfung zu unterziehen.

Um die Datenweitergabe von Telemetrie und Benutzererfahrungen zu deaktivieren, muss zuerst ein Wert im Registrierungs-Editor angepasst werden:

1. [Windows-Taste] + [R] drücken, um den Ausführen-Dialog zu öffnen.
2. regedit eingeben und mit Enter bestätigen.
3. Navigieren zu:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection
4. Diesen Schlüssel öffnen und über Rechtsklick -> Neu -> DWORD-Wert (32-Bit) einen neuen Wert mit folgenden Daten erstellen:  
Name: AllowTelemetry  
Wert: 0

Nun müssen noch zwei Dienste, die für die eigentliche Datenweitergabe der Benutzererfahrung und Telemetrie an Microsoft zuständig sind, deaktiviert werden. Dies kann entweder über die Oberfläche »Dienste« durchgeführt werden oder über zwei kurze Befehle in der Eingabeaufforderung.

## Über die Dienste

1. Im Suchfeld der Taskleiste »Dienste« eingeben und den Eintrag mit Enter bestätigen.
2. Folgende Dienste müssen deaktiviert werden:  
WAP-Push-Nachrichten-Routing-Dienst (Wireless Application Protocol, früher: Benutzererfahrung und Telemetrie im verbundenen Modus, dmwappushsvc)
3. Dazu macht man einen Doppelklick auf den jeweiligen Dienst und wählt dann als Starttyp »Deaktiviert« aus.
4. Ist der jeweilige Dienst gestartet, genügt ein Klick auf die Schaltfläche »Beenden« unter der Auswahl des Starttyps, um den Dienst zu beenden. Alternativ genügt ein Neustart des Systems.

## Über die Eingabeaufforderung

5. Im Suchfeld der Taskleiste cmd eingeben und den Eintrag über Rechtsklick -> »Als Administrator ausführen« starten.
6. Folgende beiden Befehle eingeben und jeweils mit Enter bestätigen:  
**sc config DiagTrack start=disabled**  
**sc config dmwappushservice start=disabled**
7. Um die Dienste, wenn sie noch gestartet sind, direkt zu beenden, muss man noch folgende beiden Befehle eingeben:  
**sc stop DiagTrack**  
**sc stop dmwappushservice**

Die Änderungen sind sofort aktiv, da die beiden Dienste deaktiviert wurden. Ab sofort werden keine Daten zur Benutzererfahrung und Telemetrie mehr an die Redmonder Software-Schmiede geschickt.

Sieht man sich nun nochmal die Datenschutz-Einstellungen unter Einstellungen -> Datenschutz -> Diagnose und Feedback an, sieht man auch direkt, dass die Einstellungen hier nicht mehr aktiv sind.

## Dienste unter Windows 10 beenden 4/6

### Was macht die Datei dmwappushsvc.dll ?

WAP-Push-Nachrichten-Routing-Dienst mit der Datei dmwappushsvc.dll wird als ein Typ der Dynamic Link Library-Datei (DLL) angesehen. Dynamic Link Library-Dateien, wie dmwappushsvc.dll, sind im Wesentlichen eine Art von Handbuch, in dem Informationen und Anweisungen für ausführbare Dateien (EXE) gespeichert werden. Diese Dateien wurden so erstellt, dass mehrere Programme (z.B. Windows) die gleiche dmwappushsvc.dll Datei teilen können, wodurch wertvolle Speicherzuweisung gespart wird.

Leider macht das, was DLL Dateien so praktisch und effizient macht, sie auch extrem anfällig für Probleme. Wenn eine freigegebenen DLL-Datei auf irgendeine Weise beschädigt wurde, kann sie eine »Runtime«-Fehlermeldung generieren. WAP Push ist ein System zur Verteilung verschiedener Inhalte von einem Server zu einem Mobilgerät (Client, Handy). Der Inhalt (z.B. Klingeltöne mit SMS verschicken) wird dabei prinzipiell ohne Initiative seitens des Clients vom Server auf das Mobilgerät »geschoben«.

Kurz gesagt: Dieser Dienst routet von Geräten empfangene WAP-Push-Nachrichten weiter.

### Was macht der Dienst »DiagTrack« (Diagnostics Tracking Service)?

DiagTrack ist ebenfalls eine DLL-Datei (diagtrack.dll). DiagTracks Auftrag ist es, für die Redmonder Software-Schmiede Informationen über das System- und Anwenderverhalten zu sammeln und nach Redmond zu transportieren. Oder technischer formuliert, der Dienst verwaltet die ereignisgesteuerte Sammlung und Übertragung von Diagnose- und Nutzungsdaten. Außerdem aktiviert er einige zusätzliche Features um die Benutzerfreundlichkeit zu erhöhen.

Der lesbare Name dieses Dienstes lautet «Connected User Experiences and Telemetry» oder » Benutzererfahrung und Telemetrie im verbundenen Modus«.

### Was macht der Dienst »WerSvc«?

Der Dienst »WerSvc« (Windows-Fehlerberichterstattungsdienst, siehe auch Registry: HKEY\_LOCAL\_MACHINE\ SYSTEM\ CurrentControlSet\ Services\ WerSvc) ist dafür zuständig eine Benachrichtigungsmail an die Redmonder Software-Schmiede zu versenden, wenn ein Fehler in einer Anwendung auftritt. Vor dem Versenden der Mail, wird der Anwender um die entsprechenden Erlaubnis gefragt. Der Bericht enthält Informationen aus dem entsprechenden Speicherbereich wo der Fehler aufgetreten ist.

### Was macht der Diensthost svchost.exe ?

Der Diensthost svchost startet normalerweise nicht nur einen Dienst sondern gleich mehrere Dienste und Prozesse. Unter Windows können nur exe-Dateien ausgeführt werden. Alle anderen Dateien (z.B. DLL-Dateien) werden »interpretiert«, dass heißt es ist ein weiteres Programm notwendig, um die darin enthaltenen Funktionen auszuführen. Genau diese Technik nutzen auch Dienste, Treiber und ähnliche System-Komponenten. Allerdings haben diese den Nachteil, dass sie nicht direkt ausführbar sind. Genau hier springt die svchost.exe ein. Das Programm lädt diese Bibliotheken und macht sie dadurch ausführbar. Die svchost.exe bildet einen Host für Dienste, die nicht direkt ausführbar sind.

### Status der Windows-Dienste ermitteln

Tastenkombination: [Win] + [R] -> msconfig -> Tab: Dienste

**Hinweis:** Auf dieser Seite kann man auch alle Microsoft-Dienste ausblenden, um sich nur von Windows unabhängige Dienste anzeigen zu lassen. Außerdem kann man von dort (Tab: Tools) einige systemnahe Tools starten.

# Dienste unter Windows 10 beenden 5/6

## Blockieren von Telemetriedaten bei Windows 10 über die hosts-Datei

Wer die Übermittlung der Telemetriedaten von Windows 10 an die Redmonder Software-Schmiede unterbinden will, kann etwa die Hosts-Datei (C:\Windows\System32\drivers\etc\hosts) verändern und so die eingetragenen Domains auf eine lokale IP-Adresse umleiten. Folglich kann dann Windows 10 nicht mehr von selbst mit den entsprechenden Servern kommunizieren.

Nun stuft der in Windows 10 integrierte Virenschanner namens Microsoft Defender das Blockieren der Hosts-Datei als Bedrohung ein und lässt ein Speichern der veränderte Textdatei nicht mehr zu. Hintergrund ist, dass auch Malware mittels Host-Hijacks diese Datei ändern kann, um Domains umzuleiten.

Es ist allerdings auch weiterhin möglich, die Übermittlung der Telemetriedaten an die Redmonder Software-Schmiede zu unterbinden, indem man bei Benutzung des Microsoft Defenders eine Ausnahme für die Hosts-Datei festlegt.

**Hinweis:** Die hosts-Datei dient der Auflösung von Hostnamen zu IP-Adressen.

**Ausnahme hinzufügen:** Windows-Einstellungen -> Update und Sicherheit -> Windows-Sicherheit -> Viren- & Bedrohungsschutz -> Einstellungen verwalten (Link auf der rechten Seite) -> Ausschlüsse hinzufügen oder entfernen (Link auf der rechten Seite) -> Ausschluss hinzufügen -> [...]

Alternativ können sämtliche Diagnosedaten auch in den Einstellungen von Windows 10 eingesehen und gelöscht werden oder das Anlegen der Diagnosedaten kann auch ganz untersagt werden (Windows 10 Enterprise).

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichte folgende Liste von MS-Trackingservern (Stand: April 2020)

**Datei:** hosts

# C:\Windows\System32\drivers\etc\hosts

# Beim Aufruf, werden diese Domains auf localhost (127.0.0.1) umgeleitet.

```
127.0.0.1 geo.settings-win.data.microsoft.com.akadns.net
127.0.0.1 db5-eap.settings-win.data.microsoft.com.akadns.net
127.0.0.1 settings-win.data.microsoft.com
127.0.0.1 db5.settings-win.data.microsoft.com.akadns.net
127.0.0.1 asimov-win.settings.data.microsoft.com.akadns.net
127.0.0.1 db5.vortex.data.microsoft.com.akadns.net
127.0.0.1 v10-win.vortex.data.microsoft.com.akadns.net
127.0.0.1 geo.vortex.data.microsoft.com.akadns.net
127.0.0.1 v10.vortex-win.data.microsoft.com
127.0.0.1 v10.events.data.microsoft.com
127.0.0.1 v20.events.data.microsoft.com
127.0.0.1 us.vortex-win.data.microsoft.com
127.0.0.1 eu.vortex-win.data.microsoft.com
127.0.0.1 vortex-win-sandbox.data.microsoft.com
127.0.0.1 alpha.telemetry.microsoft.com
127.0.0.1 oca.telemetry.microsoft.com
127.0.0.1 ceuswatcab01.blob.core.windows.net
127.0.0.1 ceuswatcab02.blob.core.windows.net
127.0.0.1 eaus2watcab01.blob.core.windows.net
127.0.0.1 eaus2watcab02.blob.core.windows.net
127.0.0.1 weus2watcab01.blob.core.windows.net
127.0.0.1 weus2watcab02.blob.core.windows.net
```

Zukünftige Windows Versionen können weitere oder andere Server nutzen.



## Dienste unter Windows 10 beenden 6/6

### Unnötige Windows-Dienste ausschalten

Manche Dienste von Windows werden nicht zwingend benötigt. Diese kann man relativ gefahrlos deaktivieren. Sollte es doch zu Problemen kommen, kann man den Dienst auch wieder aktivieren.

- **Diagnoserichtliniendienst (DPS)**; Der Diagnoserichtliniendienst ermöglicht die Problemerkennung und Problembehandlung für Windows-Komponenten.
- **Druckerwarteschlange (Spooler)**; wenn man keinen Drucker angeschlossen hat); Dieser Dienst spoolt Druckaufträge und verarbeitet Interaktionen mit dem Drucker. Wenn Sie diesen Dienst ausschalten, können Sie weder drucken noch Drucker anzeigen. Unter Spooling wird das Abfangen eines Druckjobs auf dem Weg zum Drucker verstanden. Stattdessen wird der Druckjob auf einem Speichermedium gespeichert.
- **Enumeratordienst für tragbare Geräte (WPDBusEnum)**; Erlaubt Gruppenrichtlinien für Geräte wie USB-Sticks und ermöglicht Programmen wie dem Windows Mediaplayer die Identifikation von MP3-Playern.
- **Fax (Fax)**; wenn man kein Fax-Gerät angeschlossen hat); Ermöglicht das Senden und Empfangen von Faxen mithilfe der Faxressourcen, die auf dem Computer oder im Netzwerk verfügbar sind.
- **IP-Hilfsdienst (iphlpvc)**; Stellt Tunnelkonnektivität mithilfe von IPv6-Übergangstechnologien (IP6-zu-IP4, ISATAP, Portproxy und Teredo) und IP-HTTPS bereit.
- **Remoteregistrierung (RemoteRegistry)**; Ermöglicht Remotebenutzern Registrierungseinstellungen eines Computers zu ändern. Wenn dieser Dienst beendet wird, kann die Registrierung nur von lokalen Benutzern dieses Computers verändert werden.
- **Sekundäre Anmeldung (seclogon)**; Aktiviert das Starten von Prozessen mit verschiedenen Anmeldeinformationen.
- **TCP/IP-NetBIOS-Hilfsdienst (lmhosts)**; Bietet Unterstützung für den NetBIOS-über-TCP/IP-Dienst (NetBT) und die NetBIOS-Namensauflösung für Clients im Netzwerk, so dass Benutzer Daten gemeinsam nutzen, drucken und sich am Netzwerk anmelden können.
- **Überwachung verteilter Verknüpfungen (TrkWks)**; Hält Verknüpfungen für NTFS-Dateien auf einem Computer oder zwischen Computern in einem Netzwerk aufrecht.
- **Windows Search (WSearch)**; Stellt Inhaltsindizierung und Eigenschaftenzwischenspeicherung und Suchergebnisse für Dateien, E-Mails und andere Inhalte bereit.
- **Windows-Bilderfassung (stisvc)**; Stellt Bilderfassungsdienste für Scanner und Kameras zur Verfügung.
- **Windows-Fehlerberichterstattungsdienst (WerSvc)**; Ermöglicht das Berichterstellen über Fehler bei nicht mehr funktionierenden und reagierenden Programmen und das Angeben von Lösungen. Ermöglicht außerdem das Generieren von Protokollen für Diagnose- und Reparaturdienste
- **Windows-Zeitgeber (W32Time)**; Behält Datums- und Zeitsynchronisation auf allen Clients und Servern im Netzwerk bei. Wird dieser Dienst deaktiviert, können keine explizit von der Synchronisation abhängigen Dienste gestartet werden.

### Deaktivierung der Windows-Dienste:

Tastenkombination: [Win] + [R] -> services.msc

Nun wird eine Übersicht der »Dienste« angezeigt. Per Doppelklick kann man die dazugehörigen Einstellungen öffnen. Um einen Dienst zu deaktivieren, wählt man bei »Starttyp« im Dropdown-Menü »Deaktiviert« aus und bestätigt die Auswahl anschließend mit »OK«.

# Browser im privaten Modus 1/3

**Der Inkognito-Modus (auch: InPrivate, privater Modus, anonymer Modus, privates Surfen) gibt vielen Internetnutzern beim Surfen ein Gefühl von Sicherheit und Privatsphäre. Doch was verbirgt er und was nicht?**

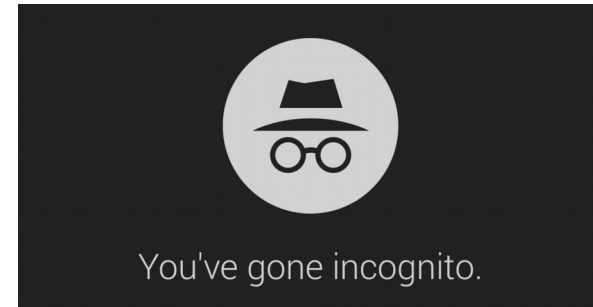
Wer mit einem normalen Browser im Internet surft, bleibt nicht anonym. Unternehmen wie Google und Facebook sowie unzählige Werbenetzwerke verfolgen jeden Klick, um die Interessen und Lebensumstände des Nutzers zu erforschen. Provider analysieren die Datenpakete, die zwischen den Anschlüssen hin- und hergeschickt werden. Auch der Staat überwacht die Internetaktivitäten seiner Bürger zur Verbrechensbekämpfung.

Viele Browser versprechen eine einfache Lösung für Nutzer, die ihre Privatsphäre vor neugierigen Blicken schützen wollen: Der Inkognito-Modus verschleiern angeblich seine Identität, sperrt Datensammler aus und macht das Surfen sicherer. Aber stimmt das?

## **Nutzer überschätzen die Wirkung**

Laut einer Studie der University of Chicago und der Leibniz-Universität zu Hannover schätzen viele Nutzer die Wirksamkeit des Inkognito-Modus völlig falsch ein. So glauben 40 Prozent der Befragten, dass ihr Standort im privaten Modus geheim bleibt. 37 Prozent denken, dass ihre Webaktivitäten dadurch vor dem Arbeitgeber verborgen werden. Und 22,6 Prozent gehen sogar davon aus, dass die Einstellungen sie vor der Regierung schützen.

Tatsächlich leistet das Öffnen eines privaten Browserfensters deutlich weniger. Unter »Google Chrome« etwa führt der Inkognito-Modus lediglich dazu, dass der Browserverlauf und in Webseiten eingegebene Informationen nicht gespeichert werden. Dadurch lässt sich beispielsweise verhindern, dass nachfolgende Nutzer (z.B. Internetcafé) auf Anhieb sehen können, welche Websites man besucht hat. Auch Formulare werden nicht mehr automatisch ausgefüllt und ergänzt.



## **Personalisierte Werbung funktioniert trotzdem**

Cookies und Websitedaten (auch Bilder, Videos) werden aber dennoch gespeichert - zumindest bis zum Ende der Sitzung (gilt nicht für modernste Technologien und Super-Cookies oder Evercookies). Werbenetzwerke und Website-Betreiber können das Surfverhalten des Nutzers also doch beobachten und analysieren. Erst wenn der Nutzer das Fenster schließt, werden die Daten gelöscht. Beim nächsten Besuch taucht derselbe Nutzer quasi wieder als »unbeschriebenes Blatt« auf. Im Firefox-Browser und in den anderen Standardbrowsern sieht es ähnlich aus.

Damit wird deutlich, wie beschränkt die Wirkung des »privaten Modus« wirklich ist. Auch gegenüber dem Arbeitgeber, dem Internet-Provider und dem Netzwerk-Administrator können sich Nutzer mit dem Inkognito-Modus nicht verstecken - und schon gar nicht vor dem Staat.

**Fazit:** Im Inkognito-Modus werden weder die Identität noch die Onlineaktivitäten des Nutzers verschleiert. Wer wirklich anonym surfen will, muss schon einen Tor-Browser nutzen. Auch sogenannte »Virtual Private Networks« (VPN) können die Privatsphäre des Nutzers schützen, indem sie seine Herkunft verschleiern und den Datenverkehr verschlüsseln.

## Browser im privaten Modus 2/3

### Was wird im Privaten Modus von Firefox nicht gespeichert?

- **Besuchte Seiten:** Die besuchten Seiten werden nicht in das Menü Chronik, in die Chronik im Bibliotheksfenster oder in die Auswahlliste der Adressleiste eingetragen.
- **Formular- und Suchfeldeinträge:** Keine der Eingaben in Textfelder auf Webseiten oder in die Suchleiste wird für die Formular-Autovervollständigung gespeichert.
- **Downloadliste:** Dateien, die man heruntergeladen hat, werden (auch nach dem Abschalten des Privaten Modus) nicht im Fenster »Alle Downloads anzeigen« angezeigt.
- **Cookies:** Cookies speichern Informationen über die besuchten Webseiten, beispielsweise Seiteneinstellungen und Anmeldestatus. Cookies können auch von Drittanbietern genutzt werden, um Ihre Online-Aktivitäten zu beobachten und diese über mehrere Webseiten hinweg zu verfolgen.

Cookies, die in privaten Fenstern gesetzt werden, bleiben vorübergehend im Speicher und zwar getrennt von den Cookies aus normalen Fenstern. Am Ende der privaten Sitzung werden diese Cookies gelöscht, nachdem das letzte private Fenster geschlossen wurde.

- **Zwischengespeicherte Webseiten und Seiten und Daten zur Offline-Verwendung:** Temporäre Dateien aus dem Internet (zwischengespeichert im Browser-Cache) und auch Daten, die von Webseiten für die Offline-Verwendung vorgesehen sind, werden nicht gespeichert.

### Was wird im Privaten Modus gespeichert

- Neue Zugangsdaten (Benutzernamen, Passwörter) und Lesezeichen, die man im Privaten Modus anlegt hat, werden gespeichert.
- Alle Dateien, die man im Privaten Modus heruntergeladen hat, werden gespeichert. Sie werden aber nicht im Downloadfenster des Browsers angezeigt.

Außerhalb des Privaten Modus kann man jederzeit beliebige Teile der von Firefox angelegten Surf-, Such- und Download-Chronik löschen, nachdem man eine oder mehrere Webseiten besucht hat (Menü: Einstellungen).

**Hinweis:** Für die anderen Internet-Browser dürfte vorgenanntes weitestgehend ebenfalls gültig sein.

Der private Modus kann in den meisten Web-Browsern leicht gefunden und aufgerufen werden. Noch schneller geht es über eine Tastenkombination:

#### Chrome und Safari:

- [Shift] + [Strg] + [N] **oder** [Strg] + [Shift] + [N]

#### Firefox und Edge:

- [Strg] + [Shift] + [P]

## Browser im privaten Modus 3/3

### Besuchte Websites verschleiern

Ein anderer Fall ist es, wenn Arbeitgeber das private Surfen am Arbeitsplatz erlauben, aber man selbst jedoch verhindern will, dass der Administrator anhand der IP-Adressen die Streifzüge durchs Internet verfolgen kann. Die im Folgenden beschriebenen Methoden kann man natürlich ebenfalls anwenden, um mit dem privaten Anschluss im Internet anonym zu bleiben. Eine einfache Lösung ist die Nutzung eines Proxy-Servers. Diese Server wurden früher als eine Art Cache benutzt und hielten häufig angesteuerte Webseiten lokal vor. Heute verwendet man sie in der Regel, um die eigene IP-Adresse und/oder den Standort gegenüber der besuchten Seite zu verschleiern. Wenn man einen Proxy-Server nutzt, sieht der Administrator lediglich, dass man die IP-Adresse des Proxy-Servers ansteuert, nicht aber, wie es danach weitergeht. Normalerweise stellt man den Proxy-Server zentral in Windows ein. Windows-Einstellungen öffnen: »Einstellungen« -> »Netzwerk und Internet« -> »Proxy« -> »Manuelle Proxyeinrichtung« -> Schalter »Proxyserver verwenden« auf »Ein« stellen und die IP-Adresse und den Port des Proxy-Servers dort eintragen. Anschließend noch die Checkbox »Proxyserver nicht für lokale Adressen (Intranet) verwenden« aktivieren und mit »Speichern« wird die Proxy-Umleitung aktiviert.

Im Internet findet man eine Vielzahl freier Proxy-Server, auf die man zugreifen kann.

### Fingerprinting - Die Alternative zu Cookies

Webseiten erkennen wiederkehrende Besucher an den Cookies, kleinen Dateien, die beim ersten Besuch auf dem eigenen Rechner gespeichert werden. Da sich Cookies jedoch einfach löschen lassen und viele Anwender die Annahme einfach verweigern, haben die Webseiten-Betreiber andere Methoden zur Identifikation entwickelt.

Beim Fingerprinting werden systematisch die vom Computer übermittelten Informationen analysiert und in einem digitalen Profil gespeichert. Hierbei unterscheidet man zwischen Browser-, Device- und Canvas-Fingerprinting.

Beim **Browser-Fingerprinting** fassen die besuchten Webseiten Informationen zum verwendeten Browser, der Version, den installierten Plug-ins, zur Sprache, Bildschirmauflösung, Zeitzone und weiteren Konfigurationsoptionen in einem Profil zusammen. All diese Informationen werden vom Browser freiwillig an die Webseite übermittelt, damit eine optimale Darstellung der Seiten entsteht.

Das **Device-Fingerprinting** wertet zusätzlich auch noch Informationen zum Betriebssystem, den installierten Schriften, der IP- und MAC-Adresse des Netzwerkadapters, zum Batteriestatus und dem Standort aus.

Beim **Canvas-Fingerprinting** wird in eine Webseite ein versteckter Text integriert. Je nach Browser und Konfiguration fällt die Darstellung geringfügig anders aus, was zur Identifikation des jeweiligen Computers genutzt werden kann.

Auf Seiten wie »Cover Your Tracks« (<https://coveryourtracks.eff.org>), Panopticlick (<https://panopticlick.eff.org/>) oder »Amiunique« (<https://amiunique.org/>) kann man testen, wie einzigartig die Konfiguration des Browsers ist. Schützen kann man sich vor Fingerprinting, indem man im Browser Javascript deaktiviert. Allerdings werden damit auch einige Webseiten nicht mehr korrekt angezeigt. Für Chrome, Firefox, Edge und Opera ist das Add-on »Privacy Badger« erhältlich, der das Tracking von Webseiten-Besuchern, also das Sammeln von Informationen, sowie das Fingerprinting erkennt und blockiert.

# Wie funktioniert TLS - Transport Layer Security? 1/7

## Wofür ist eine sichere Verbindung wichtig?

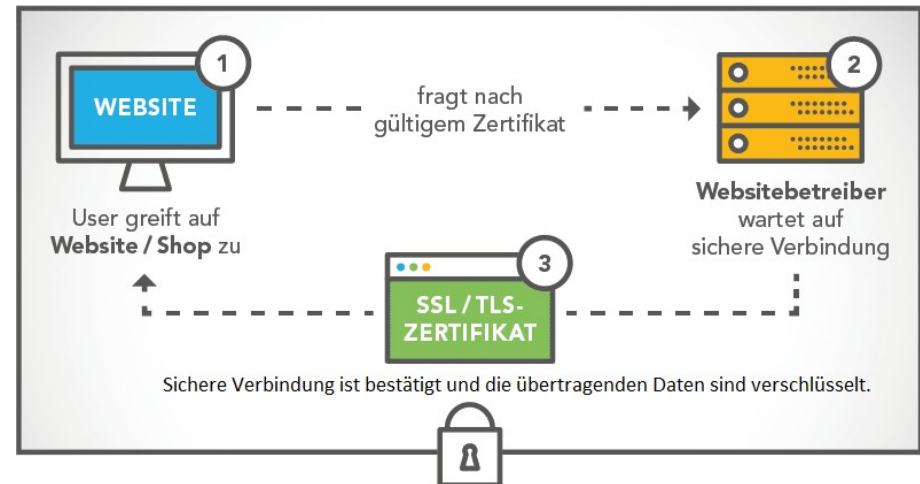
Bei der Nutzung von Webseiten oder Onlineshops werden Informationen (Daten) im Internet zwischen dem Webserver und dem aufrufendem Computer ausgetauscht. Dies erfolgt normalerweise unverschlüsselt im Textformat. Das bedeutet, jeder im gleichen Netzwerk könnte die Informationen mitlesen und verändern, ohne dass der Absender oder der Empfänger etwas davon mitbekommt. Das ist besonders dann brisant, wenn es sich um sensible Daten handelt. Eine einfache Möglichkeit das Mitlesen bzw. die Veränderung (Man-in-the-Middle-Angriff) zu verhindern, ist eine verschlüsselte Verbindung. Diese verifiziert den Absender/Empfänger der Daten. Ohne den passenden Schlüssel können die Informationen dann nicht mitgelesen werden. Somit wird der Angreifer als nicht bestimmungsgemäßer Empfänger erkannt.

## Was ist TLS/SSL?

TLS – Transport Layer Security (Transportschichtsicherheit) ist ein Protokoll zur sicheren Datenübertragung im Internet (Standard seit 1999). Oft fällt in diesem Zusammenhang auch die ältere Bezeichnung SSL – Secure Sockets Layer. SSL und TLS sind standardisierte Richtlinien zur sicheren Datenübertragung. Am häufigsten wird TLS für das HTTP-Protokoll verwendet. Dieses kontrolliert den Aufruf von Webseiten. Um TLS erweitert heißt es dann **HTTPS**. Aber auch andere Protokolle sind um TLS erweiterbar und finden Anwendung, z.B. beim Austausch von E-Mails. Aktuell bevorzugte TLS-Versionen sind die Versionen 1.2 und 1.3. Die älteren Versionen führen zu einer Sicherheitswarnung.

## Wie funktioniert die verschlüsselte Übertragung?

TLS verschlüsselt die Daten und zertifiziert den Endpunkt der Verbindung. Diese Zertifizierung geschieht über ein Handshake-Verfahren. Dieses generiert beim Absender eine zufällige Zeichenkette und sendet diese zusammen mit einigen Informationen über die Verschlüsselung an den Empfänger.



Der Empfänger identifiziert sich nun gegenüber dem Absender mit einem X.509 Zertifikat. Der Empfänger nimmt dann das X.509 Zertifikat und prüft ob es für ihn gültig ist. Fällt die Prüfung negativ aus, wird die Verbindung unterbrochen und eine Warnmeldung wird ausgegeben.

Ein aktives Zertifikat erkennt man an dem grünen Schloss und der Zeichenkette `https://` vor der Internetadresse in der Browser-Adresszeile.

Technisch gesehen spielt es dabei keine Rolle, welcher Zertifikatstyp verwendet wird. Ein gekauftes Zertifikat wird nur zusätzlich von einer Firma (Root Agency) signiert (Zertifizierungsstellen: Symantec, GeoTrust, Thawte, RapidSSL, Comodo, DigiCert, GlobalSign, AlphaSSL und EuropeanSSL, ...).

Man kann Zertifikate auch selbstständig ausstellen. Diese selbstsignierten Zertifikate haben den Nachteil, dass diese Zertifikate im Internet-Browser als nichtvertrauenswürdig markiert werden, da die Root-Zertifikate nicht im Browser der Webseiten-Besucher hinterlegt sind. Deshalb eignet sich ein selbst erstelltes SSL/TLS-Zertifikat nur für den internen Gebrauch bei kleineren Firmen und im privaten Bereich.



# Wie funktioniert TLS - Transport Layer Security? 2/7

## Welche Daten sind besonders schützenswert?

Bei Webseiten sichert man mit TLS die Übertragung zwischen Browser und Webserver. Vor allem im E-Commerce, wo vertrauliche und sensible Daten übertragen werden, ist der Einsatz eines TLS-Zertifikats unumgänglich.

Sensible Daten, die häufig durch eine TLS-Verschlüsselung geschützt werden, sind zum Beispiel:

- Registrierungsdaten: Name, Adresse, E-Mail-Adresse, Telefonnummer
- Log-in Daten: E-Mail-Adresse und Passwort
- Zahlungsinformationen: Kreditkartennummer, Bankverbindungen
- Eingabeformulare
- von Personen hochgeladene Dokumente

Mit TLS stellt man sicher, dass die Kommunikation weder mitgelesen noch manipuliert werden kann und persönliche Daten damit nicht in falsche Hände geraten.

## Welche Vorteile bringt die Verwendung von TLS?

- Datenschutz und Sicherheit für Kunden und Partner
- Risiko von Datendiebstahl und Datenmissbrauch wird vermindert
- positiver Rankingfaktor bei den Suchmaschinen
- Zertifikat ist für die Nutzer (Schloss in der Adresszeile) leicht erkennbar und weckt Vertrauen
- Schnellere Ladezeiten: die Technologien wie HTTP/2 und QUIC werden von Browsern nur über eine verschlüsselte Verbindung unterstützt

## Unterschiede zwischen freien und kostenpflichtigen Zertifikaten?

Seit ihrer Einführung im Jahr 2015 steht mit den Zertifikaten der Non-Profit-Organisation **Let's Encrypt** eine kostenfreie, einfach

zu installierende Alternative zu den klassischen kostenpflichtigen Zertifikaten zur Verfügung. Der größte Kritikpunkt an den freien Zertifikaten besteht jedoch darin, dass diese Zertifikate immer häufiger von Kriminellen genutzt werden, um Phishing-Webseiten vertrauenswürdiger erscheinen zu lassen. Nutzern dieser Webseiten, wird damit auf dem ersten Blick, eine scheinbar sichere Webseite präsentiert.

**Hinweis:** Anfang März 2020 musste Let's Encrypt mehr als drei Millionen der aktiven SSL/TLS-Zertifikate zurückziehen. Der Grund dafür war ein Fehler in der von Let's Encrypt verwendete Software bei der Überprüfung der CAA-Records (Certification Authority Authorization). Dieser Fehler machte es in der Theorie möglich, sich Zertifikate für fremde Domains erstellen zu lassen. Die einzige Lösung für die Betroffenen war die Neuerstellung eines Zertifikates.

## Unterschiede - kostenfreie und kostenpflichtige TLS-Zertifikate:

- **Gültigkeit:** Die meisten kostenpflichtigen Zertifikate sind für 12 bis 24 Monate gültig. Freie Zertifikate laufen bereits nach 90 Tagen ab.
- **Verwaltung:** Bei einem kostenpflichtigen Anbieter erhält man zusätzlich zu dem Zertifikat das passende Werkzeug, um dieses zu verwalten.
- **Domain-Zugehörigkeit:** Ein kostenloses SSL/TLS-Zertifikat lässt sich immer ausschließlich für eine einzelne Domain erzeugen, an die es dann gebunden ist. Wer sich für Paid SSL/TLS entscheidet, profitiert dagegen von domainübergreifenden Zertifikaten, die sich problemlos für mehrere Webprojekte verwenden lassen.
- **Präsentation im Adressfeld:** Schützt man ein Webprojekt mit einem kostenpflichtigen Zertifikat, kann man den aktiven Schutz und den Firmennamen in der Browserzeile anzeigen lassen. Bei kostenfreien SSL/TLS wird die Webseite zwar als HTTPS-Projekt gekennzeichnet, eine Individualisierung ist aber nicht möglich.

# Wie funktioniert TLS - Transport Layer Security? 3/7

## Die 4 Phasen des TLS-Handshakes

### Phase 1

=====

=

#### CLIENT

- ein Client möchte eine Verbindung mit einen Server aufbauen
- der Client generiert nun eine 28 Byte große **Zufallszahl** und hängt an dieser Zufallszahl noch einen 4 Byte langen **Zeitstempel**
- das Ergebnis aus Zufallszahl und Zeitstempel wird mit **weiteren Informationen** (TLS-Version, Session-ID, unterstützte Algorithmen für den Schlüsselaustausch, die Verschlüsselung und die Authentifizierung) über den Client an den Server geschickt
- aus diesen Informationen kann das sogenannte **Pre-Master-Secret** gebildet werden, um sogenannte Replay-Angriffe zu verhindern.

**Hinweis:** Ein Replay-Angriff ist eine kryptoanalytische Angriffsform auf die Authentizität von Daten in einem Kommunikationsprotokoll. Hierbei sendet der Angreifer zuvor aufgezeichnete Daten, um etwa eine fremde Identität vorzutäuschen.

#### SERVER

- der Server macht erstmal genau das Gleiche wie der Client
- er generiert ebenfalls eine Zufallszahl und schickt diese zusammen mit den Kryptoinformationen (verwendete Algorithmen, ...) an den Client
- In der 1. Phase des TLS-Handshakes findet der Austausch noch unverschlüsselt statt, d.h. es besteht noch keine wirkliche Sicherheit.

- Um eine sichere Verbindung zu ermöglichen, wird wie bei der Ende-zu-Ende-Verschlüsselung auf beiden Seiten ein mathematisch zusammengehörendes Schlüsselpaar bestehend aus einem öffentlichen und einem privaten Schlüssel generiert.

### Phase 2

=====

#### SERVER

- Der Server sendet nun ein Zertifikat mit seinem öffentlichen Schlüssel an den Client und fragt dem Client nach einen ebensolchen Zertifikat.

#### CLIENT

- Der Client überprüft jetzt u.a. mithilfe kryptografischer Verfahren die **Authentizität** bzw. die **Integrität** des empfangenen Zertifikates mit dem öffentlichen Schlüssel des Servers. Dabei geht der Client die gesamte **CA-Kette** (Kette der Certification Authorities, sprich: die Kette der Zertifizierungsstellen, die dem Internet-Browser bekannt sind) durch. Wenn alles in Ordnung ist, endet Phase 2. In dieser Phase wird immer noch keine Verschlüsselung verwendet.

### Phase 3

=====

#### CLIENT

- In dieser Phase sendet der Client sein Zertifikat mit seinem öffentlichen Schlüssel an den Server, der das ihm gesendete Zertifikat ebenfalls überprüft. Der Client berechnet nun ein sogenanntes **Pre-Master-Secret**.

# Wie funktioniert TLS - Transport Layer Security? 4/7

- Das ist einfach nur wieder eine Zufallszahl. Wird der RSA-Algorithmus für die Verschlüsselung verwendet, verschlüsselt der Client dieses Pre-Master-Secrets mit dem öffentlichen Schlüssel des Servers. Das ist der öffentliche Schlüssel den der Server in Phase 2 an den Client gesendet hat. Der Server kann mit seinem privaten Schlüssel die verschlüsselte Übermittlung des Pre-Master-Secrets vom Client entschlüsseln und so kennen beide Parteien dieses Secret. **Hinweis:** Alternativ kann man hier auch den Diffie-Hellman-Schlüsselaustausch verwenden, um ein gemeinsames Pre-Master-Secret zu generieren.
- Um sicherzustellen, dass sich während dieses Prozesses kein Angreifer einschleichen kann, nimmt der Client alle bisher ausgetauschten Informationen und bildet darüber einen sogenannten Hashwert. Ein Hashwert ist das Ergebnis einer mathematischen Einwegfunktion, d.h. einer Funktion, mit der man den Funktionswert  $f(x)=y$  sehr schnell ermitteln kann, aber das zu einem  $y$  passende  $x$  in angemessener Zeit zu berechnen, um diesen Hashwert zu fälschen, ist praktisch nicht möglich. Das Ergebnis schickt der Client, verschlüsselt mit seinem privaten Schlüssel, an den Server.

## SERVER

- Der Server kann den verschlüsselten Hashwert mit dem öffentlichen Schlüssel des Clients, den er am Anfang der Phase 3 erhalten hat, wieder entschlüsseln. Da er ebenfalls über alle ausgetauschten Informationen verfügt, kann er den Hashwert ebenfalls berechnen. Kommt bei Berechnung nicht dasselbe Ergebnis heraus, wird die Verbindung abgebrochen. Ist alles in Ordnung, dann berechnen Server bzw. Client aus dem **Pre-Master-Secret** das sogenannte **Master-Secret**, also ein gemeinsam geteiltes Geheimnis, mit dem in der nächsten Phase die symmetrisch Verschlüsselung durchgeführt wird.

## Phase 4

=====

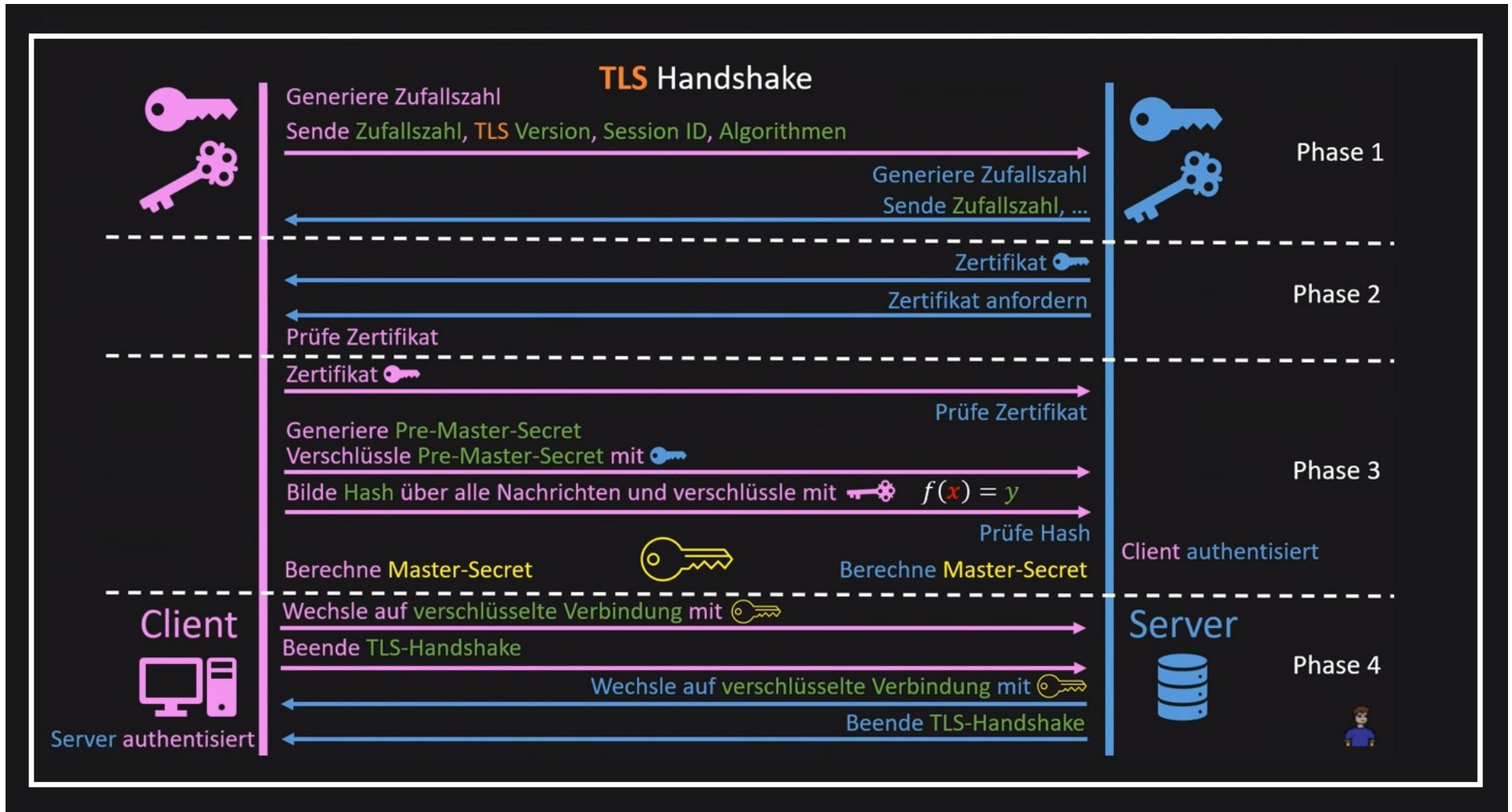
- Damit endet in Phase 4 der TLS-Handshake von der Seite des Clients und des Servers.

## Anmerkung:

Bei den Verschlüsselungsverfahren unterscheidet man zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren. Beim Austausch von öffentlichen und privaten Schlüssel spricht man von asymmetrischen Verschlüsselungen. Diese Verfahren haben den Nachteil, dass sie viel Rechenzeit in Anspruch nehmen. Deshalb wird nach dem sicheren Schlüsselaustausch, mit einem symmetrischen Verfahren weiter gearbeitet. Bei einem symmetrischen Verfahren, erfolgt die Ver- und Entschlüsselung mit demselben Schlüssel - dem Master-Secret. Von diesem Zeitpunkt ab, können beide Kommunikationspartner mit ihrem gemeinsamen »Geheimnis« während einer Sitzung (Session) sicher kommunizieren.

**Diffie-Hellman-Merkle-Schlüsselaustausch:** Das besondere an Diffie-Hellman-Merkle ist, dass nicht der geheime Sitzungsschlüssel, sondern nur das Ergebnis einer Rechenoperation übertragen wird. Bei dieser Rechenoperation geht man von der Annahme aus, dass Potenzieren von Zahlen leicht, aber den diskreten Logarithmus zu berechnen schwer ist. Solange die notwendige Rechenleistung fehlt und es keine Vereinfachung zum Lösen des Diskreten-Logarithmus-Problems gibt, so lange ist dieses Verfahren sicher.

**RSA:** RSA (Rivest–Shamir–Adleman) ist ein asymmetrisches kryptographisches Verfahren. Es verwendet ein Schlüsselpaar, bestehend aus einem privaten Schlüssel, der zum Entschlüsseln oder Signieren von Daten verwendet wird und einem öffentlichen Schlüssel, mit dem man verschlüsselt oder Signaturen prüft. Der private Schlüssel wird geheim gehalten und kann nicht mit realistischem Aufwand aus dem öffentlichen Schlüssel berechnet werden.



## Welche TLS-Versionen unterstützt das aktuelle System?

Tastenkombination: [Win] + [Pause] -> Startseite der Systemsteuerung -> Netzwerk und Internet -> Internetoptionen -> Tab: Erweitert -> zum Punkt Sicherheit scrollen: TLS 1.0, 1.1, 1.2, 1.3

Werden hier alle TLS-Versionen deaktiviert (Checkbox), können beim Aufruf des Internet-Explorers oder des Edge-Browsers viele Webseiten nicht mehr aufgerufen werden.

# Wie funktioniert TLS - Transport Layer Security? 6/7

## Zertifikate

Durch das Zertifikat authentisiert sich der Empfänger gegenüber dem Sender bzw. der Server gegenüber dem Client. Gleichzeitig kann der Client das Zertifikat überprüfen (Validierung) und somit die Vertrauenswürdigkeit feststellen (Authentizität).

Die Zertifikate koppeln eine Identität an einen öffentlichen Schlüssel, der zur Authentifizierung und Verschlüsselung verwendet wird. Es gibt insgesamt drei Zertifikatstypen, die sich durch einen unterschiedlichen Prüfaufwand bei der Zertifizierung unterscheiden.

- Domain-Validated-Zertifikat (DV)
- Organisation-Validation-Zertifikat (OV)
- Extended-Validation-Zertifikat (EV)

Die häufigsten Zertifikate sind DV- und EV-Zertifikate. Während man DV-Zertifikate schon für wenige Euro oder sogar kostenlos bekommen kann, kommen wegen des erheblichen Prüfaufwands bei EV-Zertifikaten mehrere hundert oder sogar tausend Euro zusammen. Allerdings kann man bei EV-Zertifikaten von einer höheren Vertrauenswürdigkeit ausgehen.

Welches Zertifikat bei einer verschlüsselten Verbindung zum Einsatz kommt, ist als Nutzer nicht so leicht zu erkennen. Meist ist eine verschlüsselte Verbindung in einem Client nur an einem Schloss-Symbol zu erkennen. Aber nicht, um welches Zertifikates sich handelt. Zertifikate werden von einer Zertifizierungsstelle bzw. Certification Authority (CA) ausgestellt und beglaubigt.

## Certificate Authority (CA) / Zertifizierungsstelle

Weltweit gibt es weit über 700 Zertifizierungsstellen. Jeder, der sichere Dienste im Internet anbietet, lässt sich die Echtheit

von digitalen Schlüsseln und Signaturen von einer Certificate Authority bestätigen.

Dazu lässt sich ein Unternehmen oder eine Organisation von einer Certificate Authority nach einer Überprüfung ein digitales Zertifikat ausstellen. Das kann dann zum Beispiel auf einem Webserver hinterlegt werden. Mit diesem Zertifikat weist sich die Webseite gegenüber den zugreifenden Browsern als Eigentümer aus. Der Browser des Besuchers überprüft die Angaben im Zertifikat und fragt bei Bedarf bei der ausstellenden Zertifizierungsstelle nach, ob das Zertifikat gültig ist.

Auf diese Weise können zum Beispiel die Kunden einer Bank davon ausgehen, dass sie tatsächlich mit dem Server der Bank verbunden sind und dass der Datenaustausch verschlüsselt erfolgt.

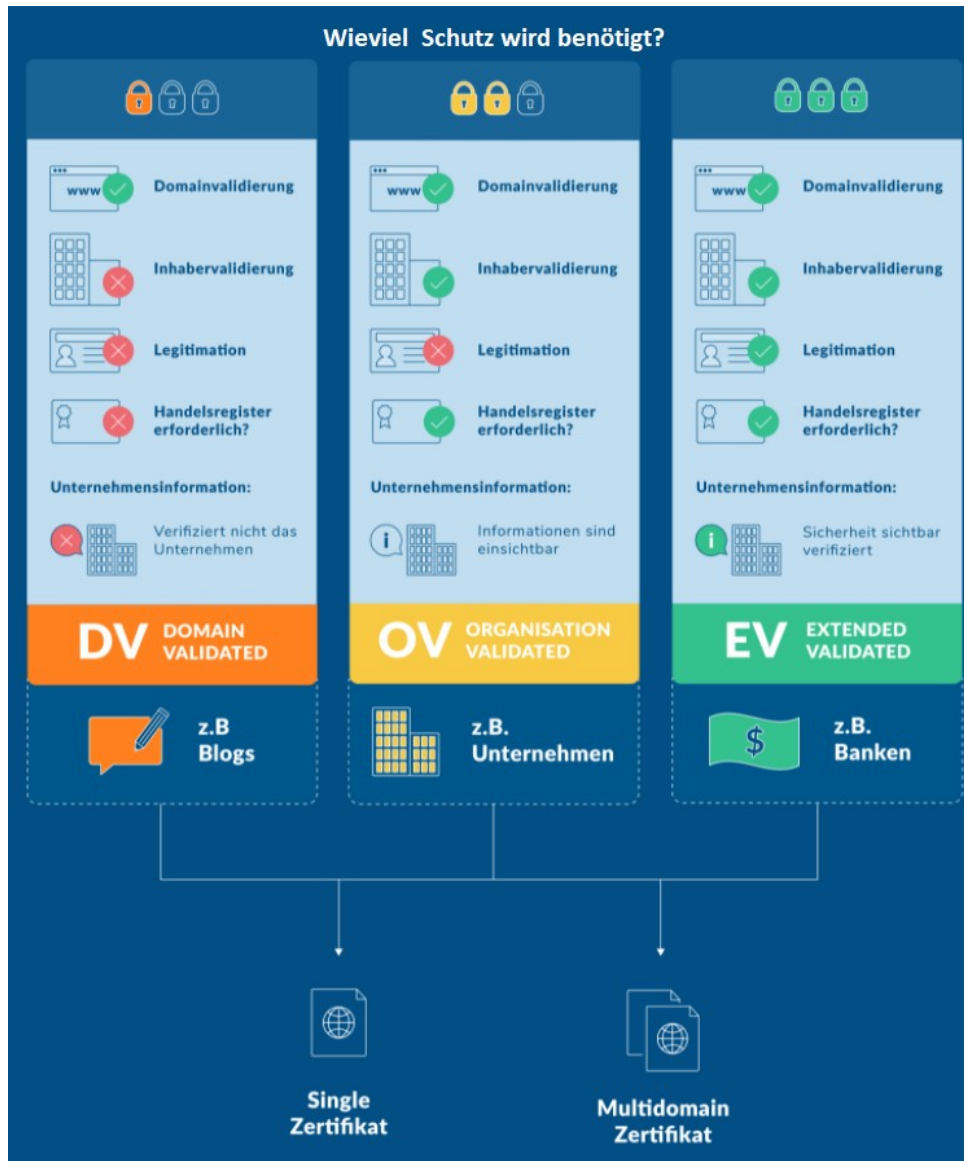
Auch die Zertifizierungsstelle besitzt ein Zertifikat, indem sich deren öffentlicher Schlüssel befindet. Dabei handelt es sich um ein Wurzel- bzw. Stammzertifikat, das in Browsern und Betriebssystemen hinterlegt ist. Diesen Stammzertifikaten wird in der Regel bedingungslos vertraut.

Das Geschäftsverhältnis zwischen Zertifizierungsinstanz und den Unternehmen, aber auch zu den Internet-Nutzern, beruht auf Vertrauen. Daher muss eine CA alles dafür tun, dass die Prüfprozesse ordnungsgemäß funktionieren und sicher vor Manipulationen sind.

Leider ist es schon vorgekommen, dass Eindringlinge auf interne Server von Zertifizierungsstellen zugegriffen und sich dort Zertifikate generiert haben. Wird ein solches Zertifikat verwendet, kann ein Internet-Nutzer einen Betrug nicht überprüfen. Und ein Unternehmen, das Dienste im Internet anbietet, kann genauso wenig feststellen, ob eine Zertifizierungsstelle unberechtigt Zertifikate ausgestellt hat. Nur die CA kann betrügerische Zertifikate sicher erkennen.



# Wie funktioniert TLS - Transport Layer Security? 7/7



## Das TLS-Zertifikat einbinden

Wenn man das TLS-Zertifikat von einem Anbieter erworben hat, erhält man in der Regel von diesem die Anleitung, wie es implementiert wird. Die Schritte sind aber immer ähnlich:

- Installation des TLS-Zertifikates auf den Server. Wenn man keinen dedizierten Server verwendet, bieten manche Webhoster mit wenigen Klicks eine Implementierung des TLS-Zertifikates an. Die Art und Weise der Implementierung hängt vom Servertyp (Apache oder Exchange) ab.
- Im nächsten Schritt, muss man auswählen, welche Seiten, Subdomains oder Domains mit dem Zertifikat geschützt werden sollen.
- Nach der Installation, sollten die geschützten Webseiten mit verschiedenen Browsern aufgerufen werden. Auch sollte man überprüfen ob noch Webseiten-Elemente ohne TLS-Verschlüsselung geladen werden. Mit verschiedenen Online-Tools, wie  
**SSL Labs**: <https://www.ssllabs.com/ssltest/>  
**SSL Checker**: <https://www.thesslstore.com/ssltools/ssl-checker.php>  
**Geekflare**: <https://gf.dev/tls-test>  
**Wormly**: [https://www.wormly.com/test\\_ssl](https://www.wormly.com/test_ssl)  
**DigiCert**: <https://www.digicert.com/help/>  
 kann man prüfen, ob die TLS/SSL-Verbindung korrekt implementiert wurde.

## Checkliste - nach erfolgter Umstellung

- Nach der Installation des TLS-Zertifikats, muss eine 301-Weiterleitung von den Webseiten mit **http** auf **https** geändert werden.
- Die Internen Links auf den Webseiten sind ebenfalls anzupassen, damit die Verbindungen sicher werden.
- Die in Programmen hinterlegten Links zur Domain sind anzupassen.

# VPN-Kaskaden oder Multi-Hop VPN 1/5

VPN-Services versuchen die Nutzer durch technische Funktionen vor Überwachung und Verfolgung im Internet zu schützen. Normale VPN-Service bietet dabei den verschlüsselten Zugang (VPN-Tunnel – Datenverkehr fließt ohne Einsehbarkeit für Dritte) zu eigenen VPN-Servern an, welche in verschiedenen Ländern betrieben werden. Die Daten welche zwischen dem Endgerät (VPN-Client) und dem VPN-Service (VPN-Server) übertragen werden sind dabei verschlüsselt. Über den VPN-Service wird dabei auch die benutzte IP-Adresse des Nutzers nach Außen hin verändert und seine eigene IP-Adresse erscheint in der Kommunikation mit Webseiten und Webservices nicht mehr.

Allerdings ist es so, dass weiterhin der eigene Internetanbieter die übertragenen Daten zumindest in dem Ausmaß erkennen kann, zu welcher IP-Adresse die Daten eines Nutzers gesendet werden. Also der Internetanbieter kann anhand der Header-Daten der Datenpakete erkennen, zu welchem VPN-Server man eine Verbindung aufgebaut hat.

Dies ist im Regelfall kein Problem für die eigene Sicherheit, jedoch gibt es auch technische Lösungen die eine weitere Verschleierung ermöglichen. Dabei werden die Daten zwar wie gewohnt an einen VPN-Server gesendet, dieser sendet die Daten aber verschlüsselt an einen weiteren VPN-Server weiter. Dadurch wird für die Beobachter der eigenen Daten es zunächst Mal unmöglich, zu erkennen, welcher VPN-Server durch einen Nutzer verwendet wird um Aktivitäten im Internet durchzuführen. Man nennt diese Technik: »VPN-Kaskadierung« oder auch »Multi-Hop VPN«.

## Die Funktionsweise einer VPN-Kaskade (Multi-Hop VPN)

Um VPN-Kaskaden besser verstehen zu können, muss man sich erst einmal die technische Umsetzung einer normalen VPN-Verbindung ansehen. Dabei werden die Daten durch einen VPN-Client zu einem VPN-Server verschlüsselt übertragen. Der VPN-Server kommuniziert dann mit den Zielen - mit seiner eigenen IP-Adresse (Identität).



**Hinweis:** Die einfache VPN-Verbindung ist der Standard bei allen VPN-Service-Anbietern.

# VPN-Kaskaden oder Multi-Hop VPN 2/5

## Einfache VPN-Kaskaden

Viele Anbieter, welche derartige Kaskaden der Verbindungen anbieten, haben feste, statische Routen für die Nutzer eingerichtet. Verbindet man sich zu einem VPN-Server »A«, dann werden die Daten immer über einen weiteren VPN-Server »B« weitergeleitet. Das ist schon ein verbesserter Schutz, da dabei die Überwachung bereits mehr als ein VPN-Standort überwachen müsste.

### Einfache VPN-Kaskaden (Double-VPN)

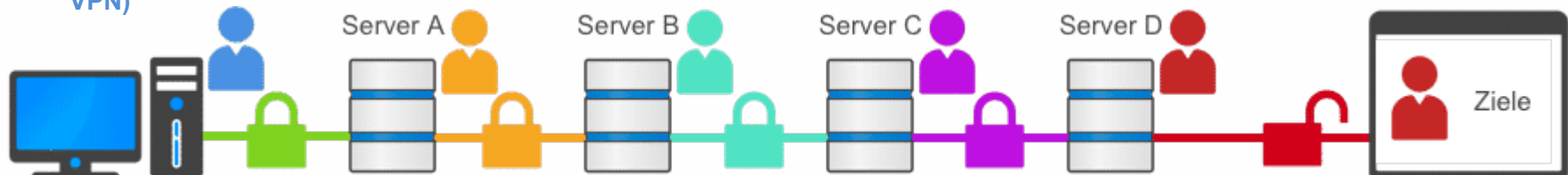


**Hinweis:** Einfache VPN-Kaskaden (feste Routen) werden von den folgenden Anbietern angeboten: **NordVPN**, **CyberGhost VPN**, **ProtonVPN**, **Surfshark**, **PureVPN** (letzteren Anbieter nur zu Testzwecken benutzen, wahrscheinlich protokolliert der Anbieter die Aktivitäten der Nutzer)

## Mehrfache individuelle VPN-Kaskaden

Noch sicherer ist es allerdings, wenn die VPN-Kaskaden selbst erstellt werden können. Die Nutzer können zu Beginn selbst einer Verbindung festlegen, über welche Standorte die Verbindungen geführt werden soll. Dabei kann man bei einigen Anbietern bis zu 4 verschiedene hintereinander geführte Möglichkeiten auswählen.

### Mehrfache und individuelle VPN-Kaskaden (Multi-Hop VPN)



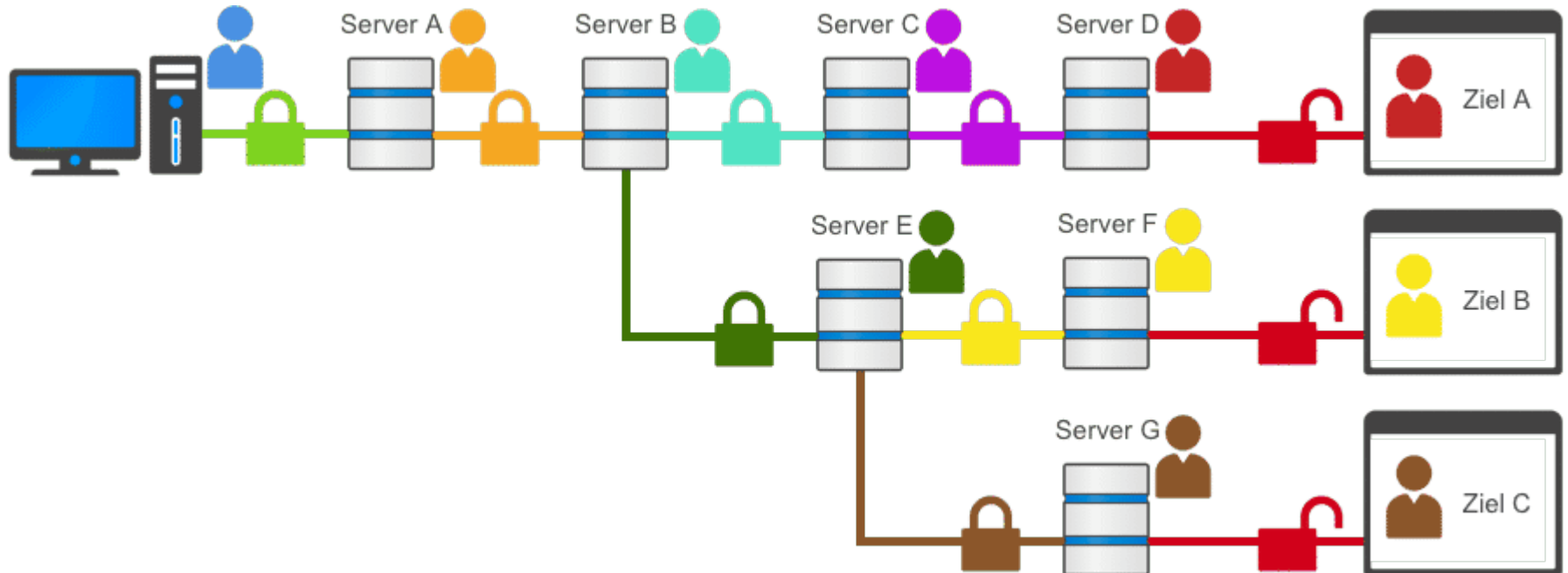
**Hinweis:** Mehrfache und individuelle VPN-Kaskaden werden von den folgenden Anbietern angeboten: **ZorroVPN**, **Perfect-Privacy VPN**, **CyberGhost VPN**

## VPN-Kaskaden oder Multi-Hop VPN 3/5

### Dynamische Kaskadierung oder Neurorouting

Wer das ganze auch noch dynamisch, also abhängig vom Ziel der Daten über ein VPN-Netzwerk leiten möchte, der kann mit »Neurorouting« von »Perfect-Privacy VPN« sogar dies ermöglichen. Dabei nimmt jedes einzelne Datenpaket das über einen VPN-Server gesendet wurde einen eigenen Weg bis zum Ziel und das über mehrre Standorte innerhalb des mittels verschlüsselt abgesicherten Netzwerkes aus VPN-Servern. Damit ist selbst nicht mehr vorhersehbar, welchen Weg oder über welche VPN-Server Daten gesendet werden und man reduziert damit auch die Übertragungswege der Daten welche über ungesicherte Verbindungen laufen auf ein Minimum.

### Dynamische Kaskadierung (Neurorouting)



**Hinweis:** Mehrfache dynamische VPN-Kaskaden (Neurorouting) wird von folgenden Anbieter angeboten: **Perfect-Privacy VPN**

# VPN-Kaskaden oder Multi-Hop VPN 4/5

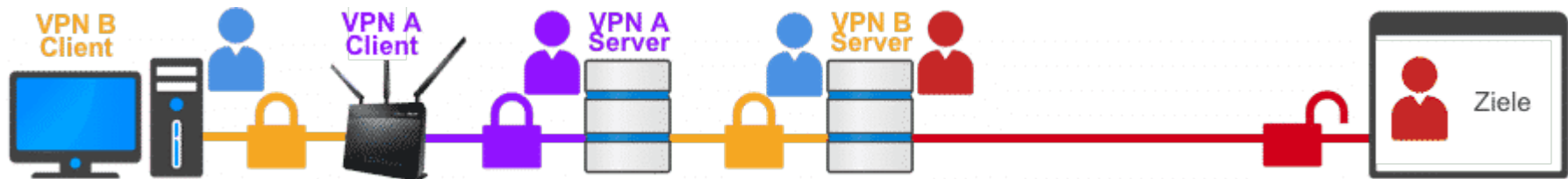
## Zwei VPN-Verbindungen parallel zu verwenden ist keine Kaskade!

Einige haben möglicherweise die Idee, einfach zwei verschiedene VPN-Services parallel oder ineinander verschachtelt zu verwenden und erwarten dabei den selben Schutz. Das ist aber ein Trugschluss und im Grunde bewirkt es einige erhebliche Probleme, weshalb in diesem Fall einfache VPN-Verbindungen noch deutlich stabiler und sicherer sind.

Das Szenario bei dem man zwei VPN-Verbindungen ineinander verschachtelt werden, bietet beiden VPN-Services Zugriff auf Daten welche eine Identifikation der Nutzer ermöglichen kann. Dabei ist es so, dass die zweite »innenliegende Verbindung« auch dem ersten VPN-Tunnel durch die verwendeten Header entsprechende Informationen zur Verfügung stellt. Angriffe auf die »äußere Verbindung« lassen sich zudem sehr einfach durchführen und diese Verbindung auch zum kollabieren bringen. Was die Folge hat, dass die »innenliegende VPN-Verbindung« durch einen plötzlichen Adresswechsel ebenso zusammenbricht. In diesem Fall, können aber getroffene Regeln z.B. KillSwitch nicht sofort eine Übermittlung der eigenen IP-Adresse verhindern. Das bedeutet, dass durch zwei ineinander liegende Verbindungen die Stabilität der Verbindung und auch die Angriffsmöglichkeiten sich deutlich vergrößern. Vorhandene Schutzmaßnahmen wie **KillSwitch** werden dabei kurzfristig wirkungslos und offenbaren damit die Identität der Nutzer.

**Hinweis:** KillSwitch ist ein Notausschalter und verhindert, dass Rechner Daten übertragen, bis die unterbrochene sichere, verschlüsselte Verbindung zum VPN-Server wiederhergestellt ist.

**Warnung:** Zwei VPN-Verbindungen parallel zu verwenden ist keine Kaskade!



**Hinweis:** Eine verschachtelte Verbindung kann ohne auffällige Probleme funktionieren, führt aber in jedem Fall nicht dazu einen verbesserten Schutz vor einer gezielten Ausforschung zu erlangen. Einfache Angriffs-Methoden lassen dabei eine Korruption beider Verbindungen und eine eindeutige Identitätsfeststellung zu. Daher sind diese Methoden zu vermeiden!

Die Verwendung von verschachtelten VPN-Verbindungen hat deutliche Nachteile und ist auch technisch gesehen relativ einfach zu korrumpieren. Der erwünschte Sicherheitsvorteil wird dadurch vollständig aufgehoben und fällt damit sogar hinter einfachen VPN-Verbindungen, aufgrund der Instabilität der Verbindungen zurück.



# VPN-Kaskaden oder Multi-Hop VPN 5/5

## Vorteile der VPN-Kaskaden

Wer VPN-Kaskaden nutzt, der muss sich im Klaren sein, dass das Senden der Daten über mehrere Standorte auch eine Auswirkung auf die erreichbare Geschwindigkeit haben wird. Da die Daten einen längeren Weg bis zum Ziel zurücklegen werden. Allerdings bieten Kaskaden auch einige technische Vorteile, welche gerade bei der Überwachung im Internet wirkungsvoll sein können.

- Für den Internetanbieter ist zwar klar, zu welchen VPN-Server man seine Daten sendet, aber nicht mehr über welchen VPN-Server man das Internet verwendet.
- Überwachung und Verfolgung durch international agierende Geheimdienste wird drastisch erschwert oder unmöglich gemacht. Da diese nicht in Echtzeit mehrere Standorte weltweit und synchron überwachen können. Im Falle von »dynamischen VPN-Kaskaden« ist es auch nicht vorhersehbar über welchen Weg die eigenen Daten das Netzwerk verwenden.
- Kaskaden können bei einer gezielten Überwachung einzelner Personen/Geräte eingesetzt werden, um weiterhin unbeobachtet Daten senden oder erhalten zu können.

## Nachteile von VPN-Kaskaden

- Große Datenmengen werden spürbar langsamer übertragen werden, was auch bedeutet, dass es nicht für Anwendungen wie Torrent oder Filesharing ideal ist. Man braucht dafür aber auch keine VPN-Kaskade verwenden, da dort keine internationale Überwachung eines einzelnen stattfinden wird.
- Dynamische Kaskaden können dazu führen, dass eine Webseite oder ein Webservice durch unterschiedliche IP-Adressen zur selben Zeit genutzt werden und können dazu führen, dass diese Dienste damit nicht nutzbar sind.

## Zusammenfassung

Kaskadierte VPN-Verbindungen sind über mehrere Standorte eine deutliche technische Verbesserung zum Schutz vor einer gezielten Verfolgung und auch Überwachung im Internet. Man muss aber auch erkennen, dass diese Maßnahmen einige Nachteile im Bezug auf die Reaktionszeiten und auch Geschwindigkeit der Datenübermittlung mitbringen. Nur wenige Nutzer werden diese Art von Schutzmaßnahmen tatsächlich benötigen, auch wenn es den Behörden damit unmöglich gemacht wird Aktivitäten zu erfassen oder zu überwachen. Wer denkt, dass er diese Art der technischen Lösung zum eigenen Schutz benötigt, sollte sich dazu im Klaren sein, dass es verschiedene Arten des Schutzes gibt, welche sich auch deutlich in ihren Möglichkeiten unterscheiden.

# VPN-Dienst Surfshark

## Surfshark: Mit dem hochwertigem VPN-Dienst sicher online surfen

Mit Surfshark kann man mittels verschlüsselter Verbindungen anonym und sicher im Internet surfen. Surfshark ist ein weltweit vertretener VPN-Dienst (2021: über 3200 Servern in 65 Länder). Surfshark bietet seinen VPN-Dienst mit Client-Software für Windows, macOS und Linux (Ubuntu, Debian, Konsolenanwendung in einem Terminalfenster) sowie Apps für Mobilgeräte mit Android oder iOS an. **Hinweis:** Surfshark ist als Unternehmen auf den Britischen Jungferninseln registriert.

Außer einer VPN-Lösung für diese Plattformen, die **alle** Internet-Aktivitäten schützt, gibt es bei Surfshark auch Browser-Erweiterungen für Chrome und Firefox. Sie leiten nur die Web-Aktivitäten mit dem jeweiligen Browser durch das VPN. Die Daten aller anderen Programme laufen ohne VPN über eine normale Internet-Verbindung.

Den digitalen Fußabdruck vermeiden: Das möchte Surfshark den Benutzern so einfach wie möglich machen. Die Suchanfragen werden über die Server des Unternehmens weitergeleitet, sodass die wahre IP-Adresse verschleiert wird. Dadurch hat man unter anderem die Möglichkeit, diverse Ländersperren (Geoblocking) zu umgehen.

Bei Surfshark gilt nach eigener Darstellung eine »strikte No-Logs-Richtlinie«, es werden also keine Verbindungs- oder Aktivitätsprotokolle gespeichert. Allerdings werden in der Android-App laut Analyse durch »Exodus Privacy« vier Tracker eingesetzt. Zu den drei Google-Trackern kommt noch der des US-amerikanischen Datensammlers »AppsFlyer«. Es sollen jedoch nur anonymisierte Nutzungsdaten für statistische Zwecke erhoben werden.

Surfshark hat 2018 das Berliner Sicherheitsunternehmen »Cure53« mit einem Audit beauftragt, bei dem die **Browser-Erweiterungen** für Firefox und Chrome untersucht wurden. Zwei dabei aufgespürte Schwachstellen hat Surfshark umgehend beseitigt.



Ansonsten zeigten sich die Pentester von »Cure53« mit der Sicherheit der Browser-Erweiterungen zufrieden. Auch das AV-Test Institut hat Surfshark eine hohe Sicherheit und Transparenz bescheinigt.

Unter den Server-Standorten sind neben Deutschland, Österreich und der Schweiz auch Großbritannien, die USA, Russland, Japan, Hongkong, Singapur, Albanien und Slowenien. In Chile steht kein physischer Server. In diesem Fall steht der Server woanders und nutzt IP-Adressen, die Chile zugeordnet sind. Das ist bei vielen VPN-Anbietern so - Surfshark geht damit relativ offen um. Der Wechsel zwischen den Standorten ist jederzeit per Mausklick möglich. Bevorzugte Standorte kann man als Favoriten markieren. Es stehen auch einige so genannte MultiHop-Verbindungen zur Verfügung, bei denen zwei VPN-Standorte hintereinandergeschaltet sind. Man kann sich also zum Beispiel zunächst nach Kanada verbinden lassen und von dort weiter in die USA.

## Kosten für den VPN-Dienst Surfshark

Beim Erwerb eines 2-Jahres-Paketes zahlt man bei Surfshark rund 2,05 Euro pro Monat (Stand: 2021). Bei dem Platzhirsch **NordVPN** hingegen wird im Abonnement eine monatliche Gebühr von 2,62 Euro fällig.

# Mesh-Network 1/2

## Was ist ein Mesh-Network?

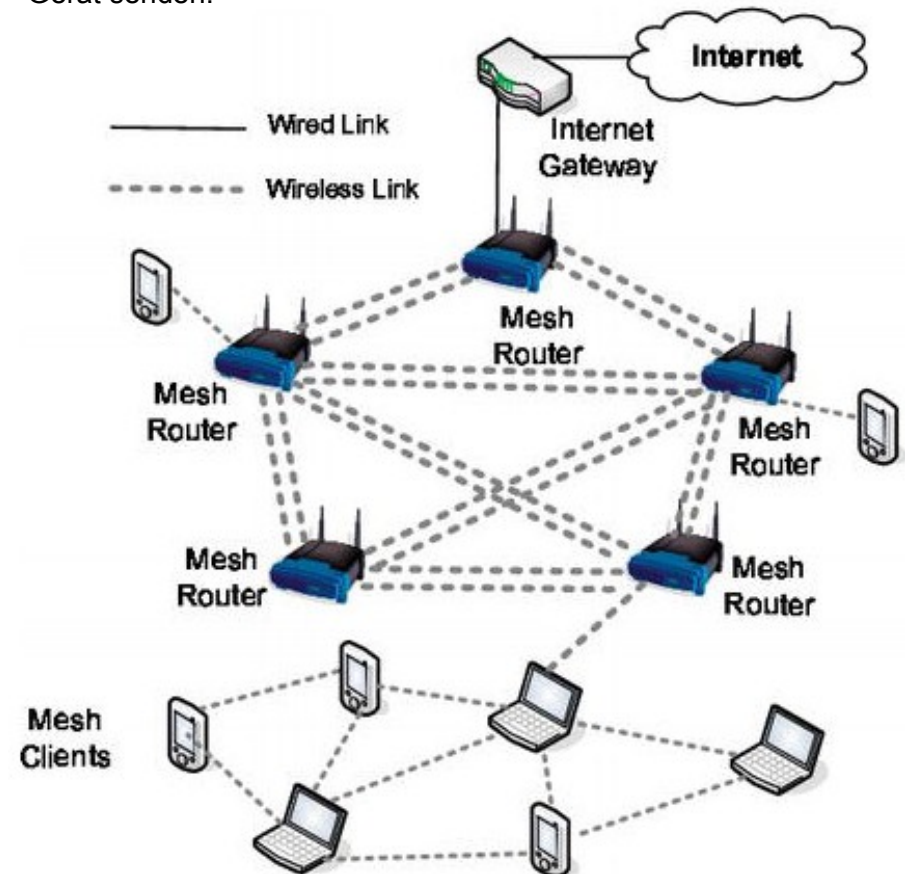
Der englische Begriff Mesh Network lässt sich mit »vermaschtes Netzwerk« übersetzen. Ein WLAN-Mesh ist also ein flächendeckendes WLAN, bei dem sich mehrere Access Points untereinander per WLAN verbinden. Um möglichst überall WLAN verfügbar zu haben, stellt man mehrere Access Points auf. Es benötigt aber nicht jeder Access Point eine Verbindung zum LAN. Mehrere Access Points lassen sich per WLAN miteinander zu einem drahtlosen Netzwerk verbinden. Jeder beteiligte Access Point dient dabei als Knoten, der Datenpakete zu den anderen Knoten weiterleitet. Das nennt man dann ein Mesh-WLAN. Eine Funktion mit der Bezeichnung Seamless-Routing (nahtloses oder unterbrechungsfreies Routing) sorgt dafür, dass sich jeder Client mit dem Access Point im Mesh verbindet, dessen Signal am stärksten zu empfangen ist.

Der Begriff »Mesh« ist mehr als Marketing und weniger als Fachbegriff zu sehen. Ein echtes Mesh wird man im Privatbereich eher selten finden. Dafür müsste man einige Access Points aufstellen, die auch noch in Reichweite zueinander sein müssten. Im professionellen Umfeld wird man bestrebt sein, jeden Access Point per Kabel mit dem Netzwerk zu verbinden, damit an jedem Access Point eine definierte Datenrate verfügbar ist.

In einem normalen WLAN kommunizieren die WLAN-Clients immer nur mit einem Access Point. In Wireless Mesh Networks sind die WLAN-Stationen untereinander vermascht. Mesh Networks agieren als Multi-Point-Netzwerke in denen die WLAN-fähigen Geräte im Ad-hoc-Modus als Relaisstationen bis zum nächstgelegenen Access Point dienen. Dabei verbessern Mesh-Network-fähige Endgeräte die Reichweite des Access Points. Als Mesh-Points können alle WLAN-Geräte dienen. Also auch typische WLAN-Clients.

In einem Mesh-WLAN bildet jeder Mesh-Point eine eigene Funkzelle. Während sich bei normalen WLANs die Funkzellen nur selten berühren,

ist das bei Mesh-WLAN Absicht. Hier liegen die Mesh-WLANs in gegenseitiger Reichweite. Andernfalls würden sie kein Netzwerk bilden. Allerdings ist ohne Änderung am Zugriffsprotokoll keine brauchbare Performance möglich. Der Grund: Benachbarte Mesh-Points teilen sich einen gemeinsamen Funkkanal. Innerhalb des gemeinsamen Funkkanals kann immer nur ein Gerät senden.



Jedes empfangene Paket muss zwischengespeichert werden, bevor es weitergesendet werden kann. Hier erkennt man auch das eigentliche Problem von Mesh-WLANs. Die Störungen durch gleichzeitige Übertragungen nehmen zu und das Zugriffsverfahren CSMA/CA gerät an seine Grenzen.

## **WLAN-Router-Kaskade**

Wenn man sich auf die teuren WLAN-Mesh-Kits nicht einlassen will, dann kann man auch mit einer WLAN-Router-Kaskade arbeiten. Es handelt sich dabei in der Regel um eine Basisstation und zusätzliche WLAN-Repeater oder WLAN-Router, die im Repeater-Betrieb konfiguriert sind. Die Geräte konfiguriert man so, dass sie hintereinandergeschaltet sind. Der Knackpunkt dabei ist, dass der Standort der Geräte gut austariert und die Geräte einheitlich konfiguriert sein müssen. Das muss man aber alles manuell machen. Dabei bekommt man aber auch die bestmögliche Abdeckung hin. Außerdem kann man dabei auch individuelle Anforderungen berücksichtigen.

## **Layer-2-Mesh mit BATMAN-Advanced**

BATMAN-Advanced ist ein Routing-Protokoll für drahtlose Ad-Hoc-Netze und arbeitet auf der OSI-Schicht 2 bzw. zwischen Schicht 2 und 3. Die Aufgabe dieses Routing-Protokolls ist es, laufend zu ermitteln, welche Knoten aktuell über welchen Weg erreichbar sind. BATMAN-Advanced wird hauptsächlich im Umfeld der Freifunk-Community entwickelt und eingesetzt. Wenn man ein solches Layer-2-Mesh aufbauen will, benötigt man in der Regel OpenWRT-fähige Access Points mit der entsprechenden Software-Erweiterung für BATMAN-Advanced.

**Hinweis:** Das Open-Source-Projekt OpenWRT ist eine alternative Firmware für Router. Es ist ein auf Linux-basiertes Betriebssystem, das man anstelle der Hersteller-Firmware auf einem Gerät installieren kann.

## **WLAN-Roaming mit IEEE 802.11k, 802.11v und 802.11r**

Wenn sich die Funkbereiche mehrerer Access Points gegenseitig ein klein wenig überlappen, dann kann sich der Client zwischen den Access Points bewegen, ohne dass die Netzwerkverbindung unterbrochen wird. Diese Funktionsweise bezeichnet man als Roaming. Der Übergang dauert jedoch 100 Millisekunden und je nach Art der Authentifizierung mehrere Sekunden. Laufende Verbindungen auf TCP/IP- und Anwendungsebene werden dabei unterbrochen. Für ein unterbrechungsfreies WLAN-Roaming gibt es Helferfunktionen, die als IEEE 802.11k, 802.11v und 802.11r standardisiert sind.

## **IEEE 802.11s / Mesh Deterministic Access**

IEEE 802.11s ist ein Standard für ein Wireless Mesh Network (WMN) in dem WLAN-fähige Geräte für andere Geräte als Relaisstationen bis zum nächstgelegenen Access Point dienen. IEEE 802.11s regelt, wie WLAN-Stationen untereinander ein drahtloses Backbone aufbauen und Frames für die Stationen außerhalb der Funkzelle weiterleiten.

## **Fazit**

Der Mesh-Betrieb im WLAN ist nichts wirklich Neues. Bereits im Grundstandard von IEEE 802.11 ist mit WDS (Wireless Distribution System, WLAN-Repeater) der Repeater-Betrieb vorgesehen. Nur leider funktionieren die Implementierungen der unterschiedlichen Hersteller nicht gut miteinander. Schon 2005 hat das IEEE mit 802.11s an einer Spezifikation für vermaschte Funknetze auf Basis von WLAN gearbeitet. Doch verbreitet hat sich das nicht. Weitere proprietäre Lösungen funktionieren auch nur mit den Geräten desselben Herstellers.

**Beispiel für ein Mesh-Network:** Das Mesh-Network Guifi.net ist ein technisch-soziales Projekt des Aufbaus eines freien, offenen, neutralen, gemeinschaftlichen und größtenteils drahtlosen Telekommunikationsnetzwerkes mit mehr als 32.000 aktiven Knoten (Stand 2017). Die überwiegende Mehrheit dieser Knoten befindet sich in Katalonien und Valencia (Spanien).

# Verschlüsselung mit VeraCrypt 1/2

VeraCrypt ist teilweise aus dem Verschlüsselungsprogramm TrueCrypt hervorgegangen. Die Freeware für die Sicherheit von Daten kann verschlüsselte Container erstellen sowie Festplatten, SSDs, USB-Sticks und SD-Karten komplett verschlüsseln. Die Bedienung von VeraCrypt ähnelt der von TrueCrypt, denn die Software zur Verschlüsselung nutzt Teile des Codes von TrueCrypt 7.1a. Zudem gibt es mit »VeraCrypt Portable« eine portable Version, die nicht installiert werden muss.

## Nachfolger von TrueCrypt

VeraCrypt ist keine Reaktion auf das Projektende von TrueCrypt im Jahre 2014. Denn VeraCrypt wurde von seinem französischen Entwickler bereits im Juni 2013 fertiggestellt und war schon eine TrueCrypt-Alternative, als das Projektende von TrueCrypt noch nicht abzusehen war. Das plattform-übergreifende Programm für Windows, macOS und Linux, lässt sich sogar auf dem Mini-Computer »Raspberry Pi« einsetzen.

## TrueCrypt hat Sicherheitslücken

Die Verschlüsselungssoftware TrueCrypt hatte immer das Manko, dass niemand so richtig wusste, wer eigentlich hinter dem Software-Projekt steht und ob Hintertürchen eingebaut sind, die den Schutz durch Passwort und Verschlüsselung umgehen. Dieses hat sich im Nachhinein als unbegründet herausgestellt, aber dennoch lässt die Sicherheit von TrueCrypt zu wünschen übrig. Denn die Software hat in der überprüften Version bekannte Sicherheitslücken, die in VeraCrypt geschlossen wurden.

## Sicherer mit VeraCrypt verschlüsseln

VeraCrypt verschlüsselt die Container oder Volumes sicherer als TrueCrypt. So nutzt VeraCrypt im Vergleich zu TrueCrypt bei der Verschlüsselung der Systempartition mit **PBKDF2-RIPEMD160** 327661 anstatt 1000 Iterationen und bei den Containern 655331 Iterationen anstatt 2000.



Außerdem gibt es Verzögerungen beim Öffnen verschlüsselter Partitionen, die für den berechtigten Eigentümer ertragbar sind, aber für Cracker sowie Hacker mehr Aufwand bedeuten. Denn beim Versuch, verschlüsselte Laufwerke oder Container zu entschlüsseln, kommen unter anderem Brutforce-Angriffe zum Einsatz, um das Passwort herauszufinden. Hierbei werden Millionen möglicher Passworte ausprobiert, sodass jede Verzögerung die Zeit zum Finden des richtigen Passworts deutlich erhöht.

## Container mit VeraCrypt verschlüsseln

Um private Dateien sicher vor einem unberechtigten Zugriff zu schützen, reicht es, diese in einem Container zu speichern, der mit VeraCrypt verschlüsselt ist. Bei einem VeraCrypt-Container handelt es sich um eine Datei, die sich auf beliebige Laufwerke, wie Festplatten, USB-Sticks oder alternativ in der Cloud speichern lässt.



## Verschlüsselung mit VeraCrypt 2/2

Die Größe der Datei gibt der Nutzer an, wenn er den Container mit VeraCrypt erstellt und verschlüsselt. Dabei ist die maximale Größe vom Speichermedium und dem darauf befindlichen Dateisystem abhängig. Ist letzteres FAT32, kann die Container-Datei maximal 4 GByte groß sein.

Beim Öffnen mit VeraCrypt durch Passwort-Eingabe, wird die Container-Datei als virtuelles Laufwerk unter Windows, macOS und Linux eingehängt und kann wie eine Partition genutzt werden. Beachten sollte man aber, dass VeraCrypt beim Öffnen der ersten Container-Datei neben dem Passwort für den Container auch ein Administrator-Passwort des Computers verlangt. Letzteres ist nötig, um den entschlüsselten Container als virtuelles Laufwerk in das System einzuhängen. Ein Nutzer mit Standard-Konto kann deswegen keinen VeraCrypt-Container öffnen.

### Versteckte Container

Ergänzend zur Verschlüsselung bietet VeraCrypt noch das Verstecken von Daten an. Dieses wird über versteckte Container realisiert, die VeraCrypt innerhalb eines verschlüsselten Laufwerks oder Containers anlegt. Versteckte Container sind für ganz geheime Dateien gedacht. Denn verschlüsselte Container und Laufwerke lassen sich zwar nur mit Passwort entschlüsseln, sind aber sichtbar. Entsprechend könnte man zur Herausgabe des Passwortes gezwungen werden. Ist dem so, bleiben die Dateien im enthaltenen, versteckten Container weiterhin unsichtbar, da sie mit einem eigenen Passwort geschützt sind. Dieses Passwort muss natürlich von dem abweichen, das für das Entschlüsseln des sichtbaren, verschlüsselten Containers oder Laufwerks gewählt wurde.

### Kompatibilität zu TrueCrypt-Containern

Wer verschlüsselte TrueCrypt-Container angelegt hat, kann diese in der Regel mit VeraCrypt öffnen und den Inhalt nicht nur lesen, sondern auch ändern.



Dazu muss nach Auswahl des TrueCrypt-Containers und Klick auf »Mount« der Haken vor »TrueCrypt Mode« gesetzt werden, was VeraCrypt in der aktuellen Version automatisch tut. Falls es Probleme geben sollte, bleibt ein Versuch im Read-Only-Modus, wonach sich der Ordner zumindest zum Lesen öffnen lässt.

Mit VeraCrypt erstellte Ordner kann TrueCrypt hingegen nicht öffnen. Dies dürfte Kenner von TrueCrypt nicht verwundern, da TrueCrypt-Container einer neueren TrueCrypt-Version auch nicht von einer älteren geöffnet werden können.

### VeraCrypt als portable Version nutzen

Wie bei TrueCrypt gibt es auch bei VeraCrypt eine portable Version, die sich als portable Software vom USB-Stick aus ohne Installation starten lässt. VeraCrypt Portable hat dieselben Funktionen wie die Standard-Variante von VeraCrypt und lässt sich am genutzten Computer mit Administrator-Rechten einsetzen.

# Was ist Splunk?

Splunk Inc. (**Big Data Analyse und Aufbereitung, IT-Security, analysegestützte SIEM-Lösung**) ist ein US-amerikanisches Unternehmen mit Sitz in San Francisco, das seit 2012 börsennotiert ist. Mehr als 6.000 Firmen, Universitäten, behördliche Einrichtungen und Service Provider in vielen Ländern nutzen Splunk Enterprise. Es bietet verschiedene Analyse-Software für Unternehmen, die ihre Betriebs- und Geschäftsdaten auswerten möchten und generiert Umsätze im Milliarden-US-Dollar-Bereich. Dabei hat sich das Unternehmen auf maschinengenerierte Daten spezialisiert, die von Webseiten, Anwendungen, Servern, Netzwerken und mobilen Endgeräten generiert werden. Es wurde eine eigene Technik entwickelt, um sowohl Echtzeit-Auswertungen als auch historische Maschinendaten zu überwachen, durchsuchen, sammeln, speichern, verarbeiten (indexieren), analysieren und zu visualisieren. Man kann Splunk vereinfacht auch als eine sehr effektive Suchmaschine bezeichnen. Eines der wichtigsten Merkmale von Splunk, ist die Fähigkeit die Daten (unstrukturierte Maschinendaten, Produktionsmaschinen, Messgeräten, Sensoren, Fahrzeugen, ...) aus beinahe jeder Quelle empfangen zu können. Mit Hilfe der splunk-spezifischen Suchsprache »Search Processing Language« (SPL) lassen sich mit einfachen Befehlen Datenmuster visuell aufbereiten. Die Pivot-Schnittstelle ermöglicht es Anwendern, Maschinendaten zu lesen, um umfassende Berichte zu erstellen, ohne die Suchsprache lernen zu müssen. Auch Anwender der Geschäftsebene können leicht relevante Datenerhebungen erstellen.



Ereignismuster werden entlang einer Zeitachse dargestellt, um Trends, Spitzen und Abweichungen auf einen Blick festzustellen. Es gibt über 140 Befehle, die es erlauben, nach Schlüsselwörtern zu suchen, beliebige Datenmengen zu filtern oder die Suche in Teilsuchen zu unterteilen. Auch die weitverbreitete »Regular-Expression-Notation« wird unterstützt.

**splunk** > turn data into doing™

splunk > aus Daten Taten machen

**Zusammenfassung:** Splunk (**Big Data Analyse und Aufbereitung**) ist eine plattformübergreifende Lösung, die Information aus verschiedenen Quellen erhält und die korrelierten Information auf einem Dashboard vereint und visualisiert.

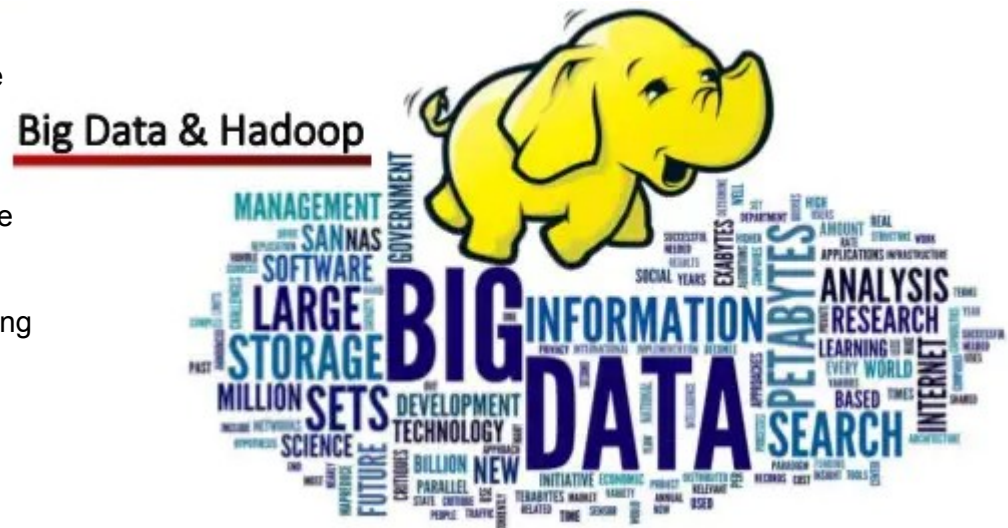
# Hadoop und Big Data

Hadoop und Big Data sind eng miteinander verbunden und werden daher oft im selben Atemzug genannt. Hadoop ist ein Framework auf Basis von Java und dem MapReduce-Algorithmus von Google. Durch die Apache-Lizenz steht Hadoop grundsätzlich jedem kostenlos zur Verfügung. Die Aufgabe von Hadoop ist es sehr große Datenmengen, effizient in Clustern verarbeiten und berechnen zu können. Für die Verarbeitung müssen Administratoren und Entwickler zusammenarbeiten, damit der Cluster optimal funktioniert. Der Dienst kann installiert oder über die Cloud betrieben werden. Hadoop wird unter anderen von den Firmen twitter, IBM, »Linked in«, Facebook, Baidu, und Yahoo verwendet.

Facebook nutzt Hadoop, um Kopien der internen Protokolle und Datenquellen zu speichern, die in sogenannten dimensionalen Data Warehouses vorliegen. Das Unternehmen verwendet diese Daten als eine Quelle für die Berichterstattung und deren Auswertung im Hinblick auf maschinelles Lernen.

Hadoop besteht aus mehreren Teilen, die beim Parsen der gespeicherten Daten ineinandergreifen. Die vier Grundbestandteile sind:

- **Hadoop Common**: sind die Grundfunktionen für die meisten Anwendungsfälle; Zum Software-Framework gehören zahlreiche Bibliotheken und Anwendungen, die auf die HDFS als auch MapReduce oder YARN angewiesen sind.
- **Hadoop Distributed File System (HDFS)**: zur Datenspeicherung in einem leicht zugänglichen Format; HDFS bildet die Voraussetzung für den MapReduce-Algorithmus, da verteilte Rechnersysteme eine spezielle Dateiverwaltung erfordern.
- **Hadoop MapReduce**: zur Datenverarbeitung durch Mapping eines großen Datensatzes und anschließendes Filtern nach bestimmten Ergebnissen; die MapReduce basiert auf einem Algorithmus von Google
- **Hadoop YARN (Yet Another Resource Negotiator)**: zur Ressourcen- und Kapazitätenverwaltung; YARN kann die Ressourcen in einem Rechnerverband managen und Ressourcen eines Clusters dynamisch verschiedenen Jobs zuordnen, d.h. Rechenarbeit auf Rechner-Cluster verteilen. Bevor YARN seinen offiziellen Namen erhielt, wurde es informell MapReduce 2 oder NextGen MapReduce genannt.



Die allgegenwärtige Präsenz von Hadoop erklärt sich durch seine leichte Verfügbarkeit und seinen benutzerfreundlichen Einstieg. Außerdem ist es erschwinglich und bietet mit seinen Modulen eine ansehnliche Anwendungsvielfalt.

# Hunk - Splunk Analytics für Hadoop

Splunk Inc., Anbieter der führenden Softwareplattform für Echtzeit-Analyse, eröffnet mit der allgemeinen Verfügbarkeit von **Hunk™** (Splunk Analytics for Hadoop) eine neue Ära der Big Data-Analyse. Die vollfunktionale, integrierte Analytics-Plattform für Hadoop ermöglicht allen Unternehmensanwendern, in Apache Hadoop gespeicherte historische Daten interaktiv zu erforschen, zu analysieren und zu visualisieren. Hunk beruht auf einer zum Patent angemeldeten Virtual Index-Technologie, die leistungsfähige Analysefunktionen bereitstellt, ohne dass spezielle Programmierkenntnisse benötigt werden. Hunk stellt zudem eine umfassende Entwicklungsumgebung bereit, zu der ein integriertes Web Framework ebenso gehört wie SDKs (Software Development Kit) für die gängigsten Programmiersprachen. Eine kostenlose Test-Version steht zum Download bereit; sie ist 60 Tage gültig und ohne Einschränkungen hinsichtlich Datenmenge und Anzahl der Hadoop-Knoten nutzbar.

## Schnelle Analyseergebnisse für Hadoop-Daten

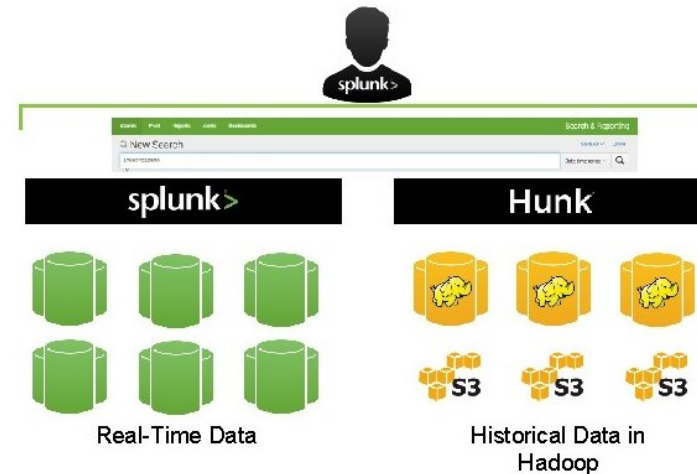
Mit Hunk können Anwender schnell und einfach Erkenntnisse aus Rohdaten sowie unstrukturierten und polystrukturierten Hadoop-Daten gewinnen.

Die wichtigsten Features und Highlights auf einen Blick:

- **Umfangreiche Analysefunktionen** - ermöglicht die Erforschung, Analyse und Visualisierung von Daten, die Erstellung von Dashboards und die gemeinsame Nutzung von Berichten über eine integrierte Plattform.
- **Schnelle Implementierung** - Ein einfacher Verweis von Hunk zu dem betreffenden Hadoop-Cluster genügt, um sofort mit der Datenexploration beginnen zu können.
- **Interaktive Suche und Voranzeige der Ergebnisse** - Dateninteraktion, flexible Änderung des Blickwinkels und Voranzeige von Suchergebnissen noch während der Ausführung von MapReduce-Jobs.
- **Drag-and-Drop Analysefunktionen** - leistungsstarke Analyse für Jedermann mit den zum Patent angemeldeten Splunk-Datenmodellen und der Pivot Interface-Technologie, die erstmals in Splunk Enterprise 6 eingesetzt wurden.
- **Reichhaltige Entwicklungsumgebung für Hadoop** - ermöglicht die Erstellung von Big Data-Applikationen auf der Grundlage von Hadoop-Daten, wobei bewährte Programmiersprachen (C#, Java, JavaScript, Python, PHP, Ruby) und Frameworks verwendet werden können.

## Splunk / Hunk Unified Search

Intelligently Search Across Real-Time and Historical Data Using the Same Splunk Interface

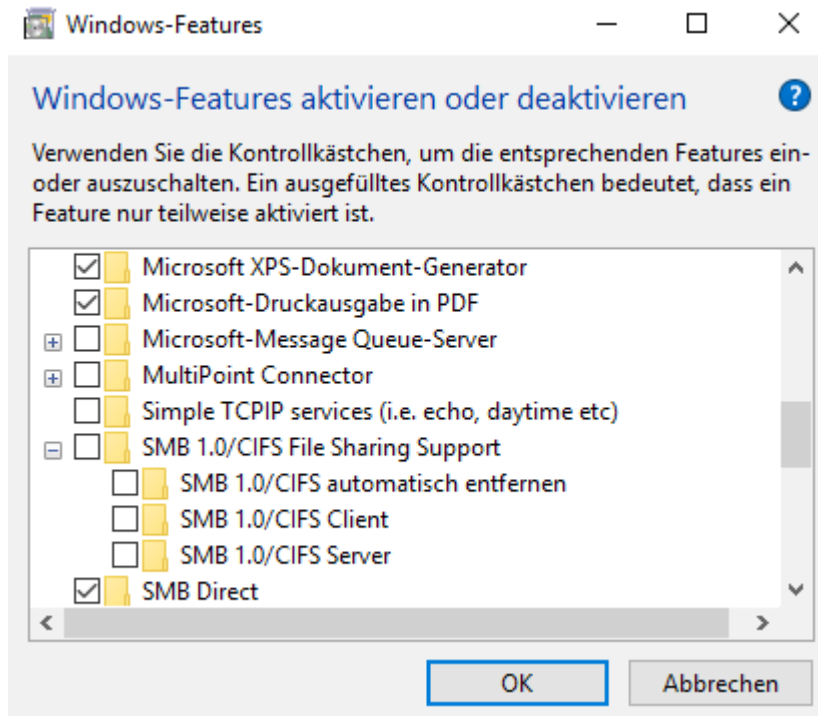


**SDK:** Ein Software Development Kit (SDK) ist eine Sammlung von Programmierwerkzeugen und Programmibibliotheken, die zur Entwicklung von Software dient. Es unterstützt Softwareentwickler, darauf basierende Anwendungen zu erstellen.



# Windows-Features

**SMB1 deaktivieren:** Der Dateizugriff und die Kommunikation zwischen Geräten und Computerprozessen wird in Windows-Systemen seit Jahrzehnten mithilfe des Netzprotokolls SMB (Server Message Block) geregelt. Heutige Betriebssystem-Editionen wie Windows 10 unterstützen beispielsweise immer noch SMBv1, die erste Version dieses Standards. Selbige ist in der jüngeren Vergangenheit jedoch vor allem durch Sicherheitslücken ins Rampenlicht gerückt, weshalb ein Verzicht auf die als veraltet eingestufte Protokoll-Edition ratsam ist.



Tastenkombination: [Win] + [Pause] -> Startseite der Systemsteuerung -> Programme -> Programme und Features -> Windows-Features aktivieren oder deaktivieren -> »SMB 1.0/CIFS File Sharing Support« suchen und den Haken in der Checkbox entfernen

Klicken Sie abschließend auf »OK«, um SMB1 in Windows 10 zu deaktivieren. Dieser Prozess nimmt einige Zeit in Anspruch, während dieser Zeit sollte das offene Fenster nicht geschlossen werden. Sobald der Vorgang abgeschlossen wurde, erhält man die Aufforderung, das System neu zu starten. Erst nach einem Neustart werden die Änderungen bezüglich des SMB-Protokolls übernommen.

## SMB1 mit der PowerShell deaktivieren:

1. PowerShell mit Administratorrechten aufrufen  
Rechtsklick auf das Windows-Icon -> Windows PowerShell (Administrator)
2. **Get-SmbServerConfiguration | Format-List EnableSMB1Protocol**  
Zeigt die PowerShell für »EnableSMB1Protocol« den Wert »False«, ist SMBv1 deaktiviert. Ist die Unterstützung aktiviert, steht an gleicher Stelle »True«.
3. **Set-SmbServerConfiguration -EnableSMB1Protocol 0**  
Dieser Befehl deaktiviert SMB1 und nach der Eingabe von »J« wird das Protokoll deaktiviert.
4. Nach einem Neustart des Rechners übernimmt das System diese Änderungen.



# Datenträgerbereinigung unter Windows

## Manuelles Löschen von Dateien und Ordner

Die Datenträgerbereinigung in Windows ist ein nützliches Werkzeug, um nicht mehr gebrauchte Dateien zu löschen - doch nicht alle temporären Dateien werden dabei entfernt, sodass ein manuelles Löschen von einigen Ordner notwendig werden kann.

Die meisten temporären Dateien befinden sich unter Windows in den Ordnern:

- **%userprofile%\AppData\Local\Temp** (%userprofile% steht für den Pfad zum Benutzerverzeichnis, also z. B. C:\Users\  
<Benutzername>)
- **%systemroot%\Temp** (%systemroot% steht für das Windows-Verzeichnis, also z. B. für C:\Windows - Zugriff benötigt Administrator-Rechte)
- **%programdata%** (falls hier noch Ordner von bereits deinstallierten Programmen auftauchen, kann man diese ebenfalls löschen)

### Beispiel:

Tastenkombination: **[Win] + [Q]** und im Suchfeld **%programdata%** eingeben

Für die Anzeige einiger Ordner und Dateien, sollte man über das Menü »Ansicht« (Checkbox: Ausgeblendete Elemente) die versteckten Dateien anzeigen lassen.

Ein weiterer Unterschied zur Datenträgerbereinigung sei noch erwähnt: Während von Hand gelöschte Dateien und Ordner zunächst im Papierkorb landen, ist das bei der Datenträgerbereinigung nicht der Fall. Hier werden die Elemente ohne Zwischenstation endgültig entfernt.

## Datenträgerbereinigung aufrufen

- Tastenkombination: **[Win] + [E]** -> »Dieser PC« -> Kontextmenü des Laufwerkes aufrufen -> Eigenschaften -> Button »Bereinigen« -> Checkboxes auswählen -> Bestätigen mit »OK«
- Tastenkombination: **[Win] + [E]** -> »Dieser PC« -> Kontextmenü des Laufwerkes aufrufen -> Eigenschaften -> Button »Bereinigen« -> Button »Systemdateien bereinigen« -> Checkboxes auswählen -> Bestätigen mit »OK«
- Tastenkombination: **[Win] + [Q]** -> im Suchfeld **Datenträgerbereinigung** eingeben

**Hinweis:** Die Reinigung der Windows-Registry über spezielle Programme, wird im Allgemeinen nicht zu empfohlen. Die Bereinigung der Registry bringt in der Praxis keinen Geschwindigkeitsvorteil. Im besten Fall bemerkt man nach der Bereinigung keinen Unterschied und im schlimmsten Fall verursachen die Eingriffe in die Registrierungsdatenbank Probleme im Windows-Alltag.

# Festplatten-Partitionen - MBR oder GPT? 1/2

## Festplatten partitionieren - GPT oder MBR?

Eine Partition kann sowohl eine ganze Festplatte umfassen, als auch nur einen Teil davon. Wie groß diese Teile sind und wie sie heißen, wird in der Partitionstabelle festgehalten; hinzu kommen weitere technische Informationen. Neben der eigentlichen Partitionstabelle wird beim Systemstart auch noch die Information benötigt, was denn überhaupt gebootet werden soll.

Traditionell wurden diese beiden Aufgaben, Boot-Information und Partitionierung, über die Technologien BIOS (Basic Input Output System) und MBR (Master Boot Record) erledigt. Die modernere Variante läuft über UEFI (Unified Extensible Firmware Interface) und GPT (GUID Partition Table, Globally Unique Identifier Partition Table). BIOS und UEFI sind die Firmware des Computers, also die grundlegendste Software, über die überhaupt erst die Kommunikation zwischen Hardware und weiterer Software wie dem Betriebssystem möglich ist.

Am Anfang der Festplatte - im MBR, werden der Bootloader, der das Betriebssystem startet und die Partitionstabelle festgelegt. Sofern es sich nicht um eine Boot-Festplatte handelt, wird nur die Tabelle verwendet. Vereinfacht steht dort: Partition 1 beginnt an Stelle X, endet an Stelle Y und heißt beispielsweise »D:« und ist vom Typ »ABC«. Als Typ gibt es eine ganze Reihe unterschiedlicher Möglichkeiten, beispielsweise »Linux Native«, »FAT32«, »NTFS«, »Dynamischer Datenträger« und viele mehr.

Die GPT-Variante ist ein wenig umfangreicher, aber nicht komplizierter: Zunächst gibt es hier aus Gründen der Abwärtskompatibilität und der Datensicherheit noch den alten MBR, der aber lediglich für Programme gedacht ist, die mit GPT nicht arbeiten können - was heutzutage nur in Ausnahmefällen vorkommen dürfte.

Anschließend folgt die GUID-Partitionstabelle, die im Wesentlichen dieselben Informationen anbietet, wie die MBR-Tabelle - schließlich erfüllt sie auch dieselbe Aufgabe. Allerdings gibt es hier noch einige Typen und Informationen mehr und natürlich unterscheidet sich der genaue Aufbau. Ein wesentlicher Unterschied: Bei GPT gibt es zwei Sicherungsmechanismen gegen Datenverlust. Zum einen gibt es ein Backup der Tabelle, zum anderen einen Prüfmechanismus, um die Integrität der Tabelle zu gewährleisten und Fehler gegebenenfalls sogar automatisch zu reparieren. Soll heißen: Die Wahrscheinlichkeit von Datenverlust ist bei GPT geringer.

Ein weiterer wesentlicher Unterschied: MBR unterstützt lediglich vier sogenannte »Primäre Partitionen«. Wenn man mehr Partitionen haben will, muss man eine oder mehrere dieser vier Primär-Partitionen als »Erweiterte Partitionen« erstellen, die sich wiederum in beliebig viele »Logische Partitionen« unterteilen lassen. Bei GPT kann man theoretisch beliebig viele Partitionen erstellen, 128 sollten alle Systeme unterstützen - ohne Unterscheidung von primären, erweiterten und logischen Partitionen.

Ein weiterer deutlicher Unterschied: Die MBR-Partitionierung funktioniert nur bis zu einer Festplattengröße von 2 Terabyte - was heute schon eine Standardgröße ist. GPT schafft hingegen 9,6 Zetabytes, also 9.600 Millionen Terabyte.

Ein weiterer Unterschied liegt im Bootloader: Beim MBR liegt dieser im ersten Sektor der Festplatte, sprich am Anfang des physischen Speichers. Bei GPT befindet er sich hingegen in einer eigenen kleinen Partition, der EFI-Systempartition. Jedes Betriebssystem fügt hier einen eigenen Eintrag hinzu, was Multiboot-Systeme deutlich einfacher und vor allem robuster macht.

# Festplatten-Partitionen - MBR oder GPT? 2/2

## GUID oder UUID einer Festplatte ermitteln

Öffnen einer Eingabeaufforderung mit Administratorrechten.  
Um die GUID für ein internes wie auch externes Laufwerk zu ermitteln, müssen Sie den folgenden Befehl eingeben.

1. **diskpart**
2. **list disk**
3. **select disk 0**
4. **uniqueid disk**
5. **exit**

## GPT oder MBR?

Erfolgt durch den nachfolgenden PowerShell-Befehl eine Ausgabe, dann wird auf dem Datenträger auch GPT verwendet.

**wmic partition get name,type | findstr "GPT"**

Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

PS C:\Windows\system32> diskpart

Microsoft DiskPart-Version 10.0.17763.1

Copyright (C) Microsoft Corporation.
Auf Computer: DDSD10911

DISKPART> list disk

   Datenträger ###  Status              Größe   Frei    Dyn  GPT
   -----
   Datenträger 0    Online              119 GB   0 B
   Datenträger 1    Online             7440 MB   0 B

DISKPART> select disk 0

Datenträger 0 ist jetzt der gewählte Datenträger.

DISKPART> uniqueid disk

Datenträger-ID: {4158F505-C5D7-4FA0-BE3A-0136B6DD2599}

DISKPART> 
```

# Speichermedien sicher löschen 1/4

## Secure Eraser schafft Sicherheit

Will man eine HDD-Festplatte physisch nicht zerstören, d.h. in winzig kleine Stückchen schreddern, so ist die einzige Möglichkeit, die persönlichen Daten wirklich sicher und endgültig zu löschen, das Überschreiben mit Zufallswerten. Dies erledigt beispielsweise das Programm **SecureEraser** der Firma Ascomp, welches für die private Nutzung kostenlos genutzt werden kann. Alternativ kann man die Live-CD **DBAN** verwenden. **Hinweis:** Für SSD-Festplatten funktioniert diese Methode nicht.

### 5 Löschmethoden stehen zur Wahl

Man hat die Wahl zwischen 5 amtlich anerkannten Standards zur Datenlöschung.

- Niedrig - Random (einmaliges Überschreiben)
- Normal - US DoD 5220.22-M e (dreifaches Überschreiben)
- Hoch - Deutscher Standard (siebenfaches Überschreiben)
- Sehr hoch - US DoD 5220.22-M ECE (siebenfaches Überschreiben)
- Höchstmöglich - Peter Gutmann Standard



**Peter-Gutmann-Algorithmus:** Der Peter-Gutmann-Algorithmus ist eine Methode zur vollständigen Löschung von Daten auf magnetischen Speichermedien, unabhängig von der Rohdatenkodierung.

Die Guttman-Methode besteht aus mehreren Reihen von Durchgängen. Der Algorithmus nimmt insgesamt 35 Überschreibungsdurchgänge vor und gilt als sicherste Methode der Datenvernichtung. Zufällige Zeichen werden bei den ersten und den letzten vier Durchgängen verwendet, die anderen Durchgänge, d. h. 5 bis 31, verwenden definierte Werte nach einem bestimmten Muster. Durch die mehrfache Überschreibung der Daten, werden die Datenreste auf den Festplatten und externen Speichermedien reduziert.

Ursprünglich wurde diese Methode für früher hergestellte Festplatten entwickelt, heutige Festplatten müssen nicht unbedingt durch eine 35-fache Überschreibung gelöscht werden. Der Erfinder selbst ist der Ansicht, dass nur noch ein paar Durchläufe der Überschreibung heutzutage von Nöten sind, um den gesamten Datenbestand zu vernichten. **Hinweis:** Durch eine 35-fache Überschreibung wird die Festplatte einer sehr großen Belastung ausgesetzt, dass die Lebensdauer des Speichermediums nicht unbedingt verlängert.

## Speichermedien sicher löschen 2/4

### Warum bei SSDs herkömmliche Lösch-Methoden versagen

Um Daten auf SSDs gründlich zu löschen, ist mit einem einfachen Überschreiben mit Zufallsdaten nicht möglich. SSDs verhalten sich bei der Organisation von Daten und ihren freiem Speicherplatz völlig anders als HDD-Festplatten.

Für die interne Aufteilung des Flash-Speicher sorgt die FTL (Flash Translation Layer, Tabelle für die Verwaltung von Datenblöcke), die dem physikalischen Speicher Adressen zuordnet. Ein direkter Zugriff auf eine bestimmte Adresse, wie bei einer Festplatte, ist nicht möglich. Außerdem übernimmt die Controller-Logik jeden Schreib- und Löschbefehl, um für die gleichmäßige Belegung, Nutzung aller Speicherzellen zu sorgen (Wear Leveling). Das Wear Leveling vermeidet einen vorzeitigen Ausfall der Speicherzellen, da die Speicherzellen nur eine begrenzte Anzahl von Schreibzyklen (etwa 100.000) erlauben.

Gelöschten Speicherplatz gibt der interne Controller einer SSD nicht sofort wieder frei. Wenn ein Block bereits teilweise belegt ist, wird zunächst in einen freien Block geschrieben. Für das Zusammenfassen freier Speicherbereiche zu kompletten, wiederbeschreibbaren Blöcken sorgt später eine interne Aufräumfunktion (Garbage Collection, Leeren von nicht benutzten ganzen Seiten, Seiten bestehen aus vielen Blöcken – etwa 2 bis 4 MB).

Neu geschriebene Daten landen auf einer SSD also nicht dort, wo gerade Speicherplatz frei geworden ist. Damit haben Überschreibmethoden und herkömmliche Löschrprogramme keinen direkten Einfluss auf die Belegung des Flash-Speichers.

### Sicheres Löschen mit »ATA Secure Erase«

Um jede Speicherzelle (auch Datenreste) einzeln auszulesen, muss man die FTL umgehen. Die ATA-Spezifikation bietet dafür ein spezielles Löschkommando: ATA Secure Erase. Dieser Befehl ist bei allen **ATA/SATA-Laufwerken** ab dem Jahr 2001 enthalten.

»ATA Secure Erase« überschreibt wie bei einem Format-Befehl den gesamten Datenträger, inklusive jener Bereiche die für den »Sector Reallocation« reserviert sind und im normalen Betrieb nicht zugänglich sind. Der »Sector Reallocation« ist zuständig für die Ersatz-Sektoren und damit für die interne Fehlerbehebung.

Der Befehl »ATA Secure Erase« ist eine Erweiterung der Firmware und im Befehlssatz des Laufwerks untergebracht.

Das Kommando »ATA Secure Erase« kann den Datenträger in den Werkszustand zurücksetzen. Es bleibt aber das Problem, dass man an den Befehl nicht so leicht herankommt. Dafür ist spezielle Software nötig, um »ATA Secure Erase« auf einem Laufwerk auszuführen.

Einige **Hersteller** liefern zu ihren SSDs passende **Dienstprogramme** (SSD Manager) mit aus, entweder auf einer CD im Lieferumfang oder per Download im Support-Bereich der Webseite. Dieser Weg über diese herstellerepezifischen Windows-Programme ist in jedem Fall der einfachste, da »ATA Secure Erase« hier einfach über einen entsprechenden Menüpunkt aufgerufen wird. Allerdings gibt es nicht von jedem Hersteller passende Dienstprogramme und **auf fremden SSDs** lassen sie sich **nicht ausführen**.

Steht kein passendes Dienstprogramm zur Verfügung, kann man es mit der Linux-Livedistribution »Parted Magic« versuchen. »Parted Magic« enthält neben vielen anderen Tools auch das Tool »Disk Erasing«.



## Speichermedien sicher löschen 3/4

### »ATA Secure Erase« mit »Parted Magic« ausführen

»Parted Magic« (**Hinweis:** die neueste Version ist kostenpflichtig) ist ein bootfähiges Live-System auf Linux-Basis und enthält unter anderem auch den Befehl »ATA Secure Erase«. Um »Parted Magic« zu nutzen, muss man im ersten Schritt eine bootfähige DVD oder einen Multiboot-Stick erstellen. Das dazugehörige ISO-Image kann man im Internet an verschiedenen Stellen finden.

### Ältere Versionen von »Parted Magic«

Nach dem erfolgreichen Bootvorgang ruft man im Hauptmenü **»Erase Disk«** unter **»System Tools«** auf. In **»Erase Disk«** wählt man die Option **»Internal: Secure Erase command writes zeroes to entire data area«** aus, sowie das Laufwerk, welches gelöscht werden soll

### Aktuelle Versionen von »Parted Magic«

1. Nach einer kurzen Wartezeit startet »Parted Magic«. Als erstes kann man die Zeitzone festlegen. Auf dem Desktop findet man bereits die Verknüpfung **»Erase Disk«**. **Hinweis:** USB-Festplatten werden nicht unterstützt, man muss sie über einen Apapter in den Rechner provisorisch einbauen.
2. Nach dem Start von **»Erase Disk«** ruft man die Option **»Secure Erase - ATA Devices«** auf.
3. Es werden die im Computer vorhandenen Laufwerke angezeigt. An dieser Stelle sollte man darauf achten, das richtige Laufwerk auszuwählen, da dieses komplett gelöscht wird.
4. Falls die Festplatte den Status **»Frozen«** hat, muss dieser zuerst gelöst werden. Hier kann es helfen, den Sleep-Button zu betätigen. Der Computer geht kurz in den Schlafzustand und aktiviert sich wieder. Idealerweise sollte die SSD nun freigegeben sein. **Hinweis:** Falls dies nicht der Fall ist, muss man die zweite Methode verwenden.
5. Die Auswahl **»Secure«** löscht alle Datenbereiche der ausgewählten SSD. Im Bestätigungsdialog muss man das Löschen nochmals bestätigen. Mit **»Start Erase«** wird der Löschvorgang gestartet.
6. Der Vorgang ist recht schnell abgeschlossen. Nach Abschluss wird noch eine Zusammenfassung angezeigt. Das wars, die SSD wurde nun relativ sicher gelöscht!



### 2. Methode den Status »Frozen« zu beenden

- Diese Methode wird über das **»Help-Menü«** aufgerufen. **»Alternative Sleep Method«** und die SSD auswählen, die aus ihrem Frozen-Status befreit werden soll. Darauf erscheint ein Dialog mit Anweisungen.
- Zuerst muss man die SSD vom Strom trennen (Stromversorgungskabel der SSD abziehen) und anschließend etwa 30 Sekunden warten. Anschließend das Stromkabel wieder anschließen und erneut 30 Sekunden warten.
- In der Software bestätigt man diese Aktion (Checkbox aktivieren) und die SSD sollte nun einen grünen **»Not Frozen-Status«** anzeigen.

## Speichermedien sicher löschen 4/4

### Mit »DiskPart Clean All« ein SSD-Laufwerk löschen

Wenn man eine SSD erfolgreich bereinigen, löschen möchte, kann man den DiskPart-Befehl »clean« oder »clean all« anwenden.

- Der Befehl »clean« löscht alle Partitionen auf dem SSD-Laufwerk. Es werden jedoch nur die Daten als gelöscht markiert, nicht die Festplatte auf Null gesetzt. Diese scheinbar gelöschten Daten können mit einer spezieller Software wiederhergestellt werden.
- Mit dem Befehl »clean all« wird der Inhalt des Laufwerks sicher gelöscht. Es wird über jeden Sektor auf der Festplatte geschrieben und vollständig auf Null gesetzt. Und diese gelöschten Daten können nicht mit üblichen Tools wiederhergestellt werden.

### SSD-Festplatte löschen

1. Im Suchfeld der Taskleiste **cmd** eingeben und den Eintrag über Rechtsklick »**Als Administrator ausführen**« starten.
2. Im Eingabeaufforderungsfenster **diskpart** eingeben und mit der Eingabetaste bestätigen.
3. **list disk**  
Man erhält jetzt eine Liste mit den Datenträger-Nummern, aus denen man eine auswählen kann.
4. **select disk #**  
Es ist die Datenträgernummer anzugeben, für die der Befehl **clean all** angewandt werden soll (z.B. select disk 2).
5. **clean all**  
Mit der Betätigung der Eingabetaste, wird die ausgewählte Festplatte gelöscht. Bei großen Festplatten kann dies mehrere Stunden dauern.
6. **exit**  
Beendet den DiskPart-Modus.

```

Administrator: C:\Windows\System32\cmd.exe - diskpart
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>diskpart

Microsoft DiskPart-Version 6.1.7600
Copyright (C) 1999-2008 Microsoft Corporation.
Auf Computer: AOMEI-PC

DISKPART> list disk

   Datenträger ###  Status              Größe   Frei    Dyn  GPT
   -----
   Datenträger 0    Online              1000 GB    8 MB
   Datenträger 1    Online              1000 GB   999 GB

DISKPART> select disk 1

Datenträger 1 ist jetzt der gewählte Datenträger.

DISKPART> clean           oder clean all
Der Datenträger wurde bereinigt.

DISKPART>
  
```

### Hinweis:

- Das Wiederherstellen von vollkommen gelöschten Daten auf SSD-Laufwerken ist aufwendig, aber möglich.
- Nur die physische Zerstörung (in kleine Teile schreddern oder hohe Temperaturen aussetzen, Schmelzpunkt der Metallteile) eines SSD-Laufwerkes gibt die Garantie für eine sichere Löschung aller Daten.
- **Ausblick in die Zukunft:** Verschlüsselung mit Teilpasswort das im TPM-Chip abgelegt wurde, um die Daten unbrauchbar zu machen
- **Fazit:** Ein unwiederbringliches Löschen von SSD-Laufwerken ist aktuell mit Hilfe von Software nicht möglich.

# Wiederherstellung mit Recuva

## Was kann die Recovery-Software Recuva?

Gehen Daten durch Löschen, Formatieren oder anderen Beschädigungen verloren, ist ein aktuelles Backup hilfreich. Ohne Backup ist eine Recovery-Software wie Recuva (Hersteller: Piriform) nötig, um die gelöschten Dateien unter bestimmten Bedingungen auf Datenträgern mit den üblichen Microsoft-Dateisystemen wiederherstellen zu können. Neben der Installer-Version ist die Recovery-Software »Recuva Portable« auch als portable Software erhältlich, die sich ohne Installation vom USB-Stick aus starten lässt. Beide Varianten unterstützen sowohl 32- als auch 64-Bit-Systeme.

## Welche Version ist die richtige für mich?

- Die kostenlose Free-Edition von »Recuva« genügt in der Regel, um versehentlich gelöschte Dateien auf Datenträger wiederherzustellen.
- Die kostenpflichtige »Recuva Edition Professional« bietet ergänzend Unterstützung für virtuelle Laufwerke und Updates, sowie Premium-Support für ein Jahr.
- Mit der »Recuva Business Edition« richtet sich der Hersteller Piriform an Unternehmen und unterstützt zusätzlich die Datenrettung für Netzwerke.

## Tiefenscan für bessere Suchergebnisse

Wer Dateien auf nicht beschädigte Datenträger vermisst oder sicher gelöscht weiß, sollte zuerst einmal den schnellen Scan von Recuva nutzen. Weiß man bereits im Voraus, dass die Suche für die Datenrettung tiefergehend sein muss, ist ein Tiefenscan angesagt, der sich auch empfiehlt, wenn der schnelle Scan erfolglos blieb. Der Tiefenscan von Recuva dauert etwas länger (über eine Stunde und länger), ist aber gründlicher und intensiver. Durch den Tiefenscan findet Recuva Dateien, auch auf frisch formatierten Festplatten und kann danach die gelöschten Dateien wiederherstellen.



Allerdings nur bei einer Schnellformatierung, die lediglich ein neues Inhaltsverzeichnis des Dateisystems anlegt, aber keine weiteren Änderungen vornimmt und die Festplatte auch nicht mit Nullen überschreibt.

## Daten komplett und unwiederbringlich löschen

Recuva kann zudem unerwünschte oder überflüssige Dateien restlos entfernen (Wiping-Funktion). Im Gegensatz zum normalen Löschen über den Windows-Papierkorb, werden beim Wiping nicht nur die Einträge im Inhaltsverzeichnis des Dateisystems entfernt, sondern auch die einzelnen Datenblöcke der zu löschenden Datei auf der Festplatte überschrieben. Dies sorgt dafür, dass selbst Recuva eine so gelöschte Datei nicht mehr wiederherstellen kann.

**Hinweis:** Das Setup-Programm der Freeware installiert gegebenenfalls zusätzliche Software auf dem Rechner. Die zusätzliche Software wird über das Internet nachgeladen und kann deshalb nicht vom Recuva-Hersteller Piriform auf Malware geprüft werden.

## Installation mit dem Microsoft Media Creation Tool

Mit dem Microsoft Media Creation Tool kann man einfach und kostenlos einen USB-Speicherstick (mindestens 8 GByte) als Installationsmedium für Windows 10 und 11 erstellen.

### 1. Download des Media Creation Tool

Neben dem »Erstellen von Installationsmedien für Windows 11«, kann man sich auch nur das Windows 11 ISO-Image herunterladen und später auf DVD brennen. Um den USB-Stick zu erstellen, klickt man auf »**Jetzt herunterladen**«. Das Media Creation Tool wird als ausführbare Datei heruntergeladen und kann unter Windows gestartet werden. Die Datei heißt hier »MediaCreationToolW11.exe«, die Datei kann aber auch einen anderen Namen haben.

### 2. Media Creation Tool starten

USB-Stick einstecken und das »Media Creation Tool« mit Administrator-Rechten (rechte Maustaste) starten.

### 3. Lizenzbedingungen akzeptieren

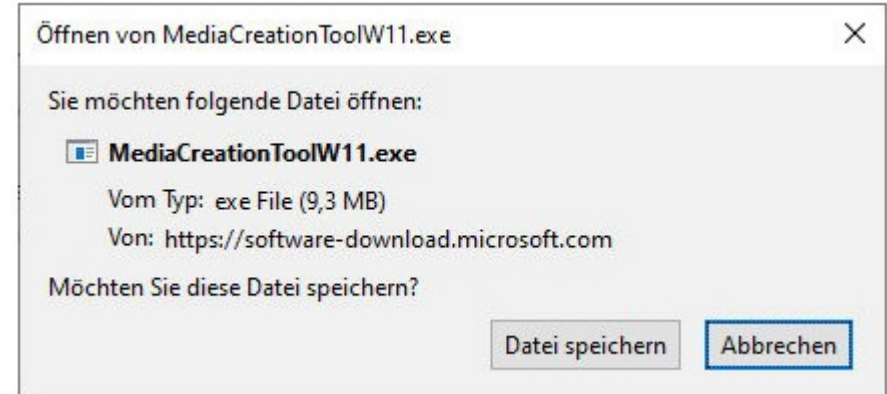
Im nächsten Schritt muss man die Lizenzbedingungen annehmen und auf »**Akzeptieren**« klicken.

### 4. Sprache und Edition auswählen

Die aktuelle Systemsprache und die Windows-Edition sind bereits eingetragen. Nach dem Entfernen des Haken in der Checkbox »**Empfohlene Optionen für diesen PC verwenden**«, kann man eine andere Sprache auswählen und auf »**Weiter**« klicken.

### 5. Zu verwendendes Medium auswählen

An dieser Stelle, kann man sich zwischen »USB-Speicherstick« und »ISO-Datei« entscheiden. »**USB-Speicherstick**« ist die richtige Auswahl.



### 6. USB-Speicherstick auswählen

USB-Stick aus der Laufwerksliste auswählen. Falls der USB-Stick nicht angezeigt wird, genügt ein Klick auf »Laufwerksliste aktualisieren«. Anschließend auf »**Weiter**« klicken.

### 7. Windows 11 wird heruntergeladen

Windows 11 (etwa 5,1 GB) wird jetzt heruntergeladen. Das Herunterladen dauert je nach Rechner und Internetverbindung mehrere Minuten. **Hinweis:** Der USB-Stick wird dabei komplett gelöscht und eventuell vorhandene Daten werden gelöscht.

### 8. Der USB-Speicherstick ist bereit

Mit einem Klick auf »**Fertig stellen**«, steht der USB-Stick zur Verfügung. Jetzt kann man sich auch noch die Verzeichnisstruktur des fertigen USB-Installationssticks anschauen. Auf dem USB-Stick können zusätzliche installierbare Programme, für die spätere Installation, gespeichert werden.

# Windows 11 und 10: Bootfähigen USB-Stick erstellen 2/3

## Windows to go: Windows auf USB-Stick installieren

»Windows To Go« installiert Windows auf einen USB-Stick und sorgt dafür, dass man das Betriebssystem immer dabei haben kann. Obwohl das Feature offiziell nur in der Enterprise-Version enthalten ist, kann man mit der Freeware »**WinToUSB**« jede Version von Windows 7, 8.1, 10 oder 11 auf einen USB-Stick bringen.

»Windows To Go« löst ein Problem, das vielen Nutzern gar nicht bewusst ist. Windows lässt sich nämlich nur auf interne Speichermedien installieren, will man es auf einen externen Datenträger installieren, verweigert der Installer seinen Dienst.

Bootet man den Windows-To-Go-Stick zum ersten Mal an einen fremden Rechner, wird die vorhandene Hardware erkannt und die nötigsten Treiber geladen. »Windows To Go« verwendet zudem automatisch die bestehende Internetverbindung, sowie die erkannten Ein- und Ausgabegeräte. Auch zusätzlich angesteckte USB-Sticks erkennt »Windows To Go« ohne Probleme. Sämtliche Änderungen, die man an Windows auf dem USB-Stick vornimmt, werden darauf gespeichert und sind beim nächsten Einsatz wieder verfügbar. Der Installation von Dropbox, Office oder Firefox steht somit nichts im Wege. Auf dem fremden Rechner hinterlässt man hingegen keine Spuren, er startet nach dem Entfernen des USB-Sticks wieder wie zuvor.

### Das wird benötigt:

- Einen USB-Stick mit mindestens 32 GB Speicherplatz, optimal mit USB 3.0.
- Eine ISO-Datei von Windows (Windows 11 oder Windows 10), optimalerweise als 64-Bit-Version.
- Das kostenlose Tool »WinToUSB«

### Anleitung

- Das Tool »WinToUSB« starten.
- Als erstes, in der oberen Zeile die heruntergeladene ISO-Datei auswählen. Danach zeigt das Tool darunter in der Liste die benutzbaren Windows-Versionen an. Eine Version auswählen und die Auswahl mit einem Klick auf »Weiter« bestätigen.
- Das USB-Laufwerk auswählen. Unter Umständen erinnert euch »WinToUSB« daran, dass der USB-Stick zu langsam ist, wenn man einen Stick mit USB 2.0 nutzt.  
**Achtung:** Der USB-Stick wird bei dem Vorgang formatiert. Alle Daten darauf gehen also verloren.
- Im nächsten Fenster wählt man die System-Partition und die Boot-Partition aus, indem man diese anklickt. Mit einem Klick auf »Weiter«, wird die Auswahl bestätigt. Das Tool »WinToUSB« kopiert Windows auf den USB-Stick. Der Vorgang kann je nach USB-Stick bis zu mehrere Stunden dauern.

### Windows vom USB-Stick starten

- Den USB-Stick mit Windows an den zu startenden Rechner einstecken.
- Den Rechner neu starten.
- Damit Windows vom USB-Stick bootet, müsst man unter Umständen die Boot-Reihenfolge im BIOS umstellen. Alternativ kann man über eine Taste oder Tastenkombination den Boot-Manager aufrufen (siehe: Handbuch des Rechners).
- Beim ersten Boot-Vorgang kann der Start von Windows etwas länger dauern (Hardware-Erkennung).



# Windows 11 und 10: Bootfähigen USB-Stick erstellen 3/3

## Windows 11 auf USB-Stick für Rechner ohne TPM 2.0 und Secure Boot

Mit Rufus lässt sich ein USB-Installationsstick (mindestens 8 GByte) für Windows 11 erstellen, bei dem die Hardware-Prüfung während der Installation nicht durchgeführt wird. **Hinweis:** Die Updates **können** durch diese Installationsmethode durch Microsoft eingeschränkt werden.

### 1. Download von Rufus (2 Varianten: Rufus und Rufus Portable)

Nach dem Download der ausführbaren Datei aus dem Internet, muss man das aktuelle Tool mit Administrator-Rechten (rechte Maustaste) starten. Eine Installation von Rufus ist nicht erforderlich.

### 2. USB-Laufwerk auswählen

Rufus sollte den bereits eingesteckten USB-Stick automatisch eingetragen haben.

### 3. Startart festlegen - ISO-Datei auswählen

Nach dem Öffnen der Anwendung ist die Quelle der ISO-Datei einzutragen. Falls keine ISO-Datei vorhanden ist, kann Rufus diese Datei auch aus offiziellen Quellen herunterladen.

### 4. Abbildeigenschaft festlegen

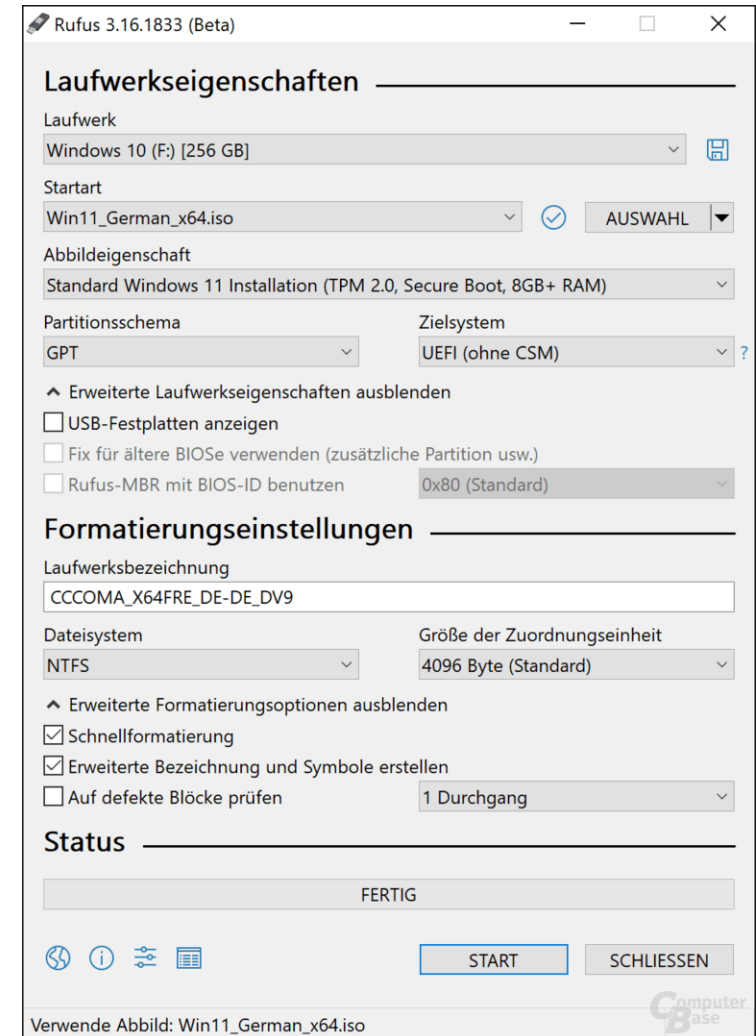
Bei Rufus ab der Version 3.16 findet man unter »**Abbildeigenschaft**« den Extended Installations-Modus für Windows 11. Auswahl des Eintrages: »**Extended Windows 11 Installation (no TPM / no Secure Boot / 8 GB- RAM)**«. Durch diese Auswahl wird während der Installation von Windows keine Hardware-Prüfung durchgeführt.

### 5. Partitionsschema und Zielsystem festlegen

In der Regel kann die Vorauswahl übernommen werden. Bei älteren Rechner, ohne GPT- und UEFI-Unterstützung, sind beim Partitionsschema der Eintrag »**MBR**« und beim Zielsystem der Eintrag »**BIOS oder UEFI**« auszuwählen. Die anderen Einträgen können ohne weiteres übernommen werden.

### 6. USB-Stick erstellen

Mit einem Klick auf den Button »**Start**« kann der bootfähige USB-Stick erstellt werden. **Hinweis:** Alle noch vorhandenen Daten auf dem USB-Stick werden gelöscht.



# Boot-Menü reparieren 1/3

Es kann immer mal wieder passieren, dass das Boot-Menü von Windows 10 oder 11 beschädigt wird. Während der Reparatur, sollte nur die Systemplatte angeschlossen sein. Bei allen anderen Festplatten sollte als Vorsichtsmaßnahme die Stromversorgung der Festplatten abgezogen werden.

## GPT (UEFI) Boot-Menü Reparatur mit der Recovery DVD oder Installations-DVD

- Die erstellte Recovery oder die Installations-DVD ins Laufwerk schieben und von der DVD starten.
- Wenn der Willkommens-Bildschirm der Windows-Installation erscheint, dann kann man unten links auf »Computerreparatur« klicken (Alternativ: [Umschalt] + [F10] -> Eingabeaufforderung).
- Nun gelangt man in die »Erweiterten Startoptionen« von Windows. An dieser Stelle die »Erweiterten Optionen« und dann »Eingabeaufforderung« anklicken.
- In der Eingabeaufforderung nun nacheinander diese Befehle eingeben und jeweils mit Enter bestätigen:

**diskpart**

**list vol**

**sel vol y** (Hinweis: y = die Nummer der Systempartition)

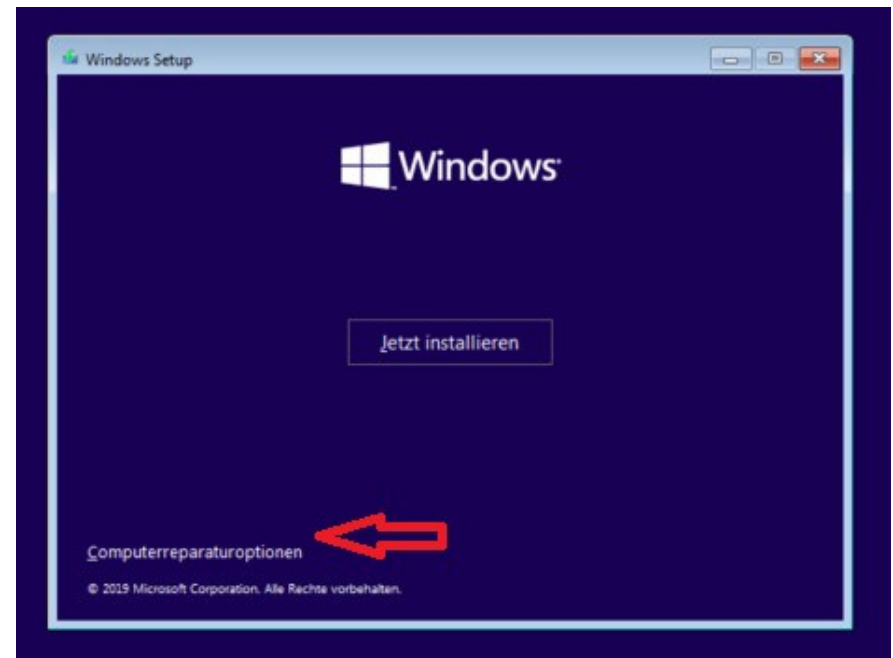
**format FS="Fat32" Quick**

Der EFI-Partition (EPS) wird nun ein Laufwerksbuchstabe zuweisen. Es können alle freien Laufwerksbuchstaben verwendet werden, mit Ausnahme des Buchstaben X. Der Buchstabe X ist für das System reserviert. Das Laufwerk X wird von Windows für die temporäre Boot-Umgebung (RAM disk) verwendet.

**assign letter=Z:** (Hinweis: Falls der Laufwerksbuchstabe vergeben ist, dann einen anderen freien Buchstaben benutzen.)

**exit**

- Jetzt sind wir wieder in der Eingabeaufforderung und können die UEFI-Bootpartition reparieren.
- In der Eingabeaufforderung nun **cd /d Z:\EFI\Microsoft\Boot\** eingeben und Enter drücken (Das Z ist hier durch den verwendeten Laufwerksbuchstaben zu ersetzen).
- **bcdboot c:\Windows /l de-de /s Z: /f UEFI** und Enter drücken für die Reparatur. c: = Startpartition, muss eventuell angepasst werden. - Auch hier ist der Laufwerksbuchstabe Z mit eurem Laufwerksbuchstaben zu ersetzen.
- Jetzt sollte das UEFI-Boot-Menü repariert sein und Windows 10 bzw. Windows 11 kann wieder starten.



## Boot-Menü reparieren 2/3

### MBR Boot-Menü Reparatur mit der Recovery DVD oder Installations-DVD

- Die erstellte Recovery oder die Installations-DVD ins Laufwerk schieben und von der DVD starten.
- Wenn der Willkommens-Bildschirm der Windows-Installation erscheint, dann kann man unten links auf »Computerreparatur« klicken.
- Nun gelangt man in die »Erweiterten Startoptionen« von Windows. An dieser Stelle die »Erweiterten Optionen« und dann »Eingabeaufforderung« anklicken.
- In der Eingabeaufforderung nun nacheinander diese Befehle eingeben ([Strg] + [C] und [Strg] + [V] - kopieren und einfügen) und jeweils mit Enter bestätigen:

**bootrec /fixmbr** (schreibt die mbr, aber überschreibt keine Partitionstabelle)

**bootrec /fixboot** (schreibt neuen Bootsektor auf die Systempartition)

**bootrec /scanos** (scannt nach anderen Betriebssystemen, die man mit bcdboot hinzufügen möchte)

**bootrec /rebuildbcd** (scannt nach einem installierten Betriebssystem und fügt diese dann in das Boot-Menü hinzu, dies ist der wichtigste Befehl)

- Nun kann der Rechner ohne DVD neu gestartet werden. **Hinweis:** Sollte der Befehl bootrec /rebuildbcd mit der Fehlermeldung »Systemgerät kann nicht gefunden werden« abgebrochen werden, kann es an den Bios-Einstellungen für UEFI/Bios liegen. Nach der Umstellung von UEFI/Legacy Boot: 'Both' auf 'Legacy Only' wird der Befehl möglicherweise ausgeführt.
- Nach der hoffentlich erfolgreichen Reparatur, ist die Umstellung im BIOS wieder rückgängig zu machen (UEFI/Legacy Boot: 'Both').

### Boot-Menü Reparatur mit der Windows-Starthilfe

Sollte Windows 10 trotzdem nicht booten, dann gibt es noch die Windows-Starthilfe.

- Auch hier wird wieder von der DVD / USB-Stick gebootet.
- Wenn der Willkommens-Bildschirm der Windows-Installation erscheint, dann kann man unten links auf »Computerreparatur« klicken.
- In den »Erweiterten Optionen« die »Starthilfe« auswählen.
- Windows versucht nun automatisch das Boot-Menü wiederherzustellen.



# Boot-Menü reparieren 3/3

## GPT (UEFI) Boot-Menü Reparatur mit der Recovery DVD oder Installations-DVD

- Die erstellten Recovery oder die Installations-DVD ins Laufwerk schieben und von der DVD starten.
- Wenn der Willkommens-Bildschirm der Windows-Installation erscheint, dann kann man unten links auf »Computerreparatur« klicken.
- Nun gelangt man in die »Erweiterten Startoptionen« von Windows. An dieser Stelle die »Erweiterten Optionen« und dann »Eingabeaufforderung« anklicken.
- In der Eingabeaufforderung nun nacheinander diese Befehle eingeben und jeweils mit Enter bestätigen:

**diskpart**

**list vol**

**sel vol y**

**Hinweis:** y = die Nummer der Systempartition

**format FS="Fat32" Quick**

Der EFI-Partition (auch EPS ... EFI-System-Partition) wird nun ein Laufwerksbuchstabe zuweisen. Es können alle freien Laufwerksbuchstaben verwendet werden, mit Ausnahme des Buchstaben X. Der Buchstabe X ist für das System reserviert. Das Laufwerk X wird von Windows für die temporäre Boot-Umgebung (RAM disk) verwendet.

**assign letter=Z:** (Hinweis: Falls der Laufwerksbuchstabe vergeben ist, dann einen anderen freien Buchstaben benutzen.)

**exit**

- Das Boot-Menü kann nun neu erstellt werden:

**bootsect /nt60 ALL /Force /MBR**

**bcdboot c:\Windows /l de-de /s Z: /f BIOS**

Der Eintrag c: für die Startpartition, muss eventuell angepasst werden. Wurde Z geändert, muss auch dieser Buchstabe angepasst werden.

Sollte, auch das nicht zum Erfolg führen, gibt es noch die Möglichkeit nachzuprüfen ob:

- Die Festplatte (HDD oder SSD) mit Windows 11 oder 10, am ersten Anschluss (Port) auf dem Motherboard angeschlossen ist.
- In der Bootreihenfolge im BIOS die HDD oder SSD an erster Stelle steht.
- Das SATA-Kabel überprüfen. Auch das Verbindungskabel kann einen Defekt haben.

**BIOS** ... Basic Input Output System; Das BIOS sind die auf einem nichtflüchtigen Speicher gespeicherten Anweisungen, welche die zentrale Hardware eines Computers (z.B. Prozessor, Chipsatz, Arbeitsspeicher) beim Gerätestart in funktionsfähigen Zustand bringt und im Anschluss daran den Start des Betriebssystems einleitet.

**UEFI** ... Unified Extensible Firmware Interface; Mit der Entwicklung von 64 Bit-Prozessoren musste aufgrund der Beschränkung von klassischen BIOS auf 32 Bit Prozessorarchitekturen ein Nachfolger entwickelt werden. EFI beziehungsweise UEFI, was für (Unified) Extensible Firmware Interface steht, wurde dieser Nachfolger. Erwähnenswert ist, dass (U)EFI abwärts kompatibel ist und somit 32 Bit und 64 Bit Architekturen unterstützt. Windows 10 unterstützt auf UEFI-Mainboards die Secure-Boot-Funktion, die nur noch den Start von als sicher eingestuft und zertifizierten Bootloadern und Treibern erlaubt.

# Abgesicherten Modus zum Boot-Menü hinzufügen Windows 10

Möchte man den Abgesicherten Modus gleich in dem Boot-Menü hinzufügen, so kann man dies mit Hilfe der Eingabeaufforderung (PowerShell) und bcdedit erledigen.

- [Win] + [X] drücken und die Eingabeaufforderung cmd oder Windows PowerShell (Administrator) starten
- **bcdedit**  
Zeigt den aktuellen Zustand mit einem Windows-Startladeprogramm (Bezeichner: current) an.

## **bcdedit /copy {current} /d "Windows 10 Abgesicherter Modus"**

Der Text zwischen den Anführungszeichen kann beliebig geändert werden. Nach dem Aufruf des Befehls erscheint eine {GUID}. Diese GUID ist für den nächsten Befehl zu verwenden.

- **bcdedit /set {guid} safeboot minimal {guid}**  
Die GUID (Zahlengruppe) ist zwischen den geschweiften Klammern (statt guid) einzutragen und zu bestätigen. Nach einem Neustart steht das blaue Boot-Menü zur Verfügung.  
Mit Netzwerktreiber sieht der bcdedit-Befehl so aus: **bcdedit /set {guid} safeboot network {guid}**  
Timeout des Boot-Menüs in Sekunden: **bcdedit /timeout 3**  
Von nun an erscheint der Abgesicherte Modus (ohne Netzwerktreiber) auch im Boot-Menü. Hat man Probleme, kann man nun ganz bequem den abgesicherten Modus aufrufen und auch über die Auswahl »Standardeinstellungen ändern oder andere Optionen auswählen« die Möglichkeit die Erweiterten Startoptionen von Windows aufzurufen. **Hinweis:** Falls man eine Fehlermeldung erhält »Der angegebene Kopierbefehl ist ungültig.«, dann kann man mit bcdedit den fehlerbehafteten Eintrag wieder löschen.  
**bcdedit /delete {guid}** mit **bcdedit /enum** ermittelt man die GUID (recoverysequence, siehe auch: **bcdedit /?**).

```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.99261]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>bcdedit.exe /copy {current} /d "Windows 10 Safe Mode"
The entry was successfully copied to {054cce21-a39e-11e4-99e2-de9099f7b7f1}.

C:\Windows\system32>
  
```



Boot-Menü mit den Einträgen für das Standardsystem und den Abgesicherten Modus. Im linken Bild ist die GUID zwischen den geschweiften Klammern zu erkennen.



# Was ist ein Wasserloch-Angriff? 1/2

## Woher stammt der Begriff Watering-Hole-Angriff?

In der Tierwelt bezeichnet ein Wasserloch eine Stelle, an der sich eine Gruppe Tiere regelmäßig versammelt, um zu trinken. In größeren Gruppen zum Wasserloch zu drängen ist zwar stressig, hat aber seinen Zweck. Das Auftreten in größeren Gruppen reduziert das Risiko jedes einzelnen Tieres Ziel eines Angriff durch einen Räuber zu werden.

In der Welt der IT funktioniert das Ganze etwas anders. Zwar leitet sich der Begriff »Watering-Hole-Angriff« von der gleichen Symptomatik ab, sprich eine ganz bestimmte Gruppierung von Benutzern besucht regelmäßig einen bestimmten Ort. Allerdings wird genau das Auftreten in der Gruppe hier von den Angreifern ausgenutzt. Das Risiko für einen Angriff an diesen Orten wird also nicht geringer, sondern ganz im Gegenteil höher.



## Was passiert bei einem Watering-Hole-Angriff?

Bei einem Watering-Hole-Angriff haben Angreifer eine ganz bestimmte Nutzergruppe als Ziel ausgewählt. Die Angreifer erstellen von ihrem Ziel eine Art Profil, um herauszufinden welche Websites als »Watering-Hole« dienen könnten. Daraufhin infizieren die Angreifer gezielt eine oder mehrere Websites mit Schadsoftware, die von einer Nutzergruppe regelmäßig besucht werden. Damit der Angriff auch erfolgreich sein kann, muss die gewählte Webseite auch Schwachstellen enthalten. Nun kann sich der Angreifer, ähnlich wie ein Raubtier am Wasserloch, auf die Lauer legen und warten bis seine Opfer von ganz alleine kommen. Ziel des Angriffs ist es, mindestens ein Opfer der Gruppe zu infizieren um so einen erweiterten Zugriff auf ein Netzwerk zu bekommen.

## Wie kann man sich vor dieser Art Angriff schützen?

Vor einem Watering-Hole-Angriff kann man sich auf ähnliche Art und Weise schützen, wie vor einem Drive-by-Download.

Wie häufig, ist besondere Aufmerksamkeit und das Bewusstsein für Risiken besonders wichtig:

- Klicken Sie nicht auf unbekannte Links.
- Spielen Sie Software-Updates so zeitnah wie möglich ein.
- Überlegen Sie sich, wem und wofür Sie Administratorrechte vergeben.
- Schulen Sie Ihre Mitarbeiter bezüglich möglicher Gefahren und Risiken.

**Hinweis:** Ein Drive-by-Download ist das unbewusste und unbeabsichtigte Herunterladen von Software auf einen Rechner. Unter anderem wird damit das unerwünschte Herunterladen von Schadsoftware allein durch das Aufrufen einer dafür präparierten Webseite bezeichnet.

# Was ist ein Wasserloch-Angriff? 2/2

## Cyberkriminelle und ihre psychologischen Tricks

Bei einem Watering-Hole-Attack versuchen die Angreifer von ihrem Ziel, mit verschiedenen Methoden (öffentlich zugängliche Informationen, Social Engineering, ...), eine Art Profil zu erstellen. Die Social Engineering-Strategie von Cyberkriminellen fußt auf starker zwischenmenschlicher Interaktion und besteht meist darin, das Opfer dazu zu verleiten, Standard-Sicherheitspraktiken zu missachten. Und so hängt der Erfolg von Social-Engineering von der Fähigkeit des Angreifers ab, sein Opfer so weit zu manipulieren, dass es bestimmte Aktionen ausführt oder vertrauliche Informationen preisgibt. Da Social-Engineering-Angriffe immer zahlreicher und raffinierter werden, sollten Organisationen jeder Größe eine intensive Schulung ihrer Mitarbeiter als erste Verteidigungslinie für die Unternehmenssicherheit einrichten und dauerhaft zur Verfügung stellen.

## Die Strategie der Cyberkriminellen: Trickbetrüger des digitalen Zeitalters

Social Engineering-Angreifer sind letztlich eine moderne Spielart der klassischen Trickbetrüger. Häufig verlassen sich diese Kriminellen auf die natürliche Hilfsbereitschaft von Menschen: Zum Beispiel rufen sie bei ihrem Opfer an und geben vor das ein dringendes Problem einen sofortigen Netzwerkzugang erfordert. Social Engineering-Angreifer nutzen auch gezielt bestimmte menschliche Schwächen wie Unsicherheit, Eitelkeit oder Gier aus und verwenden Informationen, die sie aus Lauschangriffen oder dem Ausspionieren sozialer Medien gewonnen haben. Dadurch versuchen sie, das Vertrauen autorisierter Benutzer zu gewinnen, damit ihre Opfer sensible Daten (Zugangsdaten für Netzwerke) preisgeben oder mit Malware infizierte E-Mail-Anhänge öffnen. Auch durch den Aufbau eines Schreckensszenarios, wie einem angeblichen Sicherheitsvorfall, kann eine Zielperson dazu bewegen getarnte Malware (Antiviren-Software oder andere

Anwendungen), zu installieren und auszuführen.

## Häufige Social Engineering-Methoden im Überblick

Technologielösungen wie E-Mail-Filter, Firewalls und Netzwerk- oder Daten-Überwachungs-Tools helfen zwar, Social Engineering-Attacken abzuschwächen, doch eine gut geschulte Belegschaft, die in der Lage ist, Social Engineering zu erkennen, ist letztlich die beste Verteidigung gegen diese Art Angriffe. Unternehmen sollten ihre Mitarbeiter deshalb umfassend über die gängigen Arten von Social-Engineering aufklären.

Social-Engineering-Methoden im Überblick:

- **Pretexting (Vorwand):** Beim Pretexting schützt ein Angreifer geschickt falsche Tatsachen vor, um ein Opfer dazu zu bringen, ihm Zugang zu sensiblen Daten oder geschützten Systemen zu gewähren.
- **Baiting (physische Köder):** Angreifer führen Köderangriffe durch, indem sie ein mit Malware infiziertes Gerät wie ein USB-Flash-Laufwerk, an einem bestimmten Ort (Parkplatz, Konferenzräume, Kaffeeautomat, ...) im Unternehmen zurücklassen, an dem es wahrscheinlich gefunden wird.
- **Tailgating (zu dichtes Auffahren):** Der Begriff Tailgating (Tailgate ... Heckklappe) erinnert an Krimiszenen, bei denen der Protagonist bei der Autofahrt einen Verfolger im Rückspiegel entdeckt, der ihm quasi an der Heckklappe klebt. Dadurch kann ein Unbefugter, der autorisierten Personen an einen ansonsten gesicherten Ort folgt, Zugang erlangen (Ausrede: Zugangskarte vergessen, Notebook für eine simple Aufgabe ausleihen, ...).
- **Quid pro quo:** Bei einem Quid pro quo-Angriff (lat.: dies für das) locken Cyberkriminelle ihre Opfer mit einer Gegenleistung oder Entschädigung, um sensible Informationen zu erlangen.

# Lieferketten-Angriffe 1/3

## Was ist ein Lieferketten-Angriff?

In unserer zunehmend digitalisierten Welt sind IT-Angriffe so selbstverständlich geworden wie Überfälle auf die Postkutsche im Wilden Westen. Bei solchen Angriffen sind allerdings nicht mehr Gold und Banknoten die Beute. Häufiges Ziel sind heutzutage sensible Daten, die beispielsweise verschlüsselt werden (Ransomware-Angriff), um anschließend Lösegeld zu erpressen. Neben den Angriffszielen haben sich auch die Täter und ihre Methoden verändert. Was gleich geblieben ist: Ein erfolgreicher Überfall will gut geplant, mögliche Schwachpunkte ausgemacht sein. Eine zunehmend beliebte Strategie, um Sicherheitsbarrieren zu umgehen, sind Angriffe, die mit der Lieferkette von IT-Systemen zusammenhängen. Die Angreifer suchen sich dabei das schwächste Glied in der Lieferkette (Supply Chain) aus, das sie infiltrieren und durch das sie Zugriff auf die eigentlich interessanten Ziele bekommen.

Solche Angriffe über die Lieferkette haben in den letzten zehn Jahren sowohl im Hinblick auf das Sicherheitsverständnis als auch auf die Angriffsmöglichkeiten an Bedeutung gewonnen. So werden beispielsweise immer mehr Vorfälle registriert, bei denen bereits mit Schadsoftware infizierte IT-Systeme geliefert und eingebaut werden. Neben der Manipulation von Hardware vor der Lieferung gibt es weitere Angriffsformen, wie das Einschleusen von schadhaftem Code in Software durch die Manipulation von Software-Updates. Eine weitere Möglichkeit sind Angriffe über identifizierte Schwachstellen im Programmcode.

Die infizierten Systeme kommen in der Regel von Zulieferern, die häufig selbst nicht wissen, dass ihr Produkt manipuliert wurde. Betroffen sind nicht nur Bürocomputer, sondern auch industrielle Steuerungssysteme einschließlich betrieblicher Leittechnik und Sicherheitsleittechnik oder sogenannte IoT-Geräte (Internet of Things), die über das Internet verknüpft sind und Daten und



Informationen austauschen. Ein prominentes Beispiel für typische IT-Angriffe über die Lieferkette ist der Angriff über manipulierte Produkte des US-amerikanischen Unternehmens SolarWinds von 2020: Tausende Kunden von SolarWinds wurden durch die Produkte kompromittiert. Eine Vielzahl von US-Behörden und Unternehmen wurde teils monatelang unbemerkt mithilfe einer Spionagesoftware ausgespäht, die sie sich über ein manipuliertes Update der Netzwerkmanagement-Software Orion von SolarWinds eingefangen hatten. Zu den Geschädigten zählten unter anderem das US-amerikanische Finanz- und Außenministerium, Teile des Pentagons sowie das US-Energieministerium mitsamt seiner untergeordneten National Nuclear Security Administration, die das Atomwaffenarsenal der USA verwaltet; auch in Deutschland und Europa gab es Betroffene.

**Hinweis:** Auch kritische Infrastrukturen wie KKW (Kernkraftwerke bzw. Atomkraftwerke) können Ziel dieser Angriffe werden.

### Kaseya - Angriff auf die Fernwartungssoftware VSA

Kaseya Limited ist ein US-amerikanisches Unternehmen, das Software für die Verwaltung von Netzwerken und Systemen sowie Informationstechnologie-Infrastruktur entwickelt. Es hat seinen Hauptsitz in Miami, Florida und verfügt über Niederlassungen in den USA, Europa und im asiatisch-pazifischen Raum. Seit seiner Gründung im Jahr 2000 hat es 13 Unternehmen übernommen, die in den meisten Fällen als eigene Marken unter dem Slogan »a Kaseya company« weitergeführt werden. Das Produkt VSA (Virtual System Administrator) des Unternehmens ist eine Fernwartungssoftware. Mit VSA lassen sich beliebige Rechner oder Rechnersysteme fernwarten, etwa für Überwachungen, Reparatur- oder Wartungsarbeiten. Unter anderem wird VSA häufig zum einfachen Einspielen von Softwareaktualisierungen verwendet.

### Cyberattacke auf die VSA-Server von Kaseya (2021)

Am 2. Juli 2021 wurden mehrere Managed Service Providers (MSPs) und deren Kunden Opfer eines Ransomware-Angriffs, der von der REvil-Gruppe (verwendeten unter anderen das Kommandozeilen-Werkzeug curl und SQL Injection-Angriffe) verübt wurde. Als Quelle des Ausbruchs wurde innerhalb weniger Stunden die Kaseya Software VSA identifiziert. Als Reaktion darauf schaltete das Unternehmen seinen VSA-Cloud-Service ab und gab einen Sicherheitshinweis für alle Kunden heraus, einschließlich solcher mit VSA-Installationen vor Ort. Die Anzahl der von dem Angriff betroffenen Unternehmen ist bisher unklar. Zu den ersten Berichten über betroffene Unternehmen gehört der norwegische Finanzsoftware-Entwickler Visma (ERP-Lösungen, ERP steht für Enterprise Resource Planning), zu dessen Kunden auch die schwedische Supermarktkette Coop gehört, die nach dem Angriff vorübergehend landesweit über 800 Filialen wegen ausgefallener Kassensysteme schließen musste. Auch die staatlichen Eisenbahnen Schwedens und eine Apothekenkette meldeten Probleme.

### So funktioniert diese Methode der Cyberkriminellen

Das Schockierende am Hack ist der Weg, den die Angreifer eingeschlagen haben. Ihnen ist es gelungen, eine Schwachstelle im System des



IT-Dienstleisters Kaseya zu finden. So konnten sie sich Zugang zum System verschaffen und in aller Ruhe einen ausgefeilten Angriff vorbereiten. Kaseya wartet die IT-Systeme mehrerer tausend Unternehmen und ist maßgeblich für deren IT-Sicherheit verantwortlich. Der Service wird gerne von Unternehmen genutzt, die keine eigenen Spezialisten für IT-Sicherheit beschäftigen und dennoch ihre Systeme auf hohem Niveau schützen möchten. Doch genau dies wurde einigen zum Verhängnis. Die Hacker nutzten den Wartungsdienst von Kaseya, um an deren Kundensysteme ihre Schadsoftware auszuspielen. Kaum war dies geschehen, konnten die Systeme auch schon verschlüsselt werden. Den Sicherheitsexperten bereiten nun gleich zwei Dinge Sorgen. Da wäre zunächst das Ausmaß solcher Angriffe. Mit nur einer gezielten Attacke ist es möglich, unzählige IT-Systeme zu erreichen. Darüber hinaus die Tatsache, dass die Opfer alles richtig gemacht haben. Sie trifft keine Schuld, schließlich haben sie die Leistungen von Kaseya gebucht, um ihre Systeme professionell abzusichern.

**Lösung:** Zur Absicherung von Systemausfällen müssen Backupsysteme bereitgestellt werden. Diese müssen von den anderen Systemen abgekoppelt sein, um im Falle eines Angriffs unversehrt zu bleiben.



## SolarWinds - Angriff auf die Orion-Plattform

SolarWinds (Sitz in Austin, Texas; Wertpapierbörse: New York Stock Exchange) ist ein auf Netzmanagement-Software spezialisiertes US-amerikanisches Unternehmen. Das rasche Wachstum der Gesellschaft und die erhebliche Ausweitung des Produktspektrums seit 2007 erfolgte vor allem durch zahlreiche Akquisitionen in den Bereichen Performance Management, Informationssicherheit, Netzwerk-Monitoring, Datenbankmanagement und Datenanalyse, wobei sie mit anderen IT-Unternehmen wie Microsoft, Oracle und Cisco zusammenarbeitet. Ein wichtiges Produkt von SolarWinds ist die Orion-Plattform, eine skalierbare Überwachungs- und Verwaltungsplattform für die gesamte IT-Infrastruktur, die außer von (meist US-amerikanischen) Großunternehmen auch von zahlreichen Regierungskunden genutzt wird. Im September 2019 wurde die Plattform Ziel des »größten digitalen Angriffs des Jahrhunderts« wie es beispielsweise im DLF-Radio, mit Bezug auf Sicherheitsexperten, heißt.

### Das Hacking-Opfer SolarWinds: Ein perfekt ausgeführter Lieferketten-Angriff

Einfach haben es sich die Hacker in diesem Fall sicherlich nicht gemacht: Sie nutzten keine herkömmlichen Angriffswege wie ungepatchte Software-Schwachstellen oder Phishing-Kampagne. Um Zugang zu erhalten, gingen sie den höchst anspruchsvollen Weg über die Lieferkette. Dabei sind die Angreifer nach der erfolgreichen Infiltrierung bei SolarWinds in behördliche und privatwirtschaftliche Rechnernetzwerke in den USA und Europa in bisher unerreichtem Umfang eingedrungen. In der Vorbereitungsphase nahmen sich die Hacker viel Zeit. Laut SolarWinds drangen die Angreifer am 4. September 2019 in die Entwicklungsumgebung des Unternehmens ein und begannen sogleich mit dem Testen ihres bösartigen Codes. Er zielte darauf ab, Backdoors in die Orion Plattform einzuschleusen. Völlig unentdeckt hielten sich die Hacker monatelang in der Softwareentwicklungs-Plattform des Unternehmens auf. Mittlerweile



weiß man aufgrund einer technischen Analyse von CrowdStrike, etwas mehr. Die Angreifer testeten, ob sie ihre bösartige Sunburst-Backdoor erfolgreich in Orion-Produkte einfügen konnten, ohne die Entwickler bei SolarWinds zu alarmieren. Die Malware Sunspot wurde von den Hackern speziell entwickelt, um den Entwicklungsprozess bei SolarWinds zu untergraben.

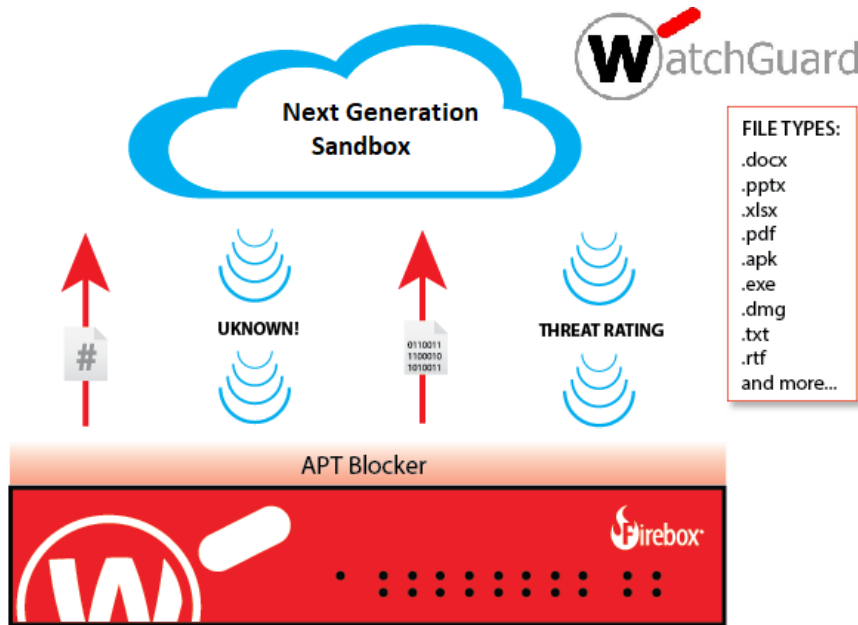
Die Sunspot Malware war so raffiniert geschrieben und getarnt, dass sie erkennen konnte, ob Entwickler auf bestimmte Orion-Quelldateien zugreifen. Quellcode-Dateien konnte gleich während des Build-Prozesses ersetzt werden. Außerdem waren auch Schutzmechanismen eingebaut, die verhinderten, dass die Backdoor-Codezeilen in den Build-Protokollen der Orion-Software auftauchen würden. Auch Überprüfungen wurden durchgeführt, um sicherzustellen, dass die Manipulationen keine Build-Fehler verursachen würden. Monate vor dem Update-Release liefen Testläufe über wechselnde IP-Adressen ab, die alle unentdeckt blieben. Ganz clever war auch, dass Sunburst im Update erst 11 Tage später aktiviert wurde, um eine Entdeckung möglichst nicht mit dem Update zu verknüpfen. Das Vorgehen der Hacker war besonders wirkungsvoll, da etwa 18.000 in- und ausländische Unternehmen und Regierungsbehörden weltweit die Orion-Software direkt verwenden. Laut dem Leiter des Bundesamtes für Sicherheit in der Informationstechnik, nutzten nur drei deutsche Behörden die Solarwinds Orion Plattform.

**Lösung:** Zur Absicherung von Systemausfällen müssen Backupsysteme bereitgestellt werden. Diese müssen von den anderen Systemen abgekoppelt sein, um im Falle eines Angriffs unversehrt zu bleiben



# APT-Blocker 1/3

## WatchGuard APT Blocker



WatchGuard Technologies (gegründet 1996 unter dem Namen Seattle Software Labs) ist ein Anbieter von Internet-Sicherheitslösungen mit Sitz in Seattle (USA). Bekannt wurde WatchGuard durch ihre Firewall und VPN-Lösung für kleine und mittelständische Unternehmen. WatchGuard ist einer der Pioniere im Bereich des Unified Threat Management und hat den Begriff Extensible Threat Management 'XTM' für Ihre Produkte kreiert.

Watchguard APT Blocker ist eine sinnvolle Ergänzung zu einer vorhandenen desktopbasierten Antivirus-Lösung. Der Einsatz von Antivirus-Software ist heute selbstverständlich. Allerdings reichen die handelsüblichen, signaturbasierten Lösungen als Schutz heute nicht mehr aus.

APT Blocker (APT.. Advanced Persistent Thread) sind ein Hilfsmittel, das auch in der Zeit zwischen dem Auftreten eines neuen Virus, dem Erkennen des Virus durch die Antiviren-Software-Hersteller und dem Update der Antivirus-Software in der Lage ist Endgeräte auch vor unbekannten Bedrohungen zu schützen.

### Funktionsweise

WatchGuard APT Blocker analysiert unter anderem alle ausführbaren Windows-Dateien, PDFs, Office-Dateien und Android-Installer-Dateien. Archive, wie z.B. ZIP-Dateien werden entpackt und analysiert. Die Dateien werden gegen die Cloud-Datenbank von Lastline geprüft und nötigenfalls (falls unbekannt) an den Cloud-Service zur genaueren Untersuchung übertragen. Die Dateien werden dann in einer Sandbox tatsächlich ausgeführt, um am Verhalten der Dateien deren Bösartigkeit feststellen zu können. Eine Rückmeldung über gefundene und geblockte Dateien mit Detailinformationen über die gefundene Bedrohung runden den Service ab.

WatchGuard APT Blocker kann in jeder Application Proxy Firewall-Regel aktiviert werden, in der auch Gateway Antivirus zur Verfügung steht. Somit ist ein Schutz der wichtigen Protokolle wie STMP, FTP, HTTP und sogar HTTPS mit Deep Inspection möglich. Das Logging und Reporting für WatchGuard APT Blocker erfolgt über den schon mit dem Basisprodukt zur Verfügung gestellten WatchGuard Dimension. Die Log-Einträge und Statistiken können über diese Plattformen gesichtet und ausgewertet werden.



**Hinweis:** Lastline, Inc. ist ein amerikanisches Cybersicherheits-Unternehmen und Anbieter einer Plattform zur Erkennung von Sicherheitsverletzungen mit Sitz in Redwood City, Kalifornien.

## Vorbeugung, Erkennung und Auflösung

WatchGuard APT Blocker konzentriert sich auf die Verhaltensanalyse, um festzustellen, ob eine Datei bösartig ist. Das Programm identifiziert verdächtige Dateien und sendet sie an eine cloudbasierte Sandbox, in der der Code emuliert und die Datei analysiert wird, um ihr Bedrohungspotenzial zu ermitteln. Wenn eine verdächtige Datei als bösartig beurteilt wird, schreitet der APT Blocker ein und stellt sicher, dass das Netzwerk und Ihre digitalen Assets (Geräte, Server, Vermögenswerte) sicher bleiben.

## Volle Systememulation simuliert physische Hardware

Moderne Schadprogramme, darunter auch Advanced Persistent Threats (APTs), Ransomware und Zero-Day-Angriffe, sind so konzipiert, dass sie die traditionellen Verteidigungsmaßnahmen erkennen und umgehen. Die volle Systememulation von APT Blocker simuliert eine physische Hardware (einschließlich CPU und Speicher) und bietet den umfassendsten Schutz vor modernen Schadprogrammen.

## Zusammenspiel von APT Blocker mit einem E-Mail-Gateway

Nach wie vor verwenden Angreifer gerne den Weg über E-Mails, um Schadsoftware - speziell Ransomware zu verbreiten. Je mehr Kontrollen und Schutzbarrieren überwunden werden müssen, bevor eine eingehende E-Mail ihren Empfänger erreicht, desto höher ist die Gesamtsicherheit des E-Mail-Systems. Im Optimalfall kombiniert man Sicherheitsprodukte von verschiedenen Herstellern. So baut man eine Produkt-Kaskade auf.

So arbeiten auf einer WatchGuard Firebox mit dem spamBlocker, Gateway Antivirus und dem APT Blocker bereits drei verschiedene Technologieanbieter Hand in Hand. Dieser Schutz kann noch weiter verbessert werden, wenn ein zusätzliches, spezialisiertes E-Mail-Security-Gateway zum Einsatz kommt, welches in der DMZ (Demilitarisierte Zone) einer WatchGuard Firebox betrieben wird.



## Wichtige Funktionen des APT Blockers

- Er bietet erweiterten Schutz vor Ransomware, Advanced Persistent Threats (APTs), Zero-Day-Exploits und sich weiterentwickelnden Malware
- Analysiert gründlich ausführbare Programme und Dokumente, sowie Office-Dateien
- Nahtlose Integration in WatchGuard Dimension für die komplette Visualisierung
- Sekundenschnelle Bereitstellung als Teil einer integrierten Sicherheitslösung
- Umgehende Reaktion auf Bedrohungen mit automatisierten Alarmen
- Durchschnittliche Analysezeit beträgt unter zwei Minuten

## Lizensierung

WatchGuard APT Blocker ist ein optionaler Security Service. Er ist Bestandteil der WatchGuard Total Security Software Suite. Er ist standardmäßig beim Kauf eines Total Security Software Bundles enthalten, kann aber auch einzeln lizenziert werden. Technische Voraussetzung ist zudem die Lizenz für »WatchGuard Gateway Antivirus«.

## Ablauf eines Advanced Persistent Threats-Angriff

Die meisten APT-Angriffe werden in mehreren Phasen durchgeführt, die den gleichen grundlegenden Ablauf widerspiegeln: sich Zugang verschaffen, den Zugang aufrechterhalten und erweitern und versuchen unentdeckt zu bleiben, bis die Ziele des Angriffs erreicht sind. Da die Durchführung von APT-Angriffen häufig viel Aufwand und Ressourcen erfordert, sind die Ziele oft entsprechend bedeutend - wie Nationalstaaten, Behörden oder große Unternehmen. Die Absicht der Angreifer ist häufig, über einen langen Zeitraum unentdeckt zu bleiben und Informationen zu stehlen.

In der Regel gehen APT-Angreifer nach folgendem Schema vor, um sich Zugang zu einem Ziel zu verschaffen und diesen aufrechtzuerhalten:

**Zugang erlangen:** APT-Gruppen verschaffen sich Zugang zu einem Ziel, indem sie von außen über das Internet auf Systeme zugreifen. Normalerweise gelangen sie an Daten und Zugang durch Spear-Phishing-Mails oder Softwareschwachstelle und können dann Schadsoftware einschleusen.

**Hinweis:** Beim klassischen Phishing werden große Mengen von E-Mails wahllos an Empfänger verschickt, um sie dazu zu bringen, auf schädliche Links zu klicken oder vertrauliche Informationen preiszugeben. Beim Spear Phishing werden die Empfänger hingegen sorgfältig recherchiert und ausgewählt und erhalten E-Mails, die auf sie persönlich zugeschnitten sind und viel glaubwürdiger wirken.

**Sich im Ziel etablieren:** Nachdem sie sich Zugang zum Ziel verschafft haben, nutzen Bedrohungsakteure ihren Zugang, um weitere Erkundungen durchzuführen. Sie nutzen die von ihnen installierte Malware, um Netzwerke mit Hintertüren und Tunneln

zu schaffen, durch die sie sich unbemerkt bewegen können. Dabei setzen APTs auch fortgeschrittene Malware-Techniken ein, wie das kontinuierliche Verändern von Code, um ihre Spuren zu verwischen.

**Zugang ausbauen und erweitern:** Sobald sie in das Zielnetzwerk eingedrungen sind, können APT-Akteure Methoden wie das Knacken von Passwörtern anwenden, um sich administrative Rechte zu verschaffen. Dadurch erhalten sie mehr Kontrolle über das System und können einen noch weitreichenderen Zugang erlangen.

**Seitwärts bewegen:** Sobald Bedrohungsakteure in ihre Zielsysteme eingedrungen sind und sich Administratorrechte verschafft haben, können sie sich nahezu beliebig im Netzwerk bewegen. Sie versuchen, auf andere Server sowie auf andere sichere Bereiche des Netzwerks zuzugreifen.

**Angriff inszenieren:** Zu diesem Zeitpunkt sammeln, verschlüsseln und komprimieren die Hacker die Daten, damit sie sie exfiltrieren können. Daten-Exfiltration, auch Data Extrusion genannt, bezeichnet den nicht autorisierten Transfer, Übertragung von Daten.

**Abziehen der Daten.** Die Angreifer sammeln die Daten und übertragen sie auf ihre eigenen Systeme.

**Bis zur Entdeckung im System bleiben:** Cyberkriminelle können diesen Vorgang über lange Zeiträume wiederholen, bis sie entdeckt werden. Oder sie legen eine Hintertür an, um später erneut auf das System zugreifen zu können.

**Hinweis:** Die Erkennung von Anomalien und ungewöhnlichem Verhalten in ausgehenden Daten ist für Security-Experten vermutlich der beste Ansatz, um festzustellen, ob ein Netzwerk das Ziel eines APT-Angriffs war.

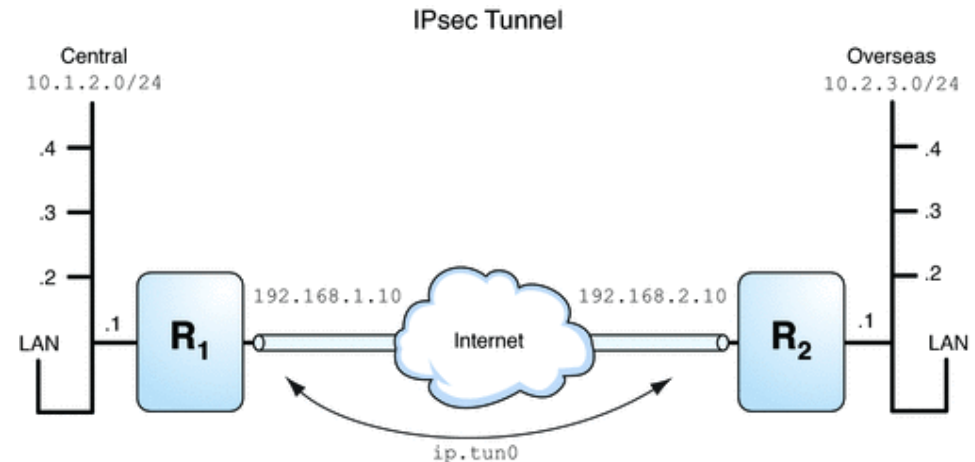
# IPsec - Verschlüsselung und Paketfilter 1/3

IPSec (Internet Protocol Security) ist eine Protokoll-Suite, die eine gesicherte Kommunikation über potentiell unsichere IP-Netze wie das Internet ermöglichen soll. IPSec ist eine Weiterentwicklung der IP-Protokolle.

## IPSEC - Verschlüsselung und Paketfilter - Nutzung von IPsec zur Verschlüsselung von Netzwerkverkehr

Das Ziel von IPSec ist es, eine verschlüsselungs-basierte Sicherheit auf Netzwerkebene bereitzustellen. IPSec bietet durch die verbindungslose Integrität sowie die Zugangskontrolle und Authentifikation der Daten diese Möglichkeit an. Zudem wird durch IPSec die Vertraulichkeit sowie Authentizität der Paketreihenfolge durch Verschlüsselung gewährleistet.

IPSec beinhaltet eine Suite von Internetstandardprotokollen, die eine sichere, verschlüsselte Kommunikation zwischen zwei Computern über ein nicht geschütztes Netzwerk ermöglichen. Die Verschlüsselung erfolgt auf der IP-Netzwerkschicht (Internet Layer-Vermittlungsschicht, entspricht OSI Layer 3, OSI .. Open Systems Interconnection), was bedeutet, dass sie für die meisten Anwendungen, die bestimmte Protokolle für die Netzwerkkommunikation verwenden, transparent ist. Darüber hinaus bietet IPSec eine End-to-End-Sicherheit. Dies bedeutet, dass die vom sendenden Computer verschlüsselten IP-Pakete während der Übertragung unlesbar sind und nur vom Empfängercomputer entschlüsselt werden können. Damit eine noch höhere Sicherheit erreicht werden kann, werden in diesem Vorgang Verschlüsselungs-Algorithmen verwendet, um einen einzigen Verschlüsselungsschlüssel zu erstellen. Dieser Schlüssel wird an beiden Enden der Verbindung verwendet, so dass er nicht über das Netzwerk weitergeleitet werden muss.



IPSec kann für die Ausführung einer oder mehrerer der folgenden Sicherheitsfunktionen konfiguriert werden:

- Authentifizieren des Absenders der IP-Datenpakete auf der Basis der Kerberos-Authentifizierung, digitaler Zertifikate oder eines gemeinsam genutzten Schlüssels (Kennwort)
- Sicherstellen der Integrität der über das Netzwerk übertragenen IP-Datenpakete
- Verschlüsseln aller über das Netzwerk gesendeten Daten mit absoluter Vertraulichkeit
- Verbergen der ursprünglichen IP-Adressen während der Übertragung

Mit diesen Funktionen kann man sicherstellen, dass der Netzwerkverkehr während der Übertragung vor Datenänderungen geschützt ist und die Daten nicht von nicht authentifizierten Benutzern abgefangen, angezeigt oder kopiert werden können. Wie auch bei anderen Sicherheitsrichtlinien kann man die IPSec-Richtlinien auf lokaler Ebene oder auf Domänenebene anwenden.

# IPsec - Verschlüsselung und Paketfilter 2/3

## Nutzung von IPsec als Paketfilter zur Isolierung vom Internet

Ohne weiteres lässt sich IPsec als leitungsfähiger Paketfilter (packetfilter-basierte Firewall) einsetzen. Sie können Ihren Server mit folgendem Verfahren gegen jegliche Angriffe aus dem Internet schützen, indem Sie alle Zugriffe aus dem Internet verbieten und nur noch das eigene vertraute Netz zulassen.

**Beispiel:** IPsec-Paketfilter unter Windows über die Kommandozeile konfigurieren, um ein System vor Angriffen zu schützen.

Das Beispiel soll die Wirksamkeit einer solchen Konfiguration verdeutlichen. Bei der Arbeit im Web infiziert Malware ein System mit einem Trojaner. Dieser Trojaner versucht eine Verbindung mit seinem Heimatsystem (Master-Rechner) aufzunehmen, um eventuell weitere Software herunterzuladen und zu installieren und/oder das Heimatsystem über eine weitere PC-Drohne zu informieren, welche für zukünftige Zwecke benutzt werden kann.

Da das System vom Internet isoliert wurde, schlägt die Verbindung zum Heimatsystem des Trojaners fehl. Somit ist der Trojaner wirkungslos.

## Konfigurieren eines IPSec-Paketfilters per Kommandozeile

Das folgende Netsh-Skript blockt sämtlichen IP-Verkehr und lässt nur den Zugriff aus dem Subnetz 192.168.1 zu. **siehe auch:** cmd -> netsh /?

### Syntax von netsh:

```
netsh [-a Aliasdatei] [-c Kontext] [-r Remotecomputer] [-u
[Domänenname]Benutzername] [-p Kennwort | *] [Befehl | -f Skriptdatei]
```

### 1. Anlegen der Policy

```
netsh.exe ipsec static add policy name="IPFilter" description="IP Filter
Policy"
```

### 2. Anlegen der Filteraktionen

```
netsh.exe ipsec static add filteraction name=Block
description="Blocks Traffic" action=block
```

```
netsh.exe ipsec static add filteraction name=Permit
description="Permit Traffic" action=permit
```

### 3. Anlegen der Filterliste »All Traffic«

```
netsh.exe ipsec static add filterlist name="All Traffic"
description="All Traffic"
```

```
netsh.exe ipsec static add filter filterlist="All Traffic" srcaddr=me
dstaddr=any description="All Traffic" protocol=any srcport=0
dstport=0
```

### 4. Anlegen der Filterliste »Trusted Traffic«

```
netsh.exe ipsec static add filterlist name="Trusted Traffic"
description="Trusted Traffic"
```

```
netsh.exe ipsec static add filter filterlist="Trusted Traffic"
srcaddr=me dstaddr=192.168.1.0 dstmask=255.255.255.0
description="Trusted Traffic" protocol=any srcport=0 dstport=0
```

### 5. Anlegen der Regel »Block« zum Blocken sämtlichen IP-Verkehrs

```
netsh.exe ipsec static add rule name="Block" policy="IPFilter"
filterlist="All Traffic" filteraction=Block
```

### 6. Anlegen der Regel »Trusted« zum Erlauben des IP-Verkehrs aus dem Subnetz 192.168.1

```
netsh.exe ipsec static add rule name="Trusted" policy="IPFilter"
filterlist="Trusted Traffic" filteraction=Permit
```



# IPsec - Verschlüsselung und Paketfilter 3/3

## 7. Aktivieren der Policy »IPFilter«

netsh.exe ipsec static set policy name="IPFilter" assign=yes

### Terminologie

Die folgenden Begriffe können für die Erstellung IPsec-Richtlinien hilfreich sein.

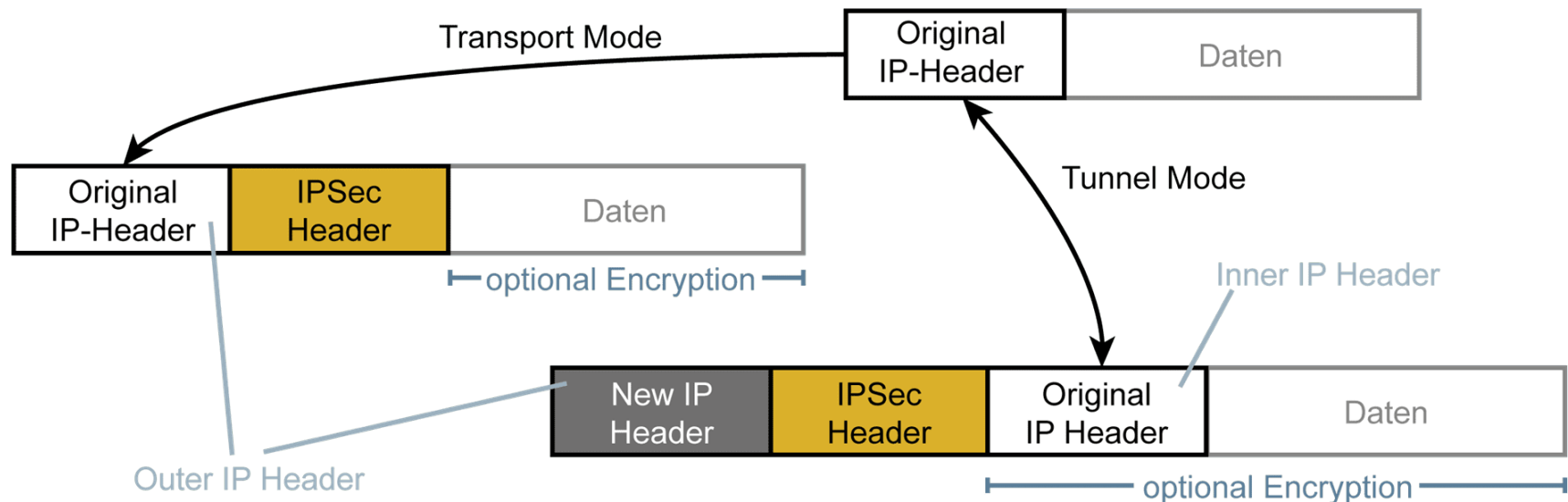
- **Filterliste:** Ports, Protokolle und Richtungen; löst eine Entscheidung aus, wenn der Datenverkehr mit den in der Liste festgelegten Kriterien übereinstimmt. Eine Liste kann mehrere Filter enthalten. Sie wird aus dem zuvor erstellten Schema abgeleitet.
- **Filteraktion:** Die erforderliche Reaktion, wenn der Datenverkehr mit einer Filterliste übereinstimmt. Im vorliegenden Fall treffen nur die Aktionen »Zulassen« und »Blockieren« zu.
- **Regel:** Direkter Zusammenhang einer Filterliste mit einer Filteraktion. Dient im Allgemeinen zum Festlegen von Parametern für die IPsec-Sicherheitsaushandlung.

- **Richtlinie:** Eine Zusammenstellung von Regeln. Es kann jeweils nur eine Richtlinie aktiv »zugewiesen« sein.

### Konfigurieren eines IPsec-Paketfilters per GUI (Graphical User Interface)

**Aufruf und Konfiguration:** Ausführen-Dialog aufrufen: [Win] + [R] -> gpedit.msc -> Computerkonfiguration -> Windows-Einstellungen -> Sicherheitseinstellungen -> IP-Sicherheitsrichtlinien auf Lokaler Computer -> rechte Maustaste -> IP-Sicherheitsrichtlinie erstellen... -> IP-Sicherheitsrichtlinie-Assistent -> [...]

**siehe auch:** [Win] + [R] -> secpol.msc -> MMC-Snap-In lokale Sicherheitsrichtlinie -> [...]



# Syntaxparameter für Netsh – was bedeuten sie? 1/2

Netsh ist ein Befehlszeilen-Skripthilfsprogramm, mit dem die Netzwerkkonfiguration eines Computers angezeigt oder geändert werden kann, die aktuell ausgeführt wird. Netsh-Befehle können durch Eingabe von Befehlen an der Netsh-Eingabeaufforderung ausgeführt und in Batchdateien oder Skripts verwendet werden. Remotecomputer und der lokale Computer können mithilfe von Netsh-Befehlen konfiguriert werden.

Netsh bietet auch eine Skriptingfunktion, mit der man eine Gruppe von Befehlen im Batchmodus für einen bestimmten Computer ausführen kann.

**Hinweis:** Für die netsh-Kommandos sollte nur die Powershell verwendet werden. **siehe auch:** netsh /?

## Zurücksetzen des TCP/IP-Stacks mit Netsh

Eine häufige Anwendung von Netsh-Befehlen ist das Zurücksetzen des TCP/IP-Stacks, der für den Austausch von Datenpaketen in Netzwerken sorgt. Bei Netzwerk- und Internetproblemen kann diese Maßnahme, die z. B. defekte oder falsch eingerichtete TCP/IP-Protokolle entfernt, sinnvoll sein.

Mit folgendem Reparaturbefehl wird ein Reset durchgeführt und TCP/IPv4 neu installiert:

### netsh int ip reset

Eine Protokolldatei, die die erfolgten Änderungen dokumentiert, kann zusätzlich angelegt werden:

### netsh int ip reset c:\tcpipreset.txt

Nach Durchführung des Resets muss der Rechner neu gestartet werden.

## Im- und Export von Netzwerkeinstellungen

Mit Netsh kann man auch aktuelle Netzwerkeinstellungen in eine einfache Textdatei exportieren. Bei Netzwerkproblemen wird dann eine funktionierende und fehlerfreie Konfiguration zügig wiederhergestellt.

Im ersten Schritt (Export) wird die Netzwerkkonfiguration ausgelesen, in eine Textdatei geschrieben (netcnfig.txt) und im Beispielvezeichnis »Netzwerkkonfiguration« auf dem Laufwerk C:\ hinterlegt.

Den Ordner »Netzwerkkonfiguration« muss man vor dem erstmaligen Export manuell auf dem Ziellaufwerk anlegen (**Hinweis:** das geschieht nicht automatisch durch Netsh).

Dann wechselt man in die Eingabeaufforderung und gibt folgenden Code ein:

### netsh -c interface dump>c:\Netzwerkkonfiguration\netcnfig.txt

Für den späteren Import der Einstellungen ist die folgende Befehlseingabe erforderlich:

### netsh -f c:\Netzwerkkonfiguration\netcnfig.txt

## IP-Konfiguration mit Netsh

Ein verbreiteter Anwendungsfall von Netsh ist die Änderung von IP-Einstellungen. Soll ein Rechner im Netzwerk keine statische, sondern eine automatisch zugewiesene IP-Adresse erhalten, setzt man dafür das Dynamic Host Configuration Protocol (DHCP) ein. Dieses Kommunikationsprotokoll weist Clients in einem Netzwerk automatisch IP-Adressen und weitere erforderliche Konfigurationsdaten zu.

# Syntaxparameter für Netsh – was bedeuten sie? 2/2

Für den Vorgang sind mehrere Schritte notwendig.

Im ersten Schritt werden die aktuellen Einstellungen und Namen der verfügbaren Netzwerkadapter abgerufen:

**netsh interface ipv4 show interface**

oder die Kommandos einzeln nacheinander eingeben

**netsh -> interface -> ipv4 show interface**

Nun wird ein bestimmter LAN-Adapter (in diesem Beispiel: Ethernet) als Adressat für die IP-Zuweisung über DHCP bestimmt:

**netsh -> interface -> ipv4 set address name="Ethernet" source=dhcp**

Danach übernimmt DHCP die dynamische Verwaltung für die Netzwerkeinstellungen, die den Ethernet-Adapter betreffen.

## Windows-Firewall ein- und ausschalten

Wenn man die Windows-Firewall aktivieren oder deaktivieren will, reicht eine einfache Netsh-Befehlssyntax aus.

Eine Firewall aktivieren man wie folgt:

**netsh -> firewall -> set opmode enable**

Die Deaktivierung der Firewall geschieht mit folgender Befehlszeile:

**netsh -> firewall -> set opmode disable**

## Beispiele:

Zeigt Routetabelleneinträge an:

**netsh interface ipv4 show route**

Zeigt Nachbarchacheeinträge an:

**netsh interface ipv4 show neighbors**

Zeigt die aktuellen IP-Adressen an:

**netsh interface ipv4 show ipaddresses**

Zeigt globale Konfigurationsparameter an:

**netsh interface ipv4 show global**

# Was ist MPLS?

MPLS bedeutet Multiprotocol Label Switching. Hierbei werden IP-Datenpaketen verschiedene Labels zugewiesen, die es Routern ermöglichen, die Pakete sehr schnell und über die optimale Route im Netz weiterzuleiten. Dadurch kann eine stabilere und leistungsstärkere Verbindungsart geschaffen werden. Außerdem wird die komplexe Vermaschung von einzelnen Standorten innerhalb eines VPNs obsolet, da sich durch die MPLS-Technik ganz einfach eine Vielzahl von VPN-Verbindungen herstellen lässt (any-to-any).

## So funktioniert eine MPLS-Verbindung

Bei einem klassischen Transfer von Daten wird ein Datenpaket von Router zu Router weitergeleitet. In jedem Router, den das Datenpaket erreicht, läuft der identische Prozess ab. Automatisch wird eine Liste an Netzen und Routern durchlaufen und daraufhin entschieden, welchen Weg das Datenpaket zu nehmen hat. Dieser Prozess wiederholt sich jedes Mal, wenn das Paket einen neuen Knotenpunkt erreicht.

Bei einer MPLS-Verbindung hingegen, wird auf eine andere Herangehensweise gesetzt, die es ermöglicht, Daten schneller vom Start- zum Zielort zu bringen. Im Gegensatz zum normalen Datentransfer wird hier die Routenberechnung nur einmal vorgenommen.

Beim Eintritt in das Netzwerk wird dem Datenpaket ein sogenanntes Label zugeordnet, das Informationen zur genauen Route, die das Paket nehmen soll, enthält.

Bei diesem Weiterleitungsmechanismus wird das Label an das Paket angehängt und bei jedem Knotenpunkt, der erreicht wird, muss nur das Label mit den Zielinformationen ausgelesen werden.

Dadurch können Datenpakete durch einen Tunnel geschickt werden, ohne auf ihrem Weg behindert zu werden. Des Weiteren können mit MPLS Datenpakete priorisiert werden.

Durch verbindliche Quality-of-Service Parameter (QoS) und durch die Zuordnung einzelner Anwendungen im Datenverkehr zu bestimmten Classes-of-Service (CoS) ist es möglich, höher priorisierten Datenpaketen eine schnellere Route zuzuweisen und benötigte Bandbreiten garantiert zur Verfügung zu stellen.

## Vorteile einer MPLS-Vernetzung

- Schnellere Übertragung von Datenpaketen, über Switching und Tunneling, durch das Netzwerk
- Hohe Sicherheit durch das Übertragen in private Netzwerke. Anders als in einem öffentlichen Netzwerk kann bei MPLS hoher Datenschutz gewährleistet werden.
- Hohe Übertragungsqualität dank QoS und Service-Level-Agreements (SLA, Dienstleistungs-Güte-Vereinbarung) für das gesamte MPLS-VPN
- Einsparmöglichkeiten und Schonung interner IT-Ressourcen, da das Netzwerk zentral vom Provider gesteuert wird

## Welche MPLS Provider gibt es überhaupt?

In Deutschland ist als bekannte MPLS VPN Anbieter-Lösung z.B. die MPLS T-Systems Lösung zu nennen. Auch Vodafone stellt eine zuverlässige Lösung zur Verfügung, die eine hohe MPLS Sicherheit gewährleistet. Darüber hinaus kann eine MPLS Anbindung in Deutschland auch über Plusnet, Versatel oder Telefonica erfolgen. Im internationalen Bereich sind z.B. MPLS Provider wie BT, NTT, Verizon, Interoute oder Colt zu nennen. Auch sie bieten ein zuverlässiges und sicheres MPLS Netz.

# PowerShell-Kommandos 1/2

Laufende PowerShell-Befehle können mit der Tastenkombination **[Strg] + [C]** abgebrochen werden. Die PowerShell-Hilfe für einen benannten Befehl, wird mit **get-help <PowerShell-Befehl>** abgerufen.

**Get-Command** ... Auflistung aller PowerShell-Befehle

**Get-Disk** ... Informationen über die angeschlossenen Festplatten

**Get-Volume** ... Informationen über die Festplatten, Partitionen (Dateisystem, Gesundheitsstatus, Speichergröße, ...)

**Get-Partition** .. Informationen über die Festplatten-Partitionen

**get-hotfix** ... Liste mit den Updates des Betriebssystems anzeigen

**Get-History** ... die History der PowerShell-Befehlseingaben aufrufen

**Get-Location** ... aktuelles Arbeitsverzeichnis

**Get-NetTCPConnection** ... liefert ohne weitere Parameter nur IP-Adressen und keine Domain-Namen

**Get-NetTCPConnection | ft**

**LocalAddress, LocalPort, RemoteAddress, RemotePort, State -a** ... liefert die locale IP-Adresse, Port und entfernte IP-Adressen, Ports

**Get-NetTCPConnection | FT -Auto CreationTime, LocalAddress, LocalPort, RemoteAddress, RemotePort, State, OwningProcess** ...

... liefert die locale IP-Adresse, Port und entfernte IP-Adressen, Ports

**Get-NetTCPConnection -AppliedSetting Internet** ... externe Internet-Verbindungen anzeigen

**Get-Printer** ... angeschlossene Drucker anzeigen

**Get-Process** ... alle Prozesse anzeigen

**Get-Service** ... anzeigen aller Dienste und des Status (Stopped, Running)

**Get-SmbShare** ... Freigaben anzeigen

**Get-NetIPConfiguration** ... IP-Adresse, Gateway, Interface, DNS-Server ausgeben

**UUID (Universally-Unique-Identifier) oder GUID (global unique identifier) ermitteln**

**Get-WmiObject -Class Win32\_Product** ... Übersicht von der installierten Software

**(get-wmiobject Win32\_ComputerSystemProduct).UUID** ... UUID oder GUID des Computers ausgeben

**get-wmiobject Win32\_ComputerSystemProduct | Select-Object -ExpandProperty UUID** ... UUID oder GUID des Computers ausgeben

**GWMI -namespace root\cimv2 -class win32\_volume | FL -property DriveLetter, DeviceID** ... UUID oder GUID der Partitionen ausgeben

**help get-process -online** ... Onlinehilfe aufrufen zum Befehl Get-Process

**Windows-Befehl säubert die Festplatte**

Die Eingabeaufforderung mit Administrator-Rechten öffnen und den folgenden Befehl eingeben: **cipher /w: X:\**

Das X ist durch den Laufwerks-Buchstaben des betreffenden Laufwerks zu ersetzen. Beispielsweise D, um den freien Speicherplatz von Laufwerk D: des Rechners zu überschreiben.

Um gelöschte Dateien in einen bekannten Ordner unwiderruflich zu löschen, benutzt man cipher wie folgt:

**cipher /w: X:\<Verzeichnisname>**

Cipher beginnt sofort damit, den von Windows als gelöscht markierten Speicherplatz zu überschreiben. Zum Ausradieren der Informationen füllt er die freien Bereiche mit neuen Zahlenfolgen (siehe auch: cipher /? bzw. cipher /help).



## PowerShell-Kommandos 2/2

### 1. Zwei Dateien auf Gleichheit überprüfen:

Die Dateien datei2.txt in 2 verschiedenen Ordner, werden über ihren Hash-Wert miteinander verglichen. Sind beide Dateien gleich, so wird »True« ausgegeben. Bei Nichtgleichheit wird entsprechend »False« ausgegeben.

```
((Get-FileHash ".\ordner_b\datei2.txt").hash) -eq ((Get-FileHash ".\ordner_a\datei2.txt").hash)
```

Mit compare kann man sich auch die Unterschiede in zwei Dateien anzeigen lassen. Die Parameter **ReferenceObject** und **DifferenceObject** bezeichnen das ursprüngliche sowie das damit zu vergleichende Objekt.

**Beispiel 1:** Groß- und Kleinschreibung wird **nicht** beachtet

```
compare -ReferenceObject (Get-Content ".\ordner_b\datei2.txt") -DifferenceObject (Get-Content ".\ordner_a\datei2.txt")
```

**Beispiel 2:** Groß- und Kleinschreibung wird beachtet

```
compare -ReferenceObject (Get-Content ".\ordner_b\datei2.txt") -DifferenceObject (Get-Content ".\ordner_a\datei2.txt") -  
CaseSensitive
```

Gibt man **-IncludeEqual** an, dann werden alle Zeilen beider Dateien aufgelistet und der so genannte Side Indicator zeigt, ob sie gleich sind oder ob eine davon nur in der ersten oder in der zweiten Datei vorkommt. Ergänzt man schließlich **-IncludeEqual** um **-ExcludeDifferent**, dann erhält man nur jene Zeilen, die in beiden Dateien gleich sind

```
compare -ReferenceObject (Get-Content ".\ordner_b\datei2.txt") -DifferenceObject (Get-Content ".\ordner_a\datei2.txt") -  
CaseSensitive -IncludeEqual -ExcludeDifferent
```

### 2. Zwei Ordner miteinander vergleichen (Dateinamen, ...)

Sind beide Ordner identisch, so erfolgt keine Bildschirmausgabe. Bei Unterschieden in der Ordner- oder Datei-Struktur, werden die Unterschiede am Bildschirm ausgegeben.

```
Compare-Object -ReferenceObject (Get-ChildItem -Recurse -Path .\ordner_a) -DifferenceObject (Get-ChildItem -Recurse -Path .\  
ordner_b) -CaseSensitive
```

# PowerShell-Skript

## Einige Hinweise zum Skript nulldatei.ps1

Das PowerShell-Skript ist ein einfaches Beispielskript für die Ermittlung der aktuellen Systemprozesse, der eigenen IP-Adresse und für die Erstellung einer Textdatei mit Nullen.

Wenn Dateien gelöscht oder Partitionen formatiert werden, können die scheinbar nicht mehr vorhandenen Dateien trotzdem relativ einfach wiederhergestellt werden (siehe auch: PowerShell-Kommandos, Cipher).

Um diese nicht erwünschte Wiederherstellung zu verhindern oder zumindest deutlich zu erschweren, kann der freigewordene Speicherbereich mit anderen unwichtigen Dateien überschrieben werden.

Anschließend können die überaus unwichtigen Dateien wieder gelöscht werden. Bei einem Wiederherstellungsversuch können dann nur noch die letzten gespeicherten Dateien wiederhergestellt werden.

Wenn man ganz sicher gehen will, sollte man den Vorgang 3-mal mit jeweils anderen Dateien wiederholen.

**Beispiel-Skript:** die 0 (Null) durch die 1 (oder andere Zahlen) ersetzen  
 For (\$k = 1; \$k -LE 80; \$k++) { \$y = \$("y" + "1") }

Die erste große Null-Datei (Erstellung kann mehrere Stunden dauern), kann über eine Komprimierung deutlich verkleinert werden.

Falls die Ausführungsrechte von PowerShell-Skripten eingeschränkt wurden, kann man die Ausführung über den Programm-Editor »PowerShell ISE« versuchen.

**Hinweis:** Falls nach dem Kopieren des Skriptes Fehlermeldungen auftauchen, so liegt dies erfahrungsgemäß daran, dass das hier verwendete Programm einige Sonderzeichen ersetzt hat.

Datei: nulldatei.ps1

```
while($true) {
    Write-Host
    "1. Prozesse
    2. IP Konfiguration
    3. Null-Datei erstellen (1 MByte)"
    $Eingabe=read-host -prompt "Bitte eine Zahl eingeben"
    if ($Eingabe -eq '1') { Get-Process }
    elseif ($Eingabe -eq '2') { Get-NetIPConfiguration }
    elseif ($Eingabe -eq '3') {
        $datei = "d:\protokoll.txt"
        $max_size = 4
        $x = ""
        For ($h = 1; $h -LE 120; $h++) { $x = ($x + "0") }
        $x | set-content -force $datei
        $i=0
        while($true) {
            $i++
            $y = ""
            For ($k = 1; $k -LE 80; $k++) { $y = ($y + "0") }
            $y | add-content $datei
            if ($i -gt 10000) {
                # $size = ((Get-Item $datei).length/1KB)
                $size = ((Get-Item $datei).length/1MB)
                # $size = ((Get-Item $datei).length/1GB)
                # Ausgabe der Dateigröße nach 10000 Schleifendurchläufe
                $size = "{0:N2}" -f $size
                Write-Host $("size" + " MByte")
                # Write-Host $("size" + " GByte")
                if ($size -gt $max_size) {break}
                $i=0
            }
        }
        if ($Eingabe -eq 3) {break}
        "Inhalt der Datei jetzt:"
        Get-content $datei
    }
    else { write-host 'Die Eingabe ist keine Zahl zwischen 1 und 3' -
        foregroundcolor red }
    pause
}
```

# CMD-Skript (Batch-Datei) 1/3

## Einige Hinweise zum Skript nulldatei.cmd

- Batch-Dateien werden mit einem **@echo off** eingeleitet. Ansonsten wird jeder Befehl der Batch-Datei am Bildschirm ausgegeben.
- mit **REM** werden Kommentare eingeleitet
- mit **SET** werden Variablen definiert
  - SET /p** – vom Benutzer wird eine Eingabe erwartet
  - SET /a** – mit dieser Optionen sind erst Berechnungen mit den Variablen möglich

Um auf die Variablen zugreifen zu können, müssen sie in Prozentzeichen (%) eingeschlossen werden.
- **:start** – Doppelpunkt und frei wählbarer Name definiert eine Sprungmarke
- **GOTO start** – springe zur Sprungmarke :start
- Mit **echo** werden Bildschirmausgaben erstellt
  - echo.** – mit echo und einen Punkt wird eine Leerzeile am Bildschirm ausgegeben
- Zeichenverkettung:
  - SET NULLWERT=0**
  - SET NULLWERT=%NULLWERT%0**
- Operatoren in IF und FOR Abfragen:
  - EQU** - ist gleich
  - NEQ** - nicht gleich
  - LSS** - kleiner als
  - LEQ** - kleiner als oder gleich
  - GTR** - größer als
  - GEQ** - größer als oder gleich

Die Operatoren können im Vorfeld mit dem Operator **NOT** kombiniert werden (NOT EQU).

**Hinweis:** Die Batch-Dateien erhalten als Dateiendung **.bat** oder **.cmd**. Falls Batch-Dateien mit der Endung **.bat** in den Ausführungsrechten eingeschränkt wurden, so kann man es mit der Dateiendung **.cmd** probieren.

Datei: nulldatei.cmd

```
@echo off
REM Skript erstellt eine Text-Datei gefuellt mit NULLEN
REM Speicherort fuer die Textdatei mit NULLEN
SET DATEI= "d:\protokoll.txt"
SET /a LINE_CHAR_COUNT = 120
SET /a KILO_BYTE = 1024
SET /a MEGA_BYTE = 1024 * 1024
SET /a GIGA_BYTE = 1024 * 1024 * 1024
SET /a MAX_SIZE=0
SET /a MAX_SIZE = 4 * %MEGA_BYTE%
: menu
echo Null-Datei erstellen - (1)
echo.
SET /p EINGABE= "Bitte eine Zahl eingeben:"
IF %EINGABE% EQU 1 (
    GOTO start
) ELSE (
    GOTO menu
)
:start
echo.
SET /a COUNTER_A=0
SET NULLWERT=0
:loop_a
SET /a COUNTER_A=%COUNTER_A%+1
SET NULLWERT=%NULLWERT%0
IF %COUNTER_A% LSS %LINE_CHAR_COUNT% GOTO loop_a
echo %NULLWERT% > %DATEI%
SET /a COUNTER_B=0
:loop_b
echo %NULLWERT% >> %DATEI%
SET /a COUNTER_B=%COUNTER_B%+1
IF %COUNTER_B% GTR 1000 (
    FOR %%F IN (%DATEI%) do SET FILE_SIZE=%%~zF
    IF %FILE_SIZE% GTR %MAX_SIZE% GOTO ende
    SET /a COUNTER_B=0
)
IF %COUNTER_B% EQU 0 echo %FILE_SIZE% Byte
GOTO :loop_b
:ende
echo.
echo File-Size: %FILE_SIZE% Byte
echo.
```

## CMD-Skript (Batch-Datei) 2/3

Eine .BAT-Datei ist eine Stapelverarbeitungsdatei, welche in PC-kompatiblen DOS-Betriebssystemen und Windows ausgeführt werden kann.

### Datei-Attribute

Die Batch-Datei zeigt Informationen über die Datei, die als Parameter übergeben wurde.

**Datei:** file\_info.cmd

```
@echo off
REM Informationen ueber eine Datei
SET DATEI="d:\php.rtf"
FOR %%F IN (%DATEI%) do (
    echo ATTRIBUTE: ..... %%~aF
    echo DRIVE: ..... %%~dF
    echo FILE_PATH: ..... %%~fF
    echo FILENAME: ..... %%~nF
    echo DIRECTORY_PATH: .. %%~pF
    echo FILENAME_SHORT: .. %%~sF
    echo CHANGE_TIME: ..... %%~tF
    echo FILE_EXTENSION: .. %%~xF
    echo FILE_SIZE: ..... %%~zF
)
```

**Datei:** read\_file.cmd

```
@echo off
REM gibt die angegebene Datei am Bildschirm aus
FOR /F %%i in (text.txt) do (
    echo %%i
)
pause
```

**Datei:** read\_file.cmd

```
@echo off
FOR /f %%f IN (text.txt) DO echo %%f
pause
```

**Datei:** read\_file.cmd

```
@echo off
more < text.txt
pause
```

**Datei:** read\_file.cmd

```
@echo off
type text.txt
Pause
```

**Datei:** read\_line.cmd

```
@echo off
REM auszulesende Zeilennummer
set LineNo=2
REM Leerzuweisung Variable line
set "line="
REM Minus 1 da Zeile mit 0 beginnt
set /a LineNo-=1
```

```
for /f %%a in ('more/e +%LineNo% ^< text.txt') do (
    if not defined line set "line=%%a"
)
```

```
echo %line%
Pause
```

## CMD-Skript (Batch-Datei) 3/3

```

Datei: read_file.cmd
@echo off & setlocal enableDelayedExpansion
REM setlocal enableDelayedExpansion
REM verzögerter Erweiterung
REM sucht in der Datei nach dem Wort "port"
for /f "delims=" %%i in ('findstr "port" text.txt') do (
    echo %%i
    break
)
pause

```

```

Datei: read_file.cmd
@echo off
REM Text ausgeben
REM die ersten 8 Zeilen werden übersprungen
FOR /F "skip=8 delims=" %%i IN (text.txt) do echo %%i

```

```

Datei: read_file.cmd
@echo off
REM gibt die angegebene Datei am Bildschirm aus
FOR /F "tokens=* " %%i in (text.txt) do (
    echo %%i
)
pause

```

```

Datei: read_file.cmd
@echo off
REM auslesen der letzten nicht leeren Zeile
setLocal EnableDelayedExpansion
for /f "tokens=* delims= " %%a in (text.txt) do (
    set var=%%a
)
echo %var%

```

Da die Powershell ab Windows 7/2008 standardmäßig auf jedem Windows-System installiert ist, kann sie für komplexere Berechnungen verwendet werden:

```

Datei: berechnungen.cmd
@echo off
set "expression=(2+3)*10/1000"
for /f %%# in ("powershell %expression%") do set result=%%#
echo %result%

```

Die zusätzlichen Anführungszeichen (einfaches Hochkomma, gefolgt von einem doppelten Hochkomma), innerhalb der Klammer, verhindern Konflikte mit der for-Befehlssyntax.

```

Datei: file_check.cmd
@echo off
if exist %1 goto anzeigen
echo Datei "%1" nicht gefunden!
goto ende

```

```

:anzeigen
echo Die Datei "%1" existiert... - es wird versucht sie am Bildschirm
auszugeben:
type "%1"

```

```

:ende

```

**Aufruf in der cmd-Konsole:**  
file\_check.cmd <Parameter>  
file\_check.cmd text.txt



# IPv6 Netzwerk-Adressbereiche

## Loopback

Adresse: ::1/128 oder vereinfacht ::1

Die wohl einfachste und zudem sehr wichtige, da auf jedem Rechner gebundene, IP ist die des loopbacks, also für den Localhost gedachte IP-Adresse. Sie hat eine identische Aufgabe zu der IPv4-Adresse 127.0.0.1.

Des Weiteren hat man sich bei IPv6 auf mehrere Präfixe geeinigt, um direkt an den ersten vier Bits erkennen zu können, für welchen Zweck diese Adresse bzw. dieses Netz genutzt wird. Im folgenden werden diese kurz dargestellt:

## Link Local Unicast

Adressraum: fe80::/10 -- fe80:: - febf::

Alle Adressen in diesem Bereich werden nicht vom Router weitergeleitet, sind somit nur im LAN erreichbar, von daher muss eine Netzwerkschnittstelle mit angegeben werden.

Die Link Local Unicast Adresse dient hauptsächlich der Autokonfiguration, kommt also nur zum Einsatz, wenn ansonsten keine Adresse gebunden ist.

## Unique Local Unicast

Adressraum: fc00::/7 -- fc00:: - fdff::

Die Local Unicast Adressen dienen der lokalen Adressvergabe, also innerhalb eines LANs. Bei IPv4 liegen die Bereiche für diesen Zweck bei 10.0.0.0/8, 172.16.0.0/12 und 192.168.0.0/16. Derzeitig dient jedoch nur das Netz fd00::/8 für lokal generierte Adressen, das Präfix fc00 hingegen soll in Zukunft der eindeutigen Zuweisung von Local Unicast Adressen dienen. Nach den 8 Bit, die für fc bzw. fd genutzt werden, folgen 40 Bit

für die eindeutige Site-ID, danach 16 Bit als Subnetzmaske. Die letzten 64 Bit sind der Interface Identifier.

## Multicast

Adressraum: ff00::/8 -- ff00:: - ffff::

Schreibweise 1: ff00:0000:0000:0000:0000:0000:0000/8

Schreibweise 2: ff00:0:0:0:0:0:0/8

vereinfachte Schreibweise 3: ff00::/8

Multicast Adressen dienen als Verteiler, über eine IP-Adresse werden somit mehrere Geräte angesprochen. Da es bei IPv6 keine eigene Broadcast Adresse gibt, werden hierfür zwei Multicast Adressen verwendet: ff01::1 und ff02::1

Des Weiteren sind noch drei IP-Adressen wichtig, da mittels dieser Multicast Adressen alle Router in einem Bereich angesprochen werden: ff01::2, ff02::2 und ff05::2

## Global Unicast

Alle andere Adressräume sind grundsätzlich Global Unicast Adressen. Jedoch wurden bis jetzt nur vier Bereiche definiert, die restlichen Adressen wurden bisher nicht zugewiesen.

0:0:0:0:0:ffff::/96 ... IPv4 mapped (abgebildet)

2000::/3 ... von der IANA an die RIRs (Regional Internet Registries) vergebene Netze

2002::/4 ... für den Tunnelmechanismus 6to4

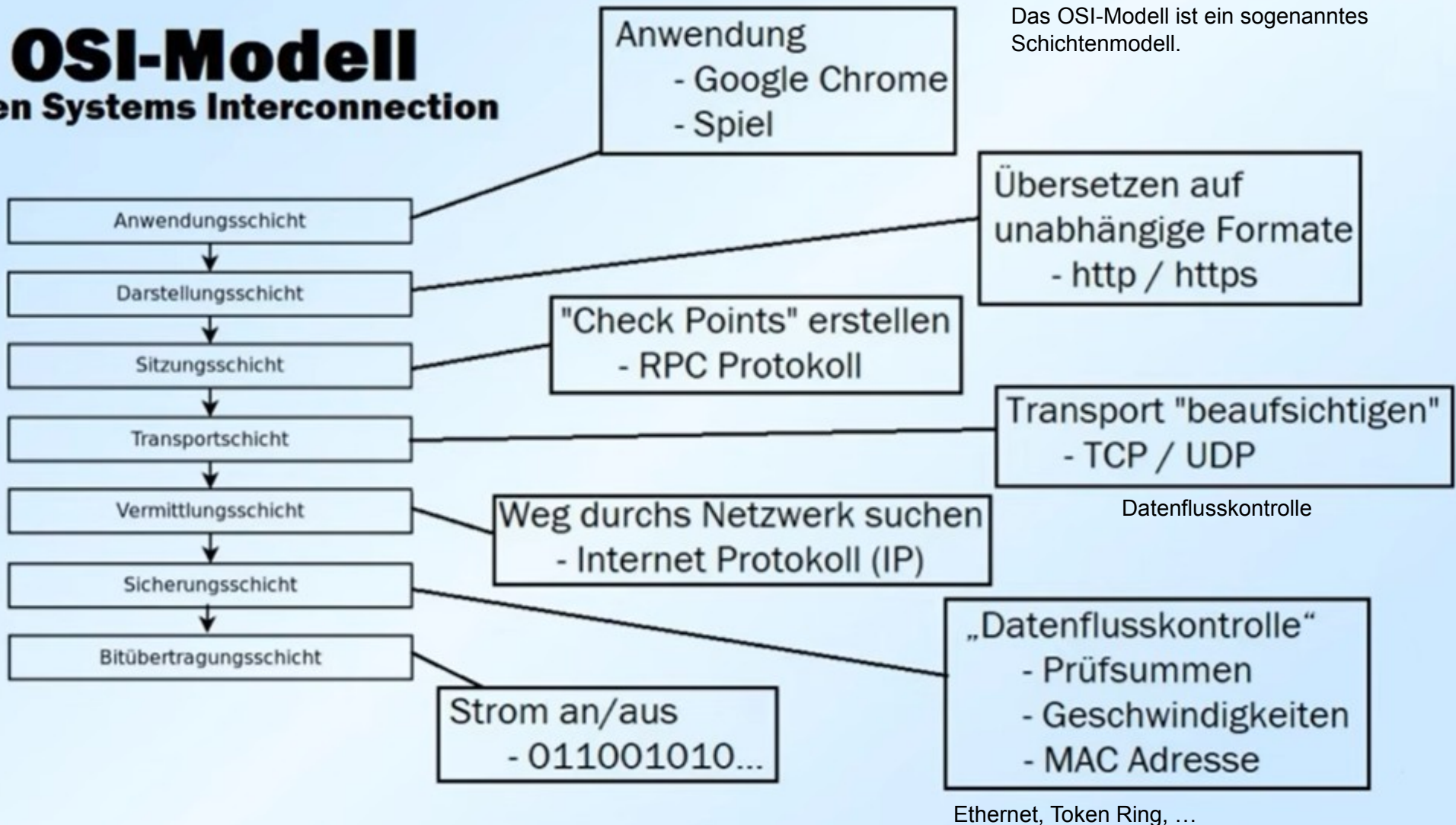
2001:db8::/32 ... für Dokumentationszwecke

Der erste Adressbereich dient dem zeitweisen Übergang von IPv4 zu IPv6. Die 32 Bit nach dem Präfix stellen die IPv4 Adresse dar, sodass ein Router zwischen den beiden Protokollen vermitteln kann, dennoch die IPv4 Adresse erkennbar bleibt.

# Open Systems Interconnection (OSI)

Das OSI-Modell ist ein Referenzsystem für die Kommunikation zwischen technischen Systemen zur Lösung von vielen unterschiedlichen Aufgaben.

## OSI-Modell Open Systems Interconnection



# Probleme und Lösungen 1/2

## Obwohl die Zugriffsberechtigungen korrekt sind, wird die Fehlermeldung »Zugriff verweigert« angezeigt

Wenn Sie versuchen, auf eine Datei auf einem NTFS-Dateisystemvolume zuzugreifen, wird möglicherweise die Fehlermeldung »Zugriff verweigert« angezeigt. Die NTFS-Berechtigungen der Datei geben aber an, dass man auf die Datei zugreifen kann.

**Ursache:** Dieses Verhalten kann auftreten, wenn ein anderer Benutzer die Datei verschlüsselt hat.

**Lösung:** Um dieses Verhalten zu beheben, muss die Datei vom Benutzer, der die Datei verschlüsselt hat oder vom Wiederherstellungs-Agent (Administrator) entschlüsselt werden. Auf Dateien, die mithilfe des verschlüsselnden Dateisystems (Encrypting File System, EFS) verschlüsselt werden, kann nur die Person zugreifen, die die Datei verschlüsselt hat, unabhängig von den anderen Berechtigungen, die sich in der Datei befinden.

So ermitteln Sie, ob eine Datei verschlüsselt wurde:

1. Starten Sie Windows Explorer, und klicken Sie dann im Menü »Ansicht« auf »Details«, um die Details des Ordnerinhalts anzuzeigen.
2. Klicken Sie im Menü »Ansicht« auf »Spalten einfügen«, und aktivieren Sie dann das Kontrollkästchen »Attribute«, um die Spalte »Attribute« zur aktuellen Ansicht hinzuzufügen und die Dateiattribute anzuzeigen.
3. Wenn in der Spalte »Attributes« für diese Datei ein »E« vorhanden ist, so ist die Datei verschlüsselt.

## Bedeutung der Dateiattribute

R = Read Only, Schreibgeschützt

H = Hidden, versteckt

S = System

D = Verzeichnis

A = Archiv, Mit den meisten Sicherungsprogrammen kann der Benutzer eine Teilsicherung durchführen, bei der nur Dateien gesichert werden, die sich seit der letzten Sicherung geändert haben. Dieses Bit wird zu diesem Zweck verwendet. Wenn die Sicherungssoftware die Datei sichert (archiviert), wird das Archivbit gelöscht und auf Null gesetzt. **Hinweis:** Man sollte sich aber nicht darauf verlassen.

E = Encrypted, verschlüsselt

## Mit Windows 10 ins BIOS gelangen

Mann kann auch ohne die bekannten Tastenkombinationen, mit Windows mehr oder weniger direkt zum BIOS gelangen.

- »Windows-Einstellungen« -> »Update und Sicherheit« -> »Wiederherstellung« -> »Erweiterte Start« (rechte Seite) und den Button »Jetzt neu starten« anklicken.
- Nach dem Neustart des Rechners gelangt man automatisch in das UEFI-BIOS von Windows.
- Von dort handelt man sich bis zum BIOS des Rechners durch. »Troubleshoot« -> »Advanced options« -> »UEFI Firmwareeinstellung« -> »Restart« -> **BIOS**

## Probleme und Lösungen 2/2

### Windows: Nicht löschbare Dateien löschen

Zuweilen kommt es vor, dass Windows sich hartnäckig weigert, bestimmte Dateien zum Löschen freizugeben. Das geschieht etwa nach dem Löschen von Benutzerprofilen: Hatte der Benutzer Rechte für seine Dateien und Verzeichnisse individuell vergeben und dabei die für Administratoren und das System entfernt, sind diese für den Administrator zunächst nicht löscherbar. Selbst wenn es das betreffende Benutzerkonto gar nicht mehr gibt, sind die ACLs mit dessen UID/GID noch mit der Datei verbunden.

Ähnlich ist es mit den Hinterlassenschaften nicht komplett deinstallierter Programme: Sie gehören eventuell weder dem Administrator noch dem System, sondern einem Dienst namens »TrustedInstaller« und zwar diesem allein.

Tastenkombination: **[Win] + [R]** -> **services.msc** -> **Windows Modules Installer** -> Kontextmenü -> Eigenschaften -> TrustedInstaller

### Eigentum übernehmen und Rechte setzen

Bei nicht löschbaren Dateien muss der Administrator diese Dateien zunächst in sein Eigentum überführen und die Rechte entsprechend setzen, um sie anschließend löschen zu können. Nach dem Aufruf einer Eingabeaufforderung ([Win] + [X]) mit Administratorrechten kann man sich zunächst mittels des Kommandos **whoami** versichern, ob man auch wirklich als Administrator angemeldet ist. Dann übernimmt man per

**takeown /f <Verzeichnisname> /r /d y**

den Besitz des fraglichen Verzeichnisses. Die Parameter hinter dem Verzeichnisnamen sorgen dafür, dass der Befehl rekursiv

durch alle Unterverzeichnisse läuft und alle Prompts, ob deren Besitz ebenfalls übernommen werden soll, positiv beantwortet werden.

Abweichend davon kann man mittels **/a** festlegen, das Verzeichnis der Administratoren-Gruppe zu übertragen.

Mittels des Kommandos

**icacls <Verzeichnisname> /grant Administratoren:F /t**

erteilt man dann der Administratoren-Gruppe alle Rechte für das angegebene Verzeichnis (hier sorgt /t für die rekursive Anwendung) und man kann zu guter Letzt mittels des Kommandos

**rd /s /q <Verzeichnisname>**

das betreffende Verzeichnis löschen.

### Lokalisierte Benutzer- und Gruppennamen ermitteln

Der Befehl **icacls** funktioniert etwa auf einem englischsprachigen Windows nicht wie oben angegeben - hier heißt die entsprechende Gruppe »**Administrators**« und behält diesen Namen auch, wenn Windows mittels eines installierbaren Sprachpakets auf eine andere Anzeigesprache umgestellt wurde. Mit Hilfe von

**whoami /groups**

kann man im Zweifel innerhalb der Eingabeaufforderung feststellen, wie die korrekten Namen für den Administrator beziehungsweise für die Administratoren-Gruppe auf einem System sind.

**Aggregation:** Im Allgemeinen ist die Aggregation eine Gruppierung von Datensätzen, die in ihrem Inhalt Ähnlichkeiten aufweisen. Mit Ähnlichkeiten sind gleiche Eigenschaften gemeint, die jeweilige Daten besitzen. In verschiedenen Themengebieten kann die Aggregation einen anderen Zweck erfüllen, jedoch ist das Ergebnis immer die Gruppierung, Ansammlung von Daten. In der Informatik bezeichnet die Aggregation entweder die Verbindung zwischen Objekten bzw. Daten oder die Auswertung von Metadaten aus einzelnen Daten, die gruppiert werden, um dann eine Aussage über die gesamte Gruppe zu erstellen.

**Appliance:** Als Appliance (engl. appliance, Vorrichtung) wird ein Ansatz zum Design für ein kombiniertes System aus Computer-Hardware und speziell auf diese Hardware optimierter Software bezeichnet, welche im Wesentlichen einer oder wenigen Anwendungen dient.

**Asset:** Asset bezeichnet Vermögenswerte und Anlagen sowie Wirtschaftsgüter. Hierzu zählen auch Aktien und Anleihen, Devisen, Immobilien sowie Sachwerte (Server und andere Hardware).

**Back Door:** Eine Backdoor (Hintertür) ist ein alternativer Zugang zu einer Software oder zu einem Hardwaresystem, der den normalen Zugriffsschutz umgeht. Mit einer Backdoor lassen sich Sicherheitsmechanismen der Hard- und Software umgehen. Der Zugang kann gewollt implementiert oder heimlich installiert sein.

**Big Data:** Der aus dem englischen Sprachraum stammende Begriff Big Data bezeichnet Datenmengen, welche beispielsweise zu groß, zu komplex, zu schnelllebig oder zu schwach strukturiert sind, um sie mit manuellen und herkömmlichen Methoden der Datenverarbeitung auszuwerten.

**BitLocker:** BitLocker ist eine Sicherheitsfunktion von Microsoft, die in bestimmten Versionen des Windows-Betriebssystems integriert ist. Das Feature sorgt für die Verschlüsselung der Systemlaufwerke, Festplatten oder Wechseldatenträger. Die gespeicherten Daten sind gegen Diebstahl und unbefugtes Lesen geschützt. Für die Ver- und Entschlüsselung kommen 128- oder 256-Bit lange AES-Schlüssel zum Einsatz. Maximalen Schutz bietet das Verschlüsselungs-Feature in Kombination mit dem sogenannten Trusted Platform Module (TPM).

**Blackhat-SEO:** Blackhat-SEO (SEO .. Search-Engine-Optimization) ist ein Begriff aus der Suchmaschinenoptimierung. Er bezeichnet Methoden, die gegen die Qualitätsrichtlinien der Suchmaschinen verstoßen. Dazu gehört unter anderem die automatische Generierung von Texten und das Eindringen in fremde Systeme zum Setzen von Backlinks. Ein Rückverweis oder Backlink bezeichnet einen Link, der von einer anderen Webseite ausgehend zu einer bestimmten Webseite führt. In vielen Suchmaschinen wird die Anzahl und Beschaffenheit der Rückverweise als Maß für die Linkpopularität oder Wichtigkeit einer Webseite verwendet.

**Blocklisten:** Blocklisten gibt es als bloße Zusammenstellungen, in denen der Autor ihm unliebsame Accounts auflistet. Aus dieser können Nutzer diejenigen Accounts auswählen, die sie selbst blocken wollen. Im Internet verbreitet werden aber auch Listen, die man im eigenen Account hochlädt. Dadurch werden alle darin aufgeführten Social-Media-Nutzer automatisch geblockt. Solche Listen umfassen teilweise mehrere Tausend Accounts - und sie werden massenhaft ungeprüft genutzt.



**Brute-Force-Angriffe:** Brute-Force-Angriffe werden von Hackern durchgeführt, die versuchen, ein Passwort zu knacken, indem eine Software schlicht in schneller Abfolge verschiedene Zeichenkombinationen ausprobiert. Der Algorithmus ist sehr einfach und beschränkt sich auf das Ausprobieren möglichst vieler Zeichenkombinationen, weshalb auch von »erschöpfender Suche« gesprochen wird. Dabei verwendet der Angreifer normalerweise einen Hochleistungsrechner, der sehr viele Berechnungen pro Sekunde durchführt und entsprechend eine hohe Anzahl an Kombinationen in kürzester Zeit austesten kann.

**Bulletproof Hosting:** Was bei Verbrechern in der realen Welt der Unterschlupf ist, sind bei Cyberkriminellen so genannte Bulletproof-Hosting-Services (»schusssicheres« Anbieten von Diensten). Sie dienen der Speicherung von Malware-Komponenten oder gestohlenen Daten, als Botnetz-Kommandozentralen (Command-and-Control Server) oder dem Hosten von Websites mit gestohlenen, betrügerischen oder pornografischen Inhalten.

Geschäftsmodelle der Anbieter von Bulletproof-Hosting-Services:

- Anbieter dedizierter Bulletproof-Server erlauben es ihren Kunden, Inhalte zu hosten, die in manchen Ländern möglicherweise als illegal gelten. Bei Beschwerden von Benutzern, Unternehmen und Ermittlungsbehörden versuchen sie dann so lange wie möglich die Anfragen zu verzögern.
- Andere Hoster bringen dedizierte Server in ihre Gewalt, die sie dann weiter vermieten. Dieses Angebot ist zeitlich begrenzt - bis die rechtmäßigen Eigentümer der infizierten Server darauf aufmerksam werden. Häufig werden diese Hosts auch für Blackhat-SEO (ein Begriff aus der Suchmaschinenoptimierung) und gewaltsame Eindringversuche genutzt, sie können zudem als Traffic-Proxy oder als Bereich für gestohlene Daten genutzt werden.
- Die Anbieter des dritten Modells sind mit Vermietern zu vergleichen, die sich nichts zuschulden kommen lassen und ihre Wohnungen ordnungsgemäß vermieten - und dann erleben müssen, dass ihre Mieter illegale Aktivitäten durchführen. Auch wenn die Anbieter das Hosten bössartiger Inhalte ausdrücklich verbieten, werden einige Kunden immer Möglichkeiten finden, die Infrastrukturen beispielsweise als Command-&-Control-(C&C)-Server oder als Download-Zone für gestohlene Daten zu missbrauchen.

Noch entscheidender als der Geschäftsumfang eines Bulletproof-Hosters ist für seine Kunden die Fähigkeit, bei Bedarf sofortigen Support zu bieten. Die leistungsfähigsten unter ihnen verfügen über ausgezeichnete Supportteams, die mit ihren Kunden über ICQ, Jabber oder eigene JavaScript-basierte Messaging-Services kommunizieren. Wie bei rechtmäßigen Anbietern nutzen diese Supportteams ein Ticketsystem, um Supportanfragen zu bearbeiten.

Ermittlungsbehörden, Sicherheitsanbieter und rechtmäßige Rootserver-Hosting-Anbieter setzen Bulletproof-Hoster auf schwarze Listen.

Manche Anbieter geben auf ihren Websites öffentlich bekannt, dass sie die Interessen der Länder schützen, in denen sie ansässig sind. Alles außerhalb dieser Grenzen wird als mögliches potenzielles Ziel ihrer Kunden betrachtet.

**Captive Portal:** Ein Captive Portal (dt. etwa unausweichliches Portal von englisch captive .. gefangen), ist eine Einrichtung, die üblicherweise in öffentlichen, drahtlosen Netzwerken eingesetzt wird, um den Zugriff von Endgeräten wie Laptops oder Smartphone auf das dahinter liegende Netzwerk oder das Internet an die Zustimmung des Nutzer an bestimmte Nutzungsregeln zu knüpfen. Zudem kann der Anbieter des Netzwerks den Zugang mit einem bestimmten Benutzerkonto verbinden, um so Verbindungskosten abzurechnen. Eingesetzt werden Captive Portals vor allem in Bereichen mit häufig wechselnden Teilnehmern. Das können Gast-WLAN-Netze in Hotels sein, öffentliche WLAN-Hot-Spots in Städten oder WLAN-Netze in Transportmitteln wie Zug, Bus oder Flugzeug. Bei einem Captive Portal kann ein Endgerät sich zunächst mit dem meist unverschlüsselten und ohne Zugangsdaten erreichbaren WLAN-Netz verbinden. In diesem Zustand wird vom Captive Portal allerdings jeder weitere Zugriff auf das dahinter liegende Netzwerk oder Internet noch blockiert, das Gerät ist quasi in diesem Bereich gefangen, wovon sich die Bezeichnung ableitet.

**CARP:** Entwickelt wurde CARP vom OpenBSD-Team. Das Common Address Redundancy Protocol (CARP) ist ein Netzwerkprotokoll, mit dessen Hilfe sich die Verfügbarkeit von IP-Systemen erhöhen lässt. Dies wird dadurch erreicht, dass mehrere Rechner innerhalb eines lokalen Netzes dieselben virtuellen IP-/MAC-Adressen für die Kommunikation mit anderen Systemen nutzen können. Haupteinsatzgebiet von CARP ist die Erstellung hochverfügbarer Gateways (Router/Firewall); mit CARP lassen sich aber auch Applikationsserver hochverfügbar machen.

**CERT:** Ein Computer Emergency Response Team (CERT), deutsch Computersicherheits-Ereignis- und Reaktionsteam, auch als Computer Security Incident Response Team (CSIRT) bezeichnet, ist eine Gruppe von IT-Sicherheitsfachleuten, die bei der Lösung von konkreten Sicherheitsvorfällen (z. B. Bekanntwerden neuer Sicherheitslücken in bestimmten Anwendungen oder Betriebssystemen, neuartige Malware-Verbreitung, bei Spam versendenden PCs oder gezielten Angriffen) als Koordinator mitwirkt bzw. sich ganz allgemein mit Computersicherheit befasst (manchmal auch branchenspezifisch), Warnungen vor Sicherheitslücken herausgibt und Lösungsansätze anbietet (engl.: advisories, dt.: Ratschläge). Außerdem helfen manche CERTs (z. B. Bürger-CERT), Sicherheitsrisiken für bestimmte Adressatengruppen zu beseitigen. Der Informationsfluss erfolgt meistens über Mailinglisten. Dort werden sicherheitskritische Themen erörtert, diskutiert und aktuelle Warnungen ausgegeben.

**Command-and-Control-Server:** Bei einem Command-and-Control-Server (C&C-Server) handelt es sich um einen Server, der dazu verwendet wird, Befehle an ein kompromittiertes System zu senden und es auf diese Art zu steuern. In den meisten Fällen wird ein solcher Server von Angreifern oder Cyberkriminellen betrieben, um unbemerkt Schadcode in das System des Opfers zu schleusen, Passwörter auszulesen, Daten zu stehlen oder zu manipulieren oder den betroffenen Rechner unbemerkt als Mitglied eines Botnetzes auszunutzen. Im Fall eines Botnetzes ist es dem Angreifer möglich, viele hunderte oder gar tausende infizierte Opfer gleichzeitig zu kontrollieren und über diesen Weg beispielsweise zentral gesteuerte DDoS-Angriffe durchzuführen oder einen Massenversand an Spam-Mails zu verursachen. Jeder kompromittierte Client muss eine Verbindung zum C&C-Server aufbauen, worüber fortlaufend die Kommunikation stattfindet. Zum Initiieren dieser Verbindung können unterschiedliche Kommunikationsprotokolle verwendet werden.

**Commodity-Server:** Ein Commodity-Server ist ein Standardcomputer, der für die Ausführung von Serverprogrammen und die Ausführung damit verbundener Aufgaben bestimmt ist. In vielen Umgebungen teilen sich mehrere Low-End-Server die Arbeitslast. Commodity-Server gelten oft als Einwegprodukte und werden daher eher ersetzt als repariert.

**Crime-as-a-Service:** Crime-as-a-Service ist eine Ableitung des Begriffs Software as a Service (SaaS). Während SaaS als Teilbereich des Cloud Computings davon ausgeht, dass die gesamte IT oder Teilbereiche bei einem externen IT-Dienstleister betrieben und vom Kunden als Service genutzt werden, werden analog bei Crime-as-a-Service von Kriminellen die notwendigen Dienste, die sie für eine Straftat benötigen, im Internet zusammengesucht und gekauft. Diese kriminellen Dienste werden im »Dark Web« beziehungsweise bei der sogenannten »Underground Economy« des Internets von Anbietern zur Verfügung gestellt. Auch kann man im Internet Cybersöldner für seine Attacken rekrutieren. In Deutschland ist die Zahl bekannt gewordener Computerbanden, die der Organisierten Kriminalität (OK) zuzurechnen sind, mit 2% (wachsender Aufwärtstrend) im Jahr 2014 noch relativ gering.

**Cross Site Scripting:** Cross Site Scripting (XSS) ist eine der am häufigsten genutzten Angriffsmethode im Internet. Ziel des webseitenübergreifenden Skriptings ist es, an vertrauliche Daten zu gelangen, Anwendungen zu übernehmen oder sonstigen Schaden anzurichten. XSS bettet den Angriffscode in einen vermeintlich sicheren Kontext ein. Cross Site Scripting zählt zu den aktiven Angriffsmethoden und kann als Grundlage für weitere Angriffe verwendet werden. Die Angriffsmethode nutzt die im Internet weit verbreiteten Skriptsprachen wie JavaScript. XSS kann erfolgreich sein, wenn die Webanwendung die entgegengenommenen Daten nicht ausreichend prüft und sie anschließend weiterverarbeitet oder weiterreicht.

**Daemon:** Als Daemon oder Dämon bezeichnet man unter Unix oder unixartigen Systemen einen Prozess, der im Hintergrund abläuft und bestimmte Dienste zur Verfügung stellt. Benutzerinteraktionen finden hierbei nur auf indirektem Weg statt.

**Dark Web:** Das Dark Web umfasst alle Daten, die mit einem Standard-Browser wie Google Chrome oder Firefox nicht zugänglich sind. Im Dark Web finden sich alle möglichen Informationen. Das Wort Dark ist lediglich ein Bezug auf die eingeschränkte Zugänglichkeit. Das gängigste Mittel für den Zugang ins Dark Web ist der anonyme Browser Tor. Dieser Browser kann genau wie Chrome, Firefox oder sonstige Browser heruntergeladen werden, funktioniert jedoch anders. Tor ist die Kurzform von »The Onion Router« (Zwiebel-Router), ein Verweis auf die Funktionsweise des Browsers. Die Internet-Aktivität mittels Tor wird über verschiedene übereinander gelagerte Netzwerke bzw. Schichten (wie die Schichten einer Zwiebel) geleitet, wobei jede einzelne Schicht dazu dient, den Datenverkehr zum Computer der Benutzer zu verschlüsseln. Aufgrund dieser zusätzlichen Sicherheitsschichten ist Tor langsamer als gewöhnliche Browser. Bei Tor handelt es sich nicht um das eigentliche Dark Web, sondern lediglich um ein Tool zum Surfen im Dark Web. Mit Tor kann man wie gewohnt auf sichere Weise auf Inhalte zugreifen. An dieser Stelle kommen Websites mit der Endung .onion ins Spiel. Wenn die Adresse einer Website diese Endung (anstatt .com, .net usw.) enthält, handelt es sich um eine Website im Dark Web, auf die nur mittels Tor zugegriffen werden kann. Websites mit der Endung .onion werden von normalen Suchmaschinen nicht angezeigt, selbst wenn Tor verwendet wird. Zu diesem Zweck verwenden Benutzer des Dark Web spezielle Verzeichnisse.

**DDoS:** Der Distributed-Denial-of-Service (DDoS) Angriff ist ein verteilter Denial-of-Service (DoS) Angriff, der wiederum eine Dienstblockade darstellt. Diese liegt vor, wenn ein angefragter Dienst nicht mehr bzw. nur noch stark eingeschränkt verfügbar ist.

**Degausser:** Löscheräte, häufig auch als Degausser bezeichnet, sind Geräte, bei denen magnetische Datenträger einem starken Magnetfeld (Gleichfeld, Wechselfeld oder gepulstes Feld) ausgesetzt werden. Bei einem ausreichend starken Magnetfeld werden alle magnetischen Aufzeichnungen auf dem Datenträger durch Entmagnetisierung zerstört, so dass eine Rekonstruktion der gespeicherten Daten mit keinen derzeit bekannten Mitteln mehr möglich ist.

**Doxing:** Doxing (von engl.: dox als Abkürzung für documents) ist das internetbasierte Zusammentragen sowie anschließende Veröffentlichen personenbezogener Daten mit zumeist böswilligen Absichten gegenüber den Betroffenen. Die Ursprünge des auch Doxxing genannten Angriffs liegen in den Veröffentlichung der Adressdaten von US-Polizeibeamten und damit deren Identifikation. Als Gründe für Doxing kommen höchst unterschiedliche Motive in Betracht, so z.B. etwa Macht- und Größenphantasien oder auch Selbstjustiz. Die betroffenen Personen werden dabei im höchsten Maße durch Folgeattacken belästigt.

**Drive-by-Download:** Ein Drive-by-Download ist das unbewusste (drive-by .. im Vorbeifahren) und unbeabsichtigte Herunterladen von Software auf einen Rechner. Unter anderem wird damit das unerwünschte Herunterladen von Schadsoftware allein durch das Aufrufen einer dafür präparierten Webseite bezeichnet. Dabei werden Sicherheitslücken des Browsers oder des Betriebssystems ausgenutzt, denn laut Definition sollte mit HTML-Inhalten oder Browser-Skriptsprachen ein Zugriff außerhalb der Browser-Umgebung ohne Benutzerinteraktion nicht möglich sein. Heute beinhalten Webseiten häufig dynamische Funktionen, die durch clientseitige Technologien wie JavaScript (auch als Teil von Ajax), Java, Adobe Flash realisiert sind. Diese Techniken erlauben eine ständige Kommunikation zwischen Browser und Server, ohne dass der Benutzer eine Aktion durchführen muss. Dies wird unter anderem eingesetzt, um Werbeflächen auszutauschen, Listen zu laden oder Daten an den Server zu übertragen. Üblicherweise werden diese Aktionen im Browser in einer Sandbox ausgeführt. Wenn aber der Browser oder die vom Browser benutzten Betriebssystembibliotheken eine Sicherheitslücke aufweisen, können Programme aus dieser Sandbox ausbrechen und direkt auf den Computer des Benutzers zugreifen. Dadurch ist es möglich, dass Schadsoftware ohne Mitwirkung des Benutzers auf dessen Computer ausgeführt wird. Zum Schutz gegen ungewollte Drive-by-Downloads hilft es, immer die aktuelle Version des Browsers zu verwenden, Plugins wie Adobe Flash sowie den Adobe Reader immer auf dem neuesten Stand zu halten oder zu deaktivieren und diese Plugins ausschließlich von der offiziellen Seite des Herstellers zu beziehen. Insbesondere im kommerziellen Umfeld werden diese Plugins auf Ebene der IT-Administration abgeschaltet oder gefiltert. Auch Java-Plugins zu deaktivieren, gar nicht erst zu installieren oder aktuell zu halten, vermindert die Wahrscheinlichkeit eines Befalls. Viele Infektionen durch Drive-by-Downloads finden nicht direkt über die angesteuerte Webseite statt, sondern durch externe, meistens kompromittierte Webseiten, die für den Benutzer unbemerkt über Skripte nachgeladen werden. Bestimmte Browser-Plug-ins verhindern das Nachladen dieser Skripte und führen sie erst nach expliziter Freigabe durch den Anwender aus, etwa NoScript für Firefox oder die für unterschiedliche Browser verfügbaren Plugins uMatrix oder FlashBlock.

**Diffie-Hellman-Merkle-Schlüsselaustausch:** Diffie-Hellman-Merkle ist ein asymmetrisches, kryptografisches Verfahren, dass man für den Schlüsselaustausch bzw. die Schlüsselvereinbarung verwendet. In der Praxis sorgt es dafür, dass sich zwei oder mehr Kommunikationspartner auf einen gemeinsamen Sitzungsschlüssel einigen, den alle zum Ver- und Entschlüsseln verwenden können. Das besondere an Diffie-Hellman-Merkle ist, dass nicht der geheime Sitzungsschlüssel, sondern nur das Ergebnis einer Rechenoperation übertragen wird. Bei dieser Rechenoperation geht man von der Annahme aus, dass Potenzieren von Zahlen leicht, aber den diskreten Logarithmus zu berechnen schwer ist. Solange die notwendige Rechenleistung fehlt und es keine Vereinfachung zum Lösen des Diskreten-Logarithmus-Problems gibt, so lange ist dieses Verfahren sicher. Der Diffie-Hellman-Merkle-Schlüsselaustausch wurde von den drei Wissenschaftlern Diffie, Hellman und Merkle im Jahr 1976 veröffentlicht. Jahrzehnte später, nach der Veröffentlichung durch Diffie, Hellman und Merkle, wurde bekannt, dass bereits ein paar Jahre zuvor drei Wissenschaftler des britischen Geheimdienstes GCHQ das Prinzip dieses Verfahrens erfunden haben. Allerdings wurde dieses Verfahren aus Gründen der Geheimhaltung damals nicht öffentlich gemacht. Deshalb wird die Entdeckung des Prinzips, das im Diffie-Hellman-Merkle-Schlüsselaustausch angewendet wird, nicht den drei Wissenschaftlern des GCHQ zugeschrieben, sondern Diffie, Hellman und Merkle. Häufig wird nur die Bezeichnung Diffie-Hellman verwendet. Der Name Merkle wird einfach weggelassen. Merkles Verdienst sollte aber nicht unerwähnt bleiben. Deshalb wird Diffie-Hellman hier vollständig mit Diffie-Hellman-Merkle benannt. Der Diffie-Hellman-Merkle-Schlüsselaustausch bildet die Grundlage für das Protokoll Secure Shell (SSH2, OpenSSH), IPSec und TLS mit Forward Secrecy und Perfect Forward Secrecy. Weil der Schlüsselaustausch eine Interaktion beider Parteien voraussetzt, kann es nicht bei der direkten Verschlüsselung von E-Mails eingesetzt werden. Bei der Transportverschlüsselung mit TLS allerdings schon.

**DMZ:** Eine Demilitarisierte Zone (DMZ, auch Demilitarized Zone, ist ein abgeschotteter Bereich) bezeichnet ein Computernetz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Server. Die in der DMZ aufgestellten Systeme werden durch eine oder mehrere Firewalls gegen andere Netze (z. B. Internet, WAN, LAN) abgeschirmt. Durch diese Trennung kann der Zugriff auf öffentlich erreichbare Dienste gestattet und gleichzeitig das interne Netz (LAN) vor unberechtigten Zugriffen von außen geschützt werden.

**DTLS:** Datagram Transport Layer Security ist ein auf TLS basierendes Verschlüsselungsprotokoll, das im Gegensatz zu TLS auch über unzuverlässige Transportprotokolle wie UDP übertragen werden kann.

**Edge Computing:** Edge Computing bezeichnet im Gegensatz zum Cloud Computing die dezentrale Datenverarbeitung am Rand des Netzwerks, der sogenannten Edge. Statt Edge Computing werden gelegentlich auch die Begriffe Fog Computing, Local Cloud bzw. Cloudlet genutzt. Beim Edge Computing werden Computer-Anwendungen, Daten und Dienste von zentralen Knoten (Rechenzentren) weg verlagert. Der Begriff bezieht sich darauf, dass beim Edge Computing die relevanten Operationen am »Rand« des Netzwerkes geschehen, also in der Netzwerkperipherie. Diese Operationen können die Erfassung, Aggregation, Aufbereitung und Analyse von Daten bedeuten.



**EGP:** Das Exterior Gateway Protocol (EGP) ist auf der Vermittlungsschicht des OSI-Referenzmodells (OSI-Schicht: 3) angesiedelt und baut auf dem IP-Protokoll auf. Das EGP-Protokoll wird zur Kommunikation zwischen Routern benutzt und dient dem Verbund mehrerer komplexer Netze, die in sich eine abgeschlossene Welt bilden und nur gelegentlich mit anderen Netzen kommunizieren.

**Exploit:** Ein Exploit (engl. to exploit: ausnutzen) ist ein kleines Schadprogramm (Malware) bzw. eine Befehlsfolge, die Sicherheitslücken und Fehlfunktionen von Hilfs- oder Anwendungsprogrammen ausnutzt, um sich programmtechnisch Möglichkeiten zur Manipulation von PC-Aktivitäten (Administratorenrechte usw.) zu verschaffen oder Internetserver lahm zu legen.

**FIN-Paket:** Sind zwischen zwei Stationen alle Daten übertragen, senden beide Stationen ein TCP-Paket mit gesetztem FIN-Flag (Final-Flag). Danach gilt die TCP-Verbindung als beendet.

**Firewall:** Eine Firewall muss mindestens 2 Netzbereiche voneinander trennen und die kontrollierte Weiterleitung (Anwendung von Regeln) von Paketen bewerkstelligen. Die Firewall sollte im Idealfall Open-Source-Software und aktuell wie in Zukunft anpassbar sein. Proprietäre Software gilt im allgemeinen nicht als verlässliche Software.

**FTL:** Ein Flash Translation Layer (FTL) ist für die effiziente Nutzung von Flash-Speichern wie zum Beispiel SSDs verantwortlich. Beheimatet ist er im Controller des Speichersystems. Der Name (deutsch: Flash-Übersetzungsschicht) ist etwas missverständlich. Bei einem Flash Translation Layer handelt es sich tatsächlich um eine Verbindung von Hard- und Software, die durch dieses Zusammenspiel eine Reihe zentraler Aufgaben für die Speichernutzung vornehmen kann. Der Flash Translation Layer übernimmt die Umwandlung (mapping) von logischen in physikalische Adressen. Das bedeutet, dass die logischen Zugriffe von der Host-Seite in physikalische Zugriffe auf der Flash-Speicher-Seite übersetzt werden.

**Fork:** Eine Abspaltung (engl. fork) ist in der Softwareentwicklung ein Entwicklungszweig nach der Aufspaltung eines Projektes in zwei oder mehrere Folgeprojekte; die Quelltexte oder Teile davon werden hierbei unabhängig vom ursprünglichen Mutterprojekt weiterentwickelt.

**Geoblocking:** Die Bedeutung des Begriffs Geoblocking lässt sich durch seine Wortbestandteile recht einfach herleiten: Geo kommt aus dem Griechischen und bezieht sich zunächst nur auf die Erde im Allgemeinen, meint oft aber auch nur eine bestimmte Region. Blocking ist eine Form des englischen Verbs »to block« und bedeutet übersetzt stoppen oder sperren. Das Wort Geoblocking ist vor allem im Internet verbreitet: Dort bezeichnet es eine Sperrung bestimmter Inhalte in einzelnen Regionen. Deutschen Usern ist diese Technik höchstwahrscheinlich von vielen US-amerikanischen YouTube-Videos bekannt, die die GEMA für Rechner mit deutscher IP-Adresse sperren lässt, da das abweichende Urheberrecht hier eine Freigabe nicht zulässt. Auch gebühren- oder werbefinanzierte TV-Sender anderer Staaten sind durch Geoblocking im Ausland im Normalfall nicht erreichbar. So erhalten deutsche Zuschauer über ihren Rechner zum Beispiel kein US-amerikanisches Fernsehen.

**GUID:** Der global unique identifier ist eine weltweit eindeutige Identifizierungsnummer, mit der Dateien versehen werden. Ein Globally Unique Identifier (GUID) ist eine Zahl mit 128 Bit (16 Bytes), die in verteilten Computersystemen zum Einsatz kommt. GUID stellt eine Implementierung des Universally-Unique-Identifier-Standards (UUID) dar. GUIDs werden üblicherweise im 8-4-4-4-12 Format XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX dargestellt, wobei jedes X für ein Zeichen aus dem Hexadezimalsystem steht und damit eine Ziffer 0–9 oder ein Buchstabe A–F sein kann, z. B. 936DA01F-9ABD-4D9D-80C7-02AF85C822A8 (32 Buchstaben/Ziffern, mit Bindestrichen 36 Zeichen). Die vier höchstwertigen Bits des dritten Blocks (von links aus gezählt) geben die Version der GUID an, aus der man auf die Art des verwendeten Algorithmus zur Erzeugung der GUID schließen kann. Die bis zu drei höchstwertigen Bits des vierten Blocks identifizieren die verwendete Variante. Im Beispiel ist die Version an der 4 erkennbar und die Variante an der 8 in 936DA01F-9ABD-4D9D-80C7-02AF85C822A8. Dieselbe Variante wie im Beispiel könnte statt durch eine 8 auch durch eine 9, ein A oder B gekennzeichnet sein, da für diese Variante nur die ersten beiden Bit zählen (10xx).

**Hadoop:** Hadoop ist ein Java-basiertes Open Source-Framework zum Speichern und Verarbeiten von Big Data. Die Daten werden dabei auf preiswerten Commodity-Servern gespeichert, die in Clustern verbunden sind. Sein verteiltes Dateisystem ist fehlertolerant und ermöglicht eine parallele Verarbeitung.

**HAProxy:** HAProxy ist eine kostenlose Open-Source-Software, die einen hochverfügbaren Load-Balancer und einen Proxy-Server für TCP- und HTTP-basierte Anwendungen bereitstellt und der die Anfragen auf mehrere Server verteilt. Es ist in C geschrieben und hat den Ruf, schnell und effizient zu sein.

**Härtung:** Der Begriff »Systemhärtung« ist die Übersetzung des Englischen »System Hardening«. Im IT-Sprachgebrauch wird vereinfacht auch nur von der »Härtung« gesprochen. Systemhärtung ist ein technischer Baustein, um mögliche Schwachstellen (Vulnerabilities) von IT-Systemen und IT-Infrastrukturen zu verringern.

**HTTPS:** HTTPS steht für Hypertext Transfer Protocol Secure und ist im technischen Sinne kein eigenständiges Protokoll. HTTPS bezeichnet die Verwendung von HTTP über SSL oder TLS. Die Verwendung von HTTPS erkennt man im Browser daran, dass der besuchten Internetadresse https statt http vorangestellt ist. Zudem heben die meisten modernen Browser eine abgesicherte Verbindung zusätzlich optisch hervor.

**Hybride Angriffe:** In modernen Konfliktszenarien setzen Angreifer auf eine Kombination aus klassischen Militäreinsätzen, wirtschaftlichem Druck, Computerangriffen bis hin zu Propaganda in den Medien und sozialen Netzwerken. Dieses Vorgehen wird auch als »hybride Angriffe« oder »hybride Kriegsführung« bezeichnet.

**Hyper-V:** Bei Hyper-V handelt es sich um eine Technologie der Redmonder Software-Schmiede, die sich zur Virtualisierung von einzelnen Rechnersystemen oder kompletten Rechenzentrumsumgebungen verwenden lässt. Hyper-V ermöglicht es, mehrere Betriebssysteme als virtuelle Computer unter Windows auszuführen.

**ICMP:** Das Internet Control Message Protocol (ICMP) ist Bestandteil des Internet Protokolls (IP, OSI-Schicht: 3). Es wird aber als eigenständiges Protokoll behandelt, das zur Übermittlung von Meldungen über IP dient. Zwei bekannte Tools sind Ping und Tracert oder Traceroute. Beide sind sehr einfache Programme, die zur Analyse von Netzwerk-Problemen gedacht sind und damit wesentlich zur Problemlösung beitragen können.

**IOS:** Internetwork Operating System Software (IOS) ist das Betriebssystem von Routern und Switches des US-amerikanischen Unternehmens Cisco. IOS wird bei modernen Geräten beim Einschalten des Gerätes aus dem nichtflüchtigen Flash-Speicher dekomprimiert und in den Hauptspeicher geladen. Nach dem Start stellt es die grundlegenden Funktionen des Routings und/oder Switching zur Verfügung. Über Zugriffskontrolllisten werden grundlegende Paketfilterfunktionen bereitgestellt. Gesteuert und konfiguriert wird dieses per Kommandozeile über eine Telnet-, SSH- oder eine direkte serielle Konsolenverbindung am Endgerät. Die Bedienung ist der von MS-DOS- oder Unix-Kommandozeilen ähnlich und enthält Funktionen wie die Autovervollständigung eines eingegebenen Kommandos. Eine enorme Hilfe ist dabei das Fragezeichen, welches an beliebiger Stelle eingegeben eine kontextabhängige Kurzhilfe ausgibt. Es sind aber auch Web- und Windows-Oberflächen verfügbar.

**IoT:** Eine allgemeingültige Definition des Internet of Things (IoT) existiert nicht. Je nach Anwendungsbereich und verwendeter Technik können sich die Definitionen des Internets der Dinge unterscheiden. Im Allgemeinen wird der Begriff Internet of Things für die Vernetzung von Gegenständen des Alltags oder von Maschinen im industriellen Umfeld per Internet verwendet. Geräte bekommen eine eindeutige Identität (Adresse) im Netzwerk und werden mit elektronischer Intelligenz ausgestattet. Dadurch sind sie in der Lage, über das Internet zu kommunizieren und Aufgaben voll automatisiert auszuführen. Die intelligenten Geräte werden oft auch als Smart Devices bezeichnet. Neben der Möglichkeit der Kommunikation der Geräte untereinander (Machine-to-Machine-Kommunikation, M2M) stellen viele der vernetzten Objekte über das Internet eine Schnittstelle zur Verfügung, über die sich die Geräte durch einen Benutzer von einem beliebigen Ort aus bedienen und steuern lassen.

**IP:** Das Internet Protocol (IP) ist ein in Computernetzen weit verbreitetes Netzwerkprotokoll und stellt durch seine Funktion die Grundlage des Internets dar. Das Internet Protokoll ist ein Netzwerkprotokoll für den Austausch von Daten in einem Netzwerk. Es wird dazu benötigt, Daten von einem Sender zu einem Empfänger im Internet zu transportieren. Das IP-Protokoll ist die Implementierung der Internetschicht des TCP/IP-Modells bzw. der Vermittlungsschicht (engl. Network Layer, OSI-Schicht: 3) des OSI-Modells. IP ist ein verbindungsloses Protokoll, das heißt der Absender wird nicht darüber informiert ob ein Datenpaket tatsächlich am Ziel angekommen ist.

**IPSec:** IPSec beinhaltet eine Suite von Internetstandardprotokollen, die eine sichere, verschlüsselte Kommunikation zwischen zwei Computern über ein nicht geschütztes Netzwerk ermöglichen. Die Verschlüsselung erfolgt auf der IP-Netzwerkschicht (OSI-Schicht: 3), was bedeutet, dass sie für die meisten Anwendungen, die bestimmte Protokolle für die Netzwerkkommunikation verwenden, transparent ist. Darüber hinaus bietet IPSec eine End-to-End-Sicherheit. Dies bedeutet, dass die vom sendenden Computer verschlüsselten IP-Pakete während der Übertragung unlesbar sind und nur vom Empfängercomputer entschlüsselt werden kann.

**ISATAP:** Ein Tunneladapter (ISATAP, Intra-Site Automatic Tunnel Addressing Protocol) verpackt Datenpakete eines anderen Verbindungsprotokolls in TCP/IP Pakete, um sie auf diese Weise über das Internet an die passende Gegenstelle zu senden. P2P-Netze arbeiten mit diesem Mechanismus, aber auch die Übersetzung von IPv6 zu IPv4 funktioniert so.

**Jailbreak:** Um die Sicherheit von Geräten (z.B. SmartPhone, Tablet) zu gewährleisten, schränken die Hersteller standardmäßig die Zugriffsrechte auf das Dateisystem ein. Bei einem Jailbreak werden diese Beschränkungen der Zugriffsrechte ganz oder teilweise wieder aufgehoben.

**Kerberos:** Kerberos ist ein Authentifizierungsdienst, der in offenen bzw. unsicheren Computernetzwerken zum Einsatz kommt. So authentifiziert das Sicherheitsprotokoll Dienstanfragen zwischen zwei oder mehreren vertrauenswürdigen Hosts über ein nicht vertrauenswürdiges Netzwerk wie das Internet. Zur Authentifizierung von Client-Server-Anwendungen und der Überprüfung von Benutzeridentitäten kommen kryptografische Verschlüsselungen und eine vertrauenswürdige dritte Partei (auch Trust Third Party) zum Einsatz. Kerberos wird als Open-Source-Projekt vom Kerberos-Konsortium gepflegt. Seine Ursprünge hat es in den 80er Jahren - das Massachusetts Institute of Technology (MIT) entwickelte das Protokoll für sein damaliges Projekt Athena. Heute ist Kerberos die Standard-Autorisierungstechnologie von Microsoft Windows. Kerberos-Implementierungen gibt es aber auch für andere Betriebssysteme wie Apple OS, FreeBSD, UNIX und Linux. Microsoft führte seine Version des Kerberos-Protokolls in Windows 2000 ein. Daraufhin entwickelte es sich auch zum Standardprotokoll für Websites und Single Sign-On-Implementierungen auf verschiedenen Plattformen.

**Keyed-Hash Message Authentication Code (HMAC):** Ein Keyed-Hash Message Authentication Code ist ein Message Authentication Code, dessen Konstruktion auf einer kryptografischen Hash-Funktion, wie beispielsweise dem Secure Hash Algorithm und einem geheimen Schlüssel basiert.

**KillSwitch:** Ein Internet Kill Switch ist ein Konzept, um das Internet oder Teile davon im Sinne eines Notausschalters stillzulegen. Bei Bedrohungen der öffentlichen Sicherheit sollen Internet und Mobiltelefonie unterbrochen werden. In einem VPN-Netz ist der KillSwitch ein Notausschalter und verhindert, dass Rechner Daten übertragen, bis die unterbrochene sichere und verschlüsselte Verbindung zum VPN-Server wiederhergestellt ist.

**Kodi:** Mediacenter Kodi, ehemals XBMC, ist eine freie und plattformübergreifende Mediaplayer-Software. Die Software ist durch Plug-ins erweiterbar.

**L2TP:** Layer 2 Tunneling Protocol (L2TP) ist ein Netzwerkprotokoll, das Frames von Protokollen der Sicherungsschicht (Schicht 2) des OSI-Modells durch Router zwischen zwei Netzwerken über ein IP-Netz tunnelt.

**Lab:** Ein »Lab« ist ein physischer oder virtueller Raum, der zur Generierung und Umsetzung neuer innovativer Ideen in einem geschützten Umfeld dient. In den kreativ gestalteten Räumlichkeiten wird eine, oft zeitlich begrenzte, Zusammenarbeit möglich gemacht, um Kommunikation und Austausch außerhalb etablierter Unternehmensstrukturen zu fördern. Mit dem Aufbau eines Digital Lab verfolgen Unternehmen und Konzerne das Ziel mit neuen digitalen Geschäftsmodellen, innovativen Produktideen und digitalen Technologien, für eine digitale Zukunft aufzurüsten.

**LDAP:** Das »Lightweight Directory Access Protocol« (LDAP) ist ein Netzwerkprotokoll zur Durchführung von Abfragen und Änderungen in einem verteilten Verzeichnisdienst. LDAP selbst ist kein Verzeichnis, sondern das Protokoll, über das es mit einer bestimmten Syntax möglich ist, Informationen eines LDAP-Verzeichnisses abzufragen. Für eine fehlerlose Zusammenarbeit ist es bei LDAP erforderlich, dass alle beteiligten Systeme auf Port 389 für eine ungesicherte Übertragung und auf Port 636 in einer TLS gesicherten Verbindung Daten austauschen können. Die Idee hinter LDAP ist einfach: Ein über verschiedene Server verteiltes Verzeichnis in einer Baumstruktur soll einfach durchsucht werden können.

**Less-Than-Zero-Day Exploit:** Ein Angriffsprogramm (Exploit), das eine unveröffentlichte - einer oder nur sehr wenigen Personen bekannte - Sicherheitslücke (Less-Than-Zero-Day Vulnerability) ausnutzt. Da man sich nur gegen etwas schützen kann, was man kennt (Angriffssignatur oder Angriffsverhalten - Heuristik), sind IT-Systeme derartigen Angriffen schutzlos ausgeliefert. Less-Than-Zero-Day Vulnerabilities können mit einem zugehörigen Less-Than-Zero-Day Exploit also grundsätzlich erfolgreich angegriffen werden. Für unveröffentlichte Vulnerabilities existieren keine spezifischen Schutzmaßnahmen; der Angegriffene kann den Angriff grundsätzlich nicht direkt erkennen. In der Vergangenheit wurden Sicherheitslücken meist dem Hersteller gemeldet; dieser stellte (allerdings nicht in allen Fällen) eine Fehlerkorrektur zur Verfügung. In jüngerer Zeit werden Sicherheitslücken systematisch durch entsprechende Algorithmen gesucht und an Nachrichtendienste, Unternehmen und auch an die organisierte Kriminalität und Botnet-Betreiber verkauft und nicht oder nicht sofort dem Hersteller gemeldet. Durch Ausnutzung dieser unveröffentlichten Sicherheitslücken wird Wirtschaftsspionage und Computersabotage unerkannt praktiziert. In jüngerer Zeit wird in den USA für Less-Than-Zero-Day Vulnerabilities eine Mitteilungspflicht an das Department of Homeland Security (DHS) diskutiert.

**LibreSSL:** LibreSSL ist eine freie Implementierung des Verschlüsselungsprotokolls Transport Layer Security (TLS), ursprünglich Secure Sockets Layer (SSL). Um den Quellcode der OpenSSL-Bibliothek im Zuge der Nachlese um das Heartbleed-Sicherheitsproblem in OpenSSL von nicht benötigten Zusatzfunktionen, redundanten Bestandteilen und anderen betriebssystemspezifischen Altlasten zu befreien, erstellte das OpenBSD-Team den Fork LibreSSL. Dabei reduzierte man den Umfang des Quellcodes von OpenSSL erheblich.

**Loadbalancing:** Mittels Loadbalancing (Lastverteilung) werden in der Informatik umfangreiche Berechnungen oder große Mengen von Anfragen auf mehrere parallel arbeitende Systeme verteilt mit dem Ziel, ihre gesamte Verarbeitung effizienter zu gestalten.



**Longlining-Mails:** Bei Longlining imitieren massenhaft angepasste Phishing-Nachrichten, die in der Regel so aussehen, als werden sie nur in geringen Mengen gesendet, zielgerichtete Angriffe. Die Angreifer nutzen die Methoden von Massenwerbungskampagnen, um Millionen unähnlicher Nachrichten zu erzeugen. Dies geschieht mithilfe von E-Mail-erzeugendem Code und Infrastrukturen, die E-Mail-Inhalt, Betreffzeilen, Absender-IP-Adressen, Absender-E-Mail-Konten und URLs austauschen können. Das bedeutet, dass für jede Organisation nicht mehr als 10 - 50 E-Mails ähnlich aussehen, wodurch schädliche E-Mails dem Radar aller Spam- und Inhaltsscanner-Systeme entgehen können. In der Regel sind keine Anhänge vorhanden, wodurch die Wahrscheinlichkeit einer Erkennung durch Virenschutzprogramme oder andere signaturbasierter Lösungen minimiert wird. Außerdem sind die mehrfachen IP-Adressen, E-Mail-Konten des Absenders und URLs der Kampagne gewöhnlich legitim, aber infiziert. Das bietet grundsätzlich »gute« Reputationseigenschaften der E-Mails, wodurch sie einer reputationsbasierenden Erkennungsmethode entgehen können. Um die Zeitspanne bis zur Erkennung des Angriffs zu verlängern, stellen Angreifer sicher, dass die infizierte Website »polymorphe« Malware (sich verändernde Malware) an die Computer der Benutzer weiterleitet. Jeder Benutzer erhält eine einzigartige Version der Malware, wodurch im Grunde der Wert neuer Signaturen umgangen wird, die bei der erstmaligen Erkennung des Angriffs erstellt werden könnten. Aufgrund des raffinierten Inhalts und der infizierten Infrastruktur, die in Longlining-Angriffen für gewöhnlich beobachtet werden, ist für die Bekämpfung dieser Angriffe eine Big Data-gesteuerte Sicherheitslösung am effektivsten. Eine solche Lösung sollte sich in der Regel nicht nur auf Signaturen und Reputationskontrollen stützen. Das Ziel der Lösung sollte sein, im historischen Verlauf nach Mustern zu suchen, neuen Traffic in Echtzeit zu untersuchen und Prognosen zu treffen, was mithilfe eines fortschrittlichen cloudbasierten Malware-Erkennungsservice analysiert werden sollte. Außerdem muss die Sicherheitslösung eine Methode zur Verwaltung der Nachrichten haben, die durch den Filter kommen. Da bei Longlining-Angriffen gewöhnlich mehrere 100.000 Nachrichten pro Minute möglich sind, können viele davon die Benutzer erreichen.

**Makroviren:** Makroviren sind eine Untergruppierung der Computerviren. Diese Viren werden nicht in einer Programmiersprache wie z.B. Assembler erstellt, sondern mit der Makrosprache, die in großen Büroanwendungen implementiert ist. Makros sollen dazu dienen, wiederkehrende Abläufe zu automatisieren und den Anwender von Standardtätigkeiten zu entlasten. Mit der Makrosprache können aber auch Computerviren erstellt werden, also Programme, die sich selbst reproduzieren. Makroviren nisten sich in den Dokumenten ein, die mit dem Anwendungsprogramm erstellt werden.

**Malware:** Malware ist ein Sammelbegriff für »böartige« Programme (Schadprpgramme), die dazu entwickelt wurden, Nutzern Schaden zuzufügen. Es gibt zahlreiche Unterarten von Malware - z.B. Viren, Trojaner, Rootkits, Würmer, Botnets, Ransomware, Adware oder Spyware. Alle Arbeiten anders und haben verschiedene Aufgaben. Ein Ziel haben alle gemeinsam: Betroffene einen Schaden zuzufügen.

**Man-in-the-Middle-Angriff:** Bei einem Man-in-the-Middle-Angriff platziert sich der Angreifer logisch oder physisch zwischen dem Opfer und den verwendeten Ressourcen. Er ist dadurch in der Lage, die Kommunikation abzufangen, mitzulesen oder zu manipulieren. Die Ende-zu-Ende-Verschlüsselung ist eine wirksame Gegenmaßnahme gegen eine Man-in-the-Middle-Attacke.

**Mapping:** Daten-Mapping bezeichnet das Verknüpfen von Feldern verschiedener Datenbanken. Bevor man Daten analysieren kann müssen diese so vereinheitlicht werden, dass sie für Entscheidungsträger leicht zugänglich sind. Daten stammen heute häufig aus verschiedenen Quellen mit unterschiedlichen Definitionen für ähnliche Datenpunkte. In einem Quellsystem kann so im Feld »Staat« für Illinois »Illinois« stehen und im Zielsystem wird diese Information jedoch unter »IL« abgespeichert. Daten-Mapping überbrückt derartige Unterschiede zwischen zwei Systemen bzw. Datenmodellen, um aus einer Quelle entnommene Daten im Zielsystem nutzen zu können. Die Menge an Daten und deren Quellen nehmen jedoch immer mehr zu und macht das Daten-Mapping zusehends komplexer, sodass für die Bewältigung großer Datenmengen automatisierte Tools erforderlich sind.

**MapReduce:** MapReduce ist ein vom Unternehmen Google Inc. eingeführtes Programmiermodell für nebenläufige Berechnungen über (mehrere Petabyte) große Datenmengen auf Computerclustern. MapReduce ist auch der Name einer Implementierung des Programmiermodells in Form einer Software-Bibliothek. Beim MapReduce-Verfahren werden die Daten in drei Phasen verarbeitet (Map, Shuffle, Reduce), von denen zwei durch den Anwender spezifiziert werden (Map und Reduce). Dadurch lassen sich Berechnungen parallelisieren und auf mehrere Rechner verteilen. Bei sehr großen Datenmengen ist die Parallelisierung unter Umständen schon deshalb erforderlich, weil die Datenmengen für einen einzelnen Prozess (und das ausführende Rechnersystem) zu groß sind. Das Programmiermodell wurde durch die in der funktionalen Programmierung häufig verwendeten Funktionen map und reduce inspiriert, auch wenn die Arbeitsweise der Bibliothek davon abweicht. 2010 wurde für MapReduce ein US-Patent erteilt. Der wesentliche Beitrag von MapReduce ist jedoch das zu Grunde liegende System, das die Berechnungen stark parallelisiert, die Reorganisation der Daten im Shuffle-Schritt (Mischen-Schritt) optimiert und automatisch auf Fehler im Cluster reagieren kann, wie beispielsweise den Ausfall von kompletten Knoten.

**Mesh-Netzwerk:** Im Gegensatz zu einem WLAN-Router mit einem einzigen Access Point existieren in einem vermaschten Netzwerk (Mesh Netzwerk) zahlreiche Knotenpunkte. So schafft jeder Einzelne von ihnen einen direkten Zugang zum heimischen Netzwerk. Zwischen diesen Knotenpunkten herrscht permanente Kommunikation, um einen möglichst effizienten Datenaustausch sowohl zwischen den Access Points als auch zum ursprünglichen Router zu gewährleisten. Damit sind alle Knotenpunkte gleichsam Empfänger und Sender. Abhängig von der Netzerkauslastung kann ein Frequenzwechsel von 2.4 und 5 Gigahertz erfolgen oder eine Umschaltung auf einen anderen Zugangspunkt.

**Mikrosegmentierung:** Bei der so genannten Mikrosegmentierung werden auf der Ebene der Netzwerktechnik die verschiedenen Server- oder Clientbereiche anstelle von ganzen Netzen, wie bei der Netztrennung, separiert und über ein Segmentierungs-Gateway, konkret über eine Firewall, getrennt. Als Resultat sind nur ein Server oder zumindest sehr wenige Server bzw. Endgeräte in einem Netzwerksegment. Damit wird fast jeder Datenstrom über die Firewall reglementiert und kontrolliert. Somit entstehen durch diese Netzwerksegmentierung viele isolierte Einzelbereiche, die von einander abgeschirmt sind.

**Microsoft Azure:** Microsoft Azure ist eine Cloud-Computing-Plattform von Microsoft mit den Diensten wie SQL Azure oder AppFabric, die sich in erster Linie an Softwareentwickler richtet. Azure wurde im Oktober 2008 angekündigt, gestartet mit dem Codenamen »Project Red Dog« und seit dem 1. Februar 2010 ist die Plattform offiziell verfügbar.

**MITRE ATT&CK:** Das MITRE ATT&CK-Framework ist eine Sammelstelle für Informationen über das Verhalten bei Cyberangriffen auf der Grundlage von realen Beobachtungen. Das Verhalten wird nach Taktiken und Techniken kategorisiert. Das Framework wurde 2013 von der MITRE Corporation geschaffen, einer gemeinnützigen Organisation, die mit Regierungsbehörden, Wirtschaftsorganisationen und akademischen Institutionen zusammenarbeitet und ist eine allgemein zugängliche Wissensdatenbank, die eine umfassende Darstellung des Angriffsverhaltens bietet. ATT&CK steht für »Adversarial Tactics, Techniques and Common Knowledge« und dokumentiert gängige Taktiken, Techniken und Prozeduren (TTPs .. tactics, techniques and procedures), die Cyberkriminelle bei Angriffen auf Netzwerke einsetzen. Dabei wird zwischen Angriffen auf Windows-, Linux-, Mac-, Cloud-basierten und mobilen Umgebungen unterschieden. Unternehmen greifen regelmäßig auf diese Wissensdatenbank zurück, um offensive und defensive Maßnahmen zur Stärkung ihrer allgemeinen Sicherheitslage zu entwickeln.

**Monitor Mode:** Monitor Mode oder Monitormodus bezeichnet einen bestimmten Betriebsmodus eines Wireless Adapters, bei dem sämtliche empfangenen Netzwerkframes an das Betriebssystem und die Anwendungen weitergeleitet werden. Im Monitor Mode werden im Gegensatz zum Promiscuous Mode alle empfangenen Frames weitergeleitet, nicht nur die des Netzwerks, mit dem der Client momentan verbunden ist. Ein Vorteil ist, dass kein einziges Frame von der eigenen Netzwerkkarte gesendet werden muss und daher das Abhören der Frames nicht in evtl. Protokolldateien erkennbar ist. Außerdem ist keinerlei Authentifizierung am Netzwerk notwendig. Sind die Framepakete verschlüsselt, zum Beispiel mit WPA2, so können sie aufgezeichnet und später entschlüsselt werden. Dies ist mit WPA3 dank Perfect Forward Secrecy nicht mehr möglich.

**Multi-Hop VPN:** VPN-Services versuchen die Nutzer durch technische Funktionen vor Überwachung und Verfolgung im Internet zu schützen. Normale VPN-Service bietet dabei den verschlüsselten Zugang zu eigenen VPN-Servern an, welche in verschiedenen Ländern betrieben werden. Die Daten welche zwischen dem Endgerät (VPN-Client) und dem VPN-Service (VPN-Server) übertragen werden sind dabei verschlüsselt. Über den VPN-Service wird dabei auch die benutzte IP-Adresse des Nutzers nach Außen hin verändert und seine eigene IP-Adresse erscheint in der Kommunikation mit Webseiten und Webservices nicht mehr. Allerdings ist es so, dass weiterhin der eigene Internetanbieter die übertragenen Daten zumindest in dem Ausmaß erkennen kann, dass er weiss, zu welcher IP-Adresse die Daten eines Nutzers gesendet werden. Also der Internetanbieter kann anhand der Header Daten der Datenpakete erkennen, zu welchem VPN-Server man eine Verbindung aufgebaut hat. Dies ist im Regelfall kein Problem für die eigene Sicherheit, jedoch gibt es auch technische Lösungen die eine weitere Verschleierung ermöglichen. Dabei werden die Daten zwar wie gewohnt an einen VPN-Server gesendet, dieser sendet die Daten aber verschlüsselt an einen weiteren VPN-Server weiter. Dadurch wird für die Beobachter der eigenen Daten es zunächst Mal unmöglich, zu erkennen, welcher VPN-Server durch einen Nutzer verwendet wird um Aktivitäten im Internet durchzuführen. Man nennt diese Technik: »VPN-Kaskadierung« oder auch »Multi-Hop VPN«.

**MPLS:** MPLS bedeutet Multiprotocol Label Switching. Bei einem klassischen Transfer von Daten wird ein Datenpaket von Router zu Router weitergeleitet. In jedem Router, den das Datenpaket erreicht, läuft der identische Prozess ab. Automatisch wird eine Liste an Netzen und Routern durchlaufen und daraufhin entschieden, welchen Weg das Datenpaket zu nehmen hat. Dieser Prozess wiederholt sich jedes Mal, wenn das Paket einen neuen Knotenpunkt erreicht. Bei einer MPLS-Verbindung hingegen, wird auf eine andere Herangehensweise gesetzt, die es ermöglicht, Daten schneller vom Start- zum Zielort zu bringen. Im Gegensatz zum normalen Datentransfer wird hier die Routenberechnung nur einmal vorgenommen. Beim Eintritt in das Netzwerk wird dem Datenpaket ein sogenanntes Label zugeordnet, das Informationen zur genauen Route, die das Paket nehmen soll, enthält. Bei diesem Weiterleitungsmechanismus wird das Label an das Paket angehängt und bei jedem Knotenpunkt, der erreicht wird, muss nur das Label mit den Zielinformationen ausgelesen werden. Dadurch können Datenpakete durch einen Tunnel geschickt werden, ohne auf ihrem Weg behindert zu werden. Des Weiteren können mit MPLS Datenpakete priorisiert werden. Durch verbindliche Quality-of-Service Parameter (QoS) und durch die Zuordnung einzelner Anwendungen im Datenverkehr zu bestimmten Classes-of-Service (CoS) ist es möglich, höher priorisierten Datenpaketen eine schnellere Route zuzuweisen und benötigte Bandbreiten garantiert zur Verfügung zu stellen.

**NAND-Gatter:** Ein NAND-Gatter ist ein Logikgatter mit zwei oder mehr Eingängen A, B, ... und einem Ausgang Y, zwischen denen die logische Verknüpfung NICHT UND besteht. Ein NAND-Gatter gibt am Ausgang 0 aus, wenn alle Eingänge 1 sind. In allen anderen Fällen, d. h., wenn mindestens ein Eingang 0 ist, wird eine 1 ausgegeben.

**NAND-Flash:** NAND-Flash bezeichnet einen Typ von Flash-Speicher, der in der sogenannten NAND-Technik gefertigt ist. Hierbei sind die Einzel-Speicherzellen wie bei einem NAND-Gatter seriell verschaltet. Es gibt vier Produzenten entsprechender Chips: Samsung, Toshiba, IM Flash Technologies sowie Hynix in Kooperation mit Numonyx.

**NAT:** Netzwerkadressübersetzung (Network Address Translation) ist in Rechnernetzen der Sammelbegriff bei Änderungen von Adressen im IP-Header von IP-Paketen. NAT ermöglicht unter anderem die gleichzeitige Verwendung einer öffentlichen Adresse durch mehrere Hosts.

**OpenVPN:** OpenVPN ist eine freie Software zum Aufbau eines Virtuellen Privaten Netzwerkes über eine verschlüsselte TLS-Verbindung.

**OpenSSL:** Die Open Source Software hilft beim Aufbau von verschlüsselten Internet-Verbindungen und implementiert dazu die Transport Layer Security (TLS). Die Arbeit mit OpenSSL findet im Terminal statt und nicht mit Hilfe einer grafischen Oberfläche.

**OSI:** : Das OSI-Modell (englisch: Open Systems Interconnection Model) ist ein Referenzmodell für Netzwerkprotokolle als Schichtenarchitektur. Es wird seit 1983 von der International Telecommunication Union (ITU) und seit 1984 auch von der International Organization for Standardization (ISO) als Standard veröffentlicht. Das OSI-Referenzmodell ist in sieben Schichten (Layers) aufgeteilt, die hierarchisch übereinander angeordnet sind, wobei Schicht 1 die unterste und Schicht 7 die oberste ist.

**OTP:** Ein Einmalkennwort (One-time password) oder Einmalpasswort ist ein Kennwort zur Authentifizierung oder auch Autorisierung. Jedes Einmalkennwort ist nur für eine einmalige Verwendung gültig und kann kein zweites Mal benutzt werden. Entsprechend erfordert jede Authentifizierung oder Autorisierung ein neues Einmalkennwort.

**Overhead:** Als Overhead (deutsch: Verwaltungsdaten) gelten in der elektronischen Datenverarbeitung (EDV-) Daten, die nicht primär zu den Nutzdaten zählen, sondern als Zusatzinformation zur Übermittlung oder Speicherung benötigt werden.

**Paket-Sniffing:** Packet Sniffing ist das Sammeln und Protokollieren einiger oder aller Pakete, die durch ein Computer-Netzwerk gehen, unabhängig davon, wie das Paket adressiert ist. Auf diese Weise kann jedes Paket oder eine bestimmte Teilmenge von Paketen zur weiteren Analyse erfasst werden. Netzwerkadministratoren können diese gesammelten Daten für eine Vielzahl von Zwecken wie z. B. zur Überwachung von Bandbreite und Datenverkehr nutzen.

**Penetrationstest:** Mit einem Penetrationstest (Penetration .. durchdringen) ist in der Informationstechnik eine Testmethode gemeint, Software und Webseiten auf Schwachstellen, zu untersuchen. Dabei versucht der Tester an geschützte Daten oder Funktionen zu kommen. Einen Penetrationstest kann man grob zwischen Black-Box-Test und White-Box-Test unterscheiden. Diese Varianten unterscheiden sich darin, dass ein Pentester vom Auftraggeber entweder wie beim White-Box-Test alle Informationen zu einem zu überprüfenden Objekt bekommt oder im Black-Box-Test versucht wird, die Schwachstellen ohne dieses Insider-Wissen zu identifizieren. Hier gibt es noch weitere Abstufungen wie z.B. Grey-Box, bei welcher dem Pentester nur eine bestimmte Anzahl von Informationen zur Verfügung gestellt wird.

**Perfect Forward Secrecy:** Perfect Forward Secrecy (PFS) ist eine Methode für den Schlüsselaustausch kryptografischer Verfahren, das die nachträgliche Entschlüsselung durch Bekanntwerden des Hauptschlüssels verhindert. Die Sitzungsschlüssel werden nicht ausgetauscht und sind nicht mehr rekonstruierbar. **Forward Secrecy** verwendet dagegen immer die gleichen Parameter während einer Kommunikation. Der Sitzungsschlüssel wird erst dann neu berechnet, wenn die Kommunikation beendet und neu aufgebaut wird. Perfect Forward Secrecy verändert regelmäßig die Parameter während einer Kommunikation. Ein Sitzungsschlüssel wird also nur temporär verwendet und immer wieder neu erstellt. **Hinweis:** Die Erzeugung der temporären Parameter bei Perfect Forward Secrecy erfordert eine relativ hohe Rechenleistung.

**Perimeter:** Perimeter sind Teile von Netzwerken. Sie bilden die Trennlinie zwischen privaten oder lokalen und öffentlichen Netzwerken. Sie haben die Aufgabe, Netzwerke vor Angriffen von außen zu schützen. Sie bilden aber nur die erste Verteidigungslinie. Perimeter war ursprünglich ein Fachbegriff, um den Umfang einer geometrischen Figur zu beschreiben. Dieser Ansatz hat sich im Laufe der Geschichte zu einer Metapher verselbständigt, die auch für den IT-Bereich wichtig ist. Der Perimeter ist die Stelle, wo ein Raum endet und ein neuer anfängt.



**Pivot-Tabellen:** Pivot-Tabellen sind eine spezielle Art von Tabellen, die die Möglichkeit bieten, Daten einer Tabelle in verschiedener Art darzustellen und auszuwerten, ohne die Ausgangsdaten bzw. -tabelle(n) dabei ändern zu müssen. Die Aufteilung der Felder auf Zeilen- und Spaltenfelder bestimmt die Struktur der Pivot-Tabelle. Bei Änderung dieser Aufteilung oder Reihenfolge werden nicht mehr oder weniger Daten angezeigt, sondern diese lediglich in anderer Form dargestellt. Durch Doppelklick auf eine Zelle in einer Pivot-Tabelle werden Gruppen ein- und ausgeblendet (Drill-down und Roll-up), um mehr oder weniger Details darzustellen. Gehört die Zelle zu einem Datenfeld, werden nach dem Doppelklick alle einzelnen Datensätze aus den Originaldaten, die in die Berechnung dieser Zelle mit einfließen, auf einem separaten Tabellenblatt dargestellt.

**Port Forwarding:** Der Begriff »Port Forwarding« beschreibt den Vorgang des Weiterleitens externer IP-Pakete an einen UDP- oder TCP-Port eines Rechners oder Servers im internen LAN (Local Area Network). Damit werden Dienste beispielsweise eines Webserver oder eines E-Mail-Servers im LAN aus dem Internet erreichbar. Private IP-Adressen werden per Source und Destination NAT (Network Address Translation) in öffentliche IP-Adressen übersetzt.

**Portknocking:** Portknocking ist ein Verfahren, um Server bzw. einzelne Serverdienste in TCP/IP-Netzwerken abzusichern, das heißt vor unbefugtem Zugriff zu schützen. Der Name kommt von »to knock« (klopfen) und »Port« (Anschluss). Er soll versinnbildlichen, dass man zunächst in einer vorher vereinbarten Sequenz »anklopft«, bevor sich ein Port öffnet und man so Zugang zu einem bestimmten Serverdienst erhält.

**PPTP:** Das Point-to-Point Tunneling Protocol ist ein Netzwerkprotokoll, das auf das Internet Protocol aufsetzt und dem Aufbau eines Virtual Private Network in einem Rechnernetz dient. Das Verfahren gilt seit 2012 betreffend Verschlüsselung als gebrochen und unsicher.

**Promiscuous-Modus:** Der promiskuitive Modus oder Promiscuous-Modus (freizügiger Modus) bezeichnet einen bestimmten Empfangsmodus für netzwerktechnische Geräte. In diesem Modus liest das Gerät den gesamten ankommenden Datenverkehr an die in diesen Modus geschaltete Netzwerkschnittstelle mit (anstatt nur den für das Gerät bestimmten Datenverkehr) und gibt die Daten zur Verarbeitung an das Betriebssystem weiter. Geräte, die diesen Modus benutzen, können Kombinationen aus Switch und Router, Netzwerktester oder auch normale Computer mit Anschluss an ein Netzwerk sein. Bei Wireless LANs (WLANs) werden im promiscuous mode auch Pakete weitergeleitet, die nicht an einen selbst gerichtet sind, aber es werden nur die Pakete des Netzwerks (Accesspoints) weitergeleitet, mit dem der Client gerade verbunden ist. Da das Herstellen einer Verbindung mit dem Netzwerk normalerweise mit einer Authentifizierung einhergeht, ist der promiscuous mode nicht geeignet, um Pakete eines Netzwerks aufzufangen, zu dem man keinen direkten Zugang hat. Will man alle Pakete, aller erreichbaren WLAN Netze empfangen, ist dazu der Monitor Mode nötig. Das Gegenteil zu diesem Modus stellt der non-promiscuous mode dar. In diesem Modus verarbeitet das Gerät nur die an sich selbst gerichteten Pakete, was zum Beispiel in Ethernetnetzen über das Auswerten der MAC-Adresse geschieht, zuzüglich Broadcast- und Multicast-Pakete.

**Proxy Server:** Der Proxy Server ist ein Vermittler oder Stellvertreter und nimmt Anfragen entgegen, die er unter seiner eigenen Identität weiterleitet. Mit Hilfe des Proxy Servers lässt sich die Kommunikation zwischen einem lokalen Client und einem Webserver absichern, verschleiern oder beschleunigen. Kommt eine Verbindung zwischen einem Client und einem Server zustande, bleiben die Adressen von Client und Server den Kommunikationspartnern jeweils verborgen. Im Gegensatz zur Network Address Translation (NAT) werden Adressen nicht nur einfach ausgetauscht, sondern der Proxy Server führt die Kommunikation selbst. Er kann übertragene Pakete analysieren und gegebenenfalls verändern.

**Public-Key-Authentifizierung:** Die Public-Key-Authentifizierung ist eine Authentifizierungsmethode, die unter anderem von SSH und OpenSSH verwendet wird, um Benutzer mit Hilfe eines Schlüsselpaars, bestehend aus privatem und öffentlichem Schlüssel, an einem Server anzumelden. Ein solches Schlüsselpaar ist wesentlich schwerer zu kompromittieren als ein Kennwort.

**RADIUS-Server:** RADIUS steht für den englischen Begriff Remote Authentication Dial-In User Service und bezeichnet einen Service, der User in einem Dial-In-Netzwerk (Einwahlverbindungen) authentifiziert und autorisiert. RADIUS lässt sich auch für die Abrechnung (Accounting) von Services nutzen. In Unternehmen wird RADIUS häufig für die Benutzer-Anmeldung in WLAN-Netzwerken eingesetzt.

**RDP:** Das Remote Desktop Protocol (RDP) ist ein proprietäres Netzwerkprotokoll von Microsoft für den Fernzugriff auf Computer. Es ermöglicht die Übertragung grafischer Bildschirminhalte eines entfernten Rechnersystems, sowie die Bereitstellung von Peripheriefunktionen eines Arbeitsplatzes (Tastatur, Maus, Audio-Ein-/Ausgabe, Videoeingabe sowie sitzungsbezogenen Datenaustausch wie Textpuffer (engl. Clipboard), Druckerkopplung und Dateisystembereitstellung). Grundsätzlich ist RDP unabhängig vom zugrundeliegenden Netzwerk und der verwendeten Übertragungstechnik. Üblicherweise wird es jedoch in IP-Netzen (IPv4 und IPv6), wie dem Internet verwendet.

**Roll-out:** Der Begriff Rollout kommt aus der englischen Sprache und heißt übersetzt so viel wie Markteinführung oder Auslieferungsbeginn. Während ein Rollout im Bereich Marketing die Einführung eines neuen Produktes auf dem Markt bezeichnet, gibt es im Technikbereich und in der IT-Branche eine Vielzahl von Bedeutungen: das erste »Herausrollen« eines Autos oder Flugzeugs, die Einführung einer neuen Software (Software Rollout) oder der Austausch von alter gegen neue Hardware (Hardware Rollout). Besonders umfangreiche Rollouts finden in der Mobilfunkbranche statt, wenn beispielsweise die Netzbetreiber ihre Mobilfunkinstallationen aufbauen oder warten.

**Rootkit:** Ein Rootkit (englisch etwa: Administratorenbausatz; root ist bei unixähnlichen Betriebssystemen der Benutzer mit Administratorrechten) ist eine Sammlung von Softwarewerkzeugen, die nach dem Einbruch in ein Softwaresystem auf dem kompromittierten System installiert wird, um zukünftige Anmeldevorgänge (Logins) des Eindringlings zu verbergen und Prozesse und Dateien zu verstecken. Der Begriff ist heute nicht mehr allein auf unixbasierte Betriebssysteme beschränkt, da es längst auch Rootkits für andere Systeme gibt. Antivirenprogramme versuchen, die Ursache der Kompromittierung zu entdecken. Zweck eines Rootkits ist es, Schadprogramme (Malware) vor den Antivirenprogrammen und dem Benutzer durch Tarnung zu verbergen. Ein Rootkit enthält oft Software, um Daten von Terminals, Netzwerkverbindungen und Tastaturanschläge und Mausklicks sowie Passwörter vom kompromittierten System abzugreifen. Hinzu können Backdoors (Hintertüren) kommen, die es dem Angreifer zukünftig vereinfachen, auf das kompromittierte System zuzugreifen.

**RSA:** RSA (Rivest–Shamir–Adleman) ist ein asymmetrisches kryptographisches Verfahren, das sowohl zum Verschlüsseln als auch zum digitalen Signieren verwendet werden kann. Es verwendet ein Schlüsselpaar, bestehend aus einem privaten Schlüssel, der zum Entschlüsseln oder Signieren von Daten verwendet wird und einem öffentlichen Schlüssel, mit dem man verschlüsselt oder Signaturen prüft. Der private Schlüssel wird geheim gehalten und kann nicht mit realistischem Aufwand aus dem öffentlichen Schlüssel berechnet werden.

**RST-Pakete:** Ist ein Abbruch der TCP-Verbindung notwendig, wird das RST-Flag (Reset) gesetzt. Der versandt eines RST-Paketes kommt auch zum Einsatz, wenn eine TCP-Verbindung abgewiesen wird.

**SaaS:** Software-as-a-Service (SaaS) ist ein Lizenz- und Vertriebsmodell, mit dem Software-Anwendungen über das Internet (Adobe Premiere, Office 365, ...), d.h. als Service, angeboten werden. **SD-WAN:** Ein Software-defined Wide Area Network (SD-WAN) ist eine virtuelle WAN-Architektur (SD-WAN = VPN plus einige Zusatzfunktionen), über die Unternehmen beliebige Wege für die Datenübertragung, einschließlich MPLS, LTE und Breitband-Internetdienste, kombinieren können, um Benutzer auf sichere Weise mit Anwendungen zu verbinden.

**Security Appliance:** Eine Security Appliance ist jede Form von Hardware oder Hardware-Software-Kombinationen (Server, Switch), die Computernetzwerke vor unerwünschtem Datenverkehr schützen.

**Session Hijacking:** Session Hijacking ist eine Methode, mit der ein Angreifer die Websitzung eines Benutzers kapert. Dazu verschafft er sich heimlich die Session-ID des Benutzers und gibt sich dann als dieser aus. Sobald der Angreifer Zugriff auf die Session-ID hat, kann er die Identität des Benutzers vortäuschen und im Netzwerk alle Aktionen ausführen, zu denen dieser Benutzer berechtigt ist. Eines der wertvollsten Nebenprodukte solcher Angriffe ist die Möglichkeit, Zugang zu einem Server zu erhalten, ohne sich bei diesem authentisieren zu müssen.

**SIEM:** Das Security Information and Event Management (SIEM) ermöglicht einen ganzheitlichen Blick auf die IT-Sicherheit, indem Meldungen und Logfiles verschiedener Systeme gesammelt und ausgewertet werden. Verdächtige Ereignisse oder gefährliche Trends lassen sich in Echtzeit erkennen. Durch das Sammeln, Korrelieren und Auswerten von Meldungen, Alarmen und Logfiles verschiedener Geräte, Netzkomponenten, Anwendungen und Security-Systeme in Echtzeit werden Angriffe, außergewöhnliche Muster oder gefährliche Trends sichtbar. Auf Basis der gewonnenen Erkenntnisse können Unternehmen oder Organisationen schnell und präzise auf Bedrohungen reagieren. Das Security Information and Event Management nutzt Verfahren des maschinellen Lernens und der Künstlichen Intelligenz (KI).

**Site-to-Site:** Eine Site-to-Site-Verbindung verbindet zwei Netzwerke miteinander. Grundsätzlich unterscheidet man zweierlei Arten von Site-to-Site-VPNs: Bei intranet-basierten Site-2-Site-VPNs verfügt das Unternehmen über einen oder mehrere Remote-Standorte (mit separaten LANs), die über ein einzelnes privates Netzwerk (WAN) verbunden werden. In einem extranet-basierten Site-2-Site-VPN werden hingegen die LANs von unterschiedlichen Unternehmen miteinander verbunden. Auf diese Weise können diese in einer sicheren, gemeinsamen Netzwerkumgebung interagieren und zugleich den Zugriff auf das eigene Intranet verhindern.

**Skill:** Den englische Begriff »Skill« kann man mit »Fähigkeit / Geschick« übersetzen. Ein Skill repräsentiert also Fähigkeiten und/oder Kenntnisse eines Menschen. Eine Maschine bietet Funktionalitäten, ein Mensch verfügt über Skills.

**SOAR:** Security Orchestration Automation and Responses, kurz SOAR stellt Software und Verfahren zur Verfügung, mit denen sich Informationen über Sicherheitsbedrohungen sammeln lassen. Auf deren Basis erfolgt eine automatische Reaktion. Ziel ist es, das Bedrohungs- und Schwachstellenmanagement in einem Unternehmen zu verbessern.

**SOC:** Beim Security Operations Center (SOC) handelt es sich um eine Sicherheitsleitstelle, die sich um den Schutz der IT-Infrastruktur eines Unternehmens oder einer Organisation kümmert. Um diese Aufgabe leisten zu können, integriert, überwacht und analysiert das SOC alle sicherheitsrelevanten Systeme wie Unternehmensnetzwerke, Server, Arbeitsplatzrechner oder Internetservices. Unter anderem werden die Log-Dateien der einzelnen Systeme gesammelt, analysiert und nach Auffälligkeiten untersucht. Neben der Analyse der verschiedenen Systeme und Log-Dateien sind das Alarmieren und Ergreifen von Maßnahmen zum Schutz von Daten und Anwendungen zentrale Aufgabe des Security Information Centers.

**Spear Phishing:** Beim klassischen Phishing werden große Mengen von E-Mails wahllos an Empfänger verschickt, um sie dazu zu bringen, auf schädliche Links zu klicken oder vertrauliche Informationen preiszugeben. Beim Spear Phishing werden die Empfänger hingegen sorgfältig recherchiert und ausgewählt und erhalten E-Mails, die auf sie persönlich zugeschnitten sind und viel glaubwürdiger wirken.

**Spyware:** Als Spyware wird üblicherweise Software bezeichnet, die Daten eines Computernutzers (Benutzerprofile) ohne dessen Wissen oder Zustimmung an den Hersteller der Software, an Dritte sendet oder dazu genutzt wird, dem Benutzer über Werbeeinblendungen Produkte anzubieten.

**SQL-Injection:** SQL ist die Sprache, die verwendet wird, um mit der Datenbank zu kommunizieren. Sie wird (in leicht abgewandelter Form) bei verschiedenen relationalen Datenbanksystemen verwendet (z.B. MySQL oder MariaDB). Bei einer SQL-Injection wird die Kommunikation der Webanwendung mit der Datenbank manipuliert. Dazu werden zusätzliche Befehle in Datenbankabfragen injiziert und so die Logik der Abfrage verändert. Genutzt werden für die Injektion Eingabemöglichkeiten für Benutzer auf der Webseite, zum Beispiel ein Such- oder Login-Feld. Anstatt der vorgesehenen Eingabe wird ein SQL-Befehl eingegeben.

**Squid:** Squid (engl. Kalmar) ist ein freier Proxyserver und Web-Cache, der unter der GNU General Public License steht. Er zeichnet sich vor allem durch seine gute Skalierbarkeit aus. Squid-Server können sowohl für sehr kleine Netze (5–10 Benutzer) als auch für sehr große Proxyverbunde in Weitverkehrsnetzen mit mehreren hunderttausend Benutzern eingesetzt werden.

**SSH:** Die Secure Shell (SSH) bezeichnet ein Protokoll, über das entsprechende Programme (Clients) auf einen entfernten Computer zugreifen und auf diesem Befehle oder Aktionen ausführen können. Auf PC und Server mit Linux oder einem anderen Unix-artigen Betriebssystem gehört SSH zu den fest installierten Standardwerkzeugen und ist für viele Administratoren die bevorzugte Wahl, um einen Computer durch einen Fernzugriff zu konfigurieren und zu betreuen.

**SSID:** Die SSID (Service Set Identifier) dient dazu, ein WLAN von anderen zu unterscheiden. Deshalb müssen alle Access Points und sonstigen Geräte, die versuchen, eine Verbindung zu einem bestimmten WLAN aufzubauen, dieselbe SSID verwenden.

**Stateful Inspection Firewalls:** Unter Stateful Packet Inspection (SPI; zustandsorientierte Paketüberprüfung) versteht man eine dynamische Paketfiltertechnik, bei der jedes Datenpaket einer bestimmten aktiven Session zugeordnet wird. Die Datenpakete werden analysiert und der Verbindungsstatus wird in die Entscheidung einbezogen. Bei dieser Technik, die in Firewalls eingesetzt wird, werden die Datenpakete (eigentlich: Segmente) während der Übertragung auf der Vermittlungsschicht (3. Schicht des OSI-Modelles) analysiert und in dynamischen Zustandstabellen gespeichert. Auf Basis des Zustands der Datenverbindungen werden die Entscheidungen für die Weiterleitung der Datenpakete getroffen.

**Suricata:** Suricata ist ein Network Intrusion Detection System (NIDS). Es wird durch die Open Information Security Foundation (OISF) entwickelt und betreut. Die Software steht unter einer freien GPLv2 Lizenz. Neben dem Betrieb als IDS bietet Suricata auch einen Network Intrusion Prevention System (NIPS) Modus an, der direkt in den Datenverkehr eingreift und Pakete blockieren kann. Suricata kommt in einigen freien Firewall-Distributionen wie IPFire, pfSense, OPNsense und SecurityOnion als IDS oder IPS zum Einsatz. Ebenso verwenden kommerzielle Anbieter wie etwa »FireEye« Suricata in ihren Produkten und leisten als Consortium Member der OISF auch finanzielle Unterstützung.

**SYN Flooding:** SYN Flooding nennt man einen Angriffsvektor, um damit sogenannte DoS-Angriffe (Denial-of-Service) auf einen Server durchzuführen. Bei diesem Angriff schickt ein Client kontinuierlich SYN-Pakete (Synchronisation) an jeden Port auf einem Server und verwendet dafür gefälschte IP-Adressen.

**SYN-Pakete:** Als verbindungsorientiertes Protokoll ist TCP für den Verbindungsaufbau und Verbindungsabbau zwischen zwei Stationen einer Ende-zu-Ende-Kommunikation zuständig. Obwohl es sich eher um eine virtuelle Verbindung handelt, stehen Sender und Empfänger während der Verbindung ständig in Kontakt zueinander. Der Empfänger bestätigt dem Sender jedes empfangene Datenpaket. Trifft keine Bestätigung beim Absender ein, wird das Paket noch mal verschickt. Der Verbindungsaufbau läuft nach dem Three-Way-Handshake ab. Zuerst schickt der Client an den Server einen Verbindungswunsch (SYN .. Synchronization). Der Server bestätigt den Erhalt der Nachricht (ACK) und äußert ebenfalls seinen Verbindungswunsch (SYN). Der Client bestätigt den Erhalt der Nachricht (ACK). Danach erfolgt der Datenaustausch zwischen Client und Server.



**Systemhärtung:** Der Begriff »Systemhärtung« ist die Übersetzung des Englischen »System Hardening«. Im IT-Sprachgebrauch wird vereinfacht auch nur von der »Härtung« gesprochen. Da auf IT-Systemen unter anderem auch höchst sensible Informationen eines Unternehmens sowie personenbezogene Daten verarbeitet und gespeichert werden, müssen die verwendeten Systeme besonderen Schutzmaßnahmen unterzogen werden.

**TCP:** Das Transmission Control Protocol (TCP, deutsch: Übertragungssteuerungsprotokoll) ist ein Netzwerkprotokoll, das definiert, auf welche Art und Weise Daten zwischen Netzwerkkomponenten ausgetauscht werden sollen. Nahezu sämtliche aktuelle Betriebssysteme moderner Computer beherrschen TCP und nutzen es für den Datenaustausch mit anderen Rechnern. Das Protokoll ist ein zuverlässiges, verbindungsorientiertes, paketvermittelltes Transportprotokoll in Computernetzwerken (OSI-Schicht: 4). Im Unterschied zum verbindungslosen UDP (User Datagram Protocol) stellt TCP eine Verbindung zwischen zwei Endpunkten einer Netzverbindung (Sockets) her. Auf dieser Verbindung können in beide Richtungen Daten übertragen werden. TCP setzt in den meisten Fällen auf das IP (Internet-Protokoll) auf, weshalb häufig auch vom »TCP/IP-Protokoll« die Rede ist.

**Telemetrie:** Unter dem Begriff Telemetrie versteht man in der Softwaretechnik das Sammeln von Rohdaten, die per automatischer Datenübertragung durch einen im Hintergrund laufenden Dienst an den Entwickler übertragen werden. Geschieht dies für den Benutzer nicht transparent, so spricht man auch von dem Nach-Hause-Telefonieren (Phoning Home oder Calling Home), da sich die Software ohne leicht zu erreichende Einflussnahme durch den Benutzer beim Hersteller meldet.

**Teredo:** Teredo (RFC 4380) ist eine Tunnel-Technik von Microsoft, die IPv6-Datenpakete in IPv4-UDP-Datenpakete kapselt, damit Windows-PCs und die Xbox (Spielekonsole) die NAT-Schranke von Internet-Zugangsroutern von innen überwinden und so miteinander reden können. Teredo kommt dabei ohne Anwendereingriffe aus. Als IPv6-Tunnel-Technik soll Teredo den Übergang von IPv4 auf IPv6 vereinfachen und an Rechnern in lokalen (IPv4-)Netzen eine global gültige IPv6-Adresse vergeben. Dazu baut Teredo einen IPv6-Tunnel über eine IPv4-Sitzung auf.

**TLS:** Bei der Transport Layer Security (TLS) handelt es sich um ein Protokoll der Schicht 5 des ISO/OSI-Schichtenmodells, das für eine verschlüsselte Übertragung von Daten im Internet sorgt. TLS ist der Nachfolger von SSL (Secure Sockets Layer) und wird beispielsweise von Browsern für sichere HTTPS-Verbindungen verwendet.

**Token:** Mit Token bzw. Security-Token, wird allgemein eine Hardwarekomponente zur Identifikation und Authentifizierung von Benutzern bezeichnet. Auch Softwaretoken fallen in diese Kategorie. Um sich als berechtigter Nutzer auszuweisen, ist der unmittelbare Besitz des Tokens hierbei immer erforderlich.

**TOTP:** Der Time-based One-time Password Algorithmus ist ein Verfahren zur Erzeugung von zeitlich limitierten Einmalkennwörtern basierend auf dem Keyed-Hash Message Authentication Code (kryptografische Hash-Funktion), welcher im Rahmen der Authentifizierung Anwendung findet.

**Torrent:** In ihrer ursprünglichen Definition bezeichnen Torrents eine bestimmte Art von Verzeichnisdatei. Diese Datei ist meist sehr klein und enthält lediglich Informationen, die für das Herunterladen der eigentlich begehrten Daten vonnöten sind. Das bedeutet: Allein der Download einer Torrent-Datei ist nicht illegal. Allerdings ist der Torrent an sich für den Nutzer wertlos. Er benötigt eine bestimmte Software - einen sogenannten BitTorrent-Client - um ihn zu nutzen. Die Software liest die Informationen aus dem Torrent aus und startet dementsprechend den eigentlichen Download. Bekannte Clients sind unter Anderem Utorrent (auch µtorrent genannt), Vuze und eMule. Die Clients erfahren durch die Torrentdatei, an welchen Punkten des Netzwerks sich die erstrebten Daten befinden. Sie prüfen, welche entsprechenden Rechner zu diesem Zeitpunkt mit dem Netz verbunden sind und laden die Dateien auf dem schnellstmöglichen Weg herunter. Diese Torrent-Verzeichnisdateien erkennen Sie an der Kennung .torrent oder .tor. Sie enthalten die Standorte, auf welchen sich die gewünschten Dateien befinden.

**TPM:** Die Abkürzung TPM steht für Trusted Platform Module. Es handelt sich dabei um einen Sicherheitschip, der auf dem Mainboard verbaut ist und das System schützen soll. Er stellt grundlegende Sicherheitsfunktionen hardwarebasiert zur Verfügung und kann Kryptographieschlüssel erzeugen, sicher speichern oder deren Einsatz kontrollieren. Er prüft beispielsweise beim Bootvorgang, ob das System durch Malware kompromittiert wurde. Ein solcher TPM-Chip steckt nicht nur in PCs, sondern beispielsweise auch in Smartphones.

**Traffic-Shaping:** Traffic-Shaping bezeichnet eine Art der Warteschlangenverwaltung, Bandbreitenverwaltung bei paketvermittelten Datennetzen, bei der Datenpakete nach bestimmten Kriterien verzögert oder verworfen werden, um bestimmten Anforderungsprofilen zu genügen. Diese Technik wird hauptsächlich verwendet, um eine hohe Servicequalität für den geschäftsbezogenen Netzwerkverkehr sicherzustellen.

**Trap Door:** Eine Trap Door (Falltür) wird durch verdeckte (undokumentierte), implementierte Folge von Instruktionen (spezielle Zeicheneingaben, Passwort-Eingaben, Ereignisfolgen, Programmteile, Programme in Hardware, Firmware und/oder Software), die einen Angriff auf ein IT-System durch Umgehung oder Durchdringung des Sicherheitssystems aufgestoßen. Eine Trap Door kann auch zu Test- und Wartungszwecken berechtigt eingebaut sein - sie ist dann allerdings meist nur für Berechtigte dokumentiert.

**Tutorial:** Mit dem englischen Lehnwort Tutorial bezeichnet man im neueren Sprachgebrauch eine schriftliche oder filmische Gebrauchsanleitung, welche ein Thema, einen gewissen Vorgang oder eine Funktion erklärt. Tutorials sind besonders im Internet auf Videoplattformen zu finden.

**UAC:** UAC (User Account Control, Benutzerkontensteuerung; verfügbar ab Windows Vista) - striktes Herabstufen und Deaktivierung automatischer Rechtegewährung für administrative Konten.

**UBA:** User Behavior Analytics (UBA) ist die Analyse des Verhaltens von IT-Usern mit dem Ziel, Attacken auf IT-Systeme und den Diebstahl von Daten durch externe und interne Angreifer zu erkennen und zu unterbinden. Zu diesem Zweck nutzen UBA-Lösungen spezielle Algorithmen und Machine-Learning-Verfahren, mit denen typische Verhaltensmuster von IT-Nutzern ermittelt und analysiert werden.

**UDP:** Das User Datagram Protocol, kurz UDP, ist ein minimales, verbindungsloses Netzwerkprotokoll, das zur Transportschicht (OSI-Schicht: 4) der Internetprotokollfamilie gehört. UDP ermöglicht Anwendungen den Versand von Datagrammen in IP-basierten Rechnernetzen. UDP eignet sich für Anwendungen, die fehlertolerant sind und Daten mit niedriger Latenz senden und empfangen möchten. Mechanismen zur Prüfung, ob Pakete verloren gegangen sind, in der falschen Reihenfolge eintreffen oder dupliziert wurden, bietet das User Datagram Protocol nicht. Der Absender wird nicht darüber informiert, ob ein Datenpaket tatsächlich am Ziel angekommen ist, da keine Bestätigungen versendet werden. Typische Anwendungen sind das Streaming von Audio- und Videodaten.

**Uroburos:** Bei Uroburos handelt es sich um ein Rootkit welches aus zwei Dateien besteht, einem Treiber sowie einem verschlüsselten virtuellen Dateisystem. Mit Hilfe dieses Rootkits kann der Angreifer die Kontrolle über den infizierten PC bekommen und so beliebigen Programmcode auf dem Computer ausführen sowie seine Systemaktivitäten verstecken. Weitere Funktionen von Uroburos sind die Möglichkeit des Dateidiebstahls sowie der Mitschnitt von Netzwerkdatenverkehr. Aufgrund dieser Flexibilität und Modularität wird das Rootkit von den Experten als sehr fortschrittlich und gefährlich eingestuft werden. Ein weiterer Anhaltspunkt für diese Einstufung ist der extrem komplexe Aufbau der Treiberkomponente bei deren Entwicklung sehr viel Wert darauf gelegt wurde, dass die Schadsoftware extrem schwierig aufzufinden ist. Die Investition, ein Framework wie Uroburos zu entwickeln, ist extrem hoch. Bei dem Entwicklerteam hinter dieser Schadsoftware handelt es sich offensichtlich um sehr gut ausgebildete Computerexperten. Uroburos wurde entwickelt, um im »peer-to-peer« Modus zu arbeiten. Hierbei kommunizieren infizierte Computer in einem geschlossenen Netzwerk direkt miteinander wobei die Kommunikation durch den Angreifer gesteuert werden kann. Durch diese Fähigkeit ist es ausreichend wenn ein einziger infizierter Rechner Zugriff auf das Internet hat. Der Angreifer kann über diesen Rechner andere Computer in dem Netzwerk infizieren und mit diesen anschließend über den infizierten Rechner kommunizieren. Dies funktioniert selbst wenn der frisch infizierte Computer nicht selber über eine Internetverbindung verfügt. Uroburos ist in der Lage seine Spionagefunktionalität auf allen diesen Computern einzusetzen und die dabei gewonnenen Informationen über weitere infizierte Rechner im infiltrierten Netzwerk aus diesem heraus zu schleusen. Sobald die Informationen an einem infizierten Rechner mit Internetanbindung angelangt sind, können diese an den Angreifer übermittelt werden. Die beschriebene Funktionalität ist typisch für Schadsoftware welche darauf ausgelegt ist, sich in großen Firmen- oder Behördennetzen zu verbreiten. Die Angreifer gehen davon aus, dass in dem Netzwerk Computer vorhanden sind, welche keine direkte Internetverbindung besitzen und benutzen diese Technik um über Umwege trotzdem an ihr Ziel zu gelangen. Uroburos unterstützt dabei sowohl 32- als auch 64-Bit Microsoft Windows Systeme. Aufgrund der Komplexität der Schadsoftware und der darin enthaltenen Spionagefunktionalität wird vermutet, dass dieses Rootkit hauptsächlich große Firmen, Forschungseinrichtungen sowie Behörden ins Visier nimmt.

**UUID:** Eine UUID (Universally Unique Identifier) ist eine 128-Bit lange Zahl. Diese ist eindeutig und wird zur Identifikation von Computer-Systemen genutzt. Im Microsoft-Umfeld wird aber auch oft der Begriff GUID (Globally Unique Identifier) verwendet. In der Regel ist die UUID im BIOS hinterlegt.

**Voucher:** Voucher ist ein einmaliger und eindeutiger Code, mit dem eine Software-Lizenz aktiviert wird. Ein Voucher ist nicht notwendigerweise mit einer gewerblichen Lizenz verknüpft. Er wird oft dazu verwendet, Testlizenzen oder kostenlose Software zu aktivieren. Das Format eines Vouchers ist xxxx-xxxx-xxxx-xxxx.

**VPN:** Ein VPN (Virtual Private Network) ist ein Dienst, der eine sichere, verschlüsselte Verbindung herstellt. Dabei kann es sich um ein Unternehmens- aber auch um ein privates Netzwerk handeln. Bei VPN handelt es sich um ein geschlossenes logisches Netzwerk, bei dem die Teilnehmer räumlich voneinander getrennt und über einen IP-Tunnel eine Verbindung haben.

**VPN Chaining** (Doppel-VPN): Ein Doppel-VPN verwendet mehrere VPNs in einer Chaining-Konfiguration, indem es durch mehr als einen VPN-Server geroutet wird. Diese Strategie bietet eine höhere Sicherheit für eine VPN-Verbindung aufgrund der doppelten Verschlüsselung.

**Wear Leveling:** Wear Leveling (deutsch: Verschleiß-Nivellierung) ist eine Methode, um die Lebensdauer von Solid-State Drives (SSD) zu verlängern. Solid-State-Storage besteht aus Microchips, welche die Daten in Blöcken speichern. Jeder dieser Speicherblöcke kann eine bestimmte und endliche Anzahl (etwa 100.000) an Program-Erase Cycles tolerieren, bevor er unzuverlässig wird. Wear Leveling arrangiert die Daten so, dass Schreib-/Lösch-Zyklen gleichmäßig auf alle Blöcke des Mediums verteilt werden.

**WebRTC:** WebRTC (Web Real Time Communication) ist ein offener Standard, der eine Sammlung von Kommunikationsprotokollen und Programmierschnittstellen definiert, die Echtzeitkommunikation über Rechner-Rechner-Verbindungen ermöglichen. WebRTC ist auf den Web-Programmiersprachen HTML (Hyper Text Markup Language) und JavaScript aufgebaut. WebRTC ist Teil des Browsers und läuft daher über die Methode der Datagram Transport Layer Security (DTLS). Diese Methode macht das Abhören der übermittelten Daten unmöglich und gewährleistet somit eine sichere direkte Kommunikation zwischen zwei oder mehreren Benutzern.

**Windows Defender Application Guard:** Windows Defender Application Guard (WDAG) kann Sitzungen im Webbrowser über Hyper-V virtualisieren und dadurch sicherstellen, dass Malware nicht über das Internet auf einen PC übertragen werden kann. Bislang steht die Funktionalität nur unter Windows 10 Enterprise und Pro zur Verfügung.

**Windows Defender Exploit Guard:** Der Windows Defender Exploit Guard wurde ins Betriebssystem integriert. Hier kann man die Angriffsfläche, die ein System bietet, deutlich reduzieren. Anwendungen lassen sich gegen typische Sicherheitslücken, wie etwa Buffer Overflows, härten. Admins können so mehr Kontrolle darüber erhalten, wie Code auf den Systemen ausgeführt wird. Auf Einzelsystemen finden sich die Windows-Einstellungen (Tastenkombination: [Win] + [I]) zum Exploit-Schutz im **Windows Defender Security Center** (siehe auch: [Win] + [Q] -> Suchwort: Windows Defender oder Firewall, regedit) im Bereich App- & Browsersteuerung unter Exploit-Schutz. Zur Funktionalität des Windows Defender Exploit Guard gehört auch der überwachte Zugriff auf Ordner.

**Windows Device Guard:** Microsoft bietet mit Windows Device Guard die Möglichkeit Arbeitsstationen so abzusichern, dass nur definierte Anwendungen (Whitelist) gestartet werden können. Windows Device Guard stellt gewisse Anforderungen an das verwendete System und die Hardware, die unterstützt werden müssen.

**Wipe:** Wipe (wischen, putzen) ist eine Eraser-Software, die zum sicheren Löschen von Dateien unter Linux und Windows dient. Wird eine Datei mit Wipe gelöscht, so überschreibt es diese mehrmals mit Nullen, speziellen Bit-Mustern und/oder Zufallsdaten.

**Zero-Day:** Zero-Day ist ein allgemeiner Begriff und steht für neu entdeckte Sicherheitslücken, über die Hacker Systeme angreifen können. Der englische Ausdruck »Zero-Day« bezieht sich auf die Tatsache, dass ein Hersteller oder Entwickler gerade erst von diesem Fehler erfahren hat und damit »Null Tage« Zeit hat, ihn zu beheben. Man spricht von einem Zero-Day-Angriff, wenn Hacker die Schwachstelle ausnutzen können, bevor die Entwickler sie beseitigen konnten.

**Zero-Day-Schwachstelle:** Eine Zero-Day-Schwachstelle ist eine Schwachstelle in der Software, die von Angreifern entdeckt wurde, bevor der Hersteller darauf aufmerksam geworden ist. Da der Hersteller nichts davon weiß, gibt es auch keinen Patch, so dass die Angriffe mit hoher Wahrscheinlichkeit erfolgreich verlaufen.

**Zero-Day-Exploit:** Eine Zero-Day-Exploit ist die Methode (Skript, Programm, ...), die die Hacker zum Angriff auf eine bislang unerkannte Schwachstelle anwenden.

**Zero-Day-Angriff:** Ein Zero-Day-Angriff ist die Anwendung eines Zero-Day-Exploits, um Schaden anzurichten oder Daten aus einem geschwächten System zu entwenden.

**Zero Trust:** Zero Trust (deutsch: Null Vertrauen) ist eine Bezeichnung für das IT-Sicherheitsprinzip »Vertraue niemandem, verifiziere, überprüfe jeden«. Dabei wird keinem Akteur, der auf Ressourcen zugreifen möchte, vertraut. Jeder einzelne Zugriff erfordert eine Authentifizierung. Dem gegenüber steht der klassische Sicherheitsansatz, der die Sicherung der Unternehmensgrenzen vorsieht. Dieser traditionelle, perimeterbasierte Ansatz stellt im Grundsatz den Schutz der Grenzen zum Unternehmensnetzwerk sicher. Dazu gehört die Aufteilung des Unternehmensnetzwerks in unterschiedliche Bereiche (Netzwerk-Segmentierung), das Aufsetzen von Systemen zur Erkennung von Angriffen (Intrusion-Detection-Systemen) und Beschränkungen der Netzwerkzugriffe über eine Firewall. Das Prinzip Zero-Trust wiederum verfolgt den granularen Ansatz, jeden einzelnen Datenfluss auf Vertrauenswürdigkeit zu überprüfen. Zero-Trust ist also ein rein datenzentrierter Sicherheitsansatz.

**Zwei-Faktor-Authentisierung:** Die Zwei-Faktor-Authentisierung (2FA), häufig auch Zwei-Faktor-Authentifizierung genannt, bezeichnet den Identitätsnachweis eines Nutzers mittels einer Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren). Typische Beispiele sind Bankkarte und PIN beim Geldautomaten, Fingerabdruck und Zugangscode in Gebäuden, oder Passphrase und Transaktionsnummer (TAN) beim Online-Banking. Die Zwei-Faktor-Authentisierung ist ein Spezialfall der Multi-Faktor-Authentisierung.



**Big Data:**

Splunk: [https://www.splunk.com/de\\_de](https://www.splunk.com/de_de)

Hadoop: <https://hadoop.apache.org/>

Hunk - Splunk Analytics für Hadoop:

[https://www.splunk.com/en\\_us/resources/videos/hunk-splunk-analytics-fur-hadoop.html](https://www.splunk.com/en_us/resources/videos/hunk-splunk-analytics-fur-hadoop.html)

**Blacklists**

Abuse (SSL-Blacklisten): <https://abuse.ch/>

Spamhaus: <https://www.spamhaus.org/drop/>

**Cisco Meraki-Netzwerk:**

<https://meraki.cisco.com/de-de/>

[https://www.cisco.com/c/de\\_de/solutions/meraki/index.htm](https://www.cisco.com/c/de_de/solutions/meraki/index.htm)

**Eigene IP-Adresse ermitteln:**

[myip.is](http://myip.is)

**Firewall:**

Palo Alto Networks: <https://www.paloaltonetworks.de/products>

pfSense: <https://www.pfsense.org/>

OPNsense: <https://opnsense.org/>

**GeoIP-Datenbanken**

Maxmind GeoLite2 Country:

<https://dev.maxmind.com/geoip/geolite2-free-geolocation-data?lang=en>

**GEO-Targeting:**

[www.netip.de](http://www.netip.de)

[www.hostip.info](http://www.hostip.info)

<https://ipleak.net/>

**Recovery:**

Recuva: <https://recuva.de.softonic.com/>

**Mesh-Network:**

<https://www.netzpiloten.de/mesh-netzwerk-geheimdienst-sicherheit-datenschutz/>

<https://guifi.net/>

**Suchmaschinen:**

StartPage (Niederlande): <https://www.startpage.com>

Qwant (Frankreich): [www.qwant.com](http://www.qwant.com), [www.qwant.fr](http://www.qwant.fr), [qwant.com](http://qwant.com)

Metager (Deutschland): <https://metager.de>

DuckDuckGo (USA): <https://duckduckgo.com>

Internet-Zeitmaschine: <https://web.archive.org>

**Security:**

HP Wolf Security: <https://www.hp.com/de-de/security/endpoint-security-solutions.html>

**Powershell:**

<https://it-learner.de/die-10-wichtigsten-powershell-cmdlets-fuer-einen-schnellen-einstieg-in-die-netzwerk-konfiguration-und-windows/>

**TLS/SSL-Online-Checker**

SSL Labs: <https://www.ssllabs.com/ssltest/>

SSL Checker: <https://www.thesslstore.com/ssltools/ssl-checker.php>

Geekflare: <https://gf.dev/tls-test>

Wormly: [https://www.wormly.com/test\\_ssl](https://www.wormly.com/test_ssl)

DigiCert: <https://www.digicert.com/help/>

**Verschlüsselung:**

VeraCrypt: <https://www.veracrypt.fr/code/VeraCrypt/>

### **Video**

Video-Download Youtube: <https://yt1s.io/de2>

### **VPN:**

NordVPN: <https://nordvpn.com/de/>

CyberGhost VPN: [https://www.cyberghostvpn.com/de\\_DE/](https://www.cyberghostvpn.com/de_DE/)

ProtonVPN: <https://protonvpn.com/de/>

Perfect-Privacy VPN: <https://www.perfect-privacy.com/de/>

Surfshark: <https://surfshark.com/de/>

ZorroVPN: <https://zorrovpn.com/>

PureVPN: <https://www.purevpn.com/de/>

### **Was übermittelt der Internet-Browser an Webseiten:**

Panopticklick: <https://panopticklick.eff.org/>

Amiunique: <https://amiunique.org/>

Cover Your Tracks: <https://coveryourtracks.eff.org>

**Der OPNsense-Praktiker: Enterprise-Firewalls mit Open-Source** von Markus Stubbig

# Index

## A

Active Directory ... 16-19, 42  
 Advanced Persistent Threat ... 107-108  
 Aktivierung und Registrierung von Windows  
 11 ... 52  
 Amiunique ... 64, 146  
 Angriffsvektor ... 6, 9, 16, 29  
 Anonym ... 2, 62, 64, 77  
 Application Layer Gateway ... 25, 35  
 APT Blocker ... 106-107  
 Assessment ... 27

## B

Baiting ... 102  
 Bcdedit ... 100  
 Best Practices ... 2-3  
 Big Data ... 82-84  
 BIOS ... 10, 48, 50-51, 87, 95-96, 98-99, 123  
 Bitcoin ... 22  
 Blackbox ... 6, 15  
 Bloodhound ... 16-18  
 Browser-Fingerprinting ... 64

## C

Canvas-Fingerprinting ... 64  
 CERT ... 6  
 cipher ... 112, 114  
 Cisco ... 32  
 Cloud ... 5, 9, 28, 32-33, 50, 53, 80, 83, 106-107  
 CMD mit Administrator-Rechten öffnen ... 55  
 Cookie ... 62-64  
 Cover Your Tracks ... 64

## D

Dashboard ... 19, 32-33, 39, 40-41, 82, 84  
 Dateiattribute ... 123  
 Datenschutz ... 30, 57-58, 66, 114  
 Demilitarized Zone ... 23, 26  
 Device-Fingerprinting ... 64  
 DiagTrack ... 56, 58-59  
 Disaster Recovery ... 4  
 Diskpart ... 88, 92, 97, 99  
 DMZ ... 23-26, 107  
 DoS ... 27  
 Drive-by-Download ... 101  
 Drucker ... 38, 61, 115

## E

EFI-Partition ... 87, 97, 99  
 Epinox ... 46  
 ERP ... 104  
 Evercookies ... 62  
 Exploit ... 10, 13, 20, 107  
 Exposed Host ... 26

## F

FAT32 ... 81, 87, 97, 99  
 Feedback ... 57-58  
 Filterung ... 35-36, 44  
 Fingerprinting ... 64  
 Firewall ... 6, 11, 14, 23-26, 28, 35-42, 46, 106, 110, 113  
 Firmware ... 32, 48, 50, 79, 87, 90, 99, 123  
 FreeBSD ... 39, 41

## G

Gartner ... 31  
 Gateway ... 24-25, 29, 35-36, 106-107, 115  
 GPExpert ... 13  
 GPT ... 87-88, 96-97, 99  
 Graybox ... 15  
 GUID ... 87-88, 100, 115

## H

Hardening ... 9, 11  
 HP Wolf Security ... 38

## I

IDS ... 28, 36  
 IoT, Internet of Things ... 103  
 IPS ... 28, 36  
 IPSec ... 11, 40, 42, 109-111  
 ISO 27001 ... 8  
 ITSec ... 5, 8

## K

Kaskade ... 72-76, 79, 107  
 Kick-off ... 15  
 KillSwitch ... 75  
 Kritische Infrastruktur, KRITIS ... 20

## L

LibreSSL ... 42  
 Lieferketten-Angriff ... 103-105  
 Lizenz ... 18, 32, 51-53, 83, 94, 107

## M

MBR ... 87-88, 96, 98-99  
 Media Creation Tool ... 94

# Index

Mesh Network ... 78-79  
 Multi-Hop ... 72-77  
 Multi Vendor Strategy ... 24  
 my.meraki.net .. 33

## N

Neo4j ... 17-18  
 Netsh ... 14, 110-113  
 Neurorouting ... 74  
 Notfall ... 7, 20  
 NTFS ... 61, 87, 123  
 Nulldatei ... 117-118

## O

Online-Tool ... 71  
 Open Source ... 5-6, 8, 17-18, 35, 39, 41-42, 79  
 OpenSSL ... 42  
 OpenWRT ... 79

## P

Packetfilter Firewall ... 35, 110  
 Panopticlick ... 64  
 Parted Magic ... 90-91  
 PATRIOT Act ... 32  
 Pentest ... 15-19, 77  
 Phishing ... 22, 66, 108  
 Pingcastle ... 16-18  
 Policy ... 13, 35, 37, 110-111  
 Portknocking ... 46  
 PowerShell ... 13-14, 17, 50, 54-55, 85, 88, 100, 112, 115-117, 120  
 Pretexting ... 102  
 Privacy Badger ... 64  
 Promiscuous ... 44

Protokollierung ... 10, 14, 43  
 Proxy ... 11, 26, 35, 42, 61, 64, 106  
 Purple Knight ... 18-19

## Q

Quid pro quo ... 102

## R

Ransomware ... 17, 21-22, 107  
 Recovery ... 4, 93, 97-100  
 Registry ... 13, 52, 55-57, 59, 61, 86  
 Rufus ... 96

## S

Screenshot ... 54  
 Security Appliance ... 33  
 Secure Erase ... 89-91  
 SIEM ... 28-31, 82  
 SMB1 deaktivieren ... 85  
 Sniffing ... 43-44  
 SOAR ... 28, 31  
 SOC ... 27-28  
 Social Engineering ... 16, 102  
 Sophos ... 22  
 Spear-Phishing ... 108  
 Specops Password Auditor ... 19  
 Spyware ... 45  
 SQL Injection ... 104  
 SSD ... 41, 80, 89, 90-92, 99  
 SSH ... 24, 46  
 SSL ... 42, 65-66, 71  
 Stateful Inspection Firewall ... 35, 37  
 Super-Cookies ... 62  
 Supply Chain Attack ... 103-105

## T

Tailgating ... 102  
 Tastatur-Kurzbefehle ... 54  
 Telemetrie ... 45, 49, 56-60  
 Telnet ... 24  
 TLS ... 42, 65-71  
 TPM, Trusted Platform Module ... 47-48, 50, 55, 92, 96  
 TrueCrypt ... 80-81

## U

UAC ... 11, 13  
 UEFI ... 48, 50, 87, 96-99, 123  
 UUID ... 88, 115

## V

VeraCrypt ... 80-81  
 Verschlüsselung ... 5, 22, 37, 46-48, 65-68, 70-71, 80-81, 92, 109  
 VPN ... 40-42, 62, 72-77, 106, 114

## W

Watering Hole Angriff ... 101-102  
 Whitebox ... 15  
 Windows Defender Application Guard ... 13  
 Windows Defender Exploit Guard ... 13  
 Windows Device Guard ... 13  
 WinToUSB ... 95

## X

XSS ... 126

## Z

Zertifikat ... 7, 32, 47, 55, 65-67, 70-71, 109