

Analytik für IT-Systembetreuer	04	Hinweise zu Lexware	66
Netzwerkschema Raum 3.12	05	Programm: testdisk	67 - 70
CMD-Befehle für die Erstellung eines Netzwerkschemas	06	Netzwerkkabel: Anschlussbelegung	71
Informationen über den Rechner	07	Netzwerk-Verbindungen	72
Tastatur-Kurzbefehle (W10)	08	Verbinder für Lichtwellenleiter (LWL)	73 - 79
Nützliche CMD-Befehle	09 - 10	Anonymität im Netz	80
Nützliche CMD- oder Powershell-Befehle	11 - 14	USB-Steckverbinder	81
Windows 10 – Dienste	15 - 16	Video- und Geräteverbinder	82
Windows Management Instrumentation ... – WMIC	17 - 20	SATA-Kabel	83
Administrieren mit WMI	21	Geräteanschlüsse	84
Elementare IT-Sicherheitsregeln	22	Montage (Assemblierung) eines Rechners	85 - 86
Sicherheit im Internet	23	mSATA-Adapter	87
Zwei-Faktor-Authentisierung	24	USB-Stick Rubber Ducky	88
Bedrohungspotentiale	25 - 26	IT-Systembetreuer: Werkzeuge	89
DDoS	27 - 29	Netzwerk-Stecksysteme der Kategorie 7	90 - 91
Aufgaben- und Schichtenmodell von Betriebssysteme	30 - 37	Generalisieren einer Windows-Installation mit Sysprep	92 - 94
OSI-Modell	38	Windows 10: Installations-Stick erstellen	95
Unterschied: Router Accesspoint	39 - 40	Hinweise zum Rechneraustausch	96
Datenschutz und Probleme unter Windows 10	41 - 47	GigaBit-Netz und VDSL-Vectoring	97
Datenschutzbeauftragter	48	5 einfache Regeln für Ethernet in der Gebäudetechnik	98 - 101
Wann dürfen Daten erhoben verarbeitet und genutzt werden? ..	49	RAID-Grundlagen	102 - 108
Mein digitales Ich	50 - 51	Memtest86	109 - 111
Ist die Kontrolle der Daten noch möglich?	52	BIOS-Update (flashen)	112 - 115
Identitätsdiebstahl	53	Netzwerkkabel – Schirmungskonzepte	116
Big-Data: Profiling und Marketing	54	BIOS-Zugang	117
Big Data: Was erzählt der Internet-Browser?	55	BIOS-Pieptöne	118 - 119
Big Data: Was ist Tracking?	56	Administrator-Passwort vergessen	120 - 122
Privatsphäre-Einstellungen unter Windows 10 härten	57 - 60	Protokollierung von USB-Geräten auf Windows-Systeme ..	123 - 124
Windows 10 Client einer Domäne hinzufügen	61	ReFS versus NTFS: Unterschiede und Leistungsvergleiche	125
Windows 10 – Bluetooth	62	Backup und Datensicherheit	126 - 127
Windows 10 – Systemwiederherstellung, Recovery	63	Storage – NAS, SAN, vSAN und Co.	128 - 132
Windows 10 – Einrichtung eines Exchange-Kontos in Outlook ..	64	Backupsoftware – VEEAM	133 - 135
Remote-Administrierung	65	Software: mention v.2018 Warenwirtschaft	136

PRTG: Ungewöhnliche Zugriffsmuster entlarven	137 - 139
Snort: Intrusion Detection System (IDS)	140 - 145
Micos: Software für soziale Einrichtungen	146
VDI: Virtual Desktop Infrastruktur	147
Projekt FIDO2 – Authentifizierungslösung	148 - 152
MySQL	153
SQL - SAP Datenbanken	154
Erweiterte Excel-Hinweise	155
Windows – Antwortdatei	156
Hinweise: spezielle Google-Suche	157
Internet-Browser (about-Befehle)	158 - 159
Hinweise für die Fehlerbeseitigung	160 - 175
Malware, Angriffe und Infektoren	176 - 180
Schutzsoftware: FireEye und DLP	181
BitLocker	182
Windows 10 reparieren	183 - 186
Hinweise und Ankündigungen für Windows 10	187
Mobilfunk-Standard 5G	188 - 190
Tipps	191
Internet-Links	192 - 193
Literatur-Tipps	194
Index	195 - 196

Analytik für IT-Systembetreuer

Analytisches Denken ist die Fähigkeit, Probleme zu erkennen, in ihre Einzelteile zu zerlegen, um eigenständige Lösungen zu entwickeln.

Für die alltägliche Arbeit als IT-Systembetreuer:

- ❖ Betreuung und Überwachung der gesamten IT-Infrastruktur
- ❖ Behebung unterschiedlicher Hardware- und Softwareprobleme
- ❖ Beseitigung von allgemeinen Störungen und Fehlern
- ❖ kurze Unterweisungen und Weiterbildungen der Computer-Benutzer am Arbeitsplatz

IT-Systembetreuer müssen eine gute Auffassungsgabe, ein fundiertes IT-Verständnis, strukturiertes und konzeptionelles Denken, ein ausgeprägtes analytisches Denken und kommunikative Fähigkeiten haben.

Ausschlussverfahren:

Bei der Suche nach Fehlern in IT-Netzwerken treten viele unerwartete Probleme auf. Zur Analyse benötigt der Troubleshooter ein umfangreiches Wissen über das IT-Netzwerk, Anwendungen und die genutzten Protokolle.

Eine Fehleranalyse beruht in der Praxis häufig auf dem Ausschlussverfahren. Es werden die möglichen Fehlerursachen so lange untersucht, bis zum Schluss nur noch der eigentliche Fehler übrig bleibt. Ist die Fehlerursache erst einmal gefunden, dann ist die Lösung des Problems meist trivial.

Vor Beginn der Problemanalyse müssen möglichst viele Informationen über das eigentliche Problem gesammelt werden.

Näherungsverfahren:

Beim Näherungsverfahren nähert man sich Schritt für Schritt der Lösung.

Funktions- und Aufbauprinzipien:

Für die Behebung von Fehlern in Netzwerken, Netzwerkgeräten, Steckkarten, Hauptspeicher, Speichergeräte und Rechnern ist das Wissen über die prinzipielle Funktionsweise und des grundsätzlichen Aufbaues erforderlich.

Prinzip-Darstellungen in Form von Grafiken erleichtern das Verständnis für Gesamtzusammenhänge für alle Beteiligten.

Konzeptionelles Denken:

Konzeptionelle Kompetenz ist die Fähigkeit, Probleme und Chancen im Zusammenhang zu erkennen.

Konzeptionelle Fähigkeiten:

- ❖ Aus einem umfassenden Blickwinkel und einer Vielzahl von Einzelaspekten Themen strukturieren,
- ❖ Vernetzungen zwischen Teilaspekten in gedanklich selbst entwickelten groben Strukturmuster integrieren und in Zusammenhängen denken, ohne sich in Teilaspekte zu verlieren,
- ❖ Dinge bis zum Ende denken,
- ❖ aus vorhandenen Erkenntnissen einen gedanklichen Plan zu deren Realisierung skizzieren.

Flussanalytik, Informationsflüsse, Bandbreite, Datenströme:

Informationsflüsse lassen sich über den Datendurchsatz messen. Der Informationsfluss sollte nicht größer sein als die durch die Bandbreite gegebene maximale Datenmenge. Informationsflüsse haben häufig mehrere Stationen. Zirkuläre Flüsse sind auch möglich.

Netzwerkschema Raum 3.12

Das Netzwerkschema enthält die schematische Darstellung der Rechner, Drucker, Router, Switches und anderer wesentlicher Geräte.

Neben dem Rechnernamen, IP-Adresse und wesentlicher Hardware-Daten können noch zusätzlich spezifische Software-Pakete im Netzwerkschema eingetragen werden.

Bei Reparaturen oder wesentlichen Änderungen, können die Änderungen - mit Datum - handschriftlich im Netzwerkschema eingetragen werden.

Hinweis: Ein Netzwerkschema umfasst in der Regel ein gesamtes Bürogebäude, Firmengebäude oder eine Organisation.

05



PC: PC-301325-5
Arbeitsgruppe: 9721-9647-MA
IP-Nr.: 192.168.20.205
MAC Wireless: 00-AD-24-xx-xx-xx
RAM- 8 Gbyte
UEFI-BIOS: [Del] oder [F2]



PC: PC-301325-7
Arbeitsgruppe: 9721-9647-MA
IP-Nr.: 192.168.20.183
MAC Wireless: 00-AD-24-xx-xx-xx
RAM- 8 Gbyte
UEFI-BIOS: [Del] oder [F2]



WLAN-Drucker: Brother DCP-L8410CDW
Arbeitsgruppe:
IP-Nr.: 192.168.20.198
MAC-Adresse Ethernet:
MAC-Adresse Wireless:



PC: PC-301325-10
Arbeitsgruppe: 9721-9647-MA
IP-Nr.: 192.168.20.178
MAC Wireless: 00-AD-xx-xx-xx
RAM- 8 Gbyte
UEFI-BIOS: [Del] oder [F2]



PC: PC-301325-11
Arbeitsgruppe: 9721-9647-MA
IP-Nr.: 192.168.20.83
MAC Wireless: 00-AD-24-44-0E-F4
RAM- 8 Gbyte
UEFI-BIOS: [Del] oder [F2]



PC: PC-301325-12
Arbeitsgruppe: 9721-9647-MA
IP-Nr.: 192.168.20.190
MAC Wireless: 00-AD-24-xx-xx-xx
RAM- 8 Gbyte
UEFI-BIOS: [Del] oder [F2]



Raum:
3.11



LANCOM-Router 1631E
IP-Nr.: 192.168.1.1
Name: IB_Gateway.intern
IP-Bereich: 87.170.131-142.10-230



WLAN-Router: IB-AP2
LANCOM LN-630acn dual
Wireless
IP-Nr.: 192.168.20.1
DNS-Name: intern
Name: IB-AP2.intern
2 Bänder – 2,4 und 5 GHz, max.
250 Mbit/s, bis zu 256 Clients
SSID: 2OGAP2



ipconfig

Ermittlung der eigenen IP-Adresse, Subnet-Adresse und die IP-Adresse des Standardgateways.

ipconfig /all

Ermittelt zusätzlich die MAC-Adressen der Netzwerkkarten (Ethernet, WLAN) und Hostname.

`ipconfig /all > %homepath%\INFO-ipconfig.txt`

Cmd-Ausgabe in eine Textdatei umleiten.

getmac

Ermittelt die MAC-Adressen des lokalen Rechners.

route print

Ermittelt die MAC-Adressen, die Gateway-Adressen und die eigene IP-Adresse.

nslookup

Ermittelt die IP-Adresse des Standardservers (Gateway) und dessen internen Namen.

net view

Ermittelt die Rechnernamen im lokalen Netzwerk \ Arbeitsgruppe.

net user

Ermittelt die Benutzer auf dem lokalen Rechner.

net share

Ermittelt die Freigaben auf dem lokalen Rechner.

pathping <IP-Adresse>

Ermitteln der Antwortstatistik im Netzwerk und den dem Netzwerk bekannten Rechnernamen, Servernamen.

whoami /all

Ermittelt den Rechnernamen und Benutzernamen des lokalen Rechners.

ver

Zeigt die interne Windowsversion an.

winver

Zeigt die offizielle Windowsversion an.

nbtstat -a <IP-Adresse>

Ermittelt die NetBIOS-Namen.

hostname

Ermittelt den Computernamen des aktuellen Rechners.

Benutzer administrator aktivieren und ein neues Passwort zuweisen

`net user administrator /active:yes`

`net user administrator [passwort]`

Administrator-Zugang ohne Passwort

`net user administrator ""`

Der Administrator kann auch über die Computerverwaltung ([W] + [X]) aktiviert werden. Die Aktivierung über die Kommandozeile (CMD, Powershell) sollte auf jeden Fall bevorzugt werden.

siehe auch: Windows Management Instrumentation Command-line
– WMIC 4/4

Hardware:

[W] + [R] -> control -> Gerätemanager

[W] + [X] -> Gerätemanager

Info zum Netzwerk: Gerätemanager -> Netzwerkadapter ->

Eigenschaften (rechte Maustaste) -> Tab: Ereignisse ->

Informationen -> Treibername

Netzwerkeinstellungen: [W] + [I] -> Netzwerk und Internet -> Status ->

Verbindungseigenschaften ändern, Verfügbare Netzwerke anzeigen, Netzwerkeigenschaften anzeigen,

Verfügbare Netzwerke anzeigen, Hardwareeigenschaften, bekannte Netzwerke verwalten, Adapteroptionen ändern, ...

Netzwerkeinstellungen: [W] + [I] -> Netzwerk und Internet -> WLAN -> [...]

Netzwerkeinstellungen: [W] + [I] -> Netzwerk und Internet -> Ethernet -> [...]

[W] + [I] -> System -> Info

[W] + [I] -> System, Geräte, Netzwerk und Internet

[W] + [R] -> powershell oder powershell.exe -> systeminfo

[W] + [R] -> cmd oder powershell -> ping <IP-Adresse oder Rechnername>

Hinweis: Der ping-Befehl arbeitet unter dem Kommandozeileninterpreter cmd zuverlässiger.

[W] + [R] -> Eingabe: taskmgr ... Taskmanager öffnen

[W] + [R] -> Eingabe: taskmgr -> Tab: Dienste -> Kontextmenü eines Dienstes öffnen -> Dienste öffnen ... öffnet die Dienstverwaltung

[W] + [R] -> cmd -> tasklist ... aktuelle Prozessliste

[W] + [X] -> Computerverwaltung

[W] + [R] -> services.msc -> öffnet die Dienstverwaltung

Hardware-Info:

Mit dem Tool »Hwinfo32« bekommt man umfangreiche Informationen über die Hardware eines Rechners. Das Tool findet man manchmal auf Zeitschriften-DVD's.

[Strg] + [C] kopieren
[Strg] + [V] einfügen
[Strg] + [X] ausschneiden
[Strg] + [A] alles markieren
[Strg] + [Z] Letzte Aktion rückgängig machen.
[Strg] + [Y] Letzte Aktion nochmals anwenden.
[Strg] + [P] Drucken-Dialog für das aktuelle Dokument aufrufen.
[Strg] + [W] + [C] ... Monitor-Farbumschaltung – Schwarzweiß <-> Farbe
[Esc] ... aktuellen Vorgang abbrechen

[W] + [R] ... Ausführen von Befehlen (cmd, regedit, calc, mspaint)
[W] + [R] -> powershell oder powershell.exe
[W] + [R] -> cmd
[W] + [R] -> Eingabe: **ms-settings:** ... Windows-Einstellungen
[W] + [R] -> Eingabe: **gpedit.msc** ... Editor - Gruppenrichtlinie öffnen.
[W] + [R] -> Eingabe: taskmgr ... Taskmanager öffnen
[W] + [R] -> cmd -> [Strg] + [Shift] + [ENTER] ... CMD mit Administrator-Rechten öffnen

[W] + [X] ... Expert-Modus (Menü)
[W] + [I] ... Windows-Einstellungen
[W] + [PAUSE] ... Windows Systemsteuerung aufrufen -> auf Link »Startseite der Systemsteuerung« klicken; Aktivierung von Windows; Produkt-ID → Produkt-Key ändern
[W] + [A] ... öffnet das Infocenter; Zugriff auf Einstellungen, Hardware, Tablet, Bluetooth, Flugzeugmodus, ...
[W] + [E] ... Explorer (Dateimanager) aufrufen.
[W] + [D] ... Geöffnete Programme minimieren. Mit [W] + [D] Programme wieder maximieren.
[W] + [Strg] + [D] ... virtuellen Desktop neu erstellen
[W] + [TAB] ... virtuelle Desktops verwalten; Geöffnete Programme übersichtlich auf dem Bildschirm anordnen. Mit [W] + [TAB] die ursprüngliche Bildschirmansicht wiederherstellen.
[W] + [Strg] + [->] oder [->] ... virtuellen Desktop wechseln

[W] + [Strg] + [F4] ... aktuellen virtuellen Desktop schließen
[W] + [P] ... Öffnet die Optionen für einen zweiten Bildschirm.
[W] + [M] ... Geöffnete Programme minimieren. Mit [Shift] + [W] + [M] geöffnete Programme wieder maximieren.
[W] + [L] ... Bildschirm sperren.
[W] + [+] bzw. [W] + [-] ... Bildschirm vergrößern (Lupe) bzw. verkleinern. Mit [W] + [ESC] die ursprüngliche Bildschirmgröße wiederherstellen.
[W] + [Strg] + [F] ... in einem Netzwerk nach PCs suchen (ActiveDirectory).
[Strg] + [Alt] + [Entf] ... Taskmanager aufrufen, Passwörter ändern, etc.
[Alt] + [F4] Aktuelles Fenster schließen. **Hinweis:** Sind auf dem Desktop keine Programme geöffnet, so erscheint ein Windows-Fenster mit den Optionen: Herunterfahren, Neustart, Abmeldung, ...
[Strg] + [S] ... Aktuelles Dokument speichern.

[pause] ... Boot-Bildschirm anhalten (z.B. Hinweis für den BIOS-Zugang lesen); weiter mit beliebiger Taste

[Strg] + [+] ... Internetbrowser, Webseite stufenweise vergrößern
[Strg] + [-] ... Internetbrowser, Webseite stufenweise verkleinern
[Strg] + [0] ... Internetbrowser, Webseite in Originalgröße anzeigen
[Strg] + [T] ... Internetbrowser, neuer Tab
[F10] ... Firefox: Menü einblenden/ausblenden
[F11] ... Programme: Fensteranzeige/Vollbild-Anzeige
[F12] ... Firefox und Edge (Windows-Browser): Anzeige des Seitenquelltextes, Expert-Modus; **Hinweis:** die Webseiten-Anzeige wird von Edge eigenständig geändert (Menü, Größe der Bilder, ...)

[DRUCK] ... Bildschirm-Schnappschuss in die Zwischenablage kopieren.
[Alt] + [DRUCK] ... Schnappschuss des aktuellen Fensters in die Zwischenablage kopieren.
[W] + [Shift] + [S] ... Frei wählbarer Bildschirm-Schnappschuss in die Zwischenablage kopieren. **Hinweis:** Nach dem Kopieren des Schnappschusses in die Zwischenablage, kann das Bild in MSPAINT eingefügt werden.

tasklist

Ermittelt die aktuelle Prozessliste (**siehe auch:** tasklist /?).

taskkill /PID <Prozessid>

Bricht einen laufenden Prozess oder eine Anwendung ab oder beendet sie (**siehe auch:** tasklist /?).

assoc

Zeigt Dateierweiterungszuordnungen (more, seitenweise Anzeige) an bzw. ändert sie.

assoc.mp3

Zeigt an mit welchem Programm MP3-Dateien geöffnet werden.

mmc

Windowsmanagementkonsole.

driverquery

Zeigt den aktuellen Gerätetreiberstatus und die Eigenschaften an.

echo

Zeigt Meldungen an bzw. schaltet die Befehlsanzeige ein oder aus.

echo %NUMBER_OF_PROCESSORS%

Anzahl der Cores (Prozessorkerne) in der CPU

echo %COMPUTERNAME%

Der vergebene Name des Rechners.

echo %DATE%

das aktuelle Datum

echo %TIME%

die aktuelle Uhrzeit

echo %RANDOM%

Eine Zufallszahl zwischen 0 und 32767

echo %PROCESSOR_ARCHITECTURE%

Prozessorarchitektur anzeigen.

exit

Beendet die CMD, schließt das CMD-Fenster

tree

Zeigt die Ordnerstruktur eines Laufwerks oder Pfads grafisch an.

calc

Öffnet den Windows Taschenrechner.

osk

Öffnet die Windows Bildschirmtastatur.

control

Öffnet die Systemsteuerung.

control netconnections

Öffnet die Übersicht aller Netzwerkverbindungen.

notepad

Öffnet den Windows-Editor.

mspaint

Öffnet Windows Paint.

snippingtool

Tool um Screenshots zu erstellen.

explorer

Öffnet den Windows Explorer (Dateiverwaltung).

charmap

Öffnet die Zeichentabelle von Windows.

msinfo32

Zeigt alle Systeminformationen an.

systeminfo

Zeigt Systeminformationen an.

compmgmt.msc

Öffnet die Computerverwaltung.

eventvwr

Öffnet die Ereignisanzeige.

taskmgr

Öffnet den Taskmanager.

services.msc

Öffnet die Dienstverwaltung.

sndvol

Öffnet den Windows-Laustärkemixer.

cd

Wechselt das Verzeichnis, den Ordner. **cd ..** wechselt in das höhere Verzeichnis

displayswitch

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

regedit

Öffnet den Registrierungs-Editor.

regedit /m

Öffnet einen zweiten Registrierungs-Editor, obwohl bereits einer geöffnet ist.

convert

Tool zum umwandeln des Dateisystem auf einem USB-Stick; FAT32 in NTFS; Speicherung von Dateien größer 4GB (z.B. **convert H: /FS:NTFS**)

powercfg

Mit dem Befehl - **powercfg -energy -output C:\Users\Ihr Benutzernamen\Desktop\energie.html** - erstellen Sie einen Bericht über die Energieeffizienz Ihres Computers (Infos zu Energieeinstellungen und Prozesse).

hdwwiz

Startet einen Installations-Assistenten für angeschlossene Geräte, falls diese einmal nicht erkannt worden sind.

timedate.cpl

Zeigt das Einstellungsfenster für Datum und Uhrzeit an.

taskschd.msc

Öffnet den Aufgabenplaner von Windows.

cleanmgr

Öffnet die Datenträgerbereinigung.

cleanmgr /verylowdisk

Öffnet die Datenträgerbereinigung und entfernt automatisch Mülldaten.

SystemPropertiesPerformance

Öffnet die Leistungsoptionen.

resmon

Öffnet den Ressourcenmonitor (Administrator-Rechte erforderlich).

perfmon

Öffnet die Leistungsüberwachung (Administrator-Rechte erforderlich).

perfmon /rel

Öffnet den Zuverlässigkeitsverlauf (Administrator-Rechte erforderlich).

driverquery

Zeigt eine Liste der installierten Treiber.

nslookup dresden.de

Zeigt die IP-Adresse einer Webseite an.

mdsched

Prüft Ihr System auf Speicherprobleme (Administrator-Rechte erforderlich).

msconfig

Öffnet die Systemkonfiguration (Administrator-Rechte erforderlich).

appwiz.cpl

Öffnet die Software-Verwaltung

del

Löscht Dateien.

chkdsk /f /r /x

Öffnet die Datenträger-Überprüfung.

chknfts

Überprüft Partitionen auf Fehler.

inetcpl.cpl

Öffnet die Internetoptionen.

rstrui

Öffnet die Systemwiederherstellung.

recdisc

Erstellt eine Rettungs-CD für Windows (Administrator-Rechte erforderlich).

diskmgmt.msc

Öffnet die Datenträgerverwaltung (Administrator-Rechte erforderlich).

devmgmt.msc

Öffnet den Geräte-Manager (Administrator-Rechte erforderlich).

dir -r | select string "SUCHWORT"

Rekursive Suche nach einem Textfragment

wmic qfe

Zeigt alle bereits installierten größeren Windows Updates an (siehe auch: Windows 10 Einstellungen [W] + [I]).

firewall.cpl ... öffnet die Firewall-Einstellungen

wf ... Öffnet die erweiterten Firewall-Einstellungen (Administrator-Rechte erforderlich).

useraccountcontrolsettings

Öffnet die Einstellungen für die Benutzerkontensteuerung (Administrator-Rechte erforderlich).

wscui.cpl

Öffnet das Wartungcenter.

mrt

Öffnet das Windows Tool zum Entfernen bösartiger Software (Administrator-Rechte erforderlich).

sc query windefend

Anfrage: Läuft der Dienst WinDefend. WinDefend wird für den Schutz gegen Spyware benötigt.

sc qc windefend

Ausgabe der Modulversion.

msinfo32.exe

Mit dem grafischen Tool msinfo32.exe kann man die Konfiguration des lokalen Rechners erkunden.

mstsc.exe

Mit dem grafischen Tool mstsc.exe ([W] + [R] -> CMD) eine Remote-Verbindung (RDP-Verbindung mittels des **Remote Desktop Protocol**) zu einem anderen Rechner aufbauen. Um RDP Verbindungen zuzulassen bzw. zu aktivieren muss man mit folgendem Befehl die Windows »**Systemeigenschaften**« ([W] + [R] -> **sysdm.cpl**) aufrufen. Die Remote-Verbindung kann über lokale Gruppenrichtlinien unterbunden werden.

net user "Benutzername"

net user "Support"

Zeigt neben dem letzten Login (Anmeldung), auch eine Reihe von weiteren Informationen über einen Benutzer an.

Shutdown und abgesicherter Systemstart des Rechners

Für den Shutdown des Rechners nach der eingestellten Zeit (hier: 6 Sekunden) gibt man beispielsweise **shutdown.exe /s /t 6** ein. Will man sich nur abmelden, lautet der Befehl **shutdown.exe /l**. Für einen Neustart sorgt **shutdown.exe /r /t 6**.

Mit der Eingabe von **shutdown /a** wird der Rechner sofort heruntergefahren.

Mit **shutdown.exe /r /o /f /t 00** gelangt man in das Menü für den »Abgesicherten Systemstart«. Anschließend klickt man auf »Problembehandlung« und dann »Erweiterte Optionen«. Mit der Auswahl »Starteinstellungen« startet man den Rechner neu und wählt anschließend »Abgesicherter Modus aktivieren« aus. Nun startet Windows in dieser Betriebsart.

Windows-Dienste starten oder beenden

net start ... NET START listet aktive Dienste auf.

net start <Servicename, Task, Dienst> ... startet einen Dienst

net stop <Servicename, Task, Dienst> ... beendet einen Dienst

NET HELP <Befehl> | MORE ... zeigt die Hilfe seitenweise an

Hinweis: Dienstnamen, Servicennamen, die aus zwei oder mehr Zeichengruppen bestehen, sind in Anführungszeichen einzuschließen

Benutzerverwaltung:

net user [Benutzername] {Kennwort | *} /ADD [Optionen] [/DOMAIN]

net user [Benutzername] [/DELETE] [/DOMAIN]

net user [Benutzername] [/TIMES:{Zeiten | ALL}]

net user [Benutzername] [/ACTIVE:{YES | NO}]

net user ... alle lokalen Benutzer anzeigen

net user [Benutzername] "" ... Zugang ohne Passwort

net user [Benutzername] /delete ... Benutzer löschen

net user [Benutzername] /passwordchg:no ... Benutzer kann das Passwort nicht ändern (yes – Vorgabe)

siehe auch: Windows Management Instrumentation Command-line – WMIC 4/4

Datenträgerverwaltung:

diskpart ... Ohne Parameter, wird der Diskpart-Prompt angezeigt.

help ... Am Diskpart-Prompt eingegeben, wird die Diskpart-Hilfe aufgerufen.

list volume ... Am Diskpart-Prompt eingegeben, wird eine Liste mit den angeschlossenen Geräten und Partitionen angezeigt.

list disk ... alle aktuell verfügbaren Laufwerke anzeigen

select disk 0 ... erste Festplatte auswählen

list partition ... Partitionen der ausgewählten Festplatte anzeigen

assign ... dem Gerät, Partition einen Laufwerksbuchstaben zuordnen

exit ... Diskpart wird beendet.

Beispiel: Formatierung eines bootfähigen USB-Stick mit FAT32 (Administratorrechte erforderlich, alle Daten auf dem USB-Stick werden durch **clean** gelöscht)

diskpart

list disk

select disk <Nummer des USB-Sticks aus list disk>

clean

create partition primary

active

format fs=fat32 quick oder format fs=ntfs quick (quick kann auch entfallen)

assign

exit

siehe auch: diskpart help, help <Befehl>, Windows 10: Installations-Stick erstellen

Set-Date -date "02.04.2019 18:00"

Datum und Uhrzeit setzen (Administratorrechte erforderlich).

Set-Date (Get-Date).AddDays(-7)

Datum des Betriebssystems sieben Tage in die Vergangenheit versetzen.

Set-Date -adjust -1:30:0

Die aktuelle Uhrzeit des Betriebssystems um 1,5 Stunden zurücksetzen.

optionalfeatures

Öffnet die Verwaltung für Windows-Feature (z.B. die Sandbox).

Die **Windows Sandbox** (Sandbox-Aktivierung – Administrator-Rechte erforderlich) ist ein isolierter Bereich, in dem man Programme geschützt ausprobieren kann. Die neue Funktion ist ab Build 18305 integriert.

Die Windows Sandbox wird ganz einfach über das Startmenü gestartet und Exe-Dateien können per Drag-and-Drop im abgeschotteten Desktop ausgeführt werden.

help chkdsk oder **chkdsk /?** ... Hilfe für CHKDISK aufrufen.

chkdsk /f ... Korrigiert Fehler am logischen Dateisystem (logical file system) auf der Festplatte.

chkdsk /r ... Erkennung und Wiederherstellung von lesbaren Informationen beschädigter Sektoren auf der Festplatte. Nach einem Rechner-Neustart startet chkdsk die Überprüfungsroutine.

Formatierung von Datenspeichern:

format k: ... Formatiert das Gerät mit dem Laufwerksbuchstaben k, mit dem Dateisystem FAT32.

Kopieren von einzelnen Dateien:

copy /v filename.txt e: ... Kopiert eine Datei auf das Laufwerk e: mit Abfrage, ob eine gleichnamige Datei überschrieben (Yes/No/All) werden soll. Die Option /v überprüft, ob der Kopiervorgang korrekt ausgeführt wurde.

copy /v /y filename.txt e: ... Kopiert eine Datei auf das Laufwerk e: ohne Abfrage (Abfrage wird unterdrückt), d.h. eine existierende, gleichnamige Datei wird ohne Nachfrage überschrieben.

Kopieren von mehreren Dateien und Verzeichnissen:

xcopy /s Documents e:\backups ... Kopiert das Verzeichnis Documents mit allen Unterverzeichnissen (/s) und Dateien auf das Laufwerk e: ins Verzeichnis backups.

Kopieren mit dem Programm robocopy:

Ohne Parameter, wird eine Kurzhilfe aufgerufen für robocopy. Robocopy (Robust Copy) ist ein verbessertes xcopy, das auch Dateien löschen kann (Option /mir).

robocopy /s Documents e:\backups ... Kopiert das Verzeichnis Documents mit allen Unterverzeichnissen (/s) und Dateien auf das Laufwerk e: ins Verzeichnis backups.

Prozesse anzeigen und beenden:

tasklist ... Zeigt alle aktuell laufenden Prozesse an.

taskkill ... Beendet den Prozess oder Programm mit der angegebenen Prozess-Nummer oder Programmnamen.

Beispiel:

taskkill /im notepad.exe

taskkill /pid 1234 /t

PS | sort -P ws | select -last 5 ... die 5 speicherhungrigsten Prozesse ermitteln

Gruppenrichtlinie (Group Policy):

gpupdate ... Update der Gruppenrichtlinie (Group Policy).

gpupdate /target:{computer | user} /force

Beispiel:

gpupdate /target:pc012 /force

gpresult ... Überprüft die Einstellungen der Gruppenrichtlinie für einen Computer oder Benutzer.

gpresult /r ... Überprüfung der Gruppenrichtlinie des aktuellen Computers.

gpresult /user sgc/user01 /v ... Überprüfung der Gruppenrichtlinie des Benutzers user01.

Dienste neu starten

Restart-Service "SERVICENAME"

Restart-Service DHCP

Version, Release-ID

reg.exe query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion" /v ReleaseID

Reg Query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion" /v ReleaseId

nur Powershell

(Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\" -Name ReleaseID).ReleaseId

Get-ComputerInfo -Property Windows*

Get-ComputerInfo | select WindowsProductName, WindowsVersion, OsHardwareAbstractionLayer

Festplatten, Partitionen

reagentc /info ... Status der Windows-Recovery-Partition anzeigen (Administratorrechte erforderlich)

Zeitzone

tzutil /l | more ... alle unterstützten Zeitzonen seitenweise auflisten

tzutil /g ... aktuelle Zeitzone anzeigen

tzutil /? ... Hilfe anzeigen

Batch-Datei

start cmd /K ping -t 8.8.8.8 ... endlos Ping in einer durch die Batch-Datei geöffneten Konsole, Terminal ausführen

start cmd /C ping 8.8.8.8 ... 4-facher Ping ausführen, Konsole wird im Hintergrund kurzzeitig geöffnet

Folgende Befehle - nur für Powershell:

Get-PSDrive ... Informationen zu allen vorhandenen Laufwerken

Get-PSDrive | Where {\$_.Free} ... freien Speicherplatz mit der PowerShell abfragen

Netzwerkconfiguration auslesen:

Get-Wmiobject Win32_NetworkAdapterConfiguration -Filter "IPEnabled=true" | select Description,IPAddress

for /l %i in (1,1,255) DO @ping 192.168.0.%i -n 1 | find "Bytes=" ... ein komplettes Netz in einer Zeile anpingen

- **for /l %i in (1,1,255)** bedeutet: beginnend von 1 in 1er Schritte bis 255
- **@ping 192.168.0.%i -n 1** .. ist der eigentliche ping-Befehl
- das **@** unterdrückt die Ausgabe des Befehls
- mit **| find "Bytes="** werden nur Zeilen die "Bytes=" enthalten ausgegeben (also nur IP-Adressen von Rechner die auf den Ping antworten)

Folgende Befehlszeile listet auch Rechner des lokalen Netzwerkes auf, bei denen die Firewall eingeschaltet ist:

(for /l %i in (1,1,255) DO start /min ping 192.168.0.%i -n 1) && timeout 10 && arp -a

- Wenn sich der Rechner in einem anderen Subnet befindet, kann die Befehlszeile entsprechend angepasst werden: ... **in (1,1,255) ... ping 192.168.0.%i** ...
- Start- und Endwert **for /l %i in (1,1,255)** bedeutet: beginnend von 1 in 1er Schritte bis 255
- Etwas Vorsicht ist dabei geboten, da **start /min** alle 255 Ping's gleichzeitig startet. Um das Netzwerk nicht zu überlasten, sollte der Start- und Endwert nicht all zu groß gewählt werden.

10 Ping's in einer Sekunden absenden:

```
1..10 | % {  
    test-connection www.TESTDOMAIN.de -count 1  
    start-sleep -milliseconds 100  
}
```

Intelligenter Hintergrundübertragungsdienst deaktivieren:

[W] + [R] -> Eingabe: taskmgr -> Tab: Dienste -> Beschreibung:
Intelligenter Hintergrundübertragungsdienst -> Kontextmenü: Anhalten
Ziel: Internetverbindungen beschleunigen (nur bei Notwendigkeit
abschalten)

Diensthost: Übermittlungsoptimierung optimieren

Info: Windows 10 führt im Hintergrund den Prozess »Diensthost:
Übermittlungsoptimierung« aus, wenn Updates herunter- oder
hochgeladen werden. Dadurch wird die verfügbare Internetbandbreite
der Benutzer stark reduziert.

[W] + [I] -> Update und Sicherheit -> Übermittlungsoptimierung ->
Erweiterte Optionen -> Download- und Upload-Einstellungen
entsprechend ändern

Quelle: <https://www.giga.de/downloads/windows-10/tipps/diensthost-uebermittlungsoptimierung-deaktivieren/>

Hinweis: Mit den Gruppenrichtlinien (GPO, Editor: gpedit.msc) kann
man dieses Problem ebenfalls beheben.

Quelle: <https://www.borncity.com/blog/2016/11/22/windows-10-updates-fressen-netzwerkbandbreite/>

Ursache für langsames Internet - Windows 10

Windows 10 nutzt zwei Dienste, um Updates einzuspielen:

1. Windows Update Delivery Optimization (WUDO). Es wird im Deutschen auch **Übermittlungsoptimierung** (DoSvc) genannt.
2. Background Intelligent Transfer Service (BITS oder Intelligenter Hintergrundübertragungsdienst).

WUDO ist dabei das Programm, das die gesamte Internet-Bandbreite belegen kann.

WUDO wird auch für Peer-to-Peer-Updates genutzt. Ab Windows 10 werden Updates nicht nur über Microsoft-Server, sondern auch von anderen Windows-10-Rechnern aus dem Internet übertragen. Das heißt, jeder Windows-10-Rechner kann Windows-10-Updates für andere Rechner über das Internet hochladen und damit Bandbreite belegen.

Um die Download-Bandbreite von Windows-10-Updates zu begrenzen, kann man WUDO deaktivieren, um alternativ BITS für Updates zu nutzen. Die Download-Rate für Updates lässt sich dann für BITS einstellen.

Quelle: <https://www.giga.de/downloads/windows-10/tipps/diensthost-uebermittlungsoptimierung-deaktivieren/>

Hinweis: Jeder Dienst kann 1 bis mehrere Prozesse starten (siehe: [W] + [X] -> Task-Manager).

Sc ist ein Befehlszeilenprogramm für die Kommunikation mit dem Dienststeuerungs-Manager und mit anderen Diensten.

sc

Aufruf der Kurzhilfe von sc.

sc query

Listet den Status aktiver Dienste und Treiber auf.

sc query type= driver

Listet nur aktive Treiber auf.

sc query type= service

Listet nur Win32-Treiber auf.

sc query state= all

Listet alle Dienste & Treiber auf.

sc query type= service type=

Listet alle interaktiven Dienste auf.

sc query type= driver group= NDIS

Listet alle NDIS-Treiber. Die Network Driver Interface Specification (**NDIS**) ist ein von Microsoft und 3Com entwickelter Standard zur Einbindung von Netzwerkkarten.

Administratoren und Systembetreuer müssen sich spätestens seit Windows Server 2012 wieder intensiver mit der Arbeit direkt an der Kommandozeile befassen. Wir zeigen, dass es nicht immer die CMD oder PowerShell sein muss: Mit **WMI** (Windows Management Instrumentation) und vor allen Dingen **WMIC** (Windows Management Instrumentation Command-line) lassen sich systemnahe Aufgaben schnell und einfach erledigen.

WMI ist eine der wichtigsten Schnittstellen für die Administration von Windows Betriebssystemen. Fast sämtliche Einstellungen können damit am lokalen Rechner oder auf Windows Installationen im Netzwerk erfolgen. Die WMI ist integraler Bestandteil von Windows 2000, Windows XP, Windows Server 2003 und allen Nachfolgeversionen.

Das Kommandozeilen-Tool wmic überwältigt den Benutzer mit einer Unmenge von möglichen Parametern und Schaltern, die beim Aufruf mit der Option /? im Hilfetext angegeben werden. Möchte man jedoch nicht den ganzen WMI-Funktionsumfang ausreizen, sondern nur Systeminformationen abrufen, dann findet man sich jedoch relativ schnell zurecht.

Startet man wmic ohne Parameter, dann wechselt es in einen interaktiven Modus, der am eigenen Prompt zu erkennen ist. Von dort kann man mit dem Befehl

/node:[Computername]

die Verbindung zu einem Remote-PC aufbauen. Praktisch an diesem Befehl ist, dass man ihm eine durch Kommata getrennte Liste von Rechnern übergeben kann, die sich anschließend gleichzeitig abfragen lassen. Falls man auf dem Zielrechner unter einem anderen Konto tätig werden muss, ruft man

/node:[Computername] /user:[Benutzername] /password:[Kennwort]

auf. Ist die Verbindung hergestellt, kann man mit Hilfe der wmic-Aliase die Systeminformationen abfragen.

Der nachfolgende Befehl ruft auf den Rechner »ComputerName« den Befehl **cmd.exe /k explorer.exe** aus. Der Befehl **WMIC**

/node:ComputerName ... beendet sich nicht und wartet auf mögliche weitere Eingaben (**siehe auch: cmd /?**).

WMIC /node:ComputerName process call create "cmd.exe /k explorer.exe"

- Die WMIC in der CMD oder PowerShell aufrufen und die Hilfe für die WMIC anzeigen. Der Befehl lautet:
wmic /?
wmic /?:FULL -> Zeigt die Hilfe und gleichzeitig die Syntaxinformationen an.
- Mit WMIC den Windows Produkt Key auslesen. Genauso wie das Auslesen der Seriennummer des Computers ist es auch möglich, den Windows Produkt Key abzurufen. Sollte die Ausgabe leer sein, so ist im BIOS / UEFI kein Produkt Key gespeichert. Der Befehl um den Produkt Key auszulesen lautet:
wmic path softwarelicensing get OA3xOriginalProductKey
wmic ProductKey ... funktioniert nicht beim Windows Server 2008; falls nur eine leere Ausgabe erfolgt, kann man es mit dem Programm Windows-Product-Key-Viewer (winproductkey.exe) versuchen (siehe Internet oder Verzeichnis: Windows-Product-Key-Viewer)
- Mit WMIC die Seriennummer auslesen. Unter anderem greifen VBScript und die Windows Powershell auf WMI zurück. Neben diesen Möglichkeiten lassen sich mit WMI auch die Werte (z.B. Seriennummer) aus dem BIOS abrufen. Der Befehl lautet:
wmic bios get serialnumber
- Mit WMIC die Betriebssystem-Version anzeigen. Der Befehl lautet:
wmic os get name
- Mit der WMIC die Prozesse (auch unscharfe Suche, Suche mit Platzhaltern) anzeigen. Der Befehl lautet:
wmic process list brief
wmic process where "name='firefox.exe'" list brief
wmic process where "Name like '%firefox%'" list brief
wmic process where "name='firefox.exe'" list status
wmic process where "name='notepad.exe'" call terminate -> den Prozess notepad.exe beenden
wmic process where "name='firefox.exe'" delete
WMIC /Node:dc1 service where "name='SNMP'" Call StopService -> den Dienst SNMP auf dem Rechner dc1 anhalten
- Mit der WMIC die Prozess-IDs des Rechners mit der IP-Nummer 192.168.20.83 bzw. mit dem Rechner-Namen server-01 anzeigen. Der Befehl lautet:
wmic /node:"192.168.20.83" process list brief
wmic /node:"server-01","192.168.0.1" process list brief
- Mit WMIC Bootdevice, Computernamen und das lokale Datum und die Zeit oder anderes anzeigen. Der Befehl lautet:
WMIC OS GET csname,bootdevice,localdatetime
WMIC OS GET osarchitecture /value -> Operating System Architecture (z.B. 64 Bit) anzeigen

- Mit WMIC eine Liste aller Dienste anzeigen. Der Befehl lautet:
WMIC SERVICE list brief
- Mit WMIC Informationen über das Motherboard anzeigen. Der Befehl lautet:
WMIC BASEBOARD list brief
- Mit WMIC einige Informationen des UEFI / BIOS anzeigen. Der Befehl lautet:
wmic bios get
Manufacturer,smbiosbiosversion,releasedate,serialnumber,status
wmic path Win32_bios get
manufacturer,name,serialnumber,releasedate,status
oder
Get-WmiObject Win32_BIOS
Get-WmiObject Win32_BIOS | select *
- Mit WMIC einige Informationen des Hauptspeichers anzeigen. Der Befehl lautet:
WMIC MEMORYCHIP list brief
- Informationen über die PC-Anmeldungen bzw. Netzwerkanmeldungen in eine HTML-Datei exportieren.
wmic logon get /all /format:htable > info1.htm
wmic netlogin get /all /format:htable > info2.htm
- Anmeldung auf den Rechner mit der IP-Nummer 192.168.20.205
wmic /node:'192.168.20.205' /user:user process list brief
- Benutzer auf dem Rechner bzw. die Anzahl der Logins auflisten.
wmic useraccount list brief
wmic netlogin get name,numberoflogons
- Informationen über die installierten Programme.
wmic product get installdate,name,version
wmic path Win32_Product get installdate,name,version
- Auflistung von Geräte-Treiber.
wmic sysdriver get name
wmic sysdriver where='SUCHWORT' get name
- Updates und Hotfixes auflisten (siehe auch: Windows 10 Einstellungen [W] + [I]).
wmic qfe list
- Informationen über die Speichergeräte.
wmic logicaldisk get name,volumename,filesystem
- Shutdown-Varianten: Neustart, Abschalten, Benutzer abmelden
wmic os where "status='ok'" call reboot
wmic os where "status='ok'" call shutdown
wmic os where "status='ok'" call Win32Shutdown 0
- Computernamen umbenennen
WMIC computersystem where caption='Aktueller-PC-NAME' rename NEW-PC-NAME
RENAME-COMPUTER –computername Aktueller-PC-NAME –newname NEW-PC-NAME -> PowerShell

- Mit WMIC eine Liste der verfügbaren Drucker (mit Ortsangabe) anzeigen. Der Befehl lautet:
WMIC PRINTER LIST STATUS -> Liste der verfügbaren Drucker anzeigen.
Get-WmiObject -class Win32_Printer
Get-WmiObject -class Win32_Printer -Filter "Name='HP Laserjet'"
- SID (Security Identifier) der Benutzer anzeigen.
wmic useraccount get name,sid
- Angemeldete Benutzer am Rechner ermitteln.
WMIC /NODE:192.168.20.83 COMPUTERSYSTEM GET USERNAME
query user -> CMD, PowerShell
- Benutzer sperren
wmic useraccount where name='username' set disabled=false
- Benutzer: Sperre wieder aufheben
wmic useraccount where name='username' set disabled=true
- Passwort für die Anmeldung entfernen
wmic useraccount where name='username' set PasswordRequired=false
- Benutzernamen ändern
wmic useraccount where name='username' rename newname
- Benutzer dürfen das Passwort nicht ändern
wmic useraccount where name='username' set passwordchangeable=false
- UUID (Universally Unique Identifier) eines Computers, die **IdentifyingNumber** - die Seriennummer des Gerätes
WMIC csproduct list /format
- Windows-Version ermitteln (nur Powershell)
Get-WmiObject Win32_OperatingSystem | Select PSComputerName, Caption, OSArchitecture, Version, BuildNumber | FL
(Get-WmiObject Win32_OperatingSystem).Version
(Get-WmiObject Win32_OperatingSystem).Caption
- Information über den Hersteller, Modell des Rechners
Get-WmiObject -class Win32_ComputerSystem
- Prozess stoppen
StopProcess -processname 'Prozessname'
StopProcess -processname calc

- Aufruf der grafischen Oberfläche der WMI-Kontrolle (Windows-Verwaltungsinstrumentation).
wmimgmt.msc
- Aufruf der WMI in der PowerShell oder CMD.
winmgmt.exe
- Aufruf des Testprogramms für das Windows-Verwaltungsinstrumentation, für die Verwaltung lokaler und entfernter Rechner.
wbemtest.exe

Elementare IT-Sicherheitsregeln

Das ewige IT-Mantra der elementaren IT-Sicherheitsregeln:

1. Aktiviere deinen gesunden Menschenverstand bei der Bewegung im Netz!
2. Misstraue allen Geschenken, die Dir per E-Mail zugesandt werden.
3. Öffne keine Dateianhänge in anlasslosen E-Mails, die von Unbekannten kommen.
4. Frage vor dem Öffnen von Dateianhänge/Links auch bei Zusendung durch Bekannte nach, wenn der Anhang Anlass für Fragen gibt.
5. Das fünfte Gebot: Du sollst nicht auf Links klicken, die Dir wilde Versprechungen machen!
6. Das sechste Gebot: Du sollst gar nicht auf Links in E-Mails klicken, wenn der Nutzen nicht klar nachvollziehbar ist.
7. Du sollst Deinen Rechner mit aktueller Schutzsoftware schützen.
8. Dateianhänge kann und sollte man vor dem Öffnen grundsätzlich auf Viren prüfen.
9. Ach ja: Und Dienst ist Dienst, Schnaps ist Schnaps. Im Büro sollte man bestimmte Sorten von E-Mails so oder so weder versenden, noch öffnen.

HINWEIS: Email-Viren sind weitgehend chancenlos, wenn der Nutzer die Verseuchung nicht selbst einleitet, indem er auf etwas klickt, worauf er nicht klicken sollte.

Von den aktuellen Viren (Malware, Trojaner, Threat, Infektor, etc.) können nur etwa die Hälfte von der aktuellen Schutzsoftware erkannt werden. Aber, ein schlechter Schutz ist besser als gar keiner.

Viren

IT-Analytiker versuchen den Begriff »Virus« zu vermeiden und bevorzugen Malware, Threat, usw. Der Grund dafür ist, dass ein Virus eine bestimmte Art von Malware ist, die ein bestimmtes Verhalten zeigt: Sie infiziert saubere Dateien. Untereinander beziehen sich Analysten auf einen Virus mit dem Begriff Infektor.

Infektoren genießen im Labor einen einzigartigen Status. Zunächst sind sie schwer zu entdecken – auf den ersten Blick scheint eine infizierte Datei sauber. Zweitens, benötigen Infektoren eine besondere Behandlung: fast alle von ihnen brauchen besondere Erfassungs- und Desinfektionsprozesse. Deshalb werden Infektoren von Experten behandelt, die auf diesen Bereich spezialisiert sind.

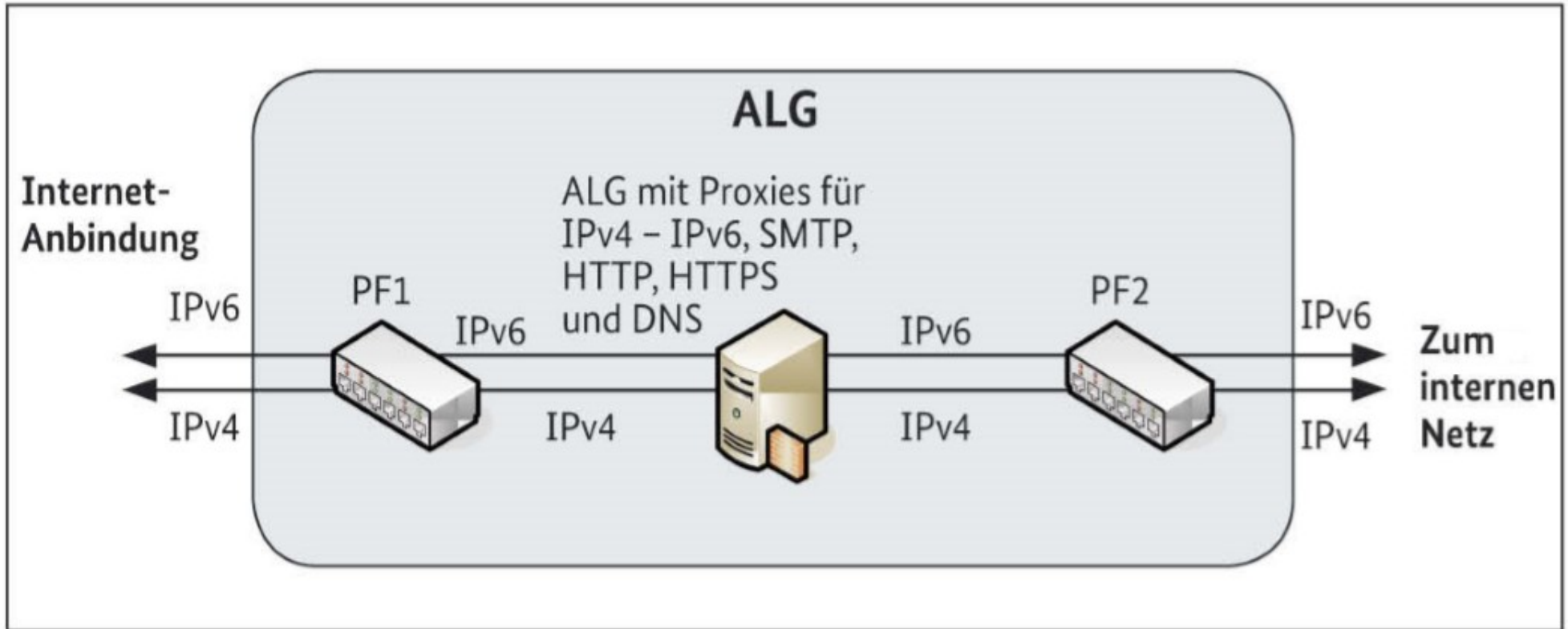
Signaturen ... Als Signaturen werden heutzutage alle Einträge in einer Antivirusdatenbank bezeichnet.

Threat ... engl.: Drohung, Bedrohung, Gefahr

APT ... Ein APT (Advanced Persistent Threat) ist ein Angriff auf das Firmen-Netzwerk, bei dem eine unautorisierte Person so lange wie möglich unentdeckt bleiben möchte.

KRITIS (Kritische Infrastrukturen) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung erhebliche Störungen der öffentlichen Sicherheit eintreten würden.

Ein Sicherheits-Gateway gewährleistet die sichere Kopplung von verschiedenen IP-Netzen. Ein solches Gateway besteht in der Regel aus einem äußeren Paketfilter, einem **Application-Level Gateway** in der Mitte und einem inneren Paketfilter.



Hierbei muss u. a. folgendes beachtet werden:

- Das Sicherheits-Gateway darf nicht umgangen werden, jeglicher Datenaustausch zwischen Internet und internem Netz muss das Sicherheits-Gateway passieren.
- Verschlüsselte Verbindungen dürfen das Sicherheits-Gateway nicht ungeprüft durchtunneln.
- Zugriffe von außen auf die angebotenen Internet-Dienste werden auf einem Server in einer DMZ (Demilitarisierter Zone) des Sicherheits-Gateways terminiert, um das interne Netz vor Zugriffen zu schützen.
- Bei der Verwendung von IPv6 bekommt das ALG (Application-Level Gateway) im Sicherheits-Gateway zusätzlich noch die Aufgabe der Adressübersetzung von IPv4 nach IPv6 und umgekehrt.

Zwei-Faktor-Authentisierung

Zwei-Faktor-Authentisierung für höhere Sicherheit

Wie funktioniert ein Log-In mit einem zweiten Faktor?

Eine Authentisierung mittels mehrerer Faktoren beginnt in vielen Fällen mit der gewöhnlichen Eingabe eines guten Passworts. Das System, in das sich Nutzerin oder Nutzer einloggen möchten, bestätigt daraufhin die Richtigkeit des eingegebenen Kennworts. Dies führt jedoch nicht - wie bei einfachen Systemen üblich - direkt zum gewünschten Inhalt, sondern zu einer weiteren Schranke. Auf diesem Weg wird verhindert, dass unbefugte Dritte Zugang zu Nutzerdaten oder Funktionen erhalten, nur weil Sie in den Besitz des Passworts gelangt sind.

Viele übliche Zwei-Faktor-Systeme (U2F bzw. 2FA) greifen nach der Passwortabfrage auf externe Systeme zurück, um eine zweistufige Überprüfung des Nutzers durchzuführen. Das kann bedeuten, dass der Anbieter, bei dem Sie sich anmelden möchten, einen Bestätigungscode an ein weiteres Ihrer Geräte sendet, z. B. Ihr Smartphone. Der zweite Faktor kann allerdings auch Ihr Fingerabdruck auf einem entsprechenden Sensor oder die Verwendung eines USB-Tokens (YubiKey 5 Serie, Security Keys) oder einer Chipkarte sein. Erst wenn sich auch dieses Mittel zur Identitätsbestätigung in Ihrem Besitz befindet, sind Sie in der Lage, die angeforderten Inhalte aufzurufen und den Online-Dienst oder das Gerät zu benutzen.

Internet-Browser

Mehrere gängige Webbrowser wie **Chrome** (Mai 2018, Version 67), **Firefox** (Mai 2018, Version 60), **Safari** (Januar 2019, Release 74), **Opera** (Juni 2018, Version 54) und **Microsoft Edge** (Oktober 2018, unter Windows 10 Version 1809) haben die Standards implementiert; **Android**, **Windows 10** und **verwandte Microsoft-Technologien** sollten ebenfalls über eine integrierte **Unterstützung für die FIDO-Authentifizierung** (Fast IDentity Online Alliance) verfügen.

Passwortfreie FIDO2-Anmeldung bei Microsoft

Microsoft hat mit dem **Windows 10 Update (V1809)**, Oktober 2018) die passwortfreie Anmeldung für alle Dienste über den FIDO2-Standard im Edge-Browser freigegeben.

Die Firma Yubico bietet FIDO2-fähigen Produkte (YubiKey 5 Serie, Security Keys) zur passwortlosen Anmeldung an Microsoft-Konten (Microsoft Accounts, MSA) an. Das bedeutet, dass sich Millionen von Nutzern ohne Passwort mit dem YubiKey 5 oder dem Security Key von Yubico bei ihren persönlichen Microsoft-Konten anmelden können.

Das heißt: Nur eine einzige Anmeldung, keine Passwörter und müheloser Zugriff auf viele Microsoft-Dienste. Sicherheitsschlüssel für Windows Hello bieten neben Yubico auch HID Global, OnlyKey, Key-ID, Google und Feitian an.

Quelle: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/OnlineBanking/Zwei_Faktor_Authentisierung/Zwei-Faktor-Authentisierung_node.html

Bedrohungspotentiale 1/2

Bedrohungspotenzial nimmt stetig zu

Die zunehmende Digitalisierung und Vernetzung führen zu Effizienzsteigerungen durch vereinfachte Prozesse, zu mehr Transparenz und zu mehr Komfort im Alltag. Gleichzeitig steigt das Bedrohungspotenzial deutlich an, da sich die Anzahl möglicher Angriffspunkte erhöht und die zu verarbeitenden Datenmengen sich vervielfachen. Die Wahrscheinlichkeit erfolgreicher Angriffe auf digitalisierte Infrastrukturen wird damit größer. Das Internet der Dinge (Internet of Things, IoT) entwickelt sich immer mehr zu einer Gefahrenquelle für die IT-Sicherheit. Dazu trägt entscheidend bei, dass IoT-Geräte einfacher angreifbar sind, weil deren IT-Sicherheit derzeit weder bei der Herstellung noch bei der Kaufentscheidung des Kunden eine ausreichende Rolle spielt.

Angreifer im Besitz eines Gerätes

Systemtest

Durch konkrete Analysen eines Endgerätes kann der Angreifer Versionsstände und Art der eingesetzten Software auslesen. Dadurch lassen sich Rückschlüsse auf die Sicherheitspolicy des Unternehmens ziehen und zudem können mit Hilfe von Schwachstellenkatalogen konkrete wirkungsvolle Angriffe gefunden werden.

Manipulation/Zerstörung

Der Angreifer kann das Betriebssystem und alle Dienste des Gerätes beliebig manipulieren. Insbesondere die enthaltenen Sicherheitsmechanismen werden dadurch wirkungslos.

Software – Schädlinge oder Malware

Es existieren zahlreiche Varianten von Software-Schädlingen für Endgeräte, die unterschiedlichste Schäden anrichten. Der Angreifer kann sowohl verschiedene Viren, Würmer und Trojaner in das System einbringen, als auch entsprechende Gegenmaßnahmen aushebeln.

Umgehung von Autorisationsprüfungen

Der Angreifer kann mangelhaft implementierte oder unzureichend konfigurierte Zugriffskontrollen ausnutzen, um an gespeicherte Daten zu gelangen.

Ausspionieren des Passworts

Das Erraten der Benutzerkennwörter kann durch einfaches Ausprobieren geschehen. Da der Angreifer das Gerät stets zurücksetzen kann, kann er das praktisch beliebig oft wiederholen. Zusätzlich kann er mit höherem Aufwand das Passwort im Klartext oder verschlüsselt aus dem Speicher des Gerätes auslesen. Eine weitere Gefahr ist das Einbringen von Spyware in das Betriebssystem, die das Passwort beim nächsten Anmeldeversuch des Benutzers aufzeichnet.

Angreifer nicht im Besitz des mobilen Gerätes

DoS

Verschiedene Angriffe erlauben Denial-of-Service-Attacken gegen Systemdienste und Anwendungen.

Pufferüberlauf

Über fehlerhafte Netzwerkprotokolle kann ein Angreifer so genannte Pufferüberläufe provozieren. Dabei werden vom Angreifer bewusst unzulässige Eingaben getätigt, die spezielle Seiteneffekte auslösen können.

Ausführung von nicht vertrauenswürdigem Code

Da einige mobile Endgeräte keine getrennten Vertrauensbereiche für Systemsoftware, Anwendungen des Benutzers und fremden Code besitzen, birgt das Ausführen von nicht vertrauenswürdigem Code besondere Gefahren.

Übernahme bestehender Sessions (Man in the Middle)

Kommunikationsprotokolle können durch Replay- und Man-in-the-middle-Attacken verletzbar sein, wodurch der Datenaustausch vom Angreifer abgehört und kontrolliert werden kann.

Kryptografie

Die kryptografischen Verfahren, die zur Kommunikation eingesetzt werden, können durch Brute-Force-Attacken oder das Ausnutzen bekannter Schwachstellen in Verschlüsselung und Authentisierung umgangen werden.

Bedrohungspotentiale 2/2

Angriffsziel: Infrastruktur

Einschleusung von Schadsoftware

Durch mobile Geräte (Smartphone, USB-Stick) als Träger von Schadsoftware können in manchen Fällen bestehende Sicherheitskonzepte umgangen werden.

Denial of Service

Der normale Betrieb kann dadurch gestört werden, dass ein Gerät innerhalb eines geschützten Bereiches als Quellknoten für Angriffe fungiert und damit wirkungsvolle Gegenmaßnahmen erschwert.

Unerlaubte Dienstnutzung

Durch physische Kontrolle eines Gerätes (angemeldetes Gerät mit erhöhten Rechten) lassen sich in vielen Fällen Sicherheitsmechanismen aushebeln, die Service- oder Contentprovider vor einem unbefugten Zugang zu bestimmten Onlinediensten oder vor der Verbreitung geschützter digitaler Inhalte schützen sollen.

Illegaler Datentransport großer Datenmengen

Aktuelle mobile Endgeräte, insbesondere multimedialfähige Geräte wie MP3-Spieler mit Videofunktionen, besitzen große Datenspeicher (>100 GByte). Da diese Geräte über Datenverbindungen mit hohen Bandbreiten angeschlossen werden können, ist Datendiebstahl sehr großer Datenmengen möglich.

Rechtemissbrauch

Der Benutzer und Endgeräte besitzen innerhalb der Unternehmens-Infrastrukturen gewisse Rechte. Gehen diese über die für seine Arbeit notwendigen Rechte hinaus, so kann der Benutzer diese ausnutzen.

Bedrohung durch Malware: Schadsoftware ist üblicherweise für eine Betriebssystemvariante oder für einen bestimmten Mobilgerätetyp konzipiert. Es sind Schädlingversionen denkbar, die auf einem höheren Abstraktionsniveau arbeiten, und systemübergreifend und damit unabhängig vom Betriebssystem und der Gerätehardware funktionieren. Ein Backdoor ist ein üblicherweise durch Viren, Würmer oder Trojanische Pferde installiertes Programm, das Dritten einen unbefugten Zugang (»Hintertür«) zum Computer verschafft, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen. Backdoors werden oft für Denial-of-Service-Angriffe benutzt.

Passive Angriffe: Beobachtung der Kommunikation

Sniffing Angriffe

Die Aufzeichnung von Kommunikationsbeziehungen erfolgt durch passives Abhören von Verbindungen. Der Kommunikationskanal kann dazu auch stark verschlüsselt sein, solange die Verbindungsdaten (z. B. Quell- und Zieladressangaben) unverschlüsselt sind, ist eine Entschlüsselung der Nutzdaten für diesen Angriff nicht nötig. Alleine die Erkenntnis des Angreifers, wer mit wem kommuniziert, ist bereits ein (teils sehr mächtiger) Angriff.

Bewegungsprofile aufzeichnen

Ein mobiles Endgerät mit integrierten aktiven Kommunikations-Schnittstellen wie Bluetooth oder WLAN-Modulen besitzt für die entsprechenden Protokolle eindeutige Adressen, die durch die Hardware festgelegt sind. Das Gerät, und damit auch der Benutzer, kann so eindeutig identifiziert werden. Bestimmte Konfigurationen der Kommunikationsgeräte erlauben anderen Geräten in Funkreichweite, diese Adressen gezielt abzufragen und zu sammeln. Da die Reichweite dieser Funktechniken zwischen 1 und 100 Meter liegt, kann man in diesem Rahmen Bewegungsprofile aufzeichnen.

Gewinn nicht technischer Informationen

Der Angreifer kann auf verschiedene Arten Informationen über die im Unternehmen eingesetzte Infrastruktur erhalten. Dazu zählen das Benutzen angebotener Dienste, persönliche Gespräche mit Mitarbeitern und die Beobachtung vor Ort. In Schwachstellenkatalogen kann er mit Hilfe dieser gewonnenen Fakten gezielt mögliche Angriffe auf die Infrastruktur suchen, eine Reihe von Angriffen vorbereiten und praktisch gleichzeitig durchführen.

DDoS 1/3

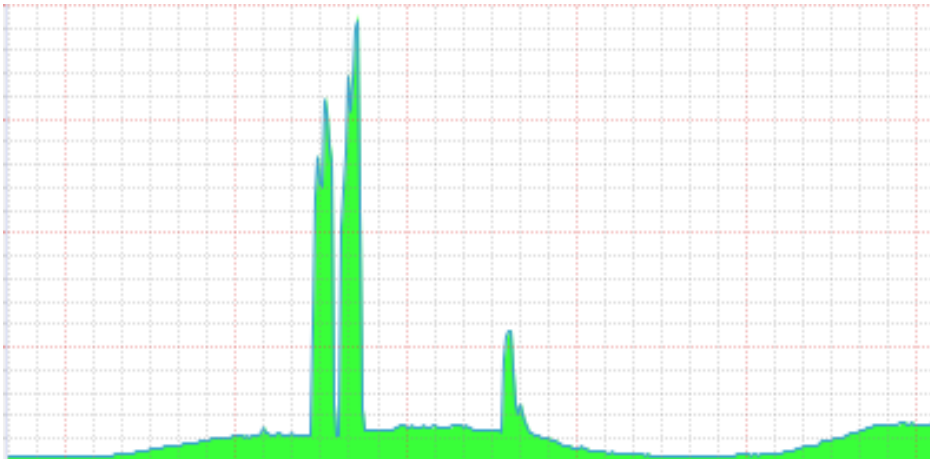
Was ist ein DDoS-Angriff?

Seit Jahren nutzen Kriminelle DDoS-Angriffe, um Unternehmen gezielt zu schädigen. Ihre immense Schlagkraft macht sie zu einer unkalkulierbaren, ernstzunehmenden Gefahr. Mit dem DDoS-Schutz von Myra (<https://myracloud.com/de/ddos-schutz/>) kann die IT-Infrastruktur sicherer werden.

Definition: (englisch: Distributed Denial of Service) meint die Nichtverfügbarkeit eines Dienstes durch mutwillige, von verteilten Endgeräten ausgehende Überlastangriffe.

Was bedeutet DDoS?

Ein DDoS-Angriff ist eine spezielle Art der Cyber-Kriminalität. Der Distributed-Denial-of-Service (DDoS) ist ein »verteilter« Denial-of-Service (DoS), der wiederum eine Dienstblockade darstellt. Diese liegt vor, wenn ein angefragter Dienst nicht mehr bzw. nur noch stark eingeschränkt verfügbar ist. Auslöser ist in den meisten Fällen eine Überlastung der IT-Infrastruktur. Angreifer nutzen diese Art der Cyber-Kriminalität, um von ungeschützten Unternehmen Lösegelder zu erpressen.



Wie sieht ein DDoS-Angriff aus?

Bei einem DDoS-Angriff führen Angreifer die Nichtverfügbarkeit eines Dienstes oder Servers gezielt herbei. Dafür infizieren sie einen oder mehrere Rechner mit Schadsoftware. Die Angreifer missbrauchen dieses infizierte Rechner-Netz, auch Botnetz genannt, ferngesteuert für ihre DDoS-Attacken. Mit dem Botnetz greifen sie parallel ihr Ziel an und beschießen dabei dessen Infrastruktur mit zahllosen Anfragen. Je mehr Rechner zusammengeschaltet werden, desto schlagkräftiger ist die Attacke. Angegriffene Server ohne DDoS-Schutz sind mit den unzähligen Anfragen überfordert, ihre Internetleitung ist überlastet. Webseiten bauen sich nur noch stark verlangsamt auf oder sind überhaupt nicht mehr verfügbar.

Wer sind die Angreifer?

Einzelne Kriminelle oder Gruppierungen, politische Aktivisten, Wettbewerber, enttäuschte Kunden – die Liste der Angreifer ist lang. Ihre Motive für einen DDoS-Angriff sind ebenfalls vielfältig: Erpressung, Konkurrenz schädigen, Neid oder Signale gegen politische Entscheidungen setzen. Das Ziel von Angreifern ist jedoch immer dasselbe: Der dahinterstehenden Organisation soll ein möglichst großer Schaden zugefügt werden.

Motivationsrichtungen und Tätertypen

Am häufigsten ist professioneller Hacktivismus verbreitet, um Aufmerksamkeit zu erregen und auf politische Ziele hinzuweisen. Kriminelle hingegen nutzen DDoS-Angriffe regelmäßig als komfortable Einnahmequelle, um Schutzgeld mittels anonymer Bezahlmethoden zu erpressen. Darüber hinaus buchen konkurrierende Marktteilnehmer, verärgerte Mitarbeiter und unzufriedene Kunden »DDoS-Angriffe als Dienstleistung« im Internet, wo man bereits für 50 Euro, die »Abschaltung« einer selbst ausgewählten Webseite in Auftrag geben kann.

DDoS 2/3

Welche Methoden setzen Angreifer ein?

Cyber-Kriminelle nutzen unterschiedliche Arten von DDoS-Angriffen. Die Methoden lassen sich nach den jeweiligen Schichten ordnen, auf die der Angriff abzielt.

Eine der häufigsten Methoden ist, Systemressourcen oder Netzwerkbandbreiten zu überlasten (Layer 3 und 4). Als Trend zeichnet sich unter den Cyber-Kriminellen in den letzten Jahren ab, die Angriffe auf die Anwendungsebene (Layer 7) zu verlagern. Muster und Bandbreiten von DDoS-Angriffen ändern sich jedoch täglich. Mit dem DDoS-Schutz von Myra kann man sich vor jeglichen Angriffsmustern schützen.

Was sind die Folgen eines Angriffs?

Ein Angriff schadet betroffene Unternehmen immer, unabhängig von der gewählten Methode. An den Folgen leiden Unternehmen noch Jahre später. Ein effizienter DDoS-Schutz ist deshalb für einige Firmen und Organisation unbedingt notwendig.

Welche Branche ist betroffen?

Opfer einer DDoS-Attacke kann jede Branche und jedes Unternehmen werden. Die Frage ist nicht ob, sondern wann ein Angriff auf das eigene Unternehmen stattfindet. Im Fokus von Cyber-Kriminellen und Erpressern stehen E-Commerce-Unternehmen, Versicherungen und Finanzinstitute, produzierende Unternehmen, Medien oder das Gesundheitswesen. Auch Rechenzentren und Organisationen aus dem öffentlichen Sektor sind beliebte Ziele der DDoS-Angreifer. Die Motive der Kriminellen gehen weit über Lösegeldforderungen hinaus: Mit ihren Angriffen wollen sie Fertigungsanlagen und Produktionsprozesse lahmlegen, die Strom- oder Energieversorgung unterbrechen und Einfluss auf die Berichterstattung nehmen.

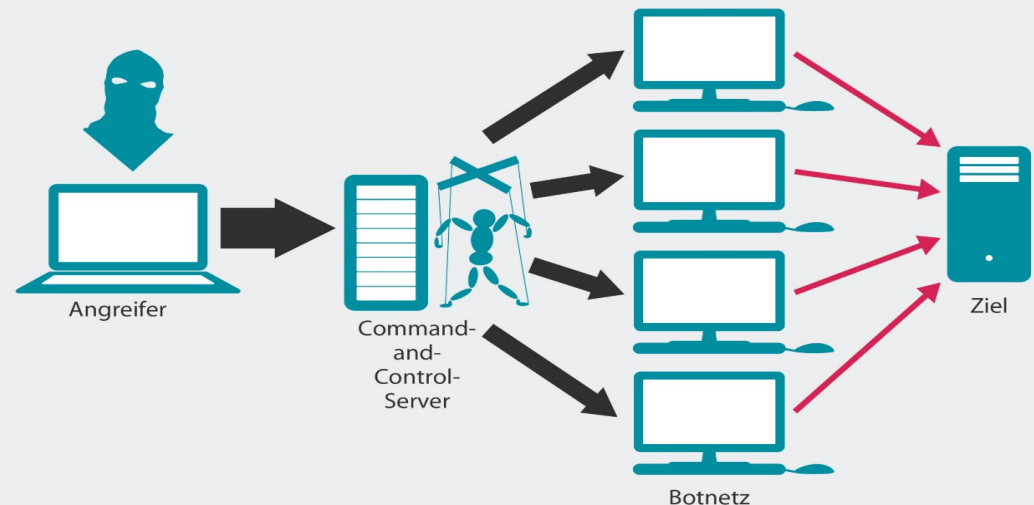
Der DDoS-Schutz von Myra

Wirksamen Schutz vor einem DDoS-Angriff gewährleisten nur professionelle Lösungen. Das cloudbasierte Schutzsystem von Myra (<https://myracloud.com/de/ddos-schutz/>) versteckt Ihre IP-Adresse hinter einem Filtersystem. Intelligente Algorithmen filtern die Trafficströme, weit bevor diese Ihre Infrastruktur erreichen.

Erkennen diese Algorithmen eine Attacke, setzen die Abwehrmechanismen unmittelbar ein. Valider Traffic (z.B. Kundenanfragen) erreicht Ihre Infrastruktur weiterhin. Durch weltweites Caching und Content-Optimierung werden Verzögerungen beim Ausliefern der Webseiten verhindert. Für Unternehmen bedeutet das: zuverlässiger Schutz vor DDoS-Angriffen und hochverfügbare Webseiten. Für Firmenkunden heißt das: optimale Auslieferungszeiten – egal ob im Normal- oder Angriffsfall.

Botnetz-Attacke

Mit Hilfe eines Botnetzes aus gekaperten Rechnern überlastet der Angreifer den Zielsystem. Die Bots werden über den Command-and-Control-Server mit Befehlen versorgt. Mittlerweile können Dritte solche Botnetze bequem über ein Web-Interface mieten.



DDoS 3/3

Wonach richten sich die Kosten eines DDoS-Schutzes?

Neben den einmaligen Bereitstellungskosten ist der größte Kostenfaktor, die zu buchende DDoS-Schutzbandbreite, die mindestens so hoch liegen muss, wie es dem Angriffsvolumen auf die Infrastruktur des Kunden entspricht oder voraussichtlich entsprechen könnte.

Hinweis: Die Lastverteilung bei DDoS-Attacken und normaler Last von mehr als 300 Gbit/s wird als schwierig angesehen.

DDoS-Schutz

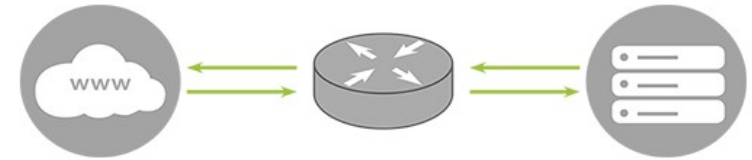
- On-Premise: Im Unternehmen oder vor der Backbone des Providers wird eine Vorrichtung im Internetzugang installiert, die ungewollten Traffic herausfiltert. **Vorteil:** Keine Änderungen am Netzwerk nötig. **Nachteil:** Nicht geeignet für große volumetrische Angriffe.
- In the Cloud: für die Cloud-Methode gibt es in zwei Optionen: Um einzelne Server zu schützen, wird der DNS-Eintrag des Unternehmens in der »Scrubbing-Abteilung« (Wasch- oder Reinigungsabteilung) des Providers in eine virtuelle Adresse konvertiert. Traffic wird geprüft und nur weitergeleitet, wenn er in Ordnung ist. Die Zweite: Um das Netzwerk komplett zu schützen, wird der Traffic über das BGP-Protokoll an die Scrubbing-Abteilung übertragen. Geprüfter Traffic wird dann über einen GRE-Tunnel (verschlüsselte Übertragung) an das Unternehmen weitergeleitet. **Vorteil:** Auch für große volumetrische Angriffe geeignet. **Nachteil:** Manuelle Eingriffe in die Netzwerk-Konfiguration nötig.

Zusätzlich gibt es Monitoring-Lösungen, die den Netzwerkverkehr auf DDoS-Angriffe untersuchen.

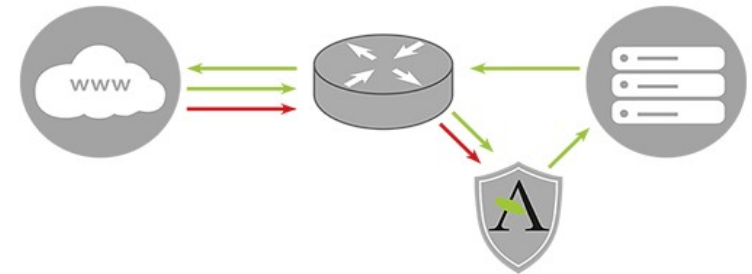
Scrubbing-Abteilung: Um Attacken im Gigabit-Bereich aufzufangen, wird der Traffic auf das Scrubbing Center umgeleitet, das den gesamten eingehenden Datenverkehr aus dem Internet filtert, das Volumen abmildert und nur die zulässigen Daten wieder zurück in die Systeme des Unternehmens leitet.

Anmerkungen: SORM (russisch Система технических средств для обеспечения функций Оперативно-Розыскных Мероприятий; COPM)

TRAFFIC-VERLAUF IM REGELBETRIEB



TRAFFIC-VERLAUF INKLUSIVE DDOS-SCHUTZ BEI ANGRIFF

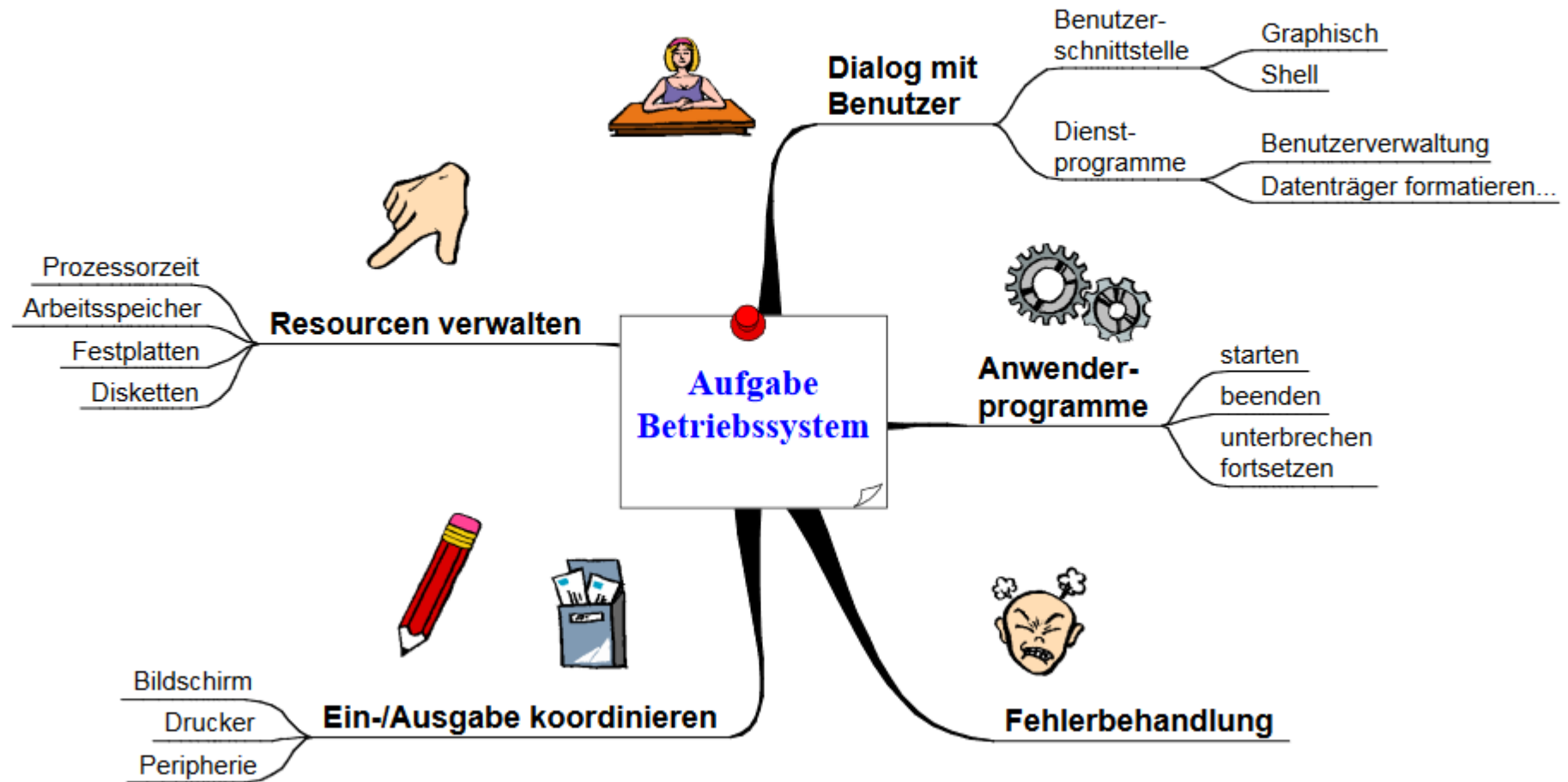


ist ein Überwachungsprogramm des russischen Inlandsgeheimdienstes FSB, das Telefon- und Internet-Daten in Russland abfängt und speichert. Technisch ist SORM mit PRISM vergleichbar. Bei beiden Diensten werden Datenpakete direkt beim Zugangsanbieter mit einer Black Box abgefangen, um sie aus der Ferne analysieren zu können.

BGP: Das Border Gateway Protocol (BGP) ist das im Internet eingesetzte Routingprotokoll und verbindet autonome Systeme miteinander. Diese autonomen Systeme werden in der Regel von Internet-Diensteanbietern gebildet. BGP wird allgemein als Exterior-Gateway-Protokoll (EGP) und Pfadvektorprotokoll bezeichnet und wird verwendet für Routing-Entscheidungen.

GRE: Das Generic Routing Encapsulation (GRE) ist ein Netzwerkprotokoll, welches dazu dient, andere Protokolle einzukapseln und so in Form eines Tunnels über das Internet Protocol (IP) zu transportieren. GRE wurde von von Cisco Systems entwickelt und setzt – wie UDP und TCP – direkt auf IP auf.

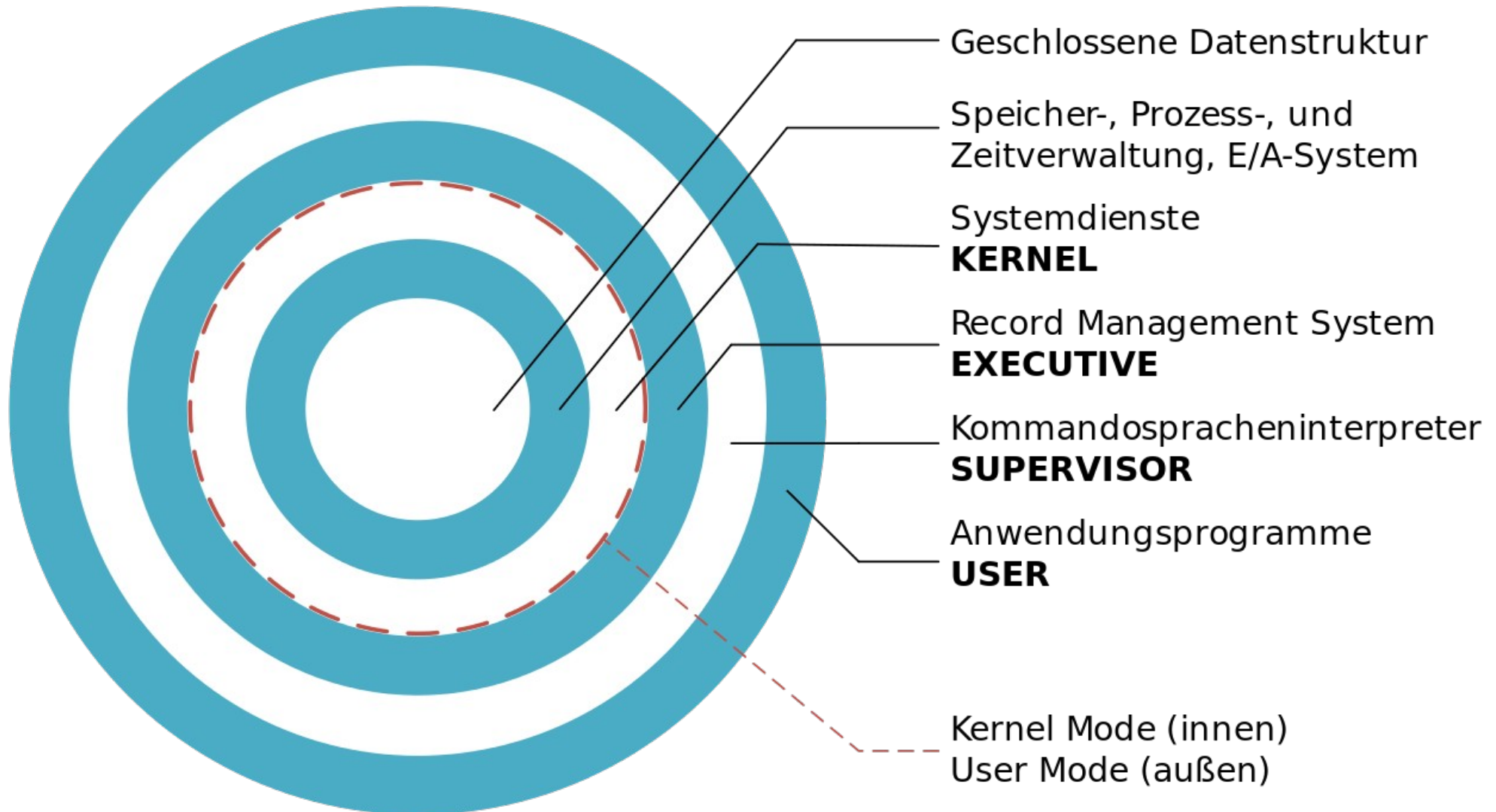
Aufgabe des Betriebssystems



Kennzeichen von Betriebssystemen



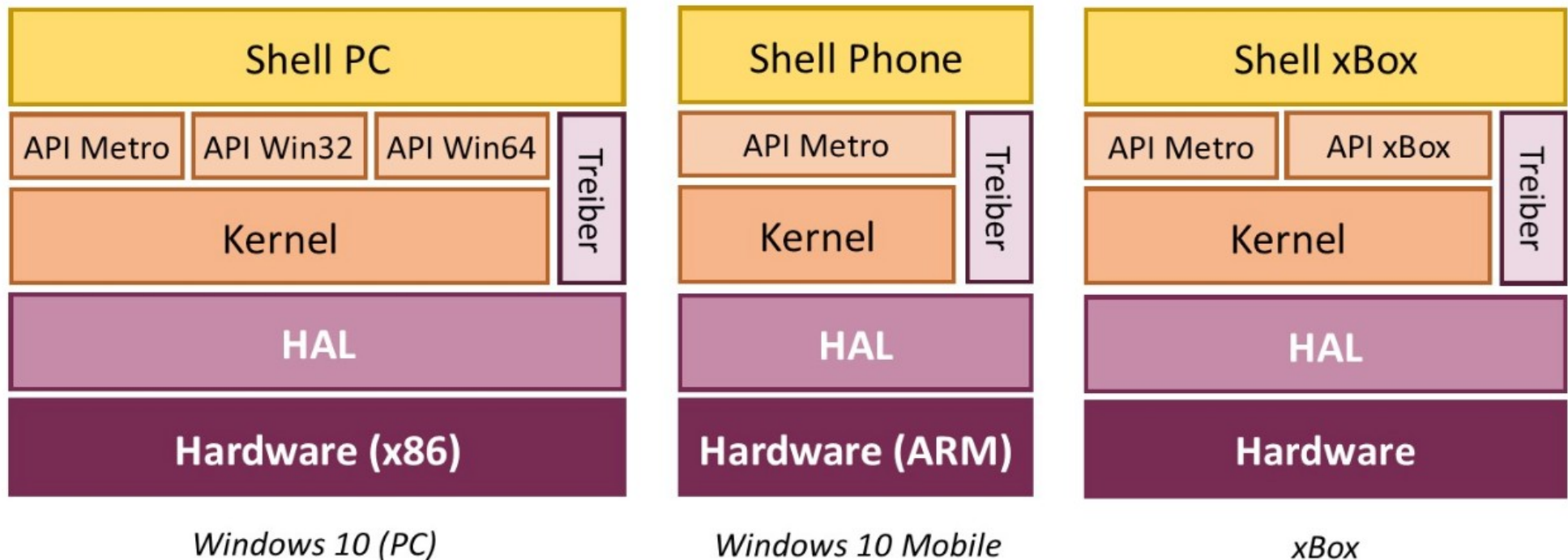
Aufgaben- und Schichtenmodell von Betriebssysteme 3/8



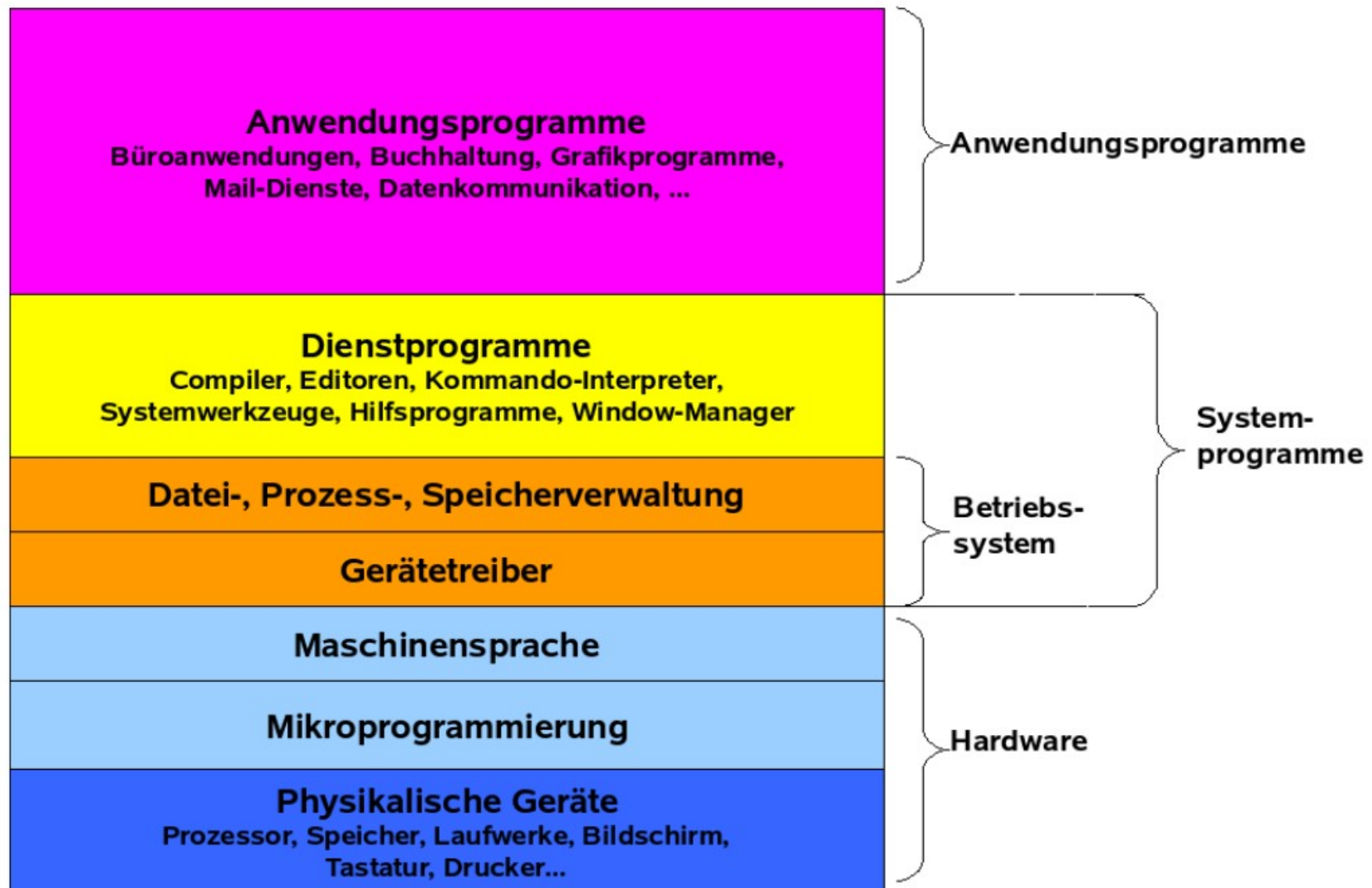
Aufgaben- und Schichtenmodell von Betriebssysteme 4/8

Stark vereinfacht folgt Windows dabei einem „Schichten-Modell“, das zuunterst mit der benutzten Hardware beginnt. Damit der Windows Kernel, der immer gleich ist, auch mit jeder Hardware funktioniert, folgt auf die Hardware (und deren Firmware, nicht abgebildet) der *Hardware Abstraction Layer (HAL)*.

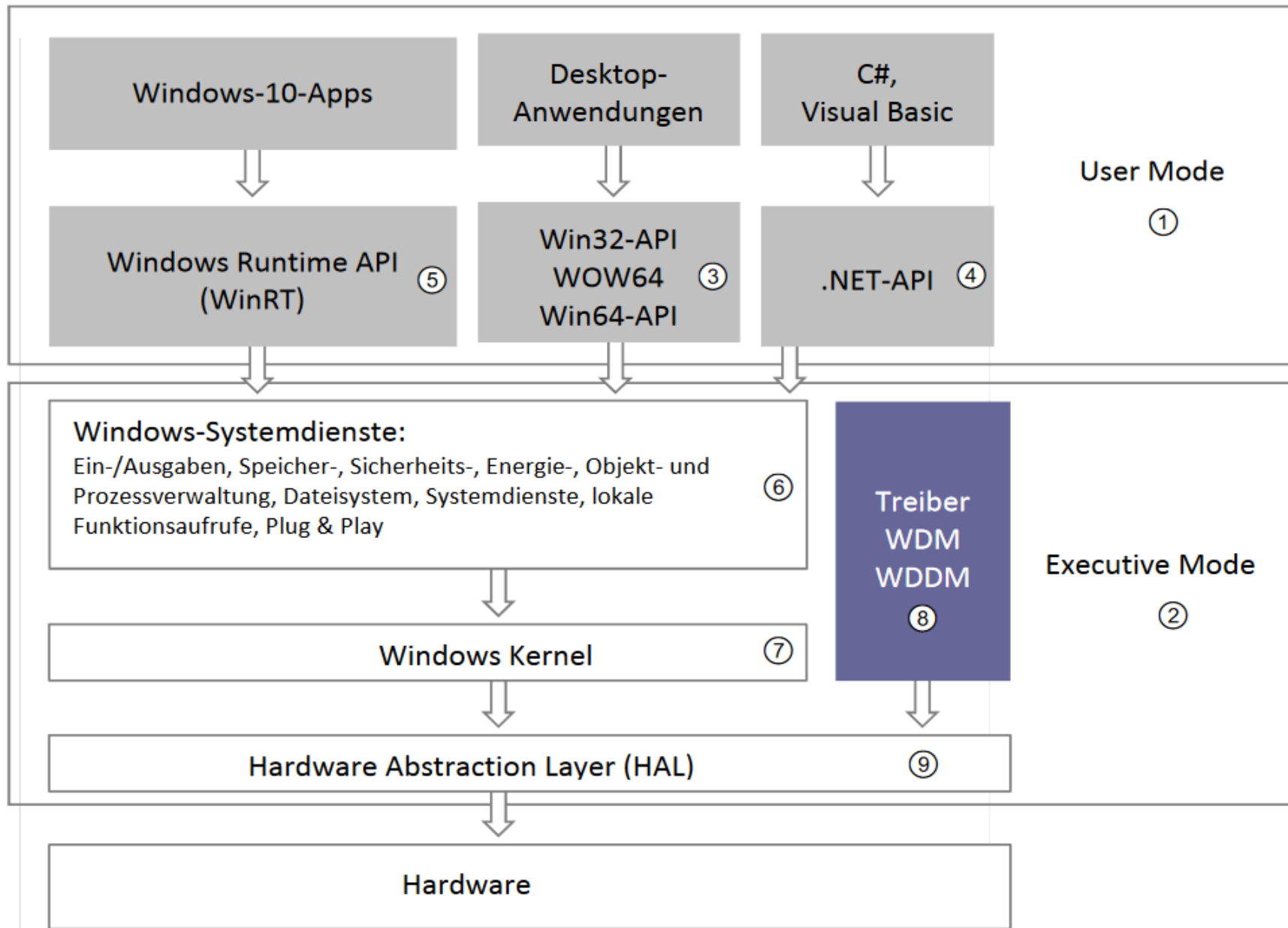
Nach dem Windows Kernel folgt der *Services Layer*, der die Kommunikation mit den Applikationen übernimmt, hier durch Subsets an API-Funktionen je nach verwendeter Applikationsgruppe (64 Bit, 32 Bit oder Metro/UWP) dargestellt. Zuoberst kommt die Shell, also das *User Interface*.



Aufgaben- und Schichtenmodell von Betriebssysteme 5/8



Aufgaben- und Schichtenmodell von Betriebssysteme 6/8



Aufgaben- und Schichtenmodell von Betriebssysteme 7/8

Windows 10 besteht aus mehreren Systemkomponenten, die eine Trennung von Anwendungsprogrammen, Betriebssystemkern und Hardware ermöglichen:

- Anwendungsmodus (User Mode)
- Prozessormodus (Executive Mode oder Kernel Mode)
- Betriebssystemkern (Kernel)
- Hardware Abstraction Layer (HAL)
- Speicherverwaltung

Diese Trennung schützt vor Fehlern in Anwendungen, die bei einem Absturz normalerweise nicht mehr die Stabilität des Betriebssystems gefährden können.

Windows 10 ist in seinen Grundzügen immer noch so aufgebaut wie sein »Vorfahre« Windows NT. Die einzelnen Systemfunktionen werden in verschiedenen Schichten abgelegt, die sorgfältig gegeneinander abgesichert werden. Grundsätzlich gilt, dass jede Schicht nur Anfragen aus der höheren Schicht beantwortet und selbst nur Anfragen an die tiefere Schicht stellen kann. Ein Sprung über mehrere Schichten hinweg wird unterbunden.

Während Windows nach einem Schichtenmodell aufgebaut ist, verfügen UNIX-basierte Betriebssysteme wie Apple Mac OS X über einen sogenannten monolithischen Kernel, also einen Betriebssystemkern aus einem Block, in dem alle zentralen Funktionen ausgeführt werden.

Bei Windows wird ein Client-Server-Modell verfolgt, bei dem das Betriebssystem Dienste zur Verfügung stellt, die von den Anwendungen oder anderen Diensten abgerufen werden können.

Bis auf wenige Ausnahmen laufen alle diese Dienste im sogenannten Benutzermodus (User Mode) und haben keinen direkten Zugang zur Computerhardware und zum Hauptspeicher.

Alle Ein- und Ausgaben sowie die Speicher- und Objektverwaltung werden vom Executive-Teil des Betriebssystems erledigt, der im Prozessormodus (Kernel Mode) läuft.

Auch der Windows-Kern hat keinen direkten Zugang zur Computerhardware, denn dazwischen liegt noch die sogenannte Hardware-Abstraktionsschicht oder auch Hardware Abstraction Layer (HAL). Diese Schicht wurde damals eingeführt, weil Windows auf verschiedenen Plattformen laufen und ohne großen Entwicklungsaufwand portierbar sein sollte.

Anwendungsmodus: Im Anwendungsmodus (User Mode) laufen sämtliche Benutzeranwendungen, aber auch große Betriebssystemteile. Jeder dieser Prozesse läuft in einem eigenen Speicherbereich und gibt seine Ressourcenanforderungen an die darunterliegende Schicht weiter, den Prozessormodus (Executive Mode). Kein Prozess kann am Executive Mode vorbei direkt auf Kernel- oder Hardwarefunktionen zugreifen.

Prozessormodus: Im Prozessormodus (Executive Mode oder Kernel Mode) befinden sich die zentralen Bestandteile des Windows-Betriebssystems. In diesen Windows-Systemdiensten findet die gesamte Verwaltung von Speicher, Sicherheit, Energie, Objekten, Ein- und Ausgaben, Dateisystem, Plug & Play und lokalen Funktionsaufrufen statt. Nur der Executive Mode kann mit dem Kernel kommunizieren.

Aufgaben- und Schichtenmodell von Betriebssysteme 8/8

Betriebssystemkern (Kernel): Der Kernel ist der Kern des Betriebssystems, der laut Microsoft bei allen Windows-Versionen der Serie 8 (Hinweis: Windows 8.x) identisch ist. Hier befindet sich der Task Scheduler, der das Multitasking steuert. Außerdem werden im Kernel die Interrupts für CPU und Peripherie verwaltet. Der Kernel befindet sich in den Dateien ntoskrnl.exe bzw. ntkrnlmp.exe.

Windows Driver Model (WDM): Alle Windows-Treiber folgen dem Windows Driver Model (WDM) und greifen niemals direkt auf die Hardware zu. Bei früheren Windows-Versionen bildete der Grafikkartentreiber noch eine Ausnahme, aber wie bei Windows 7 und Vista erlaubt das Windows Display Driver Model (WDDM) auch bei Windows 10 aus Sicherheitsgründen keine direkte Hardware-Ansteuerung.

Hardware Abstraction Layer (HAL): Alle Zugriffe von Anwendungen auf die Hardware werden vom Betriebssystem kontrolliert. Anwendungen, die direkte Hardwarezugriffe erfordern, können deshalb unter Windows 10 nicht eingesetzt werden. Auch der Betriebssystemkern (Kernel) greift nicht direkt auf die Hardware zu. Zwischen dem Kernel und der Hardware des Computers befindet sich eine weitere Schicht, die Hardware Abstraction Layer (HAL), die sämtliche Hardwarezugriffe vermittelt.

In der HAL werden außerdem die Betriebssystemanforderungen so umgesetzt, dass sie von der Hardware interpretiert werden können, um Kompatibilität zu verschiedenen Plattformen zu ermöglichen. Deshalb werden je nach verwendeter Hardware und BIOS-Einstellungen bei der Installation von Windows verschiedene HAL-Versionen installiert.

Bei früheren Windows-Versionen war es noch möglich, das System mit einer HAL für APM (Advanced Power Management), dem Vorläufer von ACPI (Advanced Configuration and Power Interface), zu installieren.

Seit Windows 8 ist AHCI Version 2 zwingend erforderlich, ebenso wie die Aktivierung des APIC, des Advanced Programmable Interrupt Controllers, der für die Interruptsteuerung von Multiprozessorsystemen zuständig ist.

Speicherverwaltung: Entscheidende Bedeutung für die Stabilität eines Betriebssystems hat auch die Speicherverwaltung mittels VMM (Virtual Memory Manager). Zugriffe auf den Arbeitsspeicher des Computers werden vollständig vom Betriebssystem verwaltet. Fehlerhafte Speicherzugriffe einer Anwendung führen deshalb nicht unmittelbar zum Absturz des gesamten Systems, sondern zum Beenden des Prozesses.

Das Betriebssystem stellt jedem Prozess einen scheinbar zusammenhängenden Speicherbereich zur Verfügung, der in Wirklichkeit aus einer großen Anzahl von virtuellen Speicherseiten besteht, die irgendwo im existierenden Hauptspeicher oder in der Auslagerungsdatei auf einem Datenträger liegen können.

Reicht der physisch vorhandene Speicher (RAM, Random Access Memory) nicht mehr aus, kann Windows 10 zusätzlich virtuellen Speicher zuteilen. Dabei werden in einer Auslagerungsdatei namens pagefile.sys auf einer Festplatte Speicherseiten aus dem RAM gespeichert. Dabei werden bevorzugt jene Seiten ausgelagert, die im Moment nicht benötigt werden.

Hinweis: Windows 10 setzt verschiedene Komponenten (verschiedene Authentifizierungs-Methoden) ein, um die Sicherheit einzelner Computer und des gesamten Netzwerks zu gewährleisten. Ein wesentlicher Teil der Sicherheitsfunktionen von Windows 10 ist nur verfügbar, wenn als Dateisystem NTFS eingesetzt wird.

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.

OSI-Schicht	Einordnung	DoD-Schicht	Einordnung	Protokollbeispiele	Einheiten	Kopplungselemente
7 Anwendungen (Application)	Anwendungs-orientiert	Anwendung	Ende zu Ende (Multihop)	HTTP FTP HTTPS SMTP XMPP DNS LDAP NCP DHCP	Daten	Gateway, Content-Switch, Proxy, Layer-4-7-Switch
6 Darstellung (Presentation)						
5 Sitzung (Session)						
4 Transport (Transport)	Transport-orientiert	Transport		TCP UDP SCTP SPX	TCP = Segmente UDP = Datagramme	
3 Vermittlung-/Paket (Network)		Internet		ICMP IGMP IP IPsec IPX	Pakete	Router, Layer-3-Switch
2 Sicherung (Data Link)		Netzzugriff	Punkt zu Punkt	Ethernet TLAP FDDI MAC	Rahmen (Frames)	Bridge, Layer-2-Switch
1 Bitübertragung (Physical)				1000BASE-T Token Ring ARCNET	Bits, Symbole, Pakete	Netzkabel, Repeater, Hub

Unterschied: Router Accesspoint 1/2

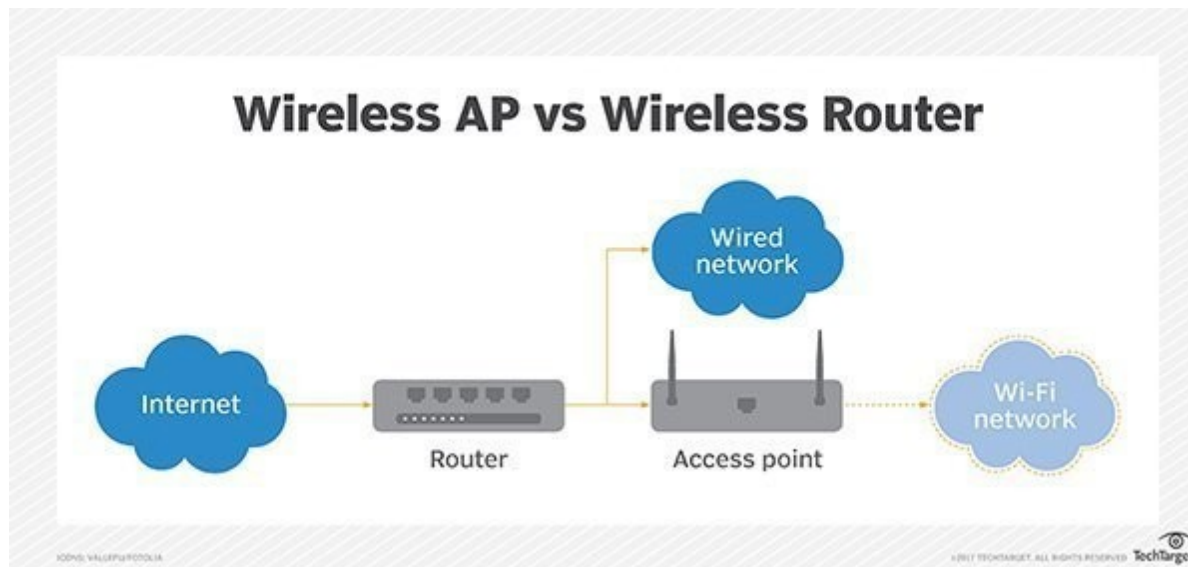
Unterschied: Router - Accesspoint

Es gibt einige **Unterschiede** zwischen einem Wireless **Router** und einem Wireless **Access Point**. Ein Wireless **Router** kombiniert die Leistungsmerkmale eines Breitband-**Routers** und eines Wireless APs in einem einzigen Gerät. Genau genommen ist ein Wireless Router ein Gateway zwischen dem Internet und dem LAN (Local Area Network). Anders gesagt kann ein Wireless Router ein Wireless AP sein, aber nicht andersherum.

Der Hauptunterschied ist, dass ein Router zwischen dem Internet und dem LAN vermittelt und damit allen Stationen im Netzwerk den Internetzugang ermöglichen kann. Ein Access Point ist dagegen nur ein Wireless-Switch.

Was ist ein Wireless Access Point?

Ein Wireless AP verbindet eine Gruppe drahtloser Stationen mit einem entsprechend angebandenen LAN. Vom Konzept her arbeitet ein AP wie ein Ethernet-Switch (verhält sich wie eine WLAN-Zentrale).



Was ist ein Wireless Router?

Ein Wireless Router verbindet eine Gruppe drahtloser Stationen mit einem angeschlossenen drahtgebundenen Netzwerk. Grundsätzlich ist ein Wireless Router eine Kombination aus AP und einem Ethernet-Router. Das Gerät leitet IP-Pakete zwischen dem drahtlosen Subnetz und allen anderen Subnetzen weiter (verhält sich wie eine WLAN-Zentrale und hat zusätzliche RJ-45 Anschlüsse und kann Anschlüsse für Telefon und USB haben).

Soll ich nun einen Wireless Access Point oder einen Wireless Router einsetzen?

In der Regel kommen Wireless Router im Heimbereich oder in kleineren Firmen zum Einsatz. Dort lassen sich alle Anwender mit einer Kombination aus AP und Router bedienen. Wireless APs setzt man in größeren Unternehmen und Orten ein, an denen viele APs für die Bereitstellung eines Services benötigt werden.

Ein Beispiel wäre ein Gelände, auf dem mehrere Tausend Anwender versorgt werden. In größeren WLANs ist es häufig sinnvoll, dass mehrere APs einen einzigen und separaten Router füttern. Die drahtlosen Stationen lassen sich in diesem Fall wie ein großes Subnetz behandeln. Das ist hilfreich, wenn man sich frei bewegen und dabei von einem AP zum nächsten wandern (Roaming) muss. Die Zugriffskontrollen (Access Control) für das Funknetz lassen sich in diesem Fall auf einen Router konzentrieren und man muss sich nicht um mehrere Geräte kümmern.

Wireless Router bieten außerdem eine einfache Firewall-Funktionalität. Mithilfe von Network Address Translation (NAT) teilt man sich eine Internetadresse mit mehreren drahtlosen Endgeräten. Die meisten Wireless Router sind darüber hinaus mit einem Vier-Port-Ethernet-Switch ausgestattet. So hat man die Möglichkeit, einige drahtgebundene PCs mit dem LAN zu verbinden, die dann ebenfalls auf das Internet zugreifen können. Die meisten Wireless Router kombinieren also die Funktionalitäten eines drahtlosen APs, eines Ethernet Routers, einer Firewall und eines kleinen Ethernet-Switches.

Was ist der Unterschied zwischen einem Access Point und einem Repeater?

Der entscheidende Unterschied zwischen einem Access Point und einem Repeater ist, dass der Repeater lediglich ein bestehendes WLAN-Signal verlängert. Das bedeutet, dass das Gerät das eingehende Signal aufnimmt, verstärkt und wieder ausstrahlt. Der größte Vorteil dabei ist also, dass ein WLAN-Repeater lediglich eine freie Steckdose benötigt. Dieses Vorgehen setzt allerdings voraus, dass das Signal bereits per WLAN eingeht.

Das ist bei einem AP anders. Ein Access Point kann ein Signal nicht nur verlängern, sondern auch grundsätzlich den Verbreitungsweg ändern.

Weil der Access Point per Kabel mit dem Router verbunden ist und es dabei zu keinem Qualitätsverlust kommt, ist diese Methode besser geeignet, um mit einer schnellen Verbindung eine große Reichweite zu erzielen. Für Privatanwender ist das nicht so relevant wie für Unternehmen. Diese sollten eine gleichbleibende Qualität des Internetsignals sicherstellen können und müssen zum Teil große Strecken überbrücken. Der Qualitätsverlust wäre bei der Verwendung von Repeatern zu groß.

Windows 10 ist ein einziger »Datenschutz-Unfall«

Aus der Datenschutzerklärung von Microsoft: Der Schutz Ihrer Daten ist uns sehr wichtig. -> Diesen 1. Satz aus der Datenschutzerklärung kann man sehr vieldeutig lesen und verstehen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bescheinigt Microsoft in einem neuen Bericht quasi zwischen den Zeilen, dass es sich bei Windows 10 um einen 'Datenschutz-Unfall' handelt. Die Telemetrie sei für normale Benutzer kaum abschaltbar. Momentan lässt das BSI laut dem aktuellen Bericht die Sicherheitseigenschaften des neuen Betriebssystems weiter untersuchen. Und die deutschen Behörden schlafen weiter. [...]

Windows 10 steht seit seinem Erscheinen im Sommer 2015 wegen der eingebauten Telemetriefunktionen und Privatsphäreneinstellungen in der Kritik. Microsoft hat zwar in den letzten Jahren etwas nachgebessert und informierte Benutzer beim Umstieg auf Windows 10 darüber, die Privatsphäreneinstellungen anzupassen.

Windows 10 und Office sammeln Daten und überträgt sie an Microsoft Server. Es besteht zwar die Möglichkeit, einige dieser Telemetriefunktionen über die Einstellungen und Gruppenrichtlinien in ihrer Wirkungsweise abzuschwächen. [...]

Quelle: www.borncity.com 2018

LTSC ... Long Term Servicing Channel und **bedeutet** übersetzt so viel wie Langfristiger Service-Zweig

Kein Grund zur Verwirrung. Bei Windows 10 hieß der Long Term Servicing Channel einmal LTSC. Das steht für Long Term Servicing Branch. Es gilt ganz einfach: LTSC = LTSCB

Was will Microsoft über die Windows-10-Benutzer wissen?

Die folgende Liste entstammt der Datenschutzerklärung von Microsoft mit Stand vom Juli 2018.

Bei jeder Installation oder Upgrade müssen die Benutzer dieser Datenschutzerklärung zustimmen, ansonsten wird die Installation oder das Upgrade abgebrochen.

- Name und Kontaktdaten
- Anmeldeinformation
- Demografische Daten (z.B. Alter, Geschlecht, Land und die bevorzugte Sprache)
- Zahlungsdaten
- Daten über Lizenzen und Abonnements
- Interaktionen
- Geräte- und Nutzungsdaten
- Zahlungsmethoden und Aktivitätsverlauf des Kontos
- Browserverlauf
- Geräte-Konnektivitäts- und Konfigurationsdaten
- Fehlerberichte
- Leistungsdaten
- Problembehandlung und Daten
- Interessen und Favoriten
- Nutzungsdaten von Inhalten
- Suchvorgänge und Befehle
- Sprachdaten
- Text, Eingabe- und Freihanddaten
- Bilder
- Kontakte und Beziehungen
- Soziale Daten (Vorlieben, Abneigungen, Ereignisse, Kontakte zu anderen Personen)
- Positionsdaten
- Andere Angaben

- Inhalt (Mitteilungen z.B. per Mail, Audio, Video, Text oder Dateien)
- Videos und Aufzeichnungen (bezieht sich auf Aufnahmen in Microsoft-Gebäuden)
- Feedback und Bewertungen

Quelle: Zeitschrift »PC-WELT« Sonderheft – Notfall-Handbuch 2019

Anmerkung: Microsoft sammelt mit Hilfe des Windows-Betriebssystems und mit vielen seiner Dienste jede Menge von Daten über die Anwender. In der vorgenannten Liste sind die **offiziell** von Microsoft gewünschten Daten aufgelistet.

Im Internet kursieren einige Batch-Skripte für die Verbesserung der Privatsphäre unter Windows 10.

siehe auch: Privatsphäre-Einstellungen unter Windows 10 härten

Datenschutzeinstellungen ändern:

[W] + [I] -> Datenschutz -> Diagnose und Feedback -> Standard oder bei Windows 10 Enterprise LTSC -> Security

Cortana und die Suchmaschine Bing können nur über die Gruppenrichtlinie (gpedit.msc) oder über einen neuen Schlüsseleintrag in der Registry deaktiviert werden.

Telemetrie:

ETW ... Event Tracing for Windows

svchost.exe

diagtrack.dll

perfmon.exe

logman.exe

Admin-Rechte für einzelne Programme

In Windows steht dazu die Registerkarte »Kompatibilität« in den Eigenschaften von Verknüpfungen für Programme zur Verfügung. Durch Aktivieren der Option »Programm als Administrator ausführen« kann festgelegt werden, dass dieses einzelne Programm mit Administrator-Rechten ausgeführt wird.

Auf diesem Weg lassen sich also einzelne Programme mit erhöhten Rechten starten, ohne dass ein Benutzer gleich Administratorrechte erhalten muss.

Datenschutzerklärung von Microsoft

Letzte Aktualisierung: Juni 2019 [Neuigkeiten](#)

✓ [Alles erweitern](#)

 [Drucken](#)

Der Schutz Ihrer Daten ist uns sehr wichtig. In dieser Datenschutzerklärung wird erläutert, welche persönlichen Daten von Microsoft erfasst, wie und wofür das Unternehmen sie verwendet.

[...]

- Dieser erste Satz aus der Datenschutzerklärung von Microsoft ist fast zu ehrlich.
- Diesen Satz kann man aus der Sichtweise der Benutzer und aus der Sichtweise von Microsoft lesen.
- In der heutigen Informationsgesellschaft (Big Data, Data Mining) sind die Daten der Menschen das neue Gold der Firmen und Organisationen.
- Das BS Windows wird lizenziert, nicht verkauft. Unter diesem Vertrag gewährt Microsoft den Benutzern das Recht, die Software auf einem Gerät zur Verwendung zu installieren und auszuführen, solange alle Bestimmungen des Vertrages eingehalten werden.

Quelle: Datenschutzerklärung von Microsoft

<https://privacy.microsoft.com/de-de/privacystatement> oder in den »Einstellungen« von Windows 10

SiSyPHuS Win10 - BSI nimmt Windows 10 unter die Lupe

Verfasst am 01. Juni 2019. Veröffentlicht in [Windows](#)

Windows 10 ist ein Datenschutz-Unfall. Diese Meinung vertreten seit Veröffentlichung der aktuellen Version des Microsoft-Betriebssystems nicht wenige. Kaum jemand hat sich aber so tief in das System eingearbeitet wie das BSI mit seinem Projekt **SiSyPHuS Win10**.

Das Thema ist nicht neu. Die [ersten Meldungen](#) diesbezüglich kamen schon aus dem vergangenen Oktober. Das gesamte Projekt lässt sich das [BSI einiges kosten](#), was aber auch an der Bedeutung von Windows für die Verwaltung liegt.

In der ersten Ankündigung gab das BSI schon einen Einblick in das Drama:

Den Analysen zufolge hat die in Windows 10 "ab Werk" eingebaute Telemetrikomponente umfassende Möglichkeiten, auf System- und Nutzungsinformationen zuzugreifen und diese an den Hersteller zu versenden. Obwohl die Nutzer unterschiedliche Telemetrielevel einstellen können, ordnet der Telemetriedienst die vorhandenen Telemetriequellen diesen Leveln im laufenden Betrieb dynamisch zu. Hierfür lädt der Dienst mehrmals pro Stunde Konfigurationsdaten nach. Eine Unterbindung der Erfassung und Übertragung von Telemetriedaten durch Windows ist technisch zwar möglich, für den einfachen Anwender allerdings nur schwer umzusetzen. Zudem haben auf dem Rechner installierte Anwendungen wie der Internet Explorer und Microsoft Office die Möglichkeit, auch ohne den zentralen Telemetriedienst des Betriebssystems Telemetriedaten zu erfassen und an den Hersteller zu versenden.

Quelle: [BSI Pressemitteilung vom 20.11.2018](#)

BSI ... Bundesamt für Sicherheit in der Informationstechnik

SiSyPHuS Win10 ... Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10

Telemetrie ... Telemetrie (nutzt die Funktionen von Windows Event Tracing - ETW) ist die Übertragung von Messwerten eines am Messort befindlichen Messfühlers zu einer räumlich getrennten Stelle. Telemetrie nutzt die Funktionen von Windows Event Tracing (ETW).

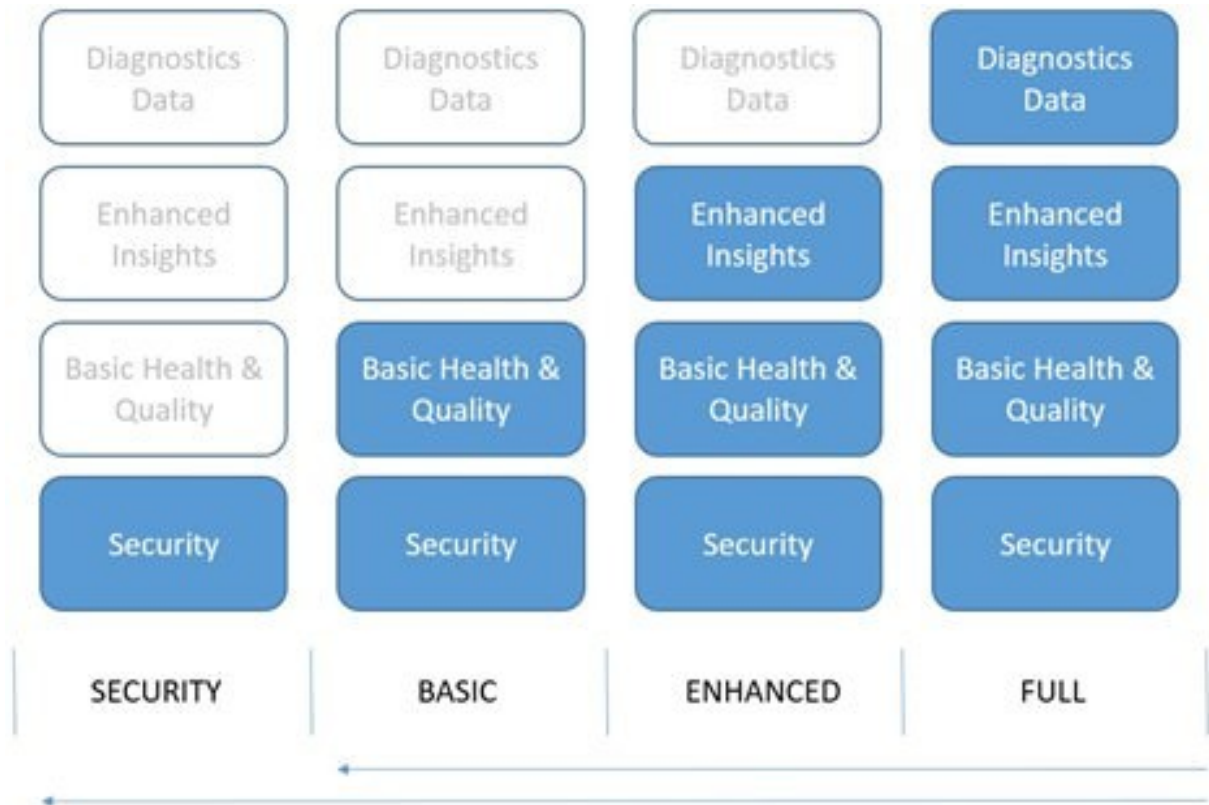
Telemetrie

Nach Einschätzung des BSI hat die in Windows 10 eingebaute Telemetrikomponente umfassende Möglichkeiten, auf System- und Nutzungsinformationen zuzugreifen und diese an Microsoft zu versenden. Nutzer können zwar unterschiedliche Telemetrie-Level einstellen, aber eine eindeutige Zuordnung der übertragenen Informationen zu diesen Stufen sei nicht möglich: Windows lade mehrmals pro Stunde Konfigurationsdaten nach und ordne damit die vorhandenen Telemetriequellen diesen Leveln im laufenden Betrieb **dynamisch** zu.

Quelle:

<https://www.heise.de/newsticker/meldung/BSI-untersucht-Sicherheitseigenschaften-von-Windows-10-4227139.html>

Telemetrie ist die Übertragung von Messwerten eines am Messort befindlichen Sensors zu einer räumlich getrennten Stelle. An dieser Empfangsstelle können die Messwerte entweder nur gesammelt und aufgezeichnet oder auch sofort ausgewertet werden.



Windows 10 Enterprise

Unter Windows laufen viele unterschiedliche Prozesse, die im Taskmanager eingesehen werden können. Die meisten davon sind harmlos und stellen die ordnungsgemäße Funktion von Windows sicher.

Hinweis: Jeder Windows-Dienst kann 1 bis mehrere Prozesse starten (siehe: [W] + [X] -> Task-Manager).

CTF-Ladeprogramm (ctfmon.exe):

Das CTF-Ladeprogramm (ctfmon.exe) ist eine Programmdatei in Microsoft Office und ist permanent im Task-Manager zu sehen. Auch nachdem Office geschlossen wurde, lässt sich die ctfmon.exe im Taskmanager nicht beenden.

Aufgaben der ctfmon.exe:

- verantwortlich für die Umwandlung von handschriftlichem Text und Rede in eine elektronische Version;
- bietet die Funktionalität der Sprachleiste in Microsoft Office;
- hilft, das Tastaturlayout bei der Arbeit mit einem Textprogramm zu wechseln;
- überwacht aktive Fenster und bietet Textunterstützung für die Sprach- und Handschrifterkennung.

Client-Server-Laufzeitprozess (csrss.exe):

Die csrss.exe (Client/Server Run-Time Subsystem) ist verantwortlich für Konsolenanwendungen, Starten und Beenden von Threads (ein Thread ist Teil eines Prozesses) und für die virtuelle 16-Bit-MS-DOS-Umgebung. Die Anzahl der laufenden csrss.exe-Prozesse kann abhängig von der Version des Betriebssystems variieren. Normalerweise werden ein, zwei und manchmal sogar mehr csrss.exe-Prozesse im Task-Manager gestartet.

Normalerweise befindet sich die csrss.exe im Windows-Ordner C:\Windows\System32. Befindet sich die Datei nicht dort, so handelt es sich eventuell um einen Virus oder einen Wurm.

Prozess »netsh«

Der Prozess netsh steht für eine ganze Gruppe von verschiedenen Diensten, die alle von der Datei svchost.exe verwaltet werden. Deshalb tauchen beide Prozesse auch immer gemeinsam auf - als **svchost.exe (netsh)**.

Der Prozess **netsh** tritt im Windows-Taskmanager, meistens mit der Systemdatei svchost.exe bei Windows-Problemen auf (z.B. bei einer zu hohen CPU-Auslastung oder hohem Arbeitsspeicherverbrauch). Falls auf dem Rechner die **Datei** netsh.exe auftaucht, ist dies sehr wahrscheinlich ein Virus oder Malware, die sich unter diesem Dateinamen tarnt.

Achtung: Die »Datei« **netsh** ist in Wirklichkeit keine Datei, sondern ein **Prozess**. Die Datei netsh.exe dürfte es also eigentlich nicht geben.

Problem: netsh verursacht eine zu hohe Auslastung in Windows

Lösung:

- Taskmanager mit Administrator-Rechte öffnen
- Reiter Prozesse: Button »Prozesse aller Benutzer anzeigen«
- den zugehörigen Prozess svchost.exe mit der rechten Maustaste anklicken und »Prozess beenden« auswählen.

Sofern der Prozess für Windows relevant ist, wird er unter Umständen automatisch neu gestartet. Falls das Problem wiederholt auftritt, so sind die aktuellen Windows-Updates zu installieren.

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 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.

GPU (Graphics Processor Unit):

Im Windows 10-Taskmanager wird die GPU-Auslastung (Grafikprozessor) angezeigt.

Anmerkung (das Windows 10-Betriebssystem verwendet einige bekannte Technologien):

Sogenannten Web-**Beacons** oder auch Zählpixel sind extrem kleine, häufig bloß 1×1 Pixel große, Bilddateien (Clear-GIF), welche in die Newsletter-E-Mail integriert werden und so eine Logdatei-Aufzeichnung sowie eine Logdatei-Analyse erlauben.

Öffnet der Nutzer nun die jeweilige vorher geladene E-Mail, so wird der Zählpixel vom Server des Newsletterbetreibers geladen und gleichzeitig einige Informationen über den E-Mail Empfänger übermittelt, wie z.B.:

- ob die E-Mail geöffnet wurde,
- Zeitpunkt des Aufrufs,
- sowie die dazugehörige IP-Adresse.

Dabei besteht auch die Möglichkeit die jeweilige Zählpixel-Bilddatei der für den Versand verwendeten E-Mail-Adresse eindeutig zuzuweisen, indem die Zählpixel-Bilddatei individuell generiert wird.

siehe auch: [W] + [I] -> Datenschutzbestimmungen

Prozess-Systemunterbrechungen:

Der Prozess Systemunterbrechungen ist ein fester Bestandteil von Windows, aber kein Prozess im herkömmlichen Sinn.

Der Task-Manager verwendet diesen Eintrag, um anzuzeigen wie viel CPU-Kapazität, Arbeitsspeicher etc. die Hardware-Interrupts des Rechners benötigen.

Interrupts sind Teil der üblichen Kommunikation zwischen dem Prozessor und den übrigen Geräten des Rechners. Benötigt z. B. die Tastatur die Aufmerksamkeit der CPU (Betätigung einer Taste), dann teilt sie das einer Komponente auf der Hauptplatine mit, welche die Nachricht wiederum an die CPU weitergibt.

In der Regel sollte der Prozess Systemunterbrechungen nur eine sehr geringe CPU-Last aufweisen. Mehr als 30 Prozent deuten auf ein Problem hin.

Datenschutzbeauftragter

1. **Begriff:** Person, die die Einhaltung datenschutzrechtlicher Vorschriften zu überwachen hat. Einen Datenschutzbeauftragten haben alle Unternehmen zu bestellen, die mindestens fünf Arbeitnehmer ständig mit der automatisierten oder 20 Arbeitnehmer mit der nicht automatisierten Verarbeitung personenbezogener Daten beschäftigen. Hinweis: Die Nichtbestellung wird als Ordnungswidrigkeit (bis 50.000 Euro) geahndet.
2. **Aufgabe:** ständige Kontrolle der Einhaltung des Bundesdatenschutzgesetzes (BDSG) in einem Unternehmen; im besonderen durch Überwachung der verwendeten Software, Schulung der Mitarbeiter und beratende Mitwirkung bei der Personalauswahl. Der Datenschutzbeauftragte kann sich bei Zweifelsfällen an eine staatliche Aufsichtsbehörde (etwa den Regierungspräsidenten) wenden, die zugleich seine Tätigkeit kontrolliert.
3. **Rechtsstellung:** Der Datenschutzbeauftragte ist unmittelbar der Geschäftsführung eines Unternehmens zu unterstellen. Er arbeitet weisungsfrei; seine Berufung kann nur aus wichtigem Grund widerrufen werden.

Hinweis: Ein Datenschutzbeauftragter kann Mitarbeiter dieser Organisation, des Unternehmens sein oder als externer Datenschutzbeauftragter bestellt werden.





Was schreibt die Datenschutz-Grundverordnung vor:

- 1. Einwilligung:** Die Person hat vor der Erfassung der persönlichen Daten, in die Verarbeitung ihrer Daten eingewilligt. **Voraussetzung:** Die Person wurde umfassend über die Verarbeitung ihrer Daten informiert. Die Einwilligung kann schriftlich, mündlich oder elektronisch erfolgen. Der Widerruf der Einwilligung ist von Gesetzes wegen jederzeit möglich.
- 2. Vertragserfüllung:** Die Verarbeitung der Daten erfolgt zur Erfüllung eines Vertrages. Dazu zählen auch vorvertragliche Maßnahmen, z.B. das Zusenden einer Broschüre oder eine Angebotserstellung.
- 3. Rechtliche Verpflichtung:** Die Verarbeitung der Daten ist gesetzlich vorgeschrieben und muss deshalb erfolgen (Buchhaltung: Erfassung von Personendaten).
- 4. Schutz lebenswichtiger Interessen:** Die Verarbeitung der Daten erfolgt zum Schutz lebenswichtiger Interessen einer Person (z.B. Gesundheitswesen, Notfallmedizin).
- 5. Öffentliches Interesse:** Die Verarbeitung der Daten erfolgt im öffentlichen Interesse.
- 6. Berechtigtes Interesse:** Ein Unternehmen hat ein berechtigtes Interesse an der Datenverarbeitung, welches gegenüber dem Interesse der betroffenen Person überwiegt (z.B. Betrugsprävention). Dieser letzte Punkt ist relativ unsicher geregelt, da hier die Interessen beider Parteien sorgfältig abgewogen werden müssen.

- ▶ **Unablässig** werden Daten von uns erhoben, gespeichert, verknüpft, bewertet und verkauft
- ▶ Das Vorgehen der Datensammler ist subtil und verdeckt
- ▶ Es entsteht ein nahezu **vollständiges** Profil

Verknüpfung von scheinbar harmlosen Daten mehrerer Anbieter, ergeben nicht mehr so harmlose Daten.

Ihr digitales Ich

- ▶ Wie viel verdienen Sie?
- ▶ Haben Sie Schulden?
- ▶ Leiden Sie an einer Blasenschwäche?
- ▶ Welches Auto fahren Sie?
- ▶ Was konsumieren Sie?
- ▶ Mit wem kommunizieren Sie?
- ▶ In welchem Viertel wohnen Sie?

[...]

Ein Drittanbieter hinter verschiedenen Webseiten, kann viele Daten sammeln. Nach einer Analyse, sind diese Daten nicht mehr so harmlos.


Fiktives Nutzerprofil

Name:..... Rainer **Hubertus**

Alter:..... 49 Jahre

Frau:..... Anna **Hubertus**



Kinder:..... Stefan [25]
Simone [22]

Interessen 

Wissenschaft
Kunst und Kultur
Sport

Krankheiten
Migräne
Allergien

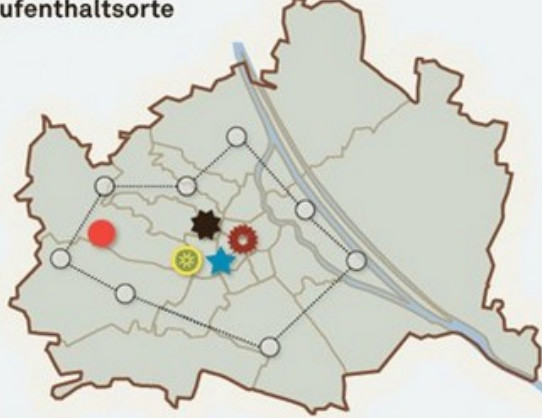
Politische Ausrichtung
Mitte-links




Hinweis: Bei jedem Internet-Besuch hinterlässt **jeder**, mehr oder weniger, harmlose Spuren. Die Verknüpfung dieser scheinbar belanglosen Daten mehrerer Anbieter, ergeben mit der Zeit **nicht mehr ganz so harmlose Daten**.




Man kann schon fasst ein Lied darüber singen:
Einmal harmlos ist harmlos, zweimal harmlos ist harmlos, dreimal harmlos ist harmlos, viermal harmlos ist nicht mehr so harmlos.

Aufenthaltssorte



Algorithmen haben immer mehr Einfluss auf die Bewertung von Menschen.

 Arbeit [8–17 h]
  Lieblingsrestaurant
  Meistbenutztes Stadtgebiet

 Wohnung
  Besuchtes Nachtlokal
  Einkaufsrouten

Jahresgehalt
63.000 €

Freizeit
Joggen, Fitness, Kino
[läuft 21,3 Kilometer pro Woche]

 **184 Freunde auf Facebook**

 **48 Follower auf Twitter**

Facebook hat ein Patent angemeldet: »Wenn ein Individuum einen Kredit beantragt, prüft der Gläubiger die Kreditwürdigkeit derjenigen Mitglieder in sozialen Netzwerken, die mit dem Individuum vernetzt sind.«

Ist die Kontrolle der Daten noch möglich?

1.

Bewusst

- ▶ Beitrag in einem sozialen Netzwerk
- ▶ Bild hochladen in die Cloud
- ▶ Versenden einer E-Mail
- ▶ Einkauf mit Payback-Karte
- ▶ [...]

Kontrolle vorhanden

2.

Unbewusst

- ▶ Cookies / IP-Adresse beim Surfen
- ▶ Smart-TV übermittelt Sehgewohnheit
- ▶ »Telemetrie-Daten« der Geräte
- ▶ SCHUFA-Scoring
- ▶ [...]

Eingeschränkte Kontrolle

3.

Heimlich

- ▶ Übermittlung eindeutiger IdNr.
- ▶ Geräte-ID
- ▶ IMSI-Nummer
- ▶ Smartphone-Apps
- ▶ Adressbuch
- ▶ SMS-Inhalte
- ▶ Adresshandel
- ▶ [...]

Kontrollverlust!

Hinweis: In der Internetgesellschaft sind bei den Kontakten zwischen eigentlich anonymen Menschen die tausende Jahre alten Verfahren zum Vertrauensaufbau, entweder über direktes Kennenlernen oder über Reputation (Ansehen einer Person) in einem gemeinsamen Umfeld, nicht mehr möglich.



Identitätsdiebstahl



Wer soll schon etwas mit meinen Daten anfangen? Die interessieren doch keinen. Außerdem habe ich sowieso nichts zu verbergen.

Bei einem Identitätsdiebstahl ist unbedingt schnelles Handeln erforderlich. **Die eigene digitale Identität sollte einmalig bleiben.**

Gefährdete Daten und Informationen, sind der vollständige Name, Geburtsdatum, Wohnort, Kreditkartennummer, Kontodaten und andere persönliche Informationen.

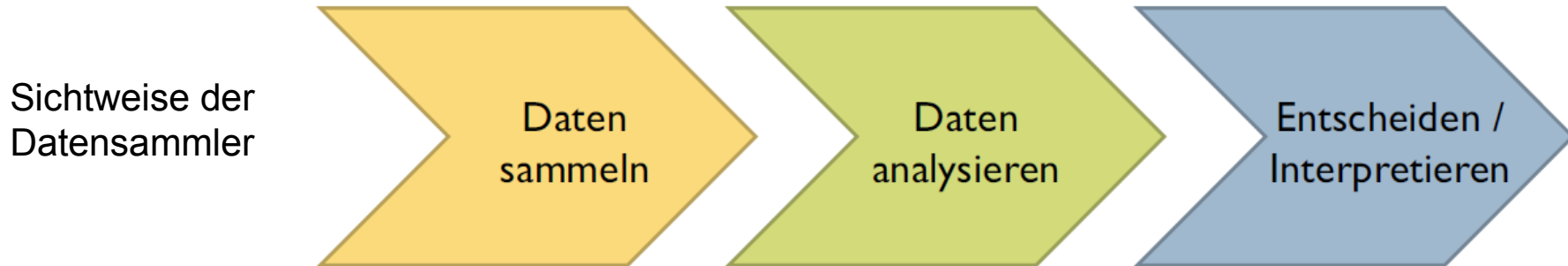
Wie erkennt man einen Identitätsdiebstahl?

- verdächtige E-Mails
- Rechnungen über nicht bestellte Waren
- verdächtige Kontoauszüge
- nicht bestellte Lieferungen
- Post von Inkasso-Unternehmen

Um weiteren Betrug zu vermeiden, sind unverzüglich

- Kredit- und Bankkarte zu sperren
- der Online-Händler ist zu informieren
- die Passwörter sind zu ändern
- eine neue E-Mail Adresse anzulegen und die alte E-Mail Adresse zu löschen
- bei größeren Beträgen ist ein Rechtsanwalt oder ein spezialisierter Verein zu konsultieren
- Strafanzeige erstatten – dieser Schritt ist notwendig für den Versicherungsanspruch

Big-Data: Profiling und Marketing



Profiling bezeichnet die nutzbare Erstellung des **Gesamtbildes einer Persönlichkeit** für bestimmte Zwecke. Die Erstellung erfolgt durch das Zusammenführen von Daten, sowie deren anschließende Analyse und zweckbezogenen Auswertung. **Ziel des Profiling ist die Vorhersage von Verhalten und dessen zielgerichtete Beeinflussung und Veränderung.**

Im **Marketing** wird Profiling zur Erstellung von möglichst genauen und individuellen Kundenprofilen eingesetzt, um den Moment einer Kaufentscheidung möglichst genau vorherzusehen und beeinflussen zu können. **Hinweis:** Ohne Einwilligung des Betroffenen illegal (DSGVO Art. 6).

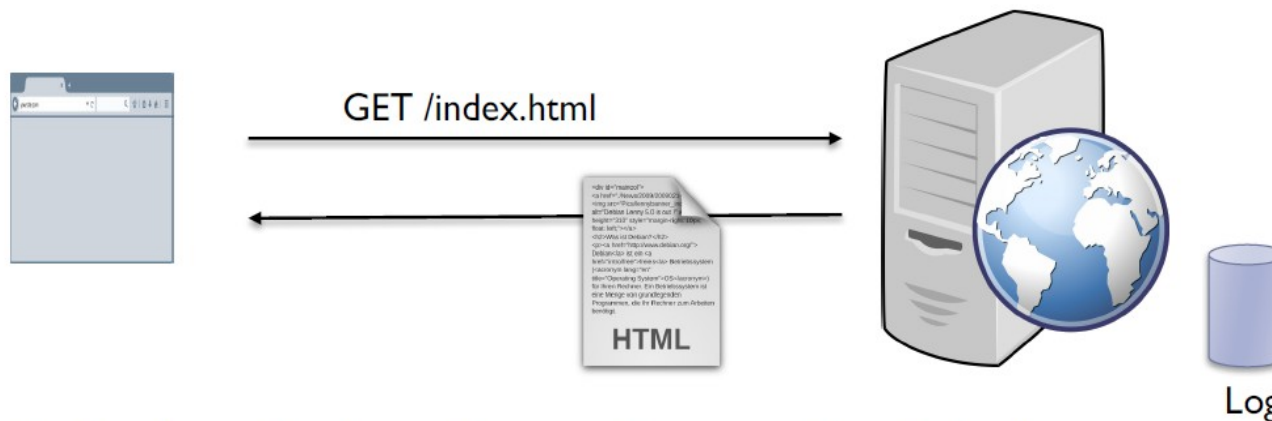
Professionelle Datensammler (Payback, Deutsche Post, Facebook, Microsoft, ...) setzen Profiling für die Erstellung von Persönlichkeits-, Verhaltens- oder Bewegungsprofilen, für die Bewertung der Kreditwürdigkeit, des Durchschnittseinkommen, Gesundheitszustand und vieles mehr ein.

Big Data: Was erzählt der Internet-Browser?

Browser Tracking

► Erkennung

- von Zugriffen auf Websites („Wer liest Spiegel Online?“)
- sowie Wiedererkennung bzw. Zuordnung von Identitäten über verschiedene Zeiten, IP-Adressen und ggf. Geräte hinweg



► Techniken: Cookies, Finger Printing, Pixel Tracking

Pixel Tracking: Ein-Pixel-Bild, 1×1 gif-Bild, Clear.gif oder Web Beacon, sind kleine Grafiken in HTML-E-Mails oder auf Webseiten, die eine Logdatei-Aufzeichnung und eine Logdateianalyse ermöglichen.

Fingerprinting: Canvas-Fingerprinting macht sich die subtilen Unterschiede beim Rendering des Textes zu nutze. Diese Unterschiede lassen sich messen und in Sekundenbruchteilen in ein Fingerabdruck umrechnen, ohne dass der Anwender etwas davon bemerkt.

Browser-Tracker wie z.B. Google Analytics verfolgen Surfer über sämtliche Websites und Geräte hinweg und erstellen so detaillierte Persönlichkeitsprofile.

Big Data: Was ist Tracking?

Tracking mit Cookies

- ▶ Cookie = Textinformation, die vom Server zum Browser gesendet und später vom Browser zurückgeschickt wird
- ▶ Erkennung von Sitzungen über mehrere Aufrufe hinweg, z.B. für Warenkorb



Super-Cookies oder Evercookies: Sie verwenden eine so große Sammlung von Methoden, dass es dem Benutzer nicht mehr möglich ist, alle Spuren zu löschen. Aus einem übersehenen Objekt, können die gelöschten Objekte wieder rekonstruiert werden. Super-Cookies oder Evercookies gehören zu den nicht löschbaren Cookies.

Hinweis: Für Unternehmen und Agenturen sind die Informationen, welche über Tracking-Cookies gesammelt werden, überaus wertvoll.

Firefox Add-on z.B. Cookie Editor, Cookie Quick Manager

Mit dem Firefox Add-on NoScript kann man, die Webseite zur Datensparsamkeit anregen.

Privatsphäre-Einstellungen unter Windows 10 härten – 1/4

BSI-Hinweise

Das BSI (Bundesamt für Sicherheit in der Informationstechnik) stellte fest (Stand: 2018), dass Windows 10 die Telemetrie-Daten bei Systemabstürzen, aber **auch bei der normalen Nutzung** von Windows 10 sammelt.

Es werden Daten über die Nutzung des Computers unter Windows 10 gesammelt und der an dem Computer angeschlossenen Geräte, Daten über die Performance des Systems, Daten, die bei Fehlern wie Programm- oder Systemabstürzen erhoben werden, sowie Daten des Windows Defenders und des Malicious Software Removal Tools (MSRT).

Diese Daten schickt Windows 10 an Microsoft-Server. Bis zu 422 sogenannte Event Tracing für Windows-Entitäten (ETW) sammeln diese Daten, wenn Windows 10 diesbezüglich maximal eingestellt ist.

In den Mindesteinstellungen (Windows 10 Enterprise) sammeln zumindest vier solche Entitäten (ETW).

Das BSI betont, dass »aufgrund der durchgeführten Analyse sich keine Verbindung zwischen Anzahl an ETW-Anbietern und Telemetrie-Datenmenge sowie deren Qualität ableiten lässt.«

Anmerkung: Auch wenige ETWs können sehr viele Daten übertragen!

Privacy-Handbuch

Windows 10 reagiert auf 1.000 - 1.200 Ereignisse, die eine Logmeldung triggern, welche dann an die Microsoft Telemetrie Server übertragen wird.

Microsoft Office sendet noch mehr Daten. Bei dem Paket MS Office Pro Plus lösen 23.000 - 25.000 Ereignisse eine Übertragung von Daten an Telemetrie Server aus. 20-30 Teams arbeiten an der Auswertung der Daten, wobei selbst Microsoft keinen Gesamtüberblick hat, welche Produkte welche Daten senden.

Das BSI hat für Windows 10 die Telemetriedaten in der Analyse SiSyPHuS Win10 genauer untersucht (preiswürdiger Titel!). Dabei kommt das BSI zu dem Ergebnis, dass die Übertragung der Telemetriedaten in Windows 10 »Basic« **nicht** durch die Konfiguration von Einstellungen **vollständig deaktivierbar** ist.

Als Schutz gegen die Datensammelwut empfiehlt das BSI, die Verbindungen zu den Windows Telemetrie Servern zu blockieren.

[...]

Quelle: www.privacy-handbuch.de/handbuch_90a2.htm

Anmerkung: Im Internet kursieren einige Batch-Skripte für die Verbesserung der Privatsphäre unter Windows 10.

Privatsphäre-Einstellungen unter Windows 10 härten – 2/4

BSI-Hinweise

Erster Teilbericht der BSI-Analyse von Windows 10 in Version 1607, 64 Bit, deutsche Sprache aus dem Long Term Servicing Channel (LTSC) trägt den Namen Sisyphus Win10.

Sisyphus Win10 ... Studie zu Systemintegrität, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10

Windows 10 sendet genauso wie Office 365 Telemetrie- und Diagnose-Daten an Microsoft-Server. Ein niederländischer Regierungsbericht hat deshalb festgestellt, dass Microsoft Office gegen die DSGVO (Datenschutzgrundverordnung) verstoße.

Das BSI stellte fest, dass Windows 10 die Telemetrie-Daten bei Systemabstürzen, aber auch bei der Nutzung von Windows 10 sammle, nämlich «Daten über die Nutzung des Computers unter Windows 10 und der an ihn angeschlossenen Geräte, Daten über die Performance des Systems, Daten, die bei Fehlern wie Programm- oder Systemabstürzen erhoben werden, sowie Daten des Windows Defenders und des Malicious Software Removal Tools (MSRT)». Diese Daten schickt Windows 10 an Microsoft-Server.

Bis zu 422 sogenannte Event Tracing für Windows-Entitäten (ETW) sammeln diese Daten, wenn Windows 10 diesbezüglich maximal eingestellt ist. In den Mindesteinstellungen sammeln zumindest vier solche Entitäten. Das BSI betont, dass »aufgrund der durchgeführten Analyse sich keine Verbindung zwischen Anzahl an ETW-Anbietern und Telemetrie-Datenmenge sowie deren Qualität ableiten lässt.«

Zwar wird laut BSI über die Telemetrie kein beliebiger Code auf den Windows-10-Rechner ausgeführt. Doch wäre es sicherer, wenn das Telemetrie-Framework komplett entfernt würde, weil damit eine Angriffsmöglichkeit für Hacker ausfalle.

Obwohl die Nutzer unterschiedliche Telemetrie-Level einstellen können, lade Windows **mehrmals pro Stunde** Konfigurationsdaten nach und ordnet der Telemetrie-Dienst die vorhandenen Telemetrie-Quellen diese Level im laufenden Betrieb **dynamisch** zu.

Eine Unterbindung der Erfassung und Übertragung von Telemetrie-Daten durch Windows ist technisch zwar möglich, für den einfachen Anwender allerdings nur schwer umzusetzen.

Selbst die Konfiguration der niedrigstmöglichen Telemetrie-Ebene unterbinde die Datenübertragung nur unvollständig. Das gelte für die in den Enterprise-Versionen von Windows verfügbare Stufe 0 (Security) ebenso, wie für die in den Consumer-Versionen minimal mögliche Stufe 1 (Einfach).

Zudem haben auf dem Rechner installierte Anwendungen wie der Internet Explorer und Microsoft Office die Möglichkeit, auch ohne den zentralen Telemetrie-Dienst des Betriebssystems Telemetrie-Daten zu erfassen und an den Hersteller zu versenden.

Quelle:

<https://www.pcwelt.de/a/bundesamt-fuer-it-sicherheit-bsi-untersucht-sicherheit-von-windows-10,3463082>

Hinweis zu Sisyphus: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat sich auf die Fahnen geschrieben, die sicherheitskritischen Funktionen von Windows 10 einer genauen Analyse zu unterziehen. Das Ziel der Untersuchung ist, die Sicherheit und Restrisiken für eine Nutzung von Windows 10 bewerten zu können. Darüber hinaus sollen Rahmenbedingungen für einen sicheren Einsatz des Betriebssystems identifiziert, sowie Empfehlungen für eine Härtung und den sicheren Einsatz von Windows 10 erstellt werden.

Privatsphäre-Einstellungen unter Windows 10 härten – 3/4

Das BSI hat in der Studie SiSyPHuS Win10 eine einfache Alternative veröffentlicht, um die Privatsphäre mit einem relativ einfachen Eingriff umfangreich zu schützen. Dazu wird der Dienst **DiagTrack**, in der deutschen Version **Benutzererfahrung und Telemetrie im verbundenen Modus**, deaktiviert. Der Dienst verschickt umfangreiche Diagnosen zum PC, die dazu dienen sollen, Windows 10 mit notwendigen Updates zu versorgen. Das sei laut BSI nicht notwendig und wichtige Updates und Systemstabilität sollen durch die Abschaltung des Dienstes nicht eingeschränkt werden.

Dazu wird die **Computerverwaltung** aufgerufen, durch Drücken auf die Windows-Taste **[W] + [X]** und dem wählen des entsprechenden Eintrages. Dort **Dienste und Anwendungen – Dienste** auswählen und **Benutzererfahrung und Telemetrie im verbundenen Modus** doppelt anklicken. Dort dann **Beenden** unter Dienststatus anklicken und anschließend aus der Liste **Starttyp Deaktiviert** auswählen. Das BSI empfiehlt zusätzlich die ETW-Sesssion AutoLogger Diagtrack Listener zu unterdrücken, was aber grundsätzlich nicht notwendig ist, da das Event Tracing durch die Deaktivierung des DiagTracks-Dienstes nicht ausgewertet wird.

ETW kann man in der Registrierdatenbank unter **HKLM\SYSTEM\CurrentControlSet\Control\WMI\Autologger\AutoLogger-Diagtrack-Listener**

abstellen (Adminstratorrechte erforderlich), indem man dort dem Eintrag Start den Wert 0 zuweist.

Bei größeren Windows-Updates können der Dienst **DiagTrack** und **ETW** wieder aktiviert sein und müssen dann erneut deaktiviert werden.

Quelle: <https://42.th2s.de/2019/01/privatsphare-einstellungen-unter.html>

Microsoft Telemetrie Server

Die vom BSI untersuchte Version von Windows 10 sendete Daten an folgende **Microsoft Telemetrie Server**:

oca.telemetry.microsoft.com
alpha.telemetry.microsoft.com
vortex-win-sandbox.data.microsoft.com
eu.vortex-win.data.microsoft.com
us.vortex-win.data.microsoft.com
v10.vortex-win.data.microsoft.com
geo.vortex.data.microsoft.com.akadns.net
v10-win.vortex.data.microsoft.com.akadns.net
db5.vortex.data.microsoft.com.akadns.net
asimov-win.settings.data.microsoft.com.akadns.net
db5.settings-win.data.microsoft.com.akadns.net
settings-win.data.microsoft.com
db5-eap.settings-win.data.microsoft.com.akadns.net
geo.settings-win.data.microsoft.com.akadns.net

Als Schutz gegen die Datensammelwut empfiehlt das BSI, die Verbindungen zu den Windows Telemetrie Servern zu blockieren.

Zukünftige Windows Versionen können weitere oder andere Server nutzen.

Quelle: www.privacy-handbuch.de/handbuch_90a2.htm

Privatsphäre-Einstellungen unter Windows 10 härten – 4/4

Telemetrie – Diagnose-Daten einsehen, löschen:

[W] + [I] -> Datenschutz -> Diagnose und Feedback -> Diagnosedaten ansehen

Die Feedbackhäufigkeit kann dort ebenfalls eingestellt werden.

Anmerkung: Im Internet kursieren einige Batch-Skripte für die Verbesserung der Privatsphäre unter Windows 10.

<https://solariz.de/de/win10-privacy-batch-script-privat.htm>

Telemetrie-Erfassung über die Registry reduzieren:

1. [W] + [R] -> regedit

HKEY_LOCAL_MACHINE -> SOFTWARE -> Policies -> Microsoft -> Windows -> DataCollection

2. DataCollection mit der rechten Maustaste anklicken -> Eintrag "Neu" wählen -> "Neuer DWORD-Wert (32 Bit)" wählen und den Eintrag AllowTelemetry anlegen

3. Auf den Eintrag **AllowTelemetry** doppelklicken und einen Wert eingeben (Ziffern 0-3)

Wert 0: Minimale Daten werden übertragen, dazu zählen, falls in den jeweiligen Anwendungen eingestellt, Malicious Software Removal Tool (MSRT) und Windows Defender. Wert 0 ist nur bei Enterprise- und Education-Systemen möglich.

Wert 1: Zusätzlich zu den Einstellungen von Wert 0 werden einige wenige Diagnosedaten wie Geräte- und Kompatibilitätsinfos übermittelt.

Wert 2: Hier werden zusätzliche Nutzungs- und Performance-Daten von Windows, Windows Server, System Center und von Apps an Microsoft Server gesendet.

Wert 3: Die vollständige Telemetrie-Übermittlung umfasst erweiterte Diagnosedaten, die auch zur Lösung etwaiger Probleme verwendet werden.

Eine vollständige Unterbindung der Erfassung und Übertragung von Telemetriedaten durch Windows sei technisch zwar möglich, für den einfachen Anwender allerdings nur schwer umzusetzen.

Windows 10 Client einer Domäne hinzufügen

Grundlagen – Voraussetzungen

Nicht jede **Windows 10**-Version kann Mitglied einer Domäne werden. Es können nur die **Versionen Pro, Education und Enterprise** einer Domäne hinzugefügt werden. In der Regel hat man in Firmennetzwerken von vorn herein die Enterprise Version.

Windows 10 Client einer Domäne hinzufügen

Das hinzufügen kann auf zwei unterschiedlichen Arten erfolgen! Einmal direkt über die **Systemsteuerung/System** und ein andermal über die **Einstellungen**.

Windows 10 Client über System hinzufügen

Das Menü kann man am schnellsten über die Tastenkombination **[Windows Taste] + [Pause]** erreichen. Anschließend geht man auf »**Einstellungen ändern**« und jetzt erhält man die Möglichkeit unter dem Punkt »**Ändern**« den PC zu einem Mitglied einer Domäne zu machen. Standardmäßig ist der PC in der Arbeitsgruppe

Workgroup. Sobald der PC die Domäne erreichen kann, benötigt man einen **Domänenadministrator Account**. Nur dieser kann den PC zu einem Mitglied einer Domäne machen. In der Regel ist das der Administrator vom Server. Sobald die Eingaben korrekt sind, erhält man einen Willkommensgruß und der PC muss zum Abschluss nur noch neugestartet werden.

Windows 10 Client über Einstellungen hinzufügen

Das neue Menü »**Einstellungen**« bietet ebenfalls den Beitritt in einer Domäne an. Die Optionen hierfür befindet sich im Menü »**System**«. Anschließend öffnet man die »**Info**«-Seite und kann dort den PC einer Domäne hinzufügen. Mit dieser Methode wird das Konto mit dem man den PC der Domäne hinzufügt automatisch als Standardbenutzerkonto für den hinzugefügten PC angelegt.

Der Kontotyp könnte natürlich dort auch geändert werden.

Wenn der PC in einer Domäne Mitglied ist, so findet man diesen auch in der **ActiveDirectory**. In dem Control Panel: **Active Directory Benutzer und Computer** kann man den PC unter der Organisationseinheit Computers wiederfinden.

Windows 10: Anmelden an der Domäne

Für das Anmelden an einer Domäne muss man links unten den Eintrag »**Anderer Benutzer**« (Anmeldung beim Start) auswählen! Anschließend wird sofort angezeigt, dass man sich jetzt an der Domäne anmelden kann. Man benötigt dann nur noch einen Benutzernamen, der in der ActiveDirectory der Domäne bekannt ist.

Lokal am PC anmelden

Möchte man sich wieder lokal am PC anmelden, so muss man dem Benutzernamen (der lokal auf dem PC existiert) den Name des PC's voranstellen.

Fazit

Das Hinzufügen von Clients zu einer Domäne geht in der Regel sehr einfach. Wenn man noch eine strukturierte Vorgehensweise haben möchte, so könnte man die Clients vorab in der **ActiveDirectory** anlegen. Hier würde sich nämlich die Möglichkeit ergeben, dass man den PC gleich einer **Organisationseinheit (OU)** zuordnen kann.

1. Bluetooth in Windows 10 aktivieren:

- Tastenkombination: [W] + [A] - öffnet den »Action-Center« von Windows
- das Bluetooth-Icon und der Zustand des Moduls wird angezeigt
- das Bluetooth-Icon anklicken um Bluetooth an- oder auszuschalten
- Klick mit der rechten Maustaste: ermöglicht den Wechsel zu den Bluetooth-Einstellungen

Alternativ lässt sich Bluetooth auch in den Einstellungen von Windows 10 aktivieren, wo die Geräte auch gleich gekoppelt werden können.

2. Alternative Methode um Bluetooth ein- und auszuschalten und die Geräte miteinander zu verbinden oder zu trennen:

Hinweis: Auf allen beteiligten Geräten muss Bluetooth aktiviert sein.

- Tastenkombination: [W] + [I] öffnet die Windows 10 Einstellungen.
- Kategorie »Geräte« und »Bluetooth- und andere Geräte« wählen
- Schalter: Bluetooth aktivieren oder deaktivieren
- Schalter: »Bluetooth- oder anderes Gerät hinzufügen« und im nächsten Fenster die Option »Bluetooth« wählen. Die Suche nach Bluetooth-Geräten wird gestartet.
- Klick mit der Maustaste auf das gewünschte und gefundene Gerät und anschließend »Verbinden« wählen
- Anschließend muss eventuell noch der angezeigte Sicherheitscode eingetragen werden und auf dem anderen Gerät die Verbindung bestätigt werden.

Das Gerät ist jetzt via Bluetooth mit Windows 10 verbunden und kann bestimmungsgemäß verwendet werden.

2. Bluetooth-Gerät von Windows 10 trennen:

- Tastenkombination: [W] + [I] öffnet die Windows 10 Einstellungen
- Kategorie »Geräte« und »Bluetooth- und andere Geräte« wählen
- Klick mit der Maustaste auf das gewünschte Gerät und anschließend »Gerät entfernen« wählen

Nach der Bestätigung, dass das Gerät wirklich entfernt werden soll, wird es sofort abgekoppelt.

Probleme bei der Bluetooth-Verbindung mit Windows 10:

Bei Probleme mit Bluetooth-Verbindungen, kann folgendes versucht werden:

- Prüfung: Ist Bluetooth am anderen Gerät überhaupt aktiviert ist?
- Prüfung: Ist der Akku am Gerät leer oder zu schwach, um noch eine stabile Verbindung aufbauen zu können?
- Manche Geräte müssen zur Kopplung erst in den »**Pairing-Modus**« versetzt werden.
- Prüfung: Sind in Windows 10 die aktuellen Bluetooth-Treiber installiert?
- Test: Läuft in Windows 10 der Bluetooth-Netzwerkdienst überhaupt?
- Powershell oder CMD mit Administrator-Rechte aufrufen:

net start "bthservv"

Entweder wird der Dienst gestartet oder die Meldung wird angezeigt, dass er bereits läuft.

Windows 10 wiederherstellen:

- Windows 10 Einstellungen öffnen: [W] + [I]
- Kategorie »Update und Sicherheit« -> Kategorie »Wiederherstellung«
- »Diesen PC zurücksetzen« -> Button »Los geht's«
An dieser Stelle kann man entscheiden, ob man die persönlichen Daten behalten oder von der Festplatte entfernen möchte und Windows anschließend neu installieren möchte.
- Nach der Bestätigung des Vorgangs, wird Windows 10 komplett wiederhergestellt.

Je nach gewählter Variante und Größe der Festplatte kann dieser Vorgang einige Minuten bis Stunden in Anspruch nehmen.

Backup-Programme:

Ashampoo Backup: Mit "Ashampoo Backup" erstellt man unkompliziert Sicherungs-Dateien des Systems und von Partitionen für den Notfall. Einige Versionen kann man auch kostenlos als Download bekommen.

Paragon Backup & Recovery: Die abgespeckte Version gibt es gratis als Download. Mit "Paragon Backup & Recovery" kann man ganze Festplatten (mit Bootbereich) und Partitionen oder einzelne Dateien sichern. Neue Festplatten können verschiedene Größen und Konfiguration haben - die Partitionsgröße wird an der Größe der Festplatte beim Kopieren angepasst.

Betriebssystem per ISO-Datei wiederherstellen:

Startet der PC nicht mehr oder er läuft nicht mehr stabil, so kann man die ISO-Datei für Windows 10 auf einem anderen Computer herunterladen und per USB-Stick auf den defekten PC übertragen.

- Das **Media Creation Tool** für Windows 10 herunterladen und starten.
- Option »Installationsmedien für einen anderen PC erstellen« auswählen
- Auswahlmöglichkeit: »USB-Stick« oder »ISO-Datei«
- Anschließend startet der Download von Windows 10.
- Die ISO-Datei ist einfach per Doppelklick im laufenden Betrieb zu starten.
- Der USB-Stick mit der ISO-Datei in den zu wiederherzustellenden Rechner stecken und den Rechner starten.
- Die Boot-Reihenfolge im BIOS ist gegebenenfalls zu ändern oder beim Rechnerstart mit der entsprechen Taste das Bootmenü aufrufen (siehe: Bedienungsanleitung).

E-Mail-Konto einrichten:

Bevor man das Exchange-Konto in Outlook konfigurieren kann, muss zunächst in Outlook ein Profil mit dem E-Mail-Konto konfiguriert werden.

Bitte wie folgt vorgehen:

- anmelden am Windows 10 Computer
- mit [W] +[I] die Windows 10 Einstellungen öffnen
- Kategorie »Konten« -> »E-Mail & Konten« -> Konto hinzufügen
- Option »Exchange - Exchange, Office 365« wählen und die E-Mail-Adresse eingeben
- Das System stellt selbstständig die Verbindung zum Exchange-Server her, meldet den E-Mail-Benutzer an und erstellt das Exchange-Konto.
- Vorgang mit »Fertig« abschließen.

Hinweis: Es gibt noch die Möglichkeit des »Erweitertes Setup« (nach unten scrollen).

Erster Start von Outlook:

- Sobald die Konfiguration abgeschlossen ist, kann Outlook gestartet werden.
- Beim erstmaligen Öffnen von Outlook nach der Konfiguration des Exchange-Kontos wird eine lokale Kopie (namens .ost) des serverbasierten Exchange-Postfachs des Benutzers erstellt.
- Dieser Vorgang kann, abhängig von der Größe Ihres Postfachs, mehrere Minuten dauern und sollte nicht unterbrochen werden, damit ein vollständiges und aktuelles Abbild Ihres Postfach-Ist-Zustandes erstellt werden kann.

GMX.de oder WEB.de

Wenn Sie versuchen, Ihr GMX.de- oder WEB.de-Konto mit den Mail- und Kalender-Apps zu verbinden, erhalten Sie in Ihrem GMX.de- bzw. WEB.de-Postfach eine E-Mail mit Anweisungen zum Aktivieren des Zugriffs.

- Melden Sie sich in einem Webbrowser bei Ihrem GMX.de- bzw. WEB.de-Konto an.
- Suchen Sie die E-Mail-Nachricht mit Anweisungen zum Herstellen einer Verbindung zwischen Ihrem Konto und den Mail- und Kalender-Apps und folgen Sie den Anweisungen.
- Ihr Konto sollte jetzt mit den Mail- und Kalender-Apps automatisch synchronisiert werden.

Weitere Infos - Outlook Exchange und Outlook:

<https://support.office.com/de-de/article/grundlegenden-einstellungen-f%C3%BCr-exchange-konten-dd0bb323-e21f-4432-9136-76ff42ec178a>

https://all-inkl.com/wichtig/anleitungen/programme/e-mail/windows-10-app/e-mail-konto-einrichten_408.html

<https://support.office.com/de-de/article/hinzuf%C3%BCgen-eines-e-mail-kontos-zu-outlook-e9da47c4-9b89-4b49-b945-a204aeea6726>

Der Fernzugriff auf Windows per RDP (Remote Desktop Protocol) ist seit vielen Jahren ein Standard-Feature, das sich in der Version 10 in einigen Punkten verändert hat. Standardmäßig ist das Remotedesktop-Feature deaktiviert, so dass man es auf einem Rechner erst konfigurieren muss, um Zugriff zu erhalten.

Per Voreinstellung können alle Benutzer, die Mitglied der Administratoren sind (lokal oder in der Domäne), eine Remotedesktop-Verbindung zu einem Rechner aufbauen, nachdem diese aktiviert ist. Sollen auch andere User in den Genuss dieses Features kommen, muss man sie erst in die lokale Gruppe Remote-Desktopbenutzer aufnehmen.

Auf PCs, die Mitglied einer Domäne sind, lässt sich das Remotedesktop-Feature über Gruppenrichtlinien aktivieren, die Einstellungen und das Vorgehen ähnelt der Vorgehensweise wie unter Windows 7. Alternativ bietet sich noch an, den RDP-Zugriff **remote** über WMI oder der PowerShell zu aktivieren.

[W] + [I] -> System -> Remotedesktop -> Remotedesktop aktivieren (Administratorrechte erforderlich, siehe auch: Erweiterte Einstellungen)

[W] + [I] -> Update und Sicherheit -> Für Entwickler -> Remotedesktop (Administratorrechte erforderlich)

[W] + [Pause] -> Remoteeinstellungen (Administratorrechte erforderlich) -> Einstellungen anzeigen

mstsc.exe

Mit dem grafischen Tool mstsc.exe (**Aufruf:** [W] + [R] -> CMD -> mstsc.exe) kann eine Remote-Verbindung zu einem anderen Rechner aufgebaut werden.

Hinweise zu Lexware

Installation von Lexware-Updates:

Bei Updates von CD oder über einen Internet-Link (Übermittlung per Email), sollte man mindestens eine Woche warten (Internet-Recherche, Hilfeseiten von Lexware). Die Internet-Webseiten mit Update- und Fehlerhinweise von Lexware sind in der Regel gut lesbar.

Bei einem Lexware-Update übers Internet auf mehreren Rechner gleichzeitig kann die verfügbare Netzwerk-Bandbreite drastisch einbrechen. Windows 10 scheint die drastische Reduzierung der Bandbreite zu bemerken und erforscht sie daraufhin. Dadurch kann die reduzierte Bandbreite bis zu 2 oder mehr Tagen erhalten bleiben.

Datensätze suchen:

Lexware-Journal – zeitlich sortierte Datensätze

»Hauptnavigation [F10]« -> »Buchhaltung« -> »Journal«

Backup:

Nach einer Standardinstallation, wird alle 7 Tage, durch die ordentliche Beendigung des Programms (»Datei« -> »Beenden«) automatisch ein Backup erstellt.

Manuelle Sicherung: »Datei« -> »Datensicherung« -> »Sicherung ...« und den Anweisungen folgen

Speicherort und Dateiname (Lexware Professional): Dieser PC/Dokumente/LxOffice[JahrMonatTag]_[StundeMinuteSekunde].zip

Hinweis: Backup-Dateien die nicht mehr benötigt werden, können nur manuell gelöscht werden. Sicherungsdateien des Jahresabschlusses sollten unbedingt 10 Jahre aufbewahrt werden.

Sicherungsmethoden: Gesamtsicherung, Firmensicherung oder Sicherung nur der Formulare (z.B. einheitliche Formulare auf jeden Rechner)

Sicherungsverlauf: »Datei« -> »Datensicherung« -> »Sicherungsverlauf«

Manuelle Rücksicherung: »Datei« -> »Datensicherung« ->

»Rücksicherung« und den Anweisungen folgen

Durch die Rücksicherung werden immer **alle** vorhandenen Daten überschrieben.

Änderung der Backupzyklen: »Datei« ->

»Datensicherung« -> »Regelmäßige Sicherung« oder :

»Extra« -> »Optionen ...« -> »Allgemein« [...]

Weitere Hinweise:

- **Andere ZIP-Programme:** Andere Packprogramme sollten während der Sicherung oder Rücksicherung der Daten nicht aktiv sein, da sonst Fehler auftreten können.
- **Fehlende Zugriffsrechte:** Bei der Installation werden andere als die Standardpfade ausgewählt. Hier ist immer zu gewährleisten, dass auch die benötigten Zugriffsrechte (Lese-, Schreib-, Löschrechte...) für den entsprechenden (Daten-)Ordner vorhanden sind.
- Die Datensicherungen sollten auf einer anderen Partition, entfernten Server oder auf externe Datenträger gespeichert werden.
- Eine **Rücksicherung von einem USB-Stick** ist allerdings nicht möglich. Hier muss die entsprechende Sicherungsdatei zuerst auf die Festplatte kopiert und von dort rückgesichert werden.
- **Datenrettung:** Im besten Fall befinden sich die gelöschten Daten noch völlig unversehrt im Papierkorb Ihres Rechners, von wo aus sie **mit einem einfachen Mausklick wiederhergestellt** werden können.
- Vor notwendigen Experimenten immer eine Gesamtsicherung, vollständiges Backup (Programm, Daten oder gesamte Partition) erstellen.

Programm: testdisk 1/4

Hinweis: TestDisk muss mit »Administratorberechtigungen« ausgeführt werden.

- Die Navigation in TestDisk erfolgt ausschließlich über die Pfeil- und Bildlauf Tasten!
- Um fortzufahren, ist die Auswahl mit der Eingabetaste zu bestätigen.
- Um zur vorherigen Anzeige zurückzukommen oder TestDisk zu beenden, ist die **q** (Quit)-Taste zu benutzen.
- Um Änderungen unter TestDisk zu speichern, ist die Auswahl mit **y** für (Ja) und/oder über die **Eingabetaste** zu bestätigen.
- Um tatsächlich Partitionsdaten in den MBR (Master Boot Record) zu schreiben, ist das **Menü "Write"** auszuwählen und die Auswahl mit der Eingabetaste zu bestätigen.

Das TestDisk-Programm ausführen: Wenn TestDisk noch nicht installiert ist, kann es aus dem Internet heruntergeladen werden. Die Dateien vom Archiv sind zu extrahieren, einschließlich der Unterverzeichnisse.

Um Dateien von einer Festplatte, USB-Stick oder Smartcard, usw. wiederherzustellen, werden entsprechende Rechte vorausgesetzt, um auf die Datenträger zugreifen zu können.

- Unter Windows, starte TestDisk (ins Verzeichnis mit dem TestDisk-Programm wechseln und die Datei aufrufen) von einem Konto in der Administrator-Gruppe. Unter Windows 10, führe einen Rechtsklick aus und rufe die Datei mit **"als Administrator ausführen"** auf.
- Unter Unix/Linux/BSD, muss TestDisk als root ausgeführt werden (ins Verzeichnis mit dem TestDisk-Programm wechseln und die Datei mit sudo »Programmname« aufrufen).

Um ein Dateisystem-Image zu reparieren, führe folgendes aus:

- Rufe **testdisk image.dd** auf, um ein RAW-Laufwerks-Image zu schneiden.
- Rufe **testdisk image.E01** auf, um Dateien von einem Encase EWF-Image wiederherzustellen.
- Rufe **testdisk 'image.E??'** auf, wenn das Encase-Image in mehrere Dateien aufgesplittet wurde.
- Um ein Dateisystem, das nicht in TestDisk gelistet ist zu reparieren, führe **testdisk device** aus.
- Rufe **testdisk /dev/mapper/truecrypt0** auf, um NTFS oder FAT32 Bootsektor-Dateien von einer TrueCrypt-Partition zu reparieren. Dieselbe Methode funktioniert auch mit einem Dateisystem, das mit cryptsetup/dm-crypt/LUKS verschlüsselt wurde.
- Rufe **testdisk /dev/md0** auf, um ein Dateisystem zu reparieren, das auf einem Linux Raid-Laufwerk liegt.

Programm: testdisk 2/4

Um eine Partition von einem Datenträger wiederherzustellen führe folgendes aus:

1. Log-Datei erstellen

- Wähle **Create**, es sei denn es gibt einen Grund um Daten an einer existierenden Log-Datei anzuhängen, oder wenn TestDisk von einem Read Only (nur-lesen)-Datenträger ausgeführt wird und nicht gespeichert werden kann.
- Bestätige mit der Eingabetaste.

2. Festplatten-Auswahl

- Alle Festplatten sollten entdeckt und in TestDisk mit der korrekten Größe gelistet sein.
- Benutze die Pfeil- nach oben/unten-Tasten um die Festplatte mit der/n verlorenen Partiton/en auszuwählen.
- Bestätige mit der Eingabetaste.

3. Auswahl des Partitionstabellen-Typs

- TestDisk zeigt die Partitionstabellen-Typen an.
- Wähle den entsprechenden Partitionstabellen-Typ aus, normalerweise ist der Standard-Wert der richtige, da TestDisk den Partitionstabellen-Typ automatisch ermittelt.
- Bestätige mit der Eingabetaste.

4. Gegenwärtiger Partitionstabellen-Status

- TestDisk zeigt die entsprechenden Menüs an.
- Verwende das Standardmenü "**Analyse**", um die gegenwärtige Partitionsstruktur zu untersuchen und um nach verlorenen Partitionen zu suchen.
- Bestätige bei der Auswahl **Analyse** mit der Eingabetaste, um fortzufahren.
- Jetzt wird die gegenwärtige Partitionsstruktur gelistet.

5. Überprüfe deine jetzige Partitionsstruktur auf verlorene Partitionen und Fehler

- Falls eine Partition zweimal gelistet ist, deutet dies auf eine korrupte Partition oder einen ungültigen Partitionstabelleneintrag hin.
- **Invalid NTFS boot** (ungültiges NTFS Boot) weist auf einen fehlerhaften Bootsektor und ein korruptes Dateisystem hin.
- Falls nur eine logische Partition (Label: Partition 2) in der erweiterten Partition verfügbar ist, könnte evtl. eine logische Partition fehlen.
- Bestätige bei Quick Search mit der Eingabetaste, um fortzufahren.

6. Die schnelle Suche "Quick Search" für Partitionen

- Bei der Quick Search-Suche kann man mit **y** für **ja** die Suche nach Partitionen starten oder mit **n** für **nein** die Suche beenden.
- TestDisk zeigt bei der Quick Search-Suche die ersten Ergebnisse in Echtzeit an.
- **Beispiel**: Während der Quick Search-Suche (schnelle Suche) findet TestDisk zwei Partitionen, einschließlich der vermissten Partition mit der Bezeichnung Partition 3.
- Markiere die Partition und drücke **p** um die Dateien zu listen (um zur vorigen Anzeige zurückzukommen, drücke **q** für Quit).
- Werden alle Verzeichnisse und Daten korrekt angezeigt, ist die Eingabetaste zu betätigen, um fortzufahren.

Programm: testdisk 3/4

7. Die Partitionstabelle abspeichern oder weitere Partitionen suchen?

- Wenn alle Partitionen bereits vorhanden sind und die Daten korrekt angezeigt wurden, kann man gleich zum **Menü Write** gehen und die Partitionsstruktur sichern. Das **Menü Extd Part** gibt eine die Möglichkeit zu entscheiden, ob die erweiterte Partition den gesamten verfügbaren oder nur den erforderlichen (minimalen) Speicherplatz benutzen darf.
- Falls die erste oder eine andere Partition immer noch vermisst wird, kann man über das **Menü Deeper Search** (tiefere Suche) eine erweiterte Suche starten (mit der Eingabetaste bestätigen um fortzufahren).

8. Fehlt immer noch eine Partition, so wird Deeper Search (tiefere Suche) erforderlich

- Deeper Search sucht nach weiteren Partitionen. Bei dieser Suche wird jeder einzelne Cylinder des Datenspeichers gescannt.
- Nach der tieferen Suche "Deeper Search", werden die Ergebnisse angezeigt.
- **Beispiel:** Die erste Partition **Partition 1** wurde anhand des Backups vom Bootsektor gefunden. Dieses wird auch ganz unten in der Anzeige in der letzten Zeile mit der Meldung **NTFS found using backup sector!**, -> (NTFS unter Verwendung des Backup vom Bootsektor gefunden) und der Größe der Partition angezeigt.
- Die Partition muss dabei markiert sein.
- **Beispiel:** Die Partition 2 wird zweimal mit unterschiedlicher Größe angezeigt.
- Beide Partitionen werden mit dem Status **D** für **deleted** (gelöscht) dargestellt, da sie sich überlappen.

- Markiere die erste Partition 2 und drücke **p** um die Daten anzuzeigen.
- **Beispiel:** Das Dateisystem der oberen Partition (Name: Partition 2) ist beschädigt (damaged file system).
- Drücke **q** für **Quit** um zur vorigen Anzeige zurück zu gelangen.
- **Beispiel:** Belasse die Partition 2 mit dem beschädigten Dateisystem als **D** (für gelöscht) markiert.
- Markiere die zweite Partition 2 darunter und Drücke **p** um die Dateien aufzulisten.

Es funktioniert, die korrekte Partition wurde gefunden!

- Benutze die Links/Rechts-Pfeiltasten um im Ordner zu navigieren und die Daten auf ihre Richtigkeit zu überprüfen.
- **Beachte:** Bei FAT ist der Verzeichniseintrag auf 10 Cluster beschränkt, einige Dateien werden deshalb nicht erscheinen, es beeinflusst aber nicht die Wiederherstellung.
- Drücke **q** für Quit um zur vorigen Anzeige zurück zu gelangen.
- Verfügbarer Status sind Primär, * (Stern) bootfähig, Logisch und D für deleted (gelöscht).
- Benutze die Links/Rechts-Pfeiltasten, um den Status der ausgewählten Partition auf **L(logical)** (für logisches Laufwerk) zu setzen.

Hinweis: Wie erkenne ich eine primäre Partition oder ein logisches Laufwerk? -> siehe nachfolgende Seite

Programm: testdisk 4/4

- **Beachte:** Wenn eine Partition als * (Stern für bootfähig) angezeigt wird, und von dieser Partition nicht gebootet wird, kann diese Partition auf **P** für primär gesetzt werden.
- Bestätige mit der Eingabetaste um fortzufahren.

9. Partitionstabellen-Wiederherstellung

- Es ist jetzt möglich, die neue Partitionsstruktur zu schreiben.
- **Beachte:** Die erweiterte Partition (E extended LBA) ist hier automatisch gesetzt. TestDisk erkennt dieses anhand der unterschiedlichen Partitionsstruktur.
- Bestätige bei **Write** mit **y** und der Eingabetaste.
- Jetzt sind alle Partitionen in der Partitionstabelle registriert.

10. Wiederherstellung des NTFS-Bootsektors

- **Beispiel:** Der Bootsektor der ersten Partition mit den Namen Partition 1 ist noch beschädigt. Es ist Zeit, dies in Ordnung zu bringen. Der Status des NTFS-Bootsektors ist bad (schlecht) und das Backup vom Bootsektor (backup boot sector Ok) wird gültig angezeigt. Auch sind beide Sektoren nicht identisch (sectors are not identical).
- Um das Backup des Bootsektors über den Bootsektor zu kopieren, wähle **Backup BS** aus, bestätige mit der Eingabetaste, bestätige weiter mit **y** und wiederum mit der Eingabetaste.
- Der Bootsektor und das Backup vom Bootsektor sind nun beide wiederhergestellt (OK) und identisch (identical): der NTFS-Bootsektor wurde erfolgreich wiederhergestellt.
- Bestätige bei Quit mit der Eingabetaste.
- Bestätige wiederum mit der Eingabetaste und beende Testdisk mit **q** für Quit.
- **Beachte:** Um auf die Daten wieder zugreifen zu können, ist ein Neustart des Rechners erforderlich.

11. Wiederherstellung gelöschter Dateien

TestDisk kann:

- Dateien und Ordner von FAT12, FAT16 und FAT32-Dateisystemen wiederherstellen,
- Dateien von ext2-Dateisysteme wiederherstellen, Dateien von einer NTFS-Partition wiederherstellen (seit Version 6.11).
- Wenn es für andere Dateisysteme nicht funktioniert, kann man mit PhotoRec, ein auf Signaturen basierendes Dateiwiederherstellungs-Hilfsprogramm, einen letzten Versuch starten.

Version: TestDisk & PhotoRec 7.0 (18 April 2015), Data Recovery (Stand: Februar 2019)

Quelle:

https://www.cgsecurity.org/wiki/TestDisk_Download
https://www.cgsecurity.org/wiki/Schritt_f%C3%BCr_Schritt_Wiederherstellungsbeispiel

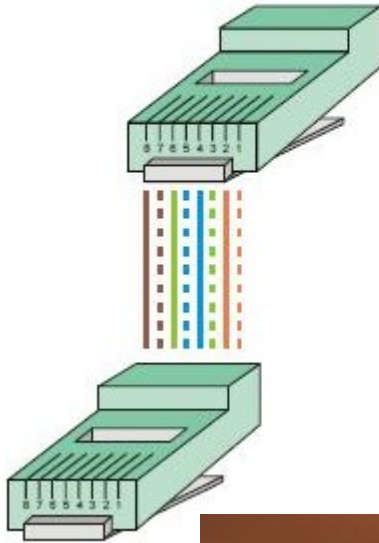
Hinweis:

»Recuva« ist ein weiteres Tool für die Wiederherstellung von gelöschten Dateien.

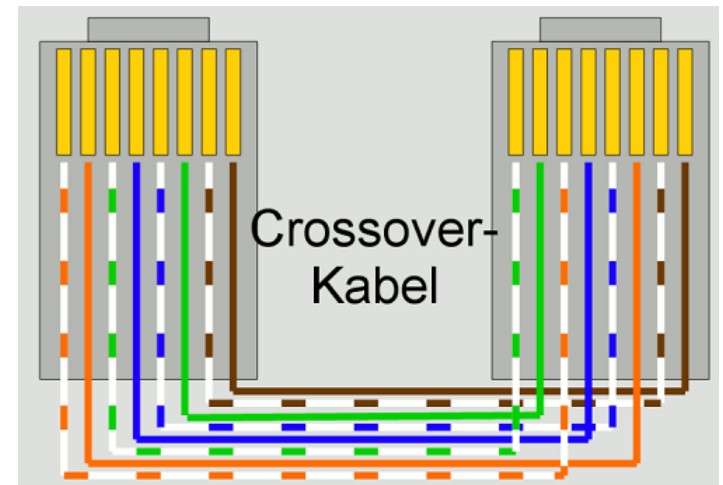
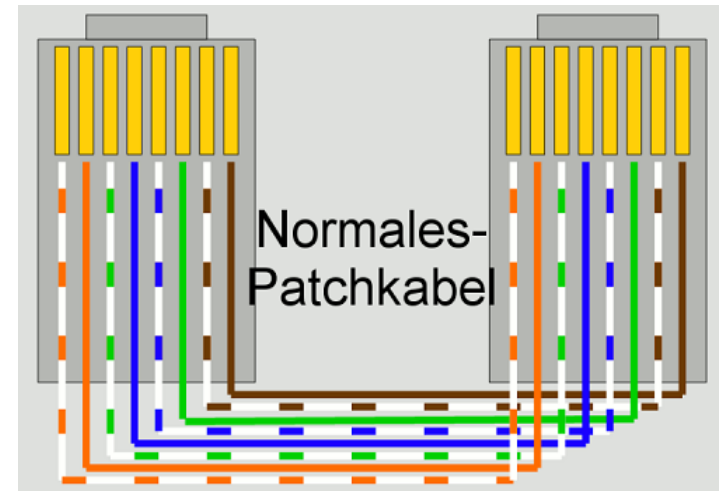
Netzwerkkabel: Anschlussbelegung

Pinnbelegung

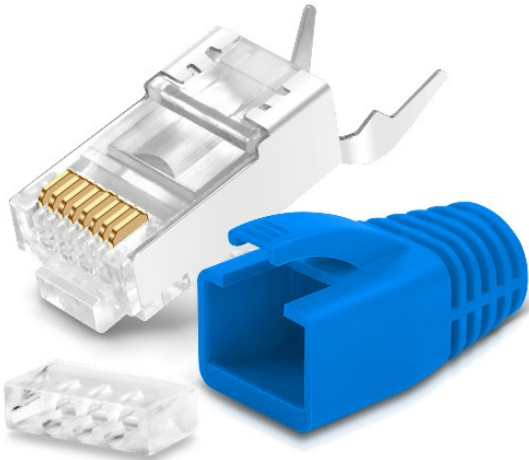
Patch - Kabel



1	Orange	1
2	Orange	2
3	Green	3
4	Blue	4
5	Blue	5
6	Green	6
7	Brown	7
8	Brown	8



Netzwerk-Verbindungen



**Netzwerkstecker RJ45
CAT5 mit Einfädelhilfe**



**Netzwerkstecker RJ45
CAT6A**

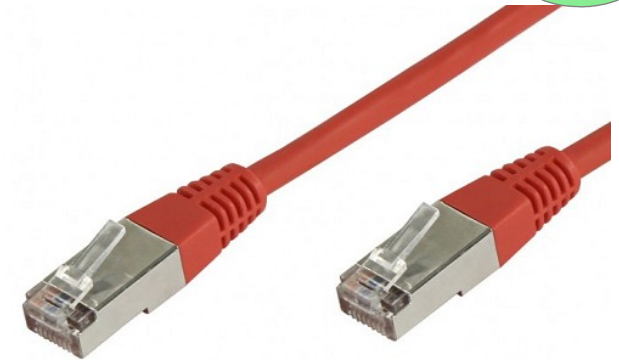
Der RJ45-Stecker behauptet sich schon seit mehr als 30 Jahren als der Allround-Stecker für Datenübertragungs-Systeme. Er hat eine sehr kompakte Bauform und bietet 8 Kontakte und eine Schirmung. Bei Standard RJ45-Steckern werden Kabel mittels der Piercing-Kontakttechnik (Kontaktmesser) unter Einsatz einer sogenannten Crimpzange angeschlossen.

In der zukünftigen Norm DIN EN IEC 60603-7-51 werden Bauarten für geschirmte freie und feste Steckverbinder für Datenübertragungsraten bis 500 MHz spezifiziert. Diese Übertragungsraten können mit einem RJ45 nur unter optimalen Bedingungen erreicht werden.

Das heißt alle Kontakte müssen sicher hergestellt und die Verluste durch Reflexionen, Einfüge-Dämpfung und Übersprechen minimiert sein. Der RJ45 Stecker hat noch lange nicht ausgedient.



**Netzwerkadapter RJ45 CAT6
zur Verlängerung von 2
Patchkabel**



**Patchkabel CAT5e
rot**



**Patchkabel CAT6
blau**

Die Beschaltung aller 8 Adern (4 Adernpaare) macht erst die volle Nutzung der Leistungsfähigkeit heutiger Kabel (CAT6 und CAT7) möglich. Um dem Bedarf an höherer Datentransferleistung von bis zu 10 GBit zu genügen, wurde die Geometrie der Adernkontaktierung optimiert. Im Stecker integrierte induktive und kapazitive Kompensationen gleichen unerwünschten Kopplungen, die bei den geforderten Frequenzen von bis zu 500 MHz vermehrt auftreten, aus und stellen die idealen symmetrischen Bedingungen für die Signalübertragung her.

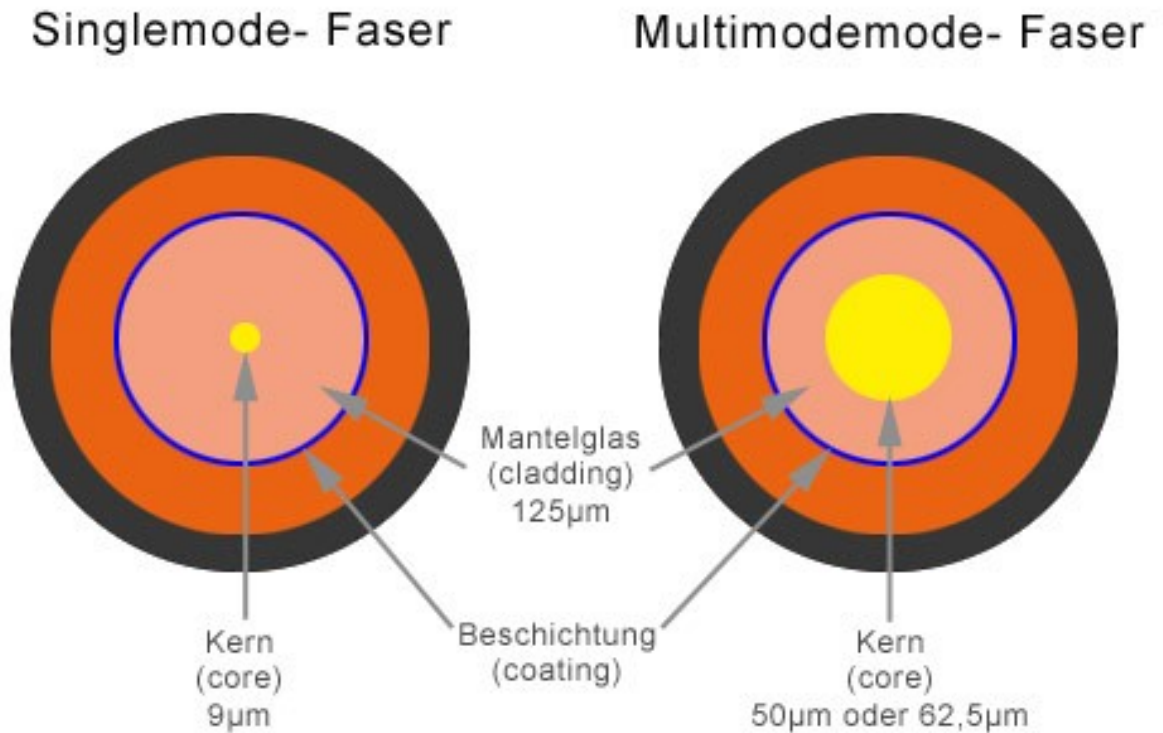
Verbinder für Lichtwellenleiter (LWL) 1/7

Glasfaserkabel sind in der Netzwerk- und Telekommunikationstechnik ein weit verbreiteter Kabeltyp. Im Vergleich zu herkömmlichen Kupferkabeln bieten sie wesentlich höhere Übertragungsraten und Reichweiten. Während auf Kupferdrähten die Informationen mithilfe elektrischer Signale und wandernden Elektronen übertragen werden, übernehmen beim Glasfaserkabel Lichtteilchen (Photonen) die Informationsübermittlung. Lichtwellenleiter erlauben die Überbrückung großer Entfernungen ohne Verstärker und unterstützen gleichzeitig hohe Bandbreiten. Beim Einsatz der Glasfaserkabel gilt es zu berücksichtigen, dass eine Vielzahl verschiedener Fasertypen mit unterschiedlichen Übertragungseigenschaften existieren.

Die Informationsübertragung mittels Lichtausbreitung im Kabel basiert auf dem Prinzip der Totalreflexion. Die Fasern besitzen einen Faserkern und einen umgebenden Fasermantel mit unterschiedlichen optischen Eigenschaften. Der Kern hat einen etwas höheren Brechungsindex als der Mantel.

Die verschiedenen Glasfasertypen unterscheiden sich vor allem durch den Durchmesser von Kern und Mantel (Singlemode- oder Multimodefasern) und durch den Verlauf des Brechungsindex (Stufenindex- oder Gradientenindexfasern).

Singlemode LWL-Kabel haben einen erheblich geringeren Faserkerndurchmesser als Multimode Kabel. Der Faserkern bei Singlemodekabeln hat einen Durchmesser von $9\mu\text{m}$, im Unterschied zu Multimodekabel, welche einen Faserkern von $50\mu\text{m}$ bzw. $62,5\mu\text{m}$ Durchmesser besitzen. Das umgebende Mantelglas weist jeweils einen Durchmesser von $125\mu\text{m}$ auf.



Verbinder für Lichtwellenleiter (LWL) 2/7

Lichtausbreitung im Glasfaser

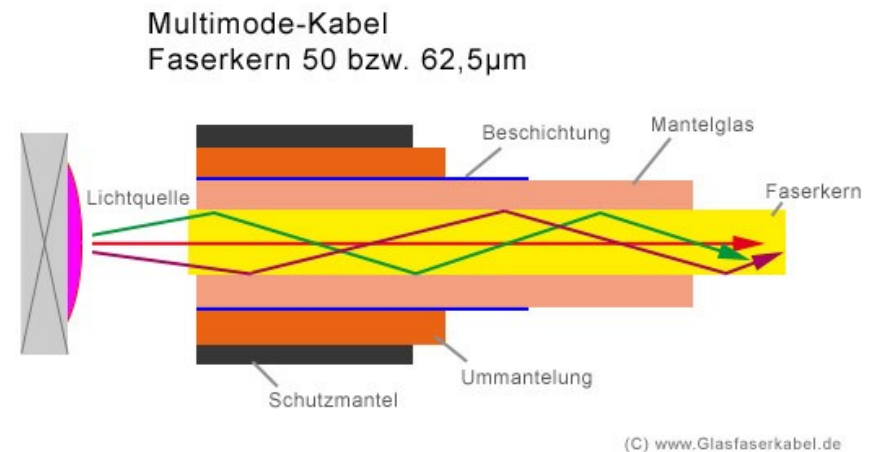
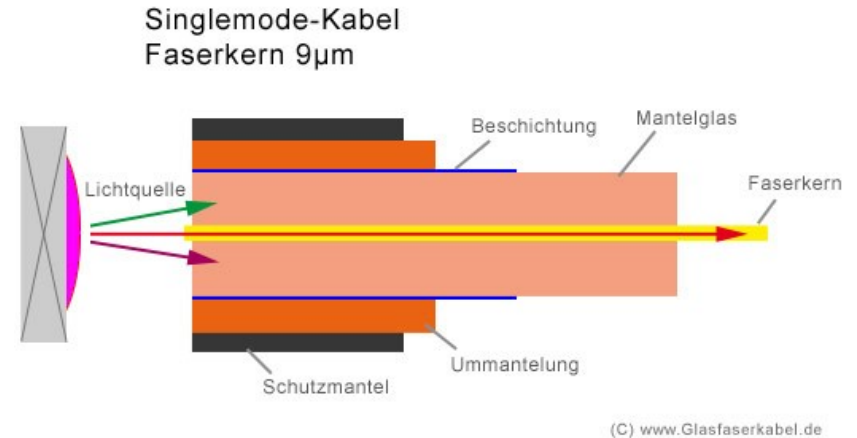
Die folgenden Grafiken verdeutlichen die Lichtausbreitung im Glasfaserkabel. In der schematischen Darstellung ist der Unterschied zwischen Singlemode und Multimode erkennbar. Im größeren Faserkern von Multimodekabel kann das Licht sich anders ausbreiten als in der Singlemodefaser mit einem Faserkern von nur 9µm Durchmesser.

Wichtige Fachbegriffe rund um die Glasfaser

Der **Brechungsindex** ist ein Maß für die optische Dichte eines Materials und gibt das Verhältnis der Lichtgeschwindigkeit in einem optischen Medium im Vergleich zum Vakuum wieder. Je höher der Brechungsindex ist, desto optisch dichter ist das Medium. An den Grenzen zweier optischer Medien mit unterschiedlichem Brechungsindex kommt es zur Brechung oder Reflexion des Lichts.

Bei **Moden** handelt es sich um verschiedene Ausbreitungsarten des Lichtes innerhalb einer Glasfaser. Multimode-Fasern unterstützen viele Ausbreitungsarten, eine Monomode-Faser nur eine einzige.

Die **Dispersion** sorgt dafür, dass ein in eine Glasfaser eingespeister Impuls über seinen Weg der Ausbreitung zeitlich immer breiter wird. Dies kann zu Überlappungen mit nachfolgenden Impulsen führen und Übertragungsfehler verursachen. Laserdioden erzeugen Impulse von wenigen Nanometern Breite und minimieren die Auswirkungen des Effekts bei hohen Bandbreiten.



Verbinder für Lichtwellenleiter (LWL) 3/7

Anwendungsbereiche: Singlemode-Glasfasern

Singlemode-Glasfaser kommen immer dann zum Einsatz, wenn große Distanzen zu überbrücken sind oder besonders hohe Datenraten erzielt werden sollen. Sie verursachen ein Minimum an Übertragungsfehlern und Interferenzen selbst bei Übertragungsstrecken von mehreren Kilometern.

Auch als Patchkabel werden Singlemode-Glasfasern immer beliebter, da sie dem ständig wachsenden Bandbreitenbedarf gerecht werden, ohne die maximal möglichen Linklängen zu reduzieren.

Vorteile:

- geringe Dämpfung des Signals
- kaum Laufzeitverschiebungen
- große Distanzen überbrückbar
- hohe Bandbreiten

Nachteile:

- teurere Laser zur Einspeisung des Lichts notwendig
- größerer Aufwand bei der Herstellung der Glasfasern aufgrund der sehr kleinen Faserkerne
- hohe Präzision beim Verbinden der Glasfasern durch Stecker oder Spleißen notwendig

Anwendungsbereiche: Multimode-Glasfaser

Im Vergleich zu den Singlemode-Fasern ist der Kerndurchmesser bei den Multimode-Fasern wesentlich größer. Er beträgt in der Regel 50 µm und erlaubt die Ausbreitung mehrerer Lichtmoden. Aufgrund der verschiedenen Ausbreitungsmoden sind die Signaldämpfung und die Laufzeitverschiebung größer.

Je höher die Datenrate, desto geringer ist die maximal mögliche überbrückbare Distanz. Daher eignen sich die Fasern eher für Verbindungen über kurze Distanzen, wie sie in einem LAN auftreten. Dank der größeren Kerndurchmesser sind Verbindungen zwischen einzelnen Multimode-Fasern oder zwischen Multimode-Fasern und dem weiteren Equipment mit weniger Aufwand herzustellen.

Typische Einsatzbereiche von Glasfaserkabel mit Stufenindexprofil sind Verbindungskabel im Nahbereich, wie sie beispielsweise in Patchfeldern zum Einsatz kommen.

Glasfaserkabel mit Gradientenindexprofil besitzen bessere Übertragungseigenschaften und sind für etwas größere Distanzen, wie für Verbindungen von Switchen und anderen Netzwerkkomponenten im Gebäude- oder Etagenbereich nutzbar. Übliche Übertragungsraten der Multimode-Glasfaserkabel sind bis zu zehn oder hundert Gigabit pro Sekunde.

Vorteile:

- geringerer Aufwand in der Herstellung der Glasfasern
- einfachere Verbindungstechnik aufgrund des größeren Kerndurchmessers
- Fasern mit Stufenindex- und Gradientenindexprofil verfügbar

Nachteile:

- größere Signaldämpfung und Laufzeitverschiebung
- geringere maximale Bandbreiten
- kürzere Distanzen überbrückbar
- Verstärker oder Signalaufbereiter sind bei größeren Distanzen erforderlich

Verbinder für Lichtwellenleiter (LWL) 4/7

Sind Singlemode- und Multimode-Glasfaserkabel untereinander kompatibel?

Grundsätzlich sind Singlemode- und Multimodekabel nicht miteinander kompatibel. Sie lassen sich schon alleine aufgrund ihrer verschiedenen Kerndurchmesser nicht miteinander verbinden. Selbst wenn ein geringer Teil des Lichtsignals am Übergang in das andere Kabel eingespeist werden kann, treten extrem hohe Dämpfungen und unvorhersehbare Effekte auf, die keine zuverlässige Signalübertragung mehr zulassen.

Innerhalb einer kompletten Netzwerkinstallation sind selbstverständlich verschiedene Glasfaserkabeltypen einsetzbar. So können beispielsweise für die Verbindungen am Patchfeld Multimode-Glasfasern mit Stufenindexprofil, für die Verbindung von Switchen im Etagenbereich Multimode-Glasfasern mit Gradientenindexprofil und für die Realisierung des Campus-Backbones Singlemode-Glasfasern verwendet werden. Sollen Übergänge zwischen kupferbasierter Verkabelung und Glasfasern hergestellt werden, sind geeignete Medienkonverter zu installieren.

Wissenswertes zu Multimode- und Singlemode-Glasfaserkabeln

Sowohl Singlemode- als auch Multimode-Glasfasern sind als sogenannte Mehrfaser-LWL-Kabel erhältlich. Diese Kabeltypen bündeln mehrere einzelne Fasern in einem Gesamtkabel. Mögliche Faserzahlen sind beispielsweise vier, acht, zwölf, 24 oder 48 Fasern. Um zukünftige Anforderungen an die Übertragungskapazität des Glasfaserkabels flexibel und ohne zusätzliche Installationsarbeiten abzudecken, werden meist Kabel mit einer größeren Anzahl an Reserveadern verlegt.

Werden Glasfaserverbindungen über Stecker miteinander verbunden, ist auf eine möglichst geringe Signaldämpfung an den Steckerübergängen zu achten.

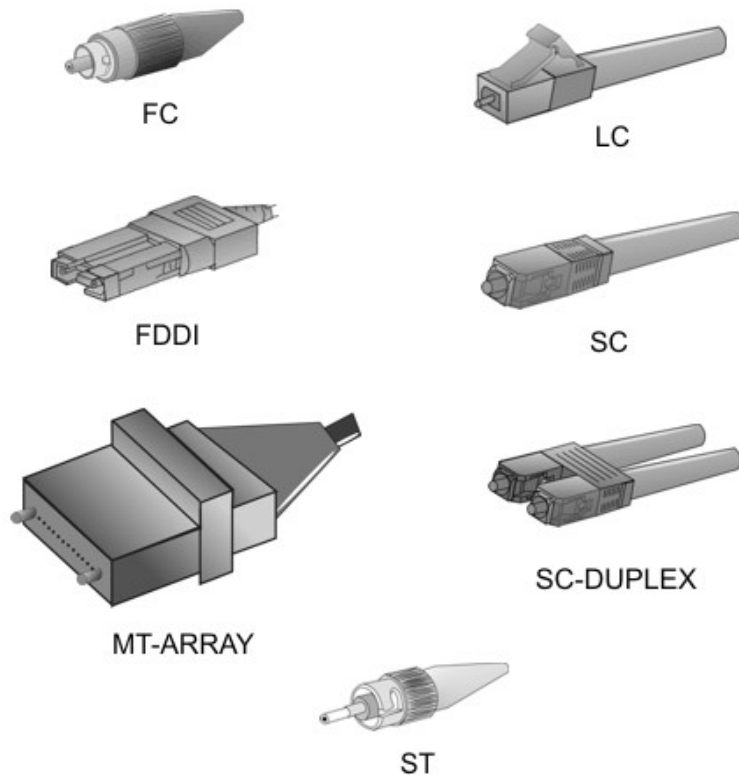
Im Bereich der modernen Glasfasertechnik kommen für die verschiedenen Kabeltypen unterschiedliche Steckverbindungen zum Einsatz. Typische Stecker sind **LC-Stecker**, **SC-Stecker**, **ST-Stecker**, **FC-Stecker**, **DIN-Stecker** oder **E2000-Stecker**.

Eine dauerhafte Verbindung zwischen zwei Glasfasern mit sehr guten Übertragungseigenschaften und geringer Dämpfung ist mit der Spleißtechnik möglich. Beim Spleißen werden die beiden Fasern mit einer speziellen Spleißmaschine miteinander verschmolzen. Es ist dabei sicherzustellen, dass der Kabelkern und der Kabelmantel exakt aufeinander ausgerichtet sind und es zu keinen Versetzungen kommt. Für das Spleißen von Singlemode-Glasfasern bestehen aufgrund des wesentlich kleineren Kerndurchmessers höhere Anforderungen hinsichtlich der Präzision.

Auch ein sogenanntes Pigtail lässt sich an eine Glasfaser anspleißen. Es handelt sich beim **Pigtail** um eine Glasfaser, die an einem Ende bereits einen konfektionierten Stecker besitzt.

Vorkonfektionierte LWL-Kabel mit Steckern in unterschiedlichen Kabelausführungen und Kabellängen (Zentimeter genaue Bestellungen), besitzen in der Regel eine höhere Qualität als LWL-Kabel die vor Ort auf der Baustelle passgerecht hergestellt werden.

Verbinder für Lichtwellenleiter (LWL) 5/7



MT

Der Stecker ist ein Mehrfaserstecker mit einer MT-Ferrule (mechanical transfer) für zwei Fasern, die mit einem Abstand von 750 µm in einen Kunststoffblock eingebettet sind. Die hoch präzisen Führungsstifte, zur Ausrichtung des Steckers, befinden sich je nach Variante (male oder female) entweder in der Steckeraufnahme (engl. receptacle) oder im Stecker selbst.

Ferrule (engl. für Hülse): Aderendhülse, zum Verpressen von flexiblen Leiterenden; Führungsröhrchen für die Faser im LWL-Stecker

FC

Die Verriegelung des FC-Stecker (fiber connector) wird über einen Schraubverschluss realisiert.

LC

Der LC-Stecker (lucent connector) benötigt nur wenig Platz und ermöglicht dadurch eine höhere Portdichte.

MIC oder FDDI

MIC-Stecker (medium interface connector) ist ein Duplex-Stecker zur Aufnahme von zwei Fasern und werden fast ausschließlich in FDDI-Netzen und manchmal an ATM-Komponenten verwendet.

FDDI: Fiber Distributed Data Interface, 100-Mbit/s-Netzwerkstruktur für lokale Netzwerke über Glasfaserkabel, marktführender Hersteller von Netzwerkkomponenten bieten für ihre Produkte keine FDDI-Unterstützung mehr an, so dass die Technik als veraltet gilt.

ATM: Asynchronous Transfer Mode ist ein Kommunikationsprotokoll, welches sich für die Übertragung von Daten, Sprache und Video eignet.

SC

Der SC-Stecker (subscriber connector) löste im Jahre 2002 den ST-Stecker aus den Normen EN50173 und ISO 11801 als Standard für LAN-Verkabelungen ab. Er wird aber voraussichtlich in der Neufassung der EN50173 und ISO 11801 durch den kleineren LC-Stecker abgelöst werden.

ST oder BFOC

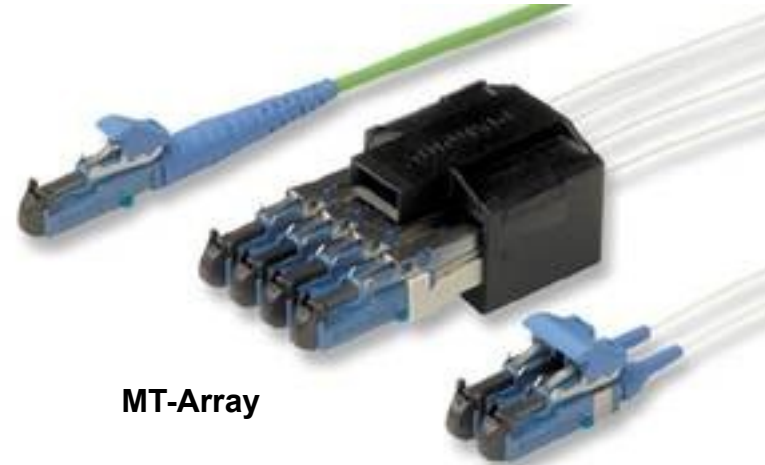
Der ST-Stecker (straight tip) ist auf Grund seines Bajonettverschlusses auch als BFOC-Stecker bekannt (bayonet fiber optic connector). Er wurde früher viel in lokalen Netzen (LAN) verwendet.

Verbinder für Lichtwellenleiter (LWL) 6/7



Glasfaser-zu-Ethernet-Konverter

Der Gigabit Glasfaser-zu-Ethernet Konverter ist ein 10/100/1000 MBit/s Media-Konverter mit automatischer Verbindungsaushandlung. Der Kupferanschluss handelt automatisch die Geschwindigkeit des angeschlossenen Gerätes und den Duplexmodus aus: 10/100/1000 Mbit/s Halbduplex oder 10/100/1000 Mbit/s Vollduplex. Der Glasfaseranschluss wird immer mit 1000 Mbit/s betrieben. Die maximale Entfernung beträgt im Multi-Modus 0,5 oder 2 km und im Single-Modus 10/20/40/60 km oder 80 km.



MT-Array



ZyXEL-Netzwerk-Switch mit 2 SFP-Ports und 10 RJ45-Ports

Verbinder für Lichtwellenleiter (LWL) 7/7



Switch von D-Link mit 2 SFP-Ports und 8 RJ45 Ports

SFP

Die Abkürzung SFP steht für Small Form-factor Pluggable. Bei einem SFP-Port handelt es sich um einen Anschlussport, in den sich standardisierte Module zum Anschluss von Netzwerkverbindungen einschieben lassen.

Vorteile von SFP-Ports

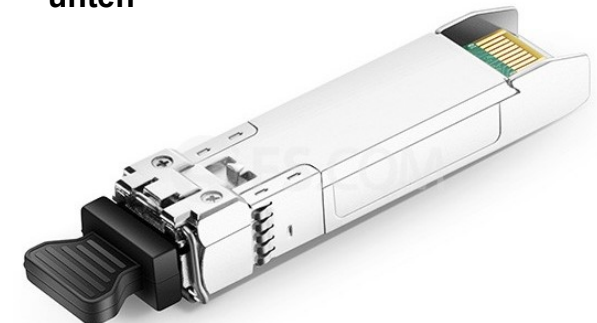
SFP-Ports in einem Netzwerkgerät, wie beispielsweise bei einem Switch, bieten zahlreiche Vorteile. Sie sorgen für mehr Flexibilität, Effizienz und Zukunftssicherheit. SFP-Module sind schnell und einfach auszutauschen. Die Netzwerkgeräte sind problemlos auf andere Übertragungstechniken und -medien umstellbar. Defekte Module sind kostengünstig zu ersetzen und erfordern keine Reparatur oder den Austausch des kompletten Switches.

Je nach Leitungstyp (Multimode- oder Monomodefaser), Wellenlänge und Datenrate sind die SFPs in unterschiedlichen Ausführungen erhältlich. Standardmäßig wird dabei der LC-Stecker verwendet. Module für Multimode-Faser haben einen schwarzen, manchmal auch beigen Entriegelungshebel, Module für Singlemode-Faser einen blauen. SFPs für Twisted-Pair-Kabel (1000BASE-T) sind ebenfalls verfügbar, werden aber nicht von allen Geräten unterstützt.

SFP-Ports sind in Ethernet-Switches, Router, Firewalls und auf Netzwerk-Interface-Karten mit einer unterschiedlichen Anzahl von SFP-Ports zu finden. In neueren Geräten kommen oft die Nachfolgestandards SFP+ und SFP28 zum Einsatz.



SFP-Port für Switch – Ansicht von oben und unten



Anonymität im Netz

Das Internet ist seit seiner Erschaffung nicht dafür geschaffen, dass die Benutzer sich im Netz anonym bewegen können. Jeder Rechner erhält eine eindeutige Adresse (IP-Adresse), die jeden Rechner und damit auch seinen Benutzer eindeutig identifizieren kann.

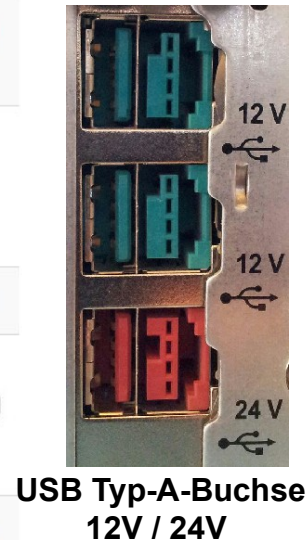
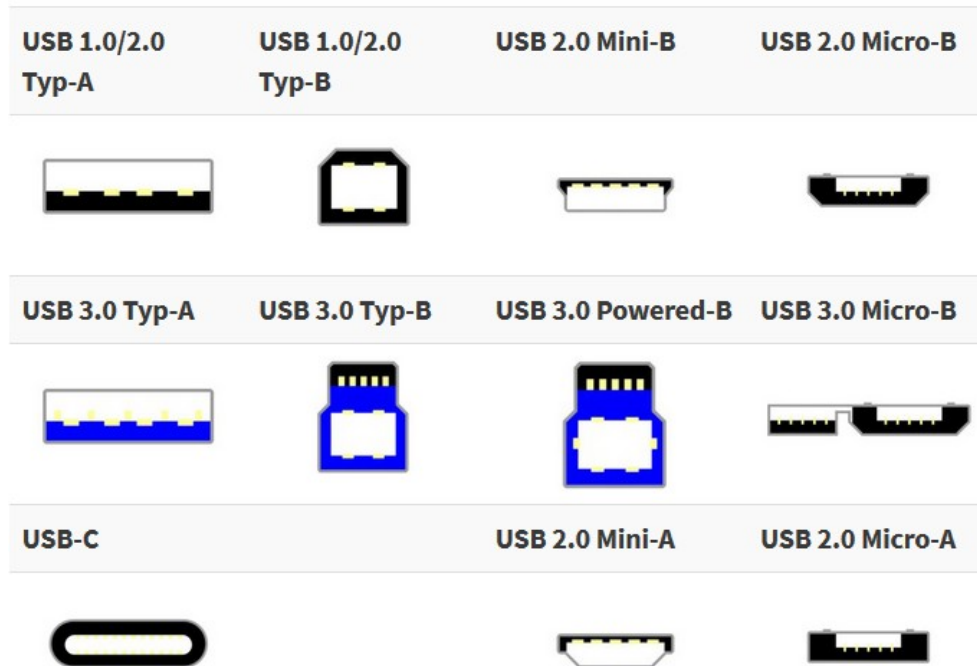
- **Anonymität im Tor-Netzwerk (Dark-Net)**

Im Netz kursiert seit Jahren, ein von offizieller Seite nicht bestätigtes Gerücht, dass etwa 20 Prozent aller Tor-Server kompromittiert sind. Das heißt, diese Server werden von regierungsnahen Organisationen oder direkt von Regierungen betrieben.

- **Anonymität mit Add-ons, Zusatzsoftware**

Mit dem Add-on **NoScript** für den Browser Firefox, kann man den Aufenthalt in Netz **etwas** anonym gestalten.

USB-Steckverbinder



USB Typ-A-Buchse
12V / 24V

USB-A auf B-Stecker - Drucker-Kabel

Hinweis: Die verdrehsichere Typ-C-Buchse befindet sich bereits an vielen Smartphones und externen SSDs und PCs.

Die Farbe der USB-Anschlüsse

Die USB-Anschlüsse haben nicht nur unterschiedliche Formen, sondern sind auch mit verschiedenen Farben gekennzeichnet. Doch was bedeuten diese überhaupt?

- Schwarzer/Weiß: USB 1.0 oder USB 2.0
- Blau: USB 3.0 oder USB 3.1 Generation 1
- Gelb: Anschluss mit permanenter Stromversorgung
- Rot/Orange: hohe Stromstärke oder Sleep-and-Wake-Anschluss (häufig USB 3.0) oder USB 3.1 Generation 2

Hinweis: Die Farbzusweisungen sind nicht Teil der USB-Spezifikationen und werden nicht immer streng eingehalten.

Name	möglich ab	max. Nutz-Datenrate	Symbolrate Modulation ^{[23][24]}
Low Speed	USB 1.0	0,15 MB/s	1,5 MBd NRZI-Code mit Bit-Stuffing
Full Speed	USB 1.0	1 MB/s	12 MBd NRZI-Code mit Bit-Stuffing
Hi-Speed	USB 2.0	40 MB/s	480 MBd NRZI-Code mit Bit-Stuffing
SuperSpeed	USB 3.0 (USB 3.1 Gen 1)	300 MB/s	5000 MBd 8b10b-Code
SuperSpeed +	USB 3.1 (USB 3.1 Gen 2)	900 MB/s	10.000 MBd 128b132b-Code
	USB 3.2 (USB 3.2 Gen 2x2)	1800 MB/s	2× 10.000 MBd 128b132b-Code

Video- und Geräteverbinder



VGA-Anschluss (Video Graphics Array)
Für 15-poligen Mini-D-Sub-Stecker (VGA-Stecker).



DVI-D-Anschluss (Digital Visual Interface)
DVI-D-Kabel (Dual-Link) haben 24 + 1 Pins.



HDMI-Anschluss (High Definition Multimedia Interface)

Der HDMI-Anschluss

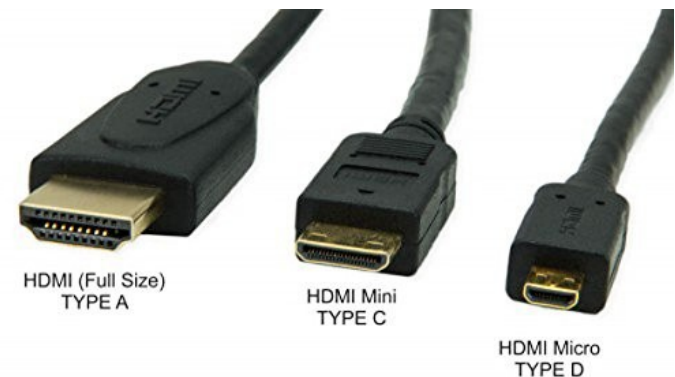
Bei HDMI gibt es unterschiedliche Größen der HDMI-Stecker und HDMI-Buchsen. Je nach vorhandenem Platz und einigen weiteren Anforderungen kommt ein anderer HDMI-Typ bzw. HDMI-Anschluss zum Einsatz. Insgesamt gibt es 4 unterschiedliche HDMI-Typen in unterschiedlichen Größen.

- Der "normale" HDMI-Typ ist Typ A. Er wird in der Unterhaltungselektronik an Fernsehern, Bluray-Playern, TV-Receiver und vielen weiteren Geräten verwendet. Der HDMI Typ A ist der größte und daher auch robusteste Typ.
- Mini-HDMI (HDMI Typ C) ist etwas kleiner und wird häufig bei Geräten mit wenig Platz für die Anschlüsse verwendet. Er kommt zum Beispiel häufig bei flachen Notebooks oder Ultrabooks und Tablets zum Einsatz.
- Micro-HDMI (HDMI Typ D) ist der kleinste HDMI-Typ. Aufgrund der sehr kleinen Bauweise wird er an Geräten mit sehr wenig Platz verwendet. An Smartphones kommen zum Beispiel HDMI-Buchsen vom Typ Micro-HDMI zum Einsatz.
- Außerdem gibt es noch den HDMI Typ E, welcher für den Einsatz in Fahrzeugen entwickelt wurde. Er ist daher für die Unterhaltungselektronik von geringer Bedeutung.

Grundsätzlich ist für die Verkabelung der heimischen Unterhaltungszentrale (z.B. Fernseher, Bluray-Player, TV-Receiver, Audio-Verstärker, Spielekonsole) der HDMI-Anschluss vom Typ A die richtige Wahl.



HDMI-Adapter - HDMI-Buchse (Typ A) zu HDMI-Stecker (Typ A)



HDMI (Full Size) TYPE A

HDMI Mini TYPE C

HDMI Micro TYPE D

SATA-Kabel

Was bedeuten die verschiedenen Farben der SATA-Anschlüsse (Serial AT Attachment oder Serial ATA) ?

Auf dem Mainboard gibt es je nach Hersteller bis zu drei verschiedenfarbige SATA-Anschlüsse (blau, rot und schwarz).

Bedeutung der Farben:

Blau: Die blauen SATA-Anschlüsse **weisen** auf den bisher schnellsten Übertragungstraffics von 6 Gbit/s (SATA III) hin. Daher sollten moderne Festplatten stets an den blauen SATA-Anschluss angeschlossen werden. Diese sind auch abwärtskompatibel. Schließt man langsamere Festplatten daran an, hat man keinen Geschwindigkeitsvorteil.

Rot und Schwarz: Die Bedeutung der schwarzen und roten SATA-Anschlüsse kann je nach Hersteller variieren. Sicherheitshalber sollte man im Benutzerhandbuch des Mainboards nachschauen. Im Zweifel orientiert man sich an folgender Regel: Neue Festplatten schließt man immer an den blauen Anschluss an. Ältere Platten steckt man an einen nicht-blauen Anschluss mit der niedrigsten Port-Nummer.

Generell bedeuten zwei gleichfarbige Anschlüsse, dass die Festplatten im RAID betrieben werden können: Im RAID können zwei Festplatten zusammengeschaltet werden, was die Lese- und Schreibgeschwindigkeit sowie die Ausfallsicherheit erhöht.

Übertragungsgeschwindigkeit: SATA I - 1.5 Gbit/s, SATA II - 3Gbit/s, SATA III - 6 Gbit/s; Mit SATA III (6 Gbit/s) können Lese- und Schreibgeschwindigkeits-Raten von bis zu 550 MByte/s bzw. 520 MByte/s erreicht werden.



SATA III – Kabel (Server-Einsatz)



SATA II - Kabel

Hinweis: Für Festplatten sind die Datenraten des aktuellen SATA-Standards seit Einführung von SATA irrelevant, da die Festplattenentwicklung nicht das gleiche Tempo aufweist. Die SATA-Schnittstelle stellt also für Festplatten keinen Flaschenhals dar. Im Gegensatz dazu reizen SSDs die Grenzen von SATA immer wieder aus.

Serial ATA (SATA) ist nicht auf Festplatten beschränkt – mittels ATAPI-Protokoll können auch SATA-Bandlaufwerke, DVD-Laufwerke und DVD-Brenner oder Speicherkartenlesegeräte verwendet werden.

Geräteschlüsse

Motherboard-Geräteanschlüsse:

Beispiel: Geräteschlüsse am Motherboard GA-AB350M-DASH von GigaByte (Taiwan)



Erläuterung: von links oben nach unten rechts

PS/2 Buchse (grün): Maus-Anschluss

PS/2 Buchse (violett): Tastatur-Anschluss

VGA (Video Graphics Array): Monitor-Anschluss

Display Port: Verbindungsstandard für die Übertragung von digitalen Bild- und Tonsignalen; im Wesentlichen für den Anschluss von Computermonitoren an PCs bzw. Notebooks

Display Port: dito.; Stromversorgung und gleichzeitige Datenübertragung ist mittels Display Port möglich; bei einigen Monitortypen kann dadurch das Energieversorgungskabel entfallen

HDMI Port (High Definition Multimedia Interface): Monitor-Anschluss

USB 3.1 Generation 1 (blau): Übertragungsrate max. 300 Mbit/s; frühere Bezeichnung USB 3.0

USB 3.1 Generation 1 (blau): dito.; Stromversorgung und gleichzeitige Datenübertragung ist mittels USB (alle USB-Varianten) möglich

USB 3.1 Generation 2 (rot): Übertragungsrate max. 900 Mbit/s

USB 3.1 Generation 2 (rot): dito.

Ethernet-Anschluss (Gigabit-Ethernet): Übertragungsraten von 100 Mbit/s bis 1Gbit/s für **RJ45-Stecker** (Registered Jack ... genormte Buchse), LAN-Port

USB 3.1 Generation 1 (blau): dito.

USB 3.1 Generation 1 (blau): dito.

Audio: **Line In** (blau) - analoger Eingang für stereophone

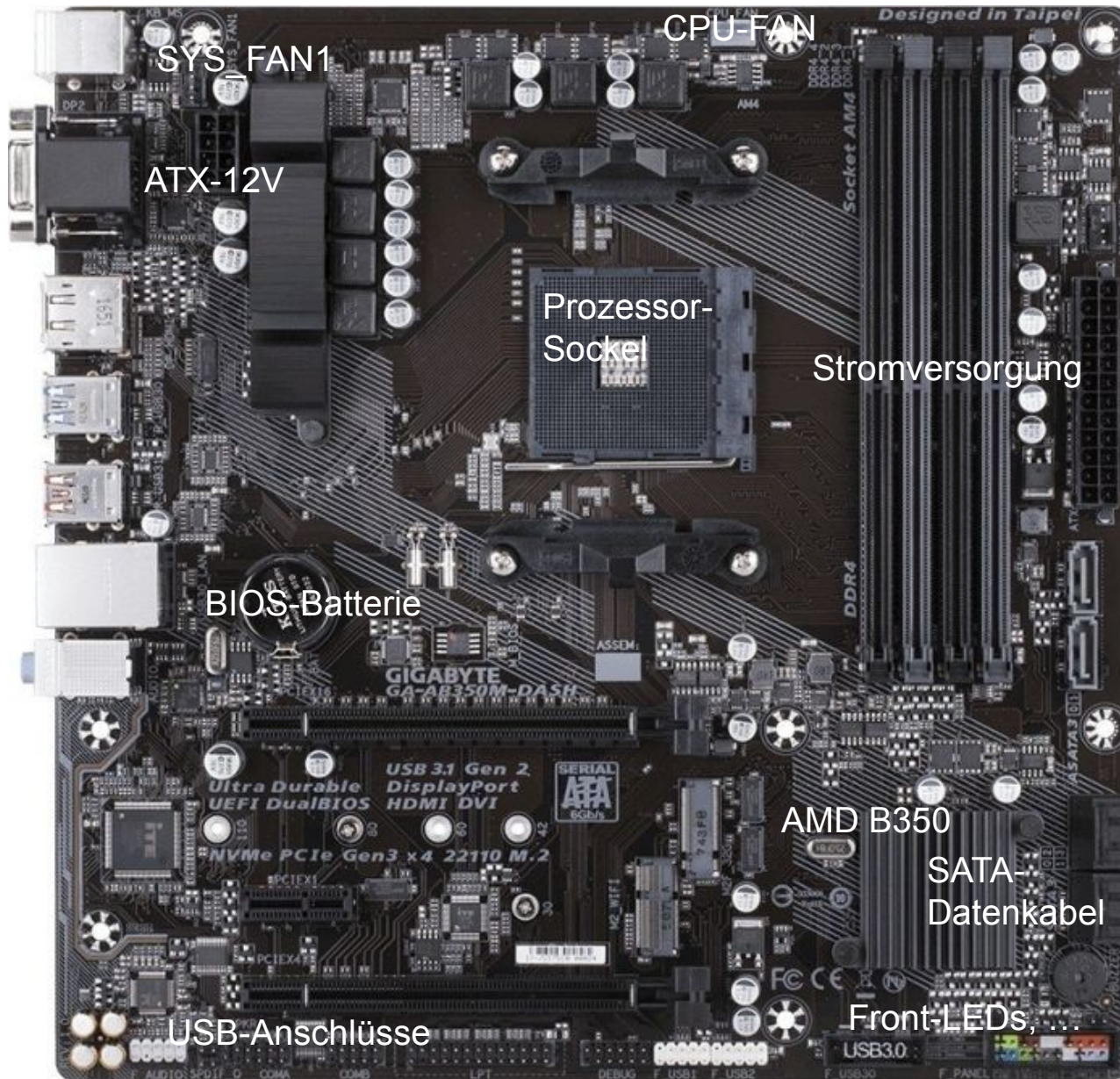
Audiosignale (AUX-Eingang für externe Quellen)

Audio: **Line Out** (grün) - Ausgang für Kopfhörer- oder Lautsprecher (stereo)

Audio: **Mic In** (pink) - Eingang für Mikrofon (mono)

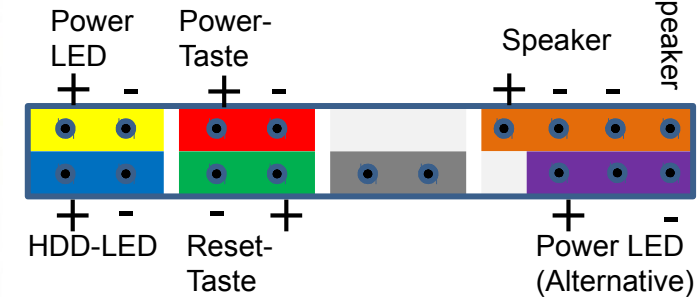
Hinweis: Power over Ethernet - Die Stromversorgung über Ethernet, englisch Power over Ethernet (PoE), bezeichnet ein Verfahren, mit dem netzwerkfähige Geräte (Überwachungskameras, Access-Points, ...) über das achtadrige Ethernet-Kabel mit Strom (Leistung am Endgerät: 12 bis 70 Watt, bei Switches sind Leistungsabgaben von mehr als 200 W möglich) versorgt werden können. Die abgegebene Spannung liegt zwischen 44 V und 54 V (in der Regel 48 V), die Leistung bis zu 15,4 W bis 71 W (je nach Leistungsklasse) bei Kabellänge bis zu 100 m.

Montage (Assemblierung) eines Rechners 1/2



Stecker 2-polig
(schwarzes Dreieck -
plus)

85



Hinweis: Die Hersteller vertauschen mitunter die Anschlusskabel für die Front-LEDs , Taster oder den Speaker.

Im nachfolgenden Beispiel wird der Rechner mit folgenden Baugruppen ausgestattet.

Gehäuse: Chieftec Mini CS-12B (Netzteil: 250W) Gehäuse

Motherboard: GA-AB350M-DASH (DASH .. Dynamic Adaptive Streaming over HTTP, GigaByte)

Prozessor: Desktop Prozessoren AMD Ryzen™, der Grafikchip ist im Prozessor integriert
Hinweis: beiliegender Lüfter wird nicht verwendet (Lüfter ist zu laut)

Lüfter: ARCTIC - Alpine 64 GT

Card-Reader: 3.5" All In 1 USB 2.0 Expresscard Micro SD TO CF Memory Internal Smart Card Reader for PC Front Panel SDHC MMC XD

DWD-LW: DVD-RW LG schwarz, SATA

SSD: Samsung 250GB SSD 860 EVO Series - 2,5 Zoll

Montage (Assemblierung) eines Rechners 2/2

Reihenfolge für den Zusammenbau eines Arbeitsplatzrechners:

1. Motherboard mit dem Prozessor und dem Lüfter bestücken (Überprüfung des Prozessors und des Steckplatzes)
2. Stromversorgung des Lüfters mit dem Motherboard verbinden
3. Gehäuse öffnen, Frontblende vorsichtig entfernen und das Motherboard einbauen (Überprüfung der Anschlussbuchsen, Anschlüsse müssen vollständig zugänglich sein)
4. Kabel sortieren und die Stromversorgung des Motherboards (ATX-Hauptstrom- 24-polig und die ATX 12V- Stromversorgung - 4-6-polig) und die Stromversorgung für den Gehäuselüfter (SYS_FAN1) anschließen
5. Card-Reader einbauen
6. DVD-Laufwerk einbauen (die Ansteckschiene befindet sich am Gehäuse für das DVD-LW)
7. SSD-Laufwerk einbauen, beim Einbau der SSD (mit der Kunststoffhalterung) ist das Typenschild lesbar
8. Stromversorgung für den Card-Reader, DVD- und SSD-Laufwerk anschließen
9. Stecker für den Speaker, Front-LEDs, Power- und Reset-Taste anschließen (siehe auch: vorherige Seite)
10. USB-Stecker für den Card-Reader und die Front-USB-Buchsen mit dem Motherboard verbinden (von vorne betrachtet - hinten links, neben den Steckplätzen für die Steckkarten)
11. Netzwerkkarte einbauen
12. Datenkabel für den Card-Reader, DVD- und SSD-Laufwerk anschließen
13. Hauptspeicher einbauen (2 Riegel), graue Einsteckplätze benutzen
14. Kabel sortieren und teilweise mit Kabelbinder fixieren
15. Baugruppen und Anschlüsse überprüfen
16. Gehäuse verschließen
17. Funktion des Rechners überprüfen (LEDs, DVD-Laufwerk, USB)

18. BIOS Einstellungen überprüfen (Datum, Zeit, Bootreihenfolge, Frage: wird die SSD und der Hauptspeicher vom BIOS erkannt)
19. Betriebssystem installieren

Zeitaufwand:

Hardware-Assemblierung: 1 Stunde, **ohne** Installation des Betriebssystems, Installation weiterer Software, Überprüfung und Test des Hauptspeichers

Hinweise:

- ◆ Prozessor: im Prozessor AMD RYZEN ist ein Teil des BUS-Systems und der Grafikprozessor bereits integriert
- ◆ Chip: AMD B350
CPU-Unterstützung, USB, PCI-Schnittstellen, Ethernet, WLAN, ...
- ◆ BIOS-Batterie: CR 2032
in der Nähe der BIOS-Batterie befindet sich meistens der BIOS-Chip
- ◆ Chip: iTE Super I/O-Chipsatz (input/output) oder Controller Hub; Chipsatz wird über die Einstellungen im BIOS konfiguriert, Kommunikation zwischen Prozessor und Hauptspeichern und anderes

mSATA-Adapter

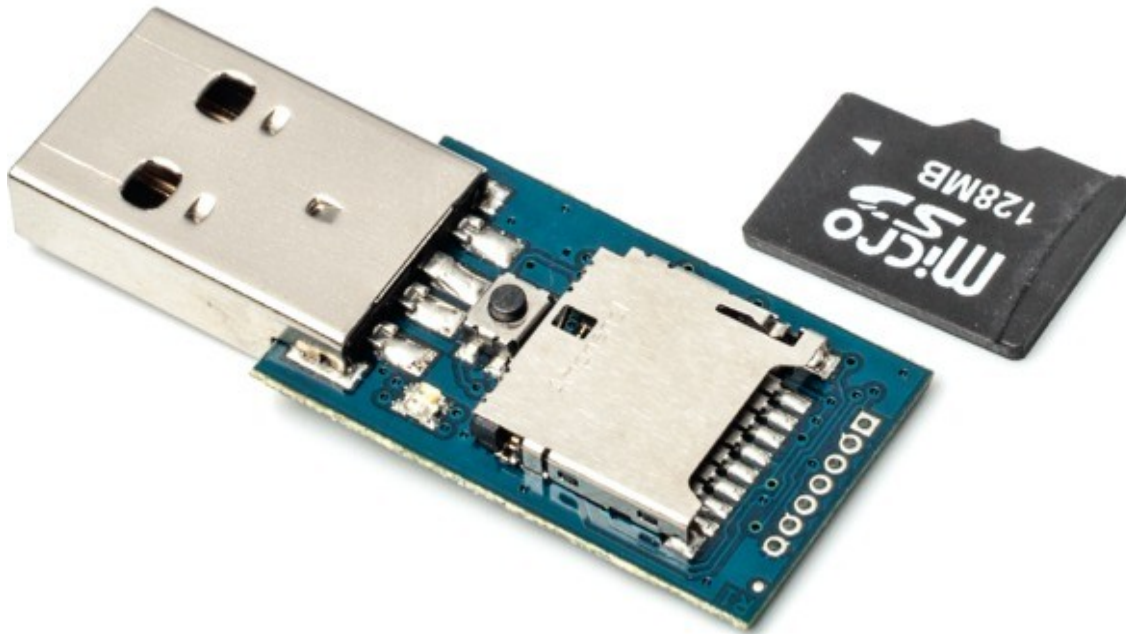


mSATA to Mini PCI-E



Hinweis: Die NAND SSD 860 EVO mSATA von Samsung sind für den Servereinsatz geeignet.

USB-Stick Rubber Ducky



Damit der Rubber Ducky als Massenspeicher und HID erkannt wird, besitzt der Configuration Descriptor im Rubber Ducky folglich zwei Interface Descriptoren, um als Massenspeicher und HID erkannt zu werden. Hat der Host-Controller die Informationen, weist er dem USB Gerät eine eindeutige Adresse zu und lädt die Treiber die zum Betrieb als HID (Tastatur), bzw. Massenspeicher notwendig sind.

Die Sicherheitskonzepte der Betriebssysteme haben dem Tipproboter nur wenig entgegenzusetzen, d.h. man kann mit dem programmierten Rubber Ducky nützliches, wie auch weniger nützliches erreichen.

Quelle:

www.hak5.org

<https://github.com/hak5darren/USB-Rubber-Ducky/wiki>

www.sempervideo.de

Rubber Ducky (Gummi-Entchen) ist ein Microcontroller (AMTEL 32bit) mit SD-Karte der aussieht wie ein USB-Stick und sich verhält wie eine Tastatur. So kann alles mit dem Gerät gemacht werden, was mit der Tastatur gemacht werden könnte. Die Scriptsprache, mit der sich die Tastenbefehle ausführen lassen, heißt Duckyscript. Das Script wird auf einer Micro-SD Karte auf dem Rubber Ducky im .bin Format gespeichert.

Der allgemeine Ablauf zum verwenden des Rubber Ducky kann wie folgt beschrieben werden:

1. SD-Karte einstecken
2. Ducky-Script encoden (.jar oder Website toolkit) zu .bin
3. Payload (.bin) auf SD-Karte ablegen und SD-Karte in den Rubber Ducky stecken
4. USB-Stick in den Rechner stecken
5. Payload führt sich automatisch aus

Warum wird der Rubber Ducky jedoch vom PC als Tastatur (HID) erkannt? Wenn ein USB Gerät in ein PC gesteckt wird, kümmert sich der Host-Controller um das Handling des USB Sticks. Dieser sendet ein USB-Reset Request an das USB Gerät. Dem USB Gerät wird darauf die Adresse 0 zugewiesen. Danach holt sich der Host-Controller die benötigten Informationen vom USB Stick über den Device Descriptor der USB Gerätes. Er enthält Informationen über den Hersteller, wie groß der USB-Stick ist, mit welcher Spannung er betrieben werden muss und einiges mehr.

IT-Systembetreuer: Werkzeuge



Auflegewerkzeug



Kabeltester



Gewindebohrer



Rechner, Notebook

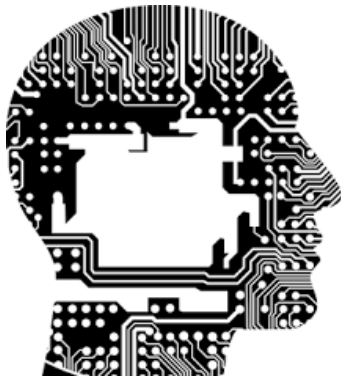
Speichermedien
für Software,
Treiber und
Informationen



Netzwerkabel RJ45



Universalschraubendreher für
die meisten Schrauben am
Rechner verwendbar



Werkzeug: Der eigene Kopf
mit dem darin geparkten
Wissen.



Öffnungswerkzeuge oder
Opening Tool Assortment



Bit-Schraubendreher



Crimpzange



Schweizermesser



Kneifzange

Netzwerk-Stecksysteme der Kategorie 7 - 1/2



GG45-
Stecker



GG45-
Buchse

Hinweis: Feldkonfektionierte Stecker und Buchsen (Anfertigung auf der Baustelle) sind einfacher zu installieren und erfüllen die Anforderungen an die Abschirmung. Alternativ können auch vorkonfektionierte Netzkabel mit Stecker verwendet werden.

GG45 ist spezifiziert für höhere Datenraten, als jene der RJ45-Stecker. Das GG45-System wurde von Nexans entwickelt, das Unternehmen erhielt auch die Schutzrechte für die Bezeichnung GG45. GG wurde als Abkürzung für GigaGate verwendet, dieser Name konnte aber nicht geschützt werden, so dass die Bezeichnung **GG45** als Markenname eingetragen und geschützt wurde.

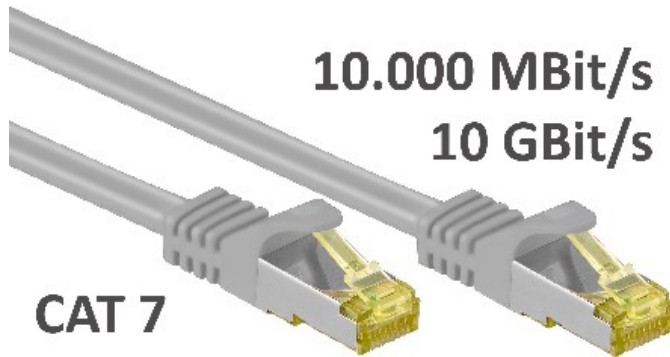
Der heutige GG45 ist eine 2-in-1-Lösung, da die GG45-Buchse (nicht der Stecker!) abwärtskompatibel zu RJ45 ist. Somit können herkömmliche RJ45-Stecker in neuen GG45-Umgebungen (Netzwerkdozen, Patchpanels) verwendet werden. Umgekehrt ist es aber nicht möglich, den GG45-Stecker in einer RJ45-Buchse zu verwenden.

Zusätzlich zu den acht Kontakten des RJ45-Systems besitzt die **GG45-Buchse** in den oberen äußeren Ecken des RJ45 Steckgesichtes **vier weitere Kontakte**. Die mittleren 4 RJ45-Kontakte sind nur im Betrieb mit einem RJ45 verbunden.

Bei Frequenzen von bis zu 500 MHz auf den RJ45-Kontakten kommt es dabei durch die unteren Kontakte nicht zu störenden Beeinflussungen des Signals. Die zusätzlichen Kontaktpaare oben rechts und links ermöglichen nach Kategorie 7 die höhere Bandbreite von 600 MHz und in der neuen Version nach Kategorie 7A von 1000 MHz. Damit können nach Aussagen des Entwicklers 40 Gigabit/s über eine Entfernung von 100 m übertragen werden.

Es werden allerdings nicht alle zwölf Kontakte gleichzeitig verwendet, da Datenkabel nach Norm nur 8 Adern haben. Stattdessen trennt ein Federmechanismus die mittleren RJ45-Kontakte und verlagert sie auf die Gehäusemasse. Dadurch sind ab Cat-7-Betrieb nur noch die äußeren Kontakte (1/2 und 7/8) der RJ45-Leiste und die zusätzlichen oberen 2 GG45-Kontaktpaare (also wiederum 8 Kontakte) im Einsatz. Durch den größeren Abstand, den nun alle Paare zueinander haben, ist eine Übertragungsbandbreite von bis zu 1000 MHz möglich.

Netzwerk-Stecksysteme der Kategorie 7 - 2/2



Hinweis: Feldkonfektionierte Stecker und Buchsen (Anfertigung auf der Baustelle) sind einfacher zu installieren und erfüllen die Anforderungen an die Abschirmung. Alternativ können auch vorkonfektionierte Netzkabel mit Stecker verwendet werden.



Cat 7 ist ein globaler Standard, außer in den USA (Stand 2018). Kategorie 7 ermöglicht Betriebsfrequenzen bis 600 MHz, Kategorie 7A bis 1000 MHz. Cat-7-Kabel haben vier einzeln abgeschirmte Adernpaare (Screened/Foiled shielded Twisted Pair S/FTP) innerhalb eines gemeinsamen Schirms. Ein Cat-7-Kabel erfüllt damit die Anforderungen für ein 10-Gigabit-Ethernet.

Als man im Jahr 2002 den Cat-7-Standard verfasste, um 10-Gigabit-Ethernet über 100 m zu ermöglichen, ging man davon aus, dass eine Betriebsfrequenz von 600 MHz notwendig sei. Da der **RJ-45-Stecker** diese Spezifikationen aufgrund der engen Kontaktanordnung nicht erfüllen kann, wurden neue Steckverbindungen konzipiert, die im Wesentlichen den Abstand zwischen den Adernpaaren vergrößern.

Auf dem Markt setzten sich diese Steckertypen (GG45, Tera) allerdings nicht durch, da RJ-45 für den im Jahr 2006 verabschiedeten 10GBASE-T-Standard genauso ausreichend war wie die Leitungen der Kategorie 6A, so dass die heute gängigen **10GBASE-T-Endgeräte auf RJ-45 basieren**.

Die dazu häufig genutzte Netzwerkverkabelung, bestehend aus Cat-7-Leitung und Cat-6-Netzwerkdoesen/-Patchpanels, erfüllt damit zwar den Geschwindigkeitsstandard, aber bezogen auf die Betriebsfrequenz sinkt die Leistungsfähigkeit der gesamten Netzwerkstrecke ungeachtet der »guten« Cat-7-Leitung auf Cat 6-Niveau.

Erst mit dem geplanten Cat 8.2-Standard und einer Datenübertragungsrate von mehr als 40 Gbit/s, könnten die neuen Steckertypen wieder relevant werden.

Hinweis - praxisorientierte Werte bei Netze mit RJ45-Steckverbinder: 100m (1Gbit/s), 75m (2,5Gbit/s), 50m (5Gbit/s) und 30m (10Gbit/s); für die Verbindung zwischen Switches sollten die SFP-Ports benutzt werden (bessere Abschirmung).

Generalisieren einer Windows-Installation mit Sysprep 1/3

Das Systemvorbereitungstool Sysprep (System Preparation, Windows\System32\Sysprep\sysprep) wird zum Generalisieren einer Windows-Installation verwendet. Soll ein Windows-Image auf unterschiedlichen PCs bereitgestellt werden, muss das Masterimage im Audit-Modus zunächst vorbereitet werden.

Nach Abschluss aller gewünschten Installationen und Konfigurationen **im Audit-Modus, werden alle eindeutigen Systeminformationen automatisch aus der Windows-Installation per Sysprep entfernt** und das System versiegelt. Dadurch wird die SID (Security Identifier) zurückgesetzt und alle Protokolle und Wiederherstellungspunkte werden gelöscht. Dies ist in Netzwerken - wie Arbeitsgruppen und vor allem in Domänen, zwingend erforderlich.

Ablauf:

1. Windows 10 ganz normal installieren
Nach dem ersten Hochfahren ist der Einrichtungsassistent durch die Tastenkombination [Strg] + [Shift] + [F3] abubrechen. Das System wird dadurch neu gestartet und automatisch im Audit-Modus hochgefahren.
2. Im Audit-Modus von Windows 10 wird automatisch das vordefinierte Benutzerkonto Administrator (ohne ein Passwort) aktiviert. Jetzt können alle Treiber, Programme und Windows Updates installiert werden und das System bei Bedarf individuell konfiguriert werden. **Das Programm-Fenster des Systemvorbereitungstool Sysprep ist beim Neustart geöffnet und kann vorerst geschlossen werden.** Bei jedem Neustart fährt das System automatisch wieder im Audit-Modus hoch, bis das System per Sysprep versiegelt wird.

3. Im letzten Schritt wird Windows jetzt mit Sysprep versiegelt, man kann dazu entweder die nach jedem Neustart geöffnete GUI verwenden und dort:

- Out-of-Box-Experience (OOBE): für System aktivieren
- Checkbox: Verallgemeinern
- Herunterfahren auswählen

Die Festplatte des heruntergefahrenen System, kann dann geklont werden (dd, Clonezilla, G4L,).

oder man kann die auf der nachfolgenden Seite beschriebenen Sysprep-Befehlszeilenoptionen verwenden.



Generalisieren einer Windows-Installation mit Sysprep 2/3

Sysprep-Befehlszeilenoptionen

Die folgenden Befehlszeilenoptionen sind für Sysprep verfügbar:

```
Sysprep.exe [/oobe | /audit]  
[/generalize]  
[/mode:vm]  
[/reboot | /shutdown | /quit]  
[/quiet]  
[/unattend:<answerfile>]
```

sysprep /audit

Startet den PC im Überwachungsmodus neu. Mit dem Überwachungsmodus können zusätzliche Treiber oder Anwendungen hinzugefügt werden.

sysprep /generalize /shutdown

Bereitet die Imageerstellung der Windows-Installation vor. Sysprep entfernt alle eindeutigen Systeminformationen aus der Windows-Installation. Sysprep setzt die Sicherheits-ID (SID) zurück und löscht alle Wiederherstellungspunkte, sowie Ereignisprotokolle.

Beim nächsten Start des Computers wird die Konfigurationsphase **specialize** ausgeführt. Die Konfigurationsphase erstellt eine neue Sicherheits-ID (SID).

/reboot

Startet den PC neu. Diese Option kann verwendet werden, um den PC zu überwachen und um sicherzustellen, dass die Erstauführung korrekt funktioniert.

sysprep /generalize /shutdown /oobe

Startet den Computer im **Modus der Windows-Willkommenseite** neu. Mit der Windows-Willkommenseite können Benutzer ihr Windows-Betriebssystem anpassen, Benutzerkonten erstellen, einen Namen für den Computer festlegen und andere Aufgaben ausführen.

Hinweis: Sysprep verarbeitet während der Konfigurationsphase die gespeicherten Einstellungen aus einer Antwortdatei (oobeSystem), bevor die Windows-Willkommenseite gestartet wird.

/shutdown

Führt den Computer herunter, nachdem die Ausführung des Befehls Sysprep abgeschlossen wurde.

/quiet

Führt das Sysprep-Tool ohne Anzeige von Bestätigungsmeldungen auf dem Bildschirm aus. Diese Option kann verwendet werden, um den Sysprep-Vorgang zu automatisieren.

/quit

Schließt das Sysprep-Tool, ohne den PC neu zu starten oder herunterzufahren, nachdem Sysprep die angegebenen Befehle ausgeführt hat.

Quelle:

[https://msdn.microsoft.com/de-de/library/windows/hardware/dn938330\(v=vs.85\).aspx](https://msdn.microsoft.com/de-de/library/windows/hardware/dn938330(v=vs.85).aspx)

Generalisieren einer Windows-Installation mit Sysprep 3/3

Windows: Eigenes Logo in den Systemeigenschaften

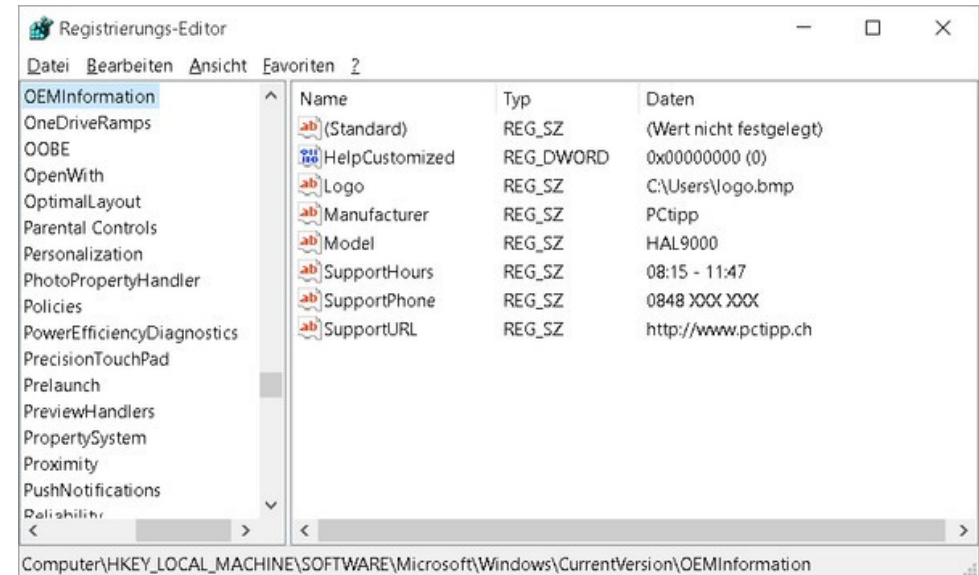
- ❖ Logo-Datei mit einer Bildbearbeitung erstellen
 - **Größe:** 120x120 (150x150) Pixel
 - **Dateityp:** 24Bit/BMP (Windows-Bitmap)
 - **Speicherort:** z.B. Windows\System32\Sysprep\Logo
- ❖ Generieren eines neuen Registry-Eintrages
 - [W] + [R] -> regedit
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \ CurrentVersion\OEMInformation
 - Jetzt sind mehrere Einträge zu erstellen. Mit der rechten Maustaste in die rechte Fensterhälfte klicken und die Optionen **Neu -> Zeichenfolge** wählen. Als Eintrags-Namen z.B. Logo eintragen. Auf den neuen Eintrag mit der linken Maustaste doppelt klicken und den gewünschten Wert (Bildpfad) z.B. **C:\Windows\System32\Sysprep\Logo\Logo.bmp** eintragen.
- ❖ Es können weitere optionale Werte eingetragen werden.

Wichtig: Falls ein Eintrag **HelpCustomized** vorhanden ist, muss dessen Wert von 1 auf 0 (Ziffer 0) geändert werden, da sonst einige der Einträge nicht erscheinen.

Hinweis: Werden die Werte in der Registry mehrmals verwendet, so kann der Registry-Eintrag exportiert werden (**Hinweis:** Import in die Registry: Doppelklick auf die exportierte Datei).

Registry-Eintrag exportieren:

- Registry-Eintrag: OEMInformation -> rechte Maustaste -> Exportieren -> Name: Logo_Registry.reg -> Speicherort festlegen -> Datei z.B. nach C:\Windows\System32\Sysprep\Logo\ verschieben



Mögliche Einträge:

Eintragsname	Beispiel
Logo	C:\PfadZum\Bild.bmp
Manufacturer	Pctipp
Model	HAL9000
SupportPhone	0848 XXX XXX
SupportURL	www.pctipp.ch
SupportHours	08:15 – 11:47

Windows 10: Installations-Stick erstellen

A: Bootfähiger USB-Stick für Windows 10 aus dem Internet erstellen

1. Media Creation Tool (MCT, MediaCreationTool1803.exe) herunterladen (Download ist nur mit einem Microsoft Betriebssystem möglich)
2. USB-Stick: größer 4 Gbyte (**Achtung:** USB-Stick wird komplett gelöscht.)
3. Media Creation Tool starten und die 2. Option (Installationsmedium für einen anderen PC erstellen) auswählen
4. Sprache, Architektur und Edition auswählen
5. Zu verwendendes Medium auswählen (USB-Speicherstick)
6. USB-Speicherstick auswählen
7. Warten bis der Download- und Kopiervorgang abgeschlossen ist
8. Fertig!

Hinweis: Von dem Installations-Stick, können ausschließlich die Varianten Windows 10 Home, Pro und Education installiert werden.

B: Aus vorhandener ISO-Datei einen bootfähigen USB-Stick erstellen

Microsoft stellt die ISO-Dateien von Windows 10 kostenlos zur Verfügung.

Für die Installation, Upgrade von / auf Windows 10 ist ein gültiger Key erforderlich (z.B. Key von einer Windows 8 Installations-CD).

9. ISO-Datei herunterladen
10. USB-Speicherstick einstecken
11. ISO-Datei als Laufwerk über das Kontextmenü bereitstellen und eine Eingabeaufforderung (CMD, Powershell) mit Administratorrechten starten
12. **diskpart** eingeben und anschließend **list disk**
13. **select disk <Nummer des USB-Sticks aus list disk>** (USB-Stick erkennt man an der Größe des Speicherplatzes)
14. **clean** (Inhalt des USB-Sticks wird gelöscht)
15. Mit **create partition primary** wird eine neue primäre Partition erstellt, die mit **active** aktiviert wird. Das USB-Stick ist jetzt bootfähig.

16. Datenträger mit **format fs=fat32 quick** formatieren
17. mit dem Befehl **assign**, wird dem Gerät, Partition im Explorer ein Laufwerksbuchstabe zugeordnet
18. Diskpart mit **exit** beenden
19. Windows 10 ISO-Datei in den Stammordner des USB-Sticks kopieren (und evt. weitere Daten und Programme)
20. bootfähiger USB-Stick – Fertig!

```
Administrator: Eingabeaufforderung - diskpart
Microsoft Windows [Version 10.0.10586]
(c) 2016 Microsoft Corporation. Alle Rechte vorbehalten.

C:\WINDOWS\system32>diskpart

Microsoft DiskPart-Version 10.0.10586

Copyright (C) 1999-2013 Microsoft Corporation.
Auf Computer: PC

DISKPART> list disk

   Datenträger ###  Status              Größe           Frei           Dyn  GPT
   -----
   Datenträger 0    Online              238 GB          1024 KB
   Datenträger 1    Online             1863 GB           0 B
   Datenträger 2    Online              238 GB           0 B
   Datenträger 3    Online             1397 GB          1024 KB
   Datenträger 4    Online               29 GB           0 B

DISKPART> select disk 4

Datenträger 4 ist jetzt der gewählte Datenträger.

DISKPART> clean

Der Datenträger wurde bereinigt.

DISKPART> create partition primary

Die angegebene Partition wurde erfolgreich erstellt.

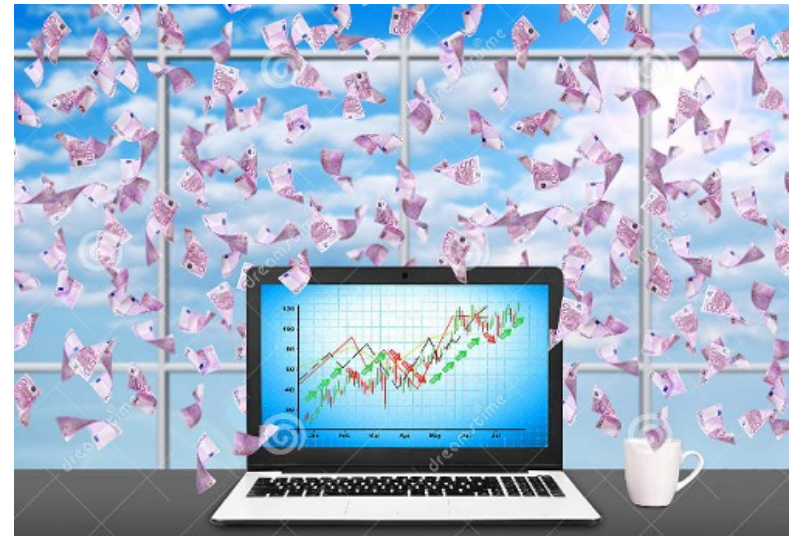
DISKPART> active

Die aktuelle Partition wurde als aktiv markiert.

DISKPART>
```

Hinweise für einen kompletten Rechneraustausch – Checkliste:

- ❖ Benutzer sollten rechtzeitig im Vorfeld informiert werden, unter Beachtung der Firmenphilosophie, Arbeitszeit, Urlaubs- oder Arzttermine und der Benutzergewohnheiten.
- ❖ Technisch versierte Benutzer benötigen im Vorfeld nur eine geprüfte Checkliste.
- ❖ Sicherung aller Daten: Anwesenheit des Benutzers ist erforderlich.
- ❖ Sicherung der persönlichen Dateien, Adress- und Telefonlisten.
- ❖ Sicherung der Email-Zugangsdaten.
- ❖ Sicherung der Internetlink-Sammlung.
- ❖ Sicherung der Zugangsdaten zu internen Netzwerk-Bereichen, Webseiten, ...
- ❖ Sicherung der Zugangsdaten zu externe Netzwerk-Bereiche, Daten-Cloud, VPN-Netzwerke, Firmenzentrale, ...
- ❖ Abfrage: zusätzliche Software (Software-Name, Version, Produkt-Keys), die auf Standard-Rechner nicht installiert werden.
- ❖ Abfrage: zusätzliche Hardware, die in Standard-Rechner nicht enthalten sind.
- ❖ Prüfung: Sind alle notwendigen Hardware-Treiber installiert?
- ❖ Prüfung: Ist die zusätzliche Hardware für das Benutzerkonto zugänglich?
- ❖ Abfrage: Konfigurationswünsche für die Standard-Einstellung des Arbeitsplatzrechners (z.B. für rechts- oder linkshändige Benutzer, Auflösung des Bildschirms, Standard-Drucker Wallpaper, ...)
- ❖ Abfrage: Einrichtung der Kopplung mit mobilen Geräten (Notebook, Tablet, Smartphone, ...)
- ❖ Überprüfung aller neu eingerichteter Zugänge (Email, Cloud, geschützte interne und externe Netzwerk-Bereiche)
- ❖ Kurze Einweisung des Benutzers. Bei Abwesenheit des Benutzers ist eine kurze Mitteilung zu hinterlassen.



Business: VDSL per Glasfaserleitung

Im Gegensatz zu DSL erreicht VDSL (Very High Speed Digital Subscriber Line) Ihren Geschäftskunden-Anschluss nicht per Kupferleitung, sondern kommt erst von einer Vermittlungsstelle über Glasfaser zu einem Verteiler in der Nähe Ihres Unternehmens. Danach läuft das VDSL vom Verteilerkasten über eine Kupferleitung zum VDSL-Router.

Sind mehrere dieser Kupferkabel in einem Bündel zusammengefasst, können gegenseitige Signalstörungen entstehen. Diese verringern die Reichweite und Datenraten und bewirken damit langsames Internet.

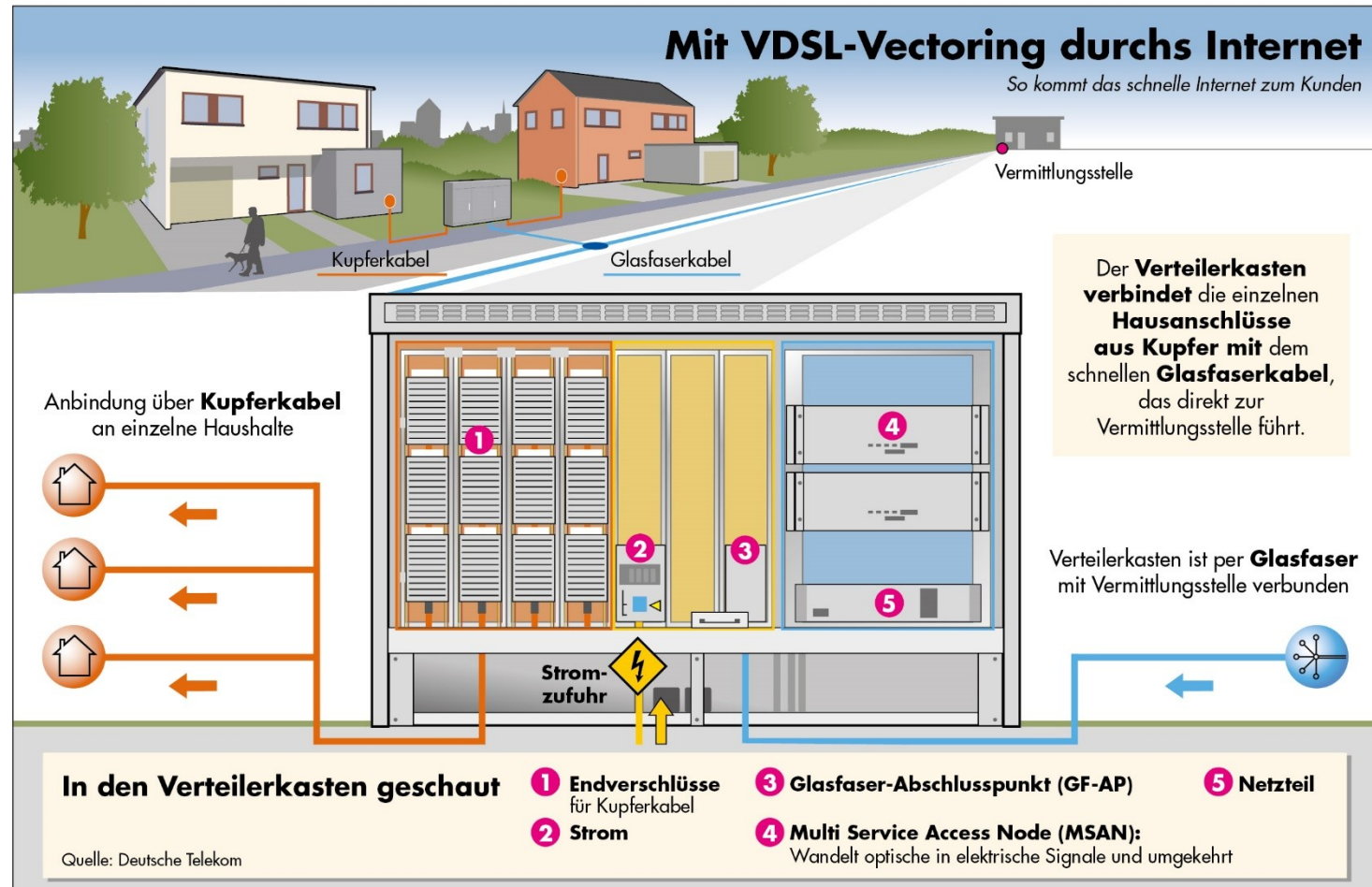
Was ist Super-Vectoring?

Um solchen Störsignalen entgegenzuwirken, wurde zunächst Vectoring entwickelt: Bei dieser VDSL-Erweiterung ist die Technik im nahegelegenen Verteilerkasten mit dem DSL-Router in Ihrem Business verknüpft, berechnet die Störsignale und eliminiert sie durch Gegenseignale.

Mit Vectoring und Super-Vectoring werden Störsignale erkannt und weitestgehend ausgelöscht. In der Folge sind höhere Geschwindigkeiten möglich.

Komfort-Anschluss Plus mit 250 Mbit/s – inklusive der FRITZ!Box 7590 (alternative: FRITZ!Box 7583)

Quelle: www.vodafone.de/business.html (Stand: 2019)






Die Art des Netzkabels und die zugehörigen Stecker dürfen nicht als eigenständige Komponenten betrachtet werden - sie sind Teil eines Ökosystems von verfügbaren und geforderten Datenraten, Switchen, Routern, Netzkarten und Transceivern.

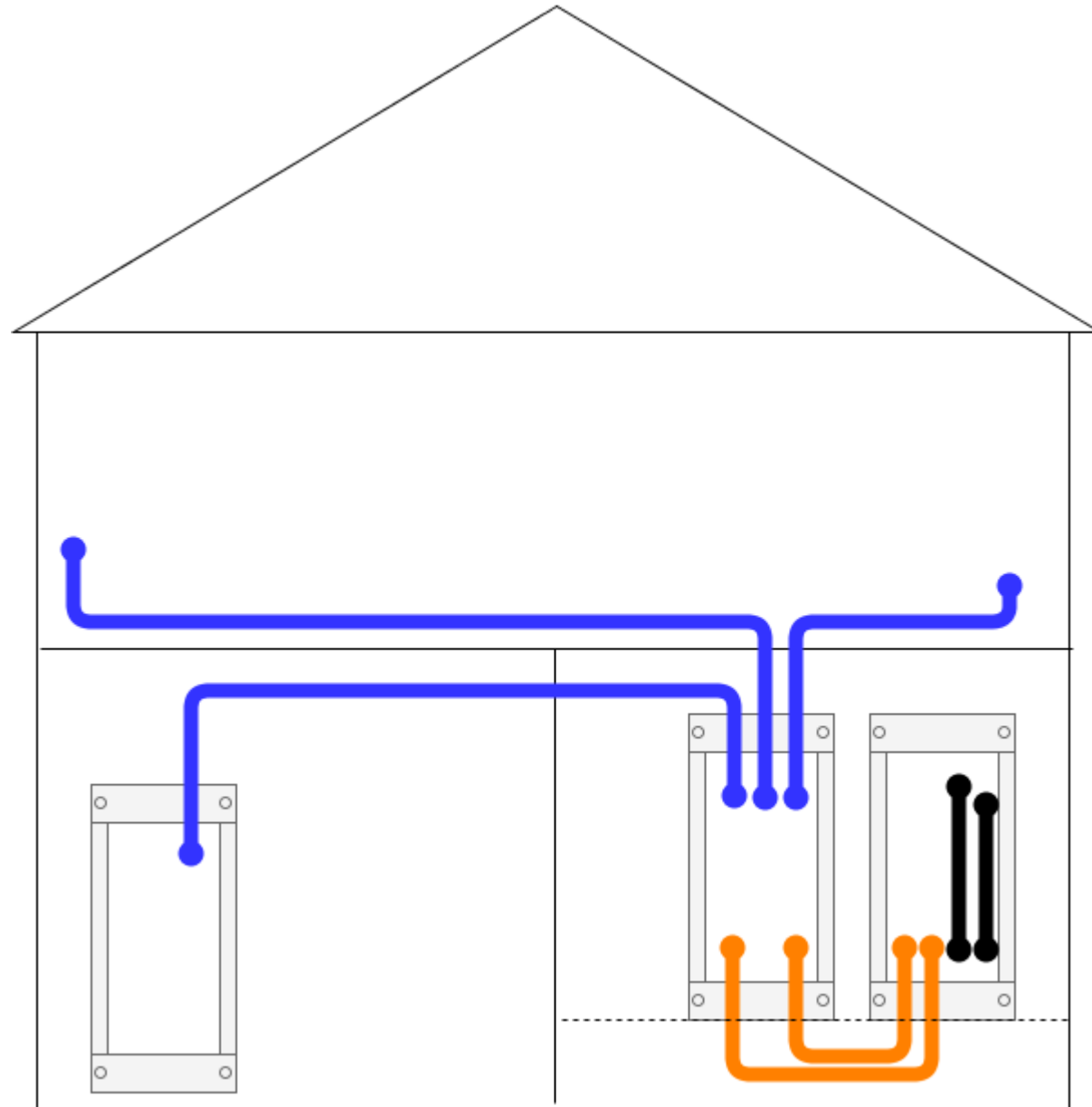
Gebäudeplaner sollten bedenken, dass für ein 40G BASE SR Netz:

- 8 Fasern für 40G benötigt werden (anstelle von 2 Fasern für 10G BASE SR - Schnittstelle mit Lichtwellenleitern)
- die maximale Distanz bei einer OM3 Faser (OM3 ... Faserkategorie) auf 100 m begrenzt ist (im Vergleich hierzu liegt die maximale Distanz bei 10G BASE SR noch bei 300 m)

Ein 40G-Link wird als ein Link betrachtet. Fällt ein Faserpaar aus (transportiert lediglich 10G), dann wird der gesamte 40G-Link stark beeinträchtigt.

Die Fehlersuche wird dann im wahrsten Sinne des Wortes zu einer Sysphus-Arbeit.

-  Patchkabel innerhalb eines Schrankes mit oder ohne Transceiver (SFP)
-  Multimode-LWL zwischen den Schrankreihen oder innerhalb eines Raumes
-  Singlemode-LWL zwischen den Stockwerken oder Gebäuden



Regel 1:

Verwende Direct Attached Cable (DAC, LWL-Patchkabel) innerhalb eines 19" Schranks. Maximale Länge: 5 m

DACs funktionieren und sind kostengünstig und verbrauchen weniger Strom als Transceiver. Falls einem DACs nicht gefallen und/oder Probleme auftreten (Achtung: wir haben mit DACs eine galvanische Verbindung auf den Highspeed-Lands von zwei Geräten), dann kann man auf SFP+ / QSFP+ SR ausweichen.

Regel 2:

Verwende Multimode OM3 zwischen Schrankreihen in einem Raum (Datacenter). Maximale Länge: 100 m

Das Kabel ist schnell verlegt und schnell ausgewechselt. Deswegen einfach OM3 Fasern / Faserbündel werfen und gut ist. Reicht das mal nicht mehr aus, dann kann man eine neue oder zusätzliche OM4 oder gar OM5, 6, 7, 8, 9 (Anmerkung: es ist derzeit nicht klar, wo die Reise mit den Multimode-Faserkategorien hingeht) verlegen. Derzeit sind Datenraten von 10/40 Gbit/s mit geeigneten Transceivern über Multimode möglich (Bsp. QSFP+ und MTP).

Regel 3:

Verwende Multimode OM3 auf der selben Stockwerksebene, wenn der gesamte Kabelweg gut zugänglich ist (es darf kein Arbeitsplatz und/oder Maschine unter oder über den Kabelwegen sein). Maximale Länge: 100 m

Gleich wie Regel 2, nur mit dem besonderen Augenmerk, dass man jederzeit den Zugang zu den Kabelwegen gewährleisten muss.

Regel 4:

Überlege Dir gut, ob Du für die Arbeitsplatzanbindung Cat.6/7/8 Kabel verlegen willst. Maximale Länge: 90 m

Ein souveräner Planer lässt diese Regel aus. Es wird gänzlich auf die Kupferverkabelung zu den Arbeitsplätzen verzichtet, da sie über mehrere Jahre meistens keine ausreichende Bandbreite gewährleisten kann oder die Netzwerkdose sich am falschen Ende des Raumes befindet. Beim Umzug innerhalb des Büros werden dann Patchkabel am Boden mehr oder weniger wild verlegt, im »besten« Falle verklebt mit Paketklebeband.

Die Alternative ist, dass man jeden Accessswitch für die Arbeitsplätze mit Singlemode anbindet (Regel 5). Die Arbeitsplätze werden direkt auf die Accessswitches gepatcht. Die Accessswitches sind entweder 1G-Kabelkanal-Switches oder 1G-Desktop/19“-Switches ohne Lüfter und direkt unter eine Schreibtischgruppe angeschraubt. Die Switches sollten typische Layer 2-Funktionen (mind. VLAN und AAA) in einem Management vereinen. Der Gerätestecker ist ein IEC-Lock, damit nicht unnötige Probleme mit wackligen Steckern (Switch Neustart) auftreten. Die Vorteile liegen auf der Hand. Je nach benötigter Portanzahl kann man handelsübliche 1HE 8-Port bis 48-Port Switches einsetzen. Reichen diese Ports nicht aus, so können mehrere Switches miteinander verbunden werden (Stacking). Der Benutzer kann im besten Fall den Anschluss selber patchen und der nicht-vorhandene Access-Schrank (meist in einer Rumpelkammer auf dem Stockwerk zu finden) wird nicht mit nicht-mehr-benötigten Patchkabeln zugemüllt. Diesen Schrank gibt es schlichtweg nicht mehr. Für PoE (Power over Ethernet) ist auch gesorgt. PoE ist mit lüfterlosen Switches realisierbar (z.B. Ethernet-Switches Juniper EX2200-C aus der EX2200-Serie vom deutschen Hersteller Juniper). Wer den Schrank als zusätzliche »Sicherheitsoption« behalten möchte, kann dies natürlich gerne tun.

Regel 5:

Verwende Singlemode zwischen Stockwerken, Gebäuden, Campus, Stadt oder wenn Du dir nicht sicher bist, ob Regel 1 bis 4 zutrifft. Maximale Länge: 60 km+ *

Ist die catch-all Regel. Wenn Regel 1 bis 4 nicht zutrifft, dann gilt diese Regel. Damit macht man nichts falsch, denn sie bietet maximal Flexibilität. Man kann die Faseranzahl deutlich reduzieren - zwei Fasern reichen aus, um mehrere Applikationen (Ethernet, Fibre Channel) parallel zu betreiben oder gar 960 Gbit/s mit geringem Aufwand (Stand Dezember 2014) zu übertragen. Es gibt keine Längen- und Bandbreitenbegrenzung - vor 30 Jahren wurden schon Singlemodedefasern im Boden auf vielen Kilometern vergraben, die damals vermutlich ein paar Megabit/s übertragen haben. Dieselben Fasern transportieren heute mehrere Terabit/s.

* Singlemode-Spans können mehrere hundert Kilometer lang sein. Dazwischen muss das Signal allerdings verstärkt werden (nicht zu verwechseln mit einem aktiven Repeater). Verstärker kommen typischerweise alle 80 bis 100 km zum Einsatz. Ohne Verstärker mittels DWDM (Dichte Wellenlängen-Multiplex oder Dense Wavelength Division Multiplex) und einer Datenrate von 10G pro Wellenlänge sind Längen von ca. 60 km ohne Weiteres überbrückbar.

Quelle: <https://www.flexoptix.net/de/blog/>

Stacking

Stacking (engl.: stacking für Stapeln oder Auf-Schichten) bezeichnet die Verbindung von zwei oder mehr Netzwerkweichen über einen internen (stapelbaren) Datenbus. Dies hat neben der hohen Portdichte den stapeltypischen Vorteil, dass die miteinander verbundenen Geräte nach außen hin als eine Systemeinheit mit nur einer IP-Adresse sichtbar und wartbar sind.

Derartige Verbindungen sind in der Regel breitbandiger als einzelne Verbindungen über Lichtwellenleiter.

DWDM

Das sogenannte Dichte Wellenlängen-Multiplex (engl. Dense Wavelength Division Multiplex, DWDM) gilt zurzeit als leistungsstärkste Variante. Hier liegen die zur Übertragung im Glasfaserkabel verwendeten Wellenlängen (Spektralfarben) sehr dicht beieinander. Der Frequenzbereich der Wellenlängen liegt üblicherweise bei einem Frequenzabstand von 0,4 nm (50 GHz) bis 1,6 nm (200 GHz). Diese geringen Frequenzabstände können nur erreicht werden, indem temperatur- und wellenlängenstabilisierte Laser und hochwertige Filter eingesetzt werden. Hierdurch erhält man Datenübertragungsraten um 10 – 100 Gbit/s pro Kanal bei bis zu 80 Kanälen.

siehe auch: wikipedia.de

AAA

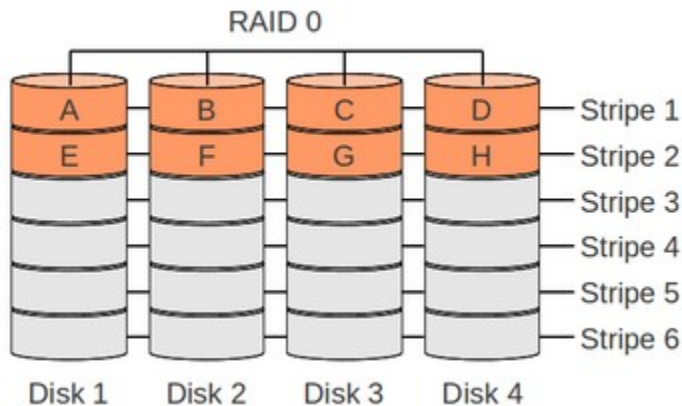
Triple-A-Systeme (oder AAA-Systeme, kurz AAA) werden in großem Umfang bei kabelgebundenen und mobilen Netzwerk-Betreibern sowie Internetdiensteanbietern eingesetzt. Die drei A stehen dabei für Authentifizierung (englisch authentication), Autorisierung (engl. authorization) und Abrechnung (engl. accounting) des Netzwerkzugangs von Kunden (Endkunden). Das Triple-A-System nimmt grundsätzlich nicht am Datenverkehr teil, den es steuert.

OM3-Faserkategorie

Ähnlich wie in der Kupfertechnik wurden zur Kennzeichnung der Übertragungsbandbreiten und des Leistungsvermögens von Multimode- und Monomodefaser optische Klassen und Kategorien eingeführt. Durch den zunehmenden Bandbreitenbedarf und immer höhere Datenraten beim Übergang vom MBit- zum GBit-Bereich, sowie der Einführung von (Multi-)GBit-Protokollen wie zum Beispiel Ethernet, Fibre Channel oder Infiniband, wurden so seit Mitte der 1980er Jahre bisher die Kategorien OM1, OM2, OM3, OM4 und OM5 für Multimodefaser, sowie die Kategorien OS1 und OS2 für Monomodefaser eingeführt.

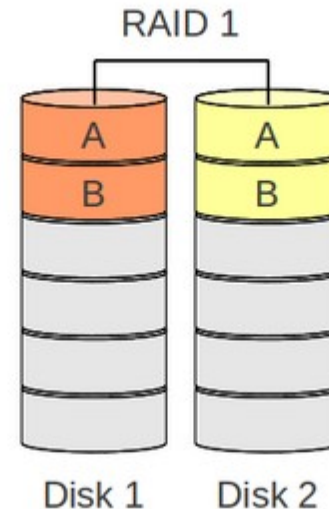
siehe auch: Verbinder für Lichtwellenleiter (LWL)

Ein RAID (Redundant Array of Independent Disks) bezeichnet das Zusammenschalten von mehreren Festplatten oder anderen Datenträgern zu einem einzelnen logischen Laufwerk. Abhängig vom jeweiligen RAID-Level ermöglicht es sowohl höhere Ausfallsicherheit als auch höhere Performance als sie mit einer Festplatte erreichbar ist. RAIDs können dabei mithilfe von Hardware-RAID, Software-RAID oder Firmware/Driver-RAID verwendet werden.



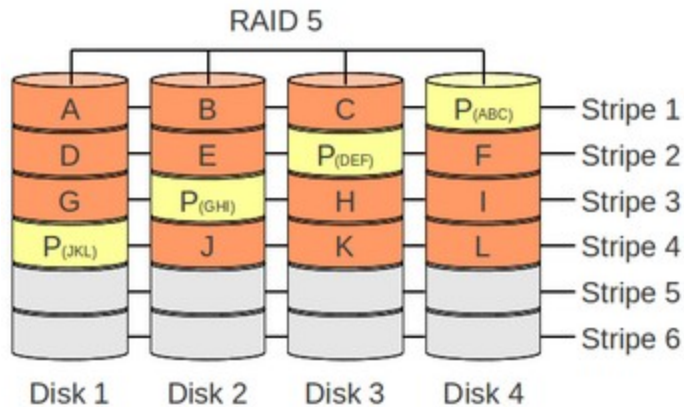
RAID 0

- **Hohe Performance:** sowohl beim Lesen als auch beim Schreiben können mehrere Festplatten parallel genutzt werden.
- **Keine Ausfallsicherheit:** bei einem Ausfall einer Festplatte gehen alle Daten des RAID-Volumes verloren.
- **Kapazitätsausnutzung:** 100%
- **Rebuild:** ein Rebuild nach einem HDD-Ausfall, wie auch bei einem doppelten HDD-Ausfall, ist **nicht** möglich
- **Mindestanzahl an HDDs:** 2



RAID 1

- **Performance:** beim Schreiben ist die Performance nahezu jene einer einzelnen Festplatte; beim Lesen von größeren Datenmengen besteht die Möglichkeit von beiden Laufwerken parallel zu lesen und somit die Lese-Performance zu steigern.
- **Ausfallsicherheit:** alle Daten sind vollständig gespiegelt, der Ausfall einer Festplatte führt zu keinem Datenverlust.
- **Kapazitätsausnutzung:** 50%
- ein Rebuild nach einem HDD-Ausfall ist möglich; die gespiegelte HDD wird einfach auf die andere HDD kopiert.
- **Rebuild nach einem doppelten HDD-Ausfall:** nicht möglich
- **Mindestanzahl an HDDs:** 2

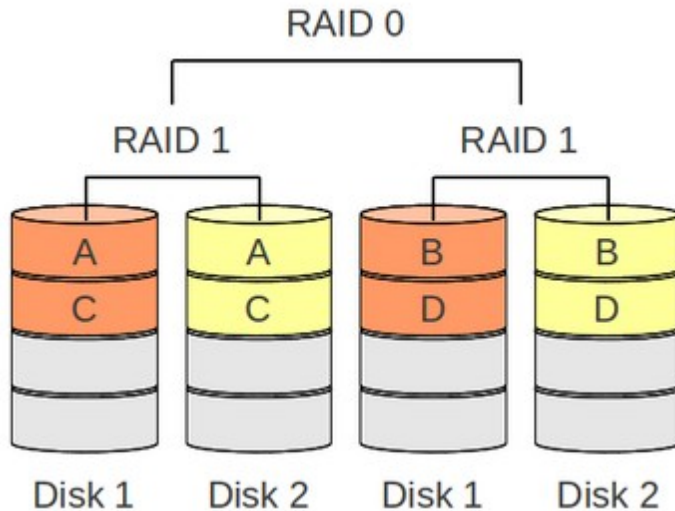


RAID 5

- **Ausfall einer Festplatte führt zu keinem Datenverlust:** da bei einem RAID 1 in Summe nur 50 Prozent der Kapazität der beiden Festplatten nutzbar ist, gibt es mit RAID 5 einen RAID-Level der mit mehreren Festplatten nutzbar ist und ebenfalls wie RAID 1 den Ausfall einer einzelnen Festplatte toleriert.
- **Paritätsdaten:** statt einer vollständigen Spiegelung der Daten werden bei einem RAID 5 Paritätsdaten berechnet. Dazu wird eine logische XOR-Operation (XOR ... Exklusiv-Oder-Gatter) genutzt.
- **Verteilung der Paritätsdaten:** die Paritätsdaten werden über alle vorhandenen Festplatten verteilt und nicht wie bei einem RAID 4 auf einer einzelnen Festplatte gespeichert. Bei einem RAID 4 unterlag diese Paritätsfestplatte einer höheren Abnutzung als die restlichen Festplatten des RAID-Verbundes, daher spielt RAID 4 im Vergleich zu RAID 5 heute kaum noch eine Rolle.
- **Kapazitätsausnutzung:** 67% - 94% (94% bei 16 HDDs)

- **Höhere Lese-Performance:** beim Lesen von größeren Datenmengen können mehrere Festplatten parallel genutzt werden und damit eine höhere Lese-Performance im Vergleich zu einer einzelnen Festplatte erzielt werden.
- **Schreib-Performance:** beim Schreiben von kleinen Datenmengen sind zuvor Lesezugriffe notwendig, damit die neuen Paritätsdaten für das betroffene Stripe berechnet und ebenfalls geschrieben werden können (read-modify-write, write penalty). Bei Hardware RAID-Controllern mit integrierten Caches federn die Caches dieses Problem ab.
- **Initialisierung bei Erstellung eines RAID 5 erforderlich:** damit read-modify-write richtig funktioniert, muss die ursprüngliche Parität korrekt sein. Dies wird durch eine Initialisierung eines RAID 5 bei der Einrichtung des RAID-Sets gewährleistet. Die Initialisierung kann ja nach Größe des RAID-Sets mehrere Stunden bis Tage in Anspruch nehmen. Im Gegensatz dazu erfordern RAID 1 und RAID 6 (zumindest bei einem Linux-Software-RAID) keine Initialisierung.
- **Aufwändiges Wiederherstellen einer ausgefallenen Festplatte:** bei einem RAID 1 genügt es nach einem Festplattenausfall zum Wiederherstellen des RAID-Volumes den Inhalt der verbliebenen Festplatte auf eine neue Festplatte zu kopieren. Fällt eine Festplatte in einem RAID 5 aus, werden bei einem Wiederherstellen auf eine neue Festplatte die Daten aller noch vorhandenen Festplatten gelesen um mittels XOR-Berechnung den Inhalt der ersetzten Festplatte zu berechnen.
- **Rebuild nach einem HDD-Ausfall:** die Berechnung des ursprünglichen Inhalts der HDD ist im Detail von der jeweiligen Implementierung abhängig.
- **Rebuild nach einem doppelten HDD-Ausfall:** nicht möglich
- **Mindestanzahl an HDDs:** 3

siehe auch: wikipedia.de



RAID 10 (gesprochen: RAID Eins Null)

- bietet hohe Performance wie RAID 0,
- kombiniert mit der Datensicherheit von RAID 1
- **Kapazitätsausnutzung:** 50%
- **Rebuild:** Rebuild nach einem HDD-Ausfall ist möglich; die gespiegelte HDD wird einfach auf die andere HDD kopiert
- **Rebuild nach einem doppelten HDD-Ausfall:** nur möglich wenn zwei Festplatten von unterschiedlichen Spiegeln betroffen sind, dann gespiegelte HDDs jeweils kopieren
- **Mindestanzahl an HDDs:** 4

RAID Datenrettung

Hinweis: In bestimmten Fällen - etwa beim Ausfall mehrerer Festplatten - kann es auch bei RAID-Systemen zu Datenverlust kommen.

Symptome: (bevorstehender) Datenverlust

- Eine oder mehrere Festplatten sind ausgefallen: Je nach RAID-Level befindet sich das RAID nach dem Ausfall einer oder mehrerer Festplatten im **degraded**- oder **offline**-Modus.

Degraded bedeutet, dass das RAID noch funktionstüchtig ist, jedoch nicht mehr "optimal" (alle Platten sind korrekt im Verbund) ist. Die defekten Festplatten müssen ausgetauscht werden, danach wird ein sogenannter Rebuild durchgeführt.

Im **Offlinemodus** sind zu viele Festplatten ausgefallen. Der RAID-Controller kann somit keine Daten mehr liefern, es liegt nicht mehr ausreichend Redundanz vor. Ein Datenretter muss gerufen werden, um professionell zu helfen.

- **Langsamerer Zugriff:** Wenn Festplatten in einem RAID-Verbund ausgefallen sind, dieser aber noch nicht offline ist, sinkt die Performance oft massiv. Somit ist in diesem Fall eine Kontrolle des RAIDs empfehlenswert.
- Der RAID-Controller oder die Monitoring-Software zeigt Fehlermeldungen wie

RAID degraded, RAID offline, RAID SUB-Optimal, RAID critical, DISK failed, Drive missing

In allen Fällen liegt ein Defekt mindestens eines Datenträgers - sei es nun eine Festplatte oder eine SSD - vor.

RAID-Gefahren

- **Rebuild-Vorgang:** Hierbei handelt es sich um die größte Gefahr. Während des normalen Betriebs werden in der Regel nur wenige Bereiche des RAID benötigt (z.B. die mit aktuellen Dokumenten oder Datenbanken). Bei einem Rebuild müssen alle Sektoren aller verbleibenden Festplatten im Verbund vollständig gelesen werden, damit die Daten für die getauschte Platte berechnet werden können. Die Wahrscheinlichkeit, dass eine weitere Festplatte bei diesem Prozess ausfällt, ist überdurchschnittlich hoch. Die Labors für Datenrettung erhalten laufend RAID-Systeme zur Datenrettung, welche während eines Rebuilds endgültig ausgefallen sind.
- **Identische Festplatten:** In der Regel werden RAID-Systeme mit baugleichen Festplatten aus einer Charge geliefert. Dies soll Performance-Vorteile sowie Stabilitätsvorteile mit sich bringen. Fakt ist jedoch, dass bei einem Ausfall einer dieser Festplatten die Wahrscheinlichkeit hoch ist, dass weitere Festplatten mit demselben Fehlerbild in nächster Zeit ausfallen, ganz nach dem Motto: Selbe Charge, selbe Probleme. Generell sollte darauf geachtet werden, dass die Parameter (Umdrehung, Zugriffszeit, etc.) der Festplatten identisch sind, dann kann man auch auf verschiedene Festplatten oder zumindest verschiedene Chargen eines Modells zurückgreifen.
- **Falscher Datenträger wird getauscht:** Auch beim Tausch einer defekten Festplatte lauert Gefahr. Entweder erwischt man irrtümlich die falsche Festplatte (also ein Datenträger, der in Ordnung ist und entfernt wird, dadurch geht das RAID dann offline) oder aber es wird am RAID eine falsche LED "rot" angezeigt.
- **Befehl »Force online«:** Dies ist mit Abstand eine der gefährlichsten Operationen bei einem RAID-System. Leider wird sie trotzdem oft vom Support von Server-Herstellern oder RAID-Controllern empfohlen, ist jedoch oft fatal. Gerade wenn mehrere Festplatten ausgefallen sind und das RAID offline ist, empfehlen Hersteller die ausgefallenen Festplatten "online zu forcen". Dies führt oft dazu, dass eine bereits noch früher ausgefallene Festplatte wieder in den Verbund aufgenommen wird. Beim Start des Betriebssystems wird dann aber wegen Inkonsistenzen meist ein Filesystem-Check angefordert (chkdsk, fsck) und in weiterer Folge die Dateisystemstrukturen zerstört. Also: Nie ein "Force online" ausführen, wenn wichtige Daten am RAID-System enthalten sind, die nicht gesichert sind.
- **Firmwareupgrade am RAID-Controller:** In Dateien wie readme.txt wird oft darauf hingewiesen, vor dem Firmwareupgrade ein vollständiges Backup zu machen. Jedoch halten sich die wenigsten daran. Bei einem Firmwareupgrade werden oft RAID-Parameter durch die neue Firmware geändert und es ist anschließend kein Zugriff mehr möglich.
- **Resize (expand, RAID-Level ändern, etc.):** So wie ein Firmwareupgrade ist auch ein Resizen von RAID ein sehr gefährlicher Vorgang. Wiederum gilt: Keinesfalls ohne vollständiges verifiziertes Backup ein Expand, eine Änderung des RAID-Levels oder Ähnliches durchführen.

- **Festplattenroulette:** Auch das wahllose Tauschen von Festplatten bei einem RAID-Ausfall ist nie eine Lösung, denn der Schaden wird immer nur noch größer.
- **Herstellersupport:** Wider Erwarten ist auch der Herstellersupport von Server-Systemen, sowie RAID-Systemen (auch von den Top-Herstellern) eine nicht zu unterschätzende Gefahr: vor allem bei Call-Center gibt der First-Level-Support häufig Antworten aufgrund einer Frage-Antwort-Liste. Oft bekommen dann Kunden, die bei Herstellern aufgrund eines RAID-Ausfalls angefragt haben, gesagt: löschen Sie einfach das RAID und legen Sie es neu an, dann geht das RAID wieder. Dies gilt zwar für das RAID als Laufwerk, die Daten sind dann aber weg - absolut fatal.
- Vollständiges Backup vor Resize oder Firmwareupgrades.
- Eine generelle Backup-Strategie, deren Funktion auch regelmäßig verifiziert wird.

Korrektes Verhalten im Ernstfall

Das oberste Gebot lautet: Keine Panikreaktionen! Reagieren Sie nicht unüberlegt! Die Gefahr, dass der Schaden größer wird, ist sehr hoch.

Vorbeugung von Datenverlust

- Höhere Redundanz: Bei einem RAID 6, statt eines RAID 5, dürfen zwei Festplatten, statt nur einer ausfallen.
- Einsatz von Spare Festplatte(n): Sind Spare-Festplatten in einem RAID-System vorhanden, wird bei einem Ausfall einer Platte das RAID sofort auf die Spare-Festplatte rebuildet, ohne dass eine Festplatte ausgetauscht werden muss. Der Einsatz von Spare-Festplatten ist somit jedenfalls empfehlenswert.

SATA-Controller-Modi

Serial-ATA- (SATA-)Controller-Modi bestimmen, wie die Festplatte mit dem Computer kommuniziert. Sie können einen von drei Controller-Modi für eine SATA-Festplatte festlegen: IDE, AHCI oder RAID. Der RAID-Modus aktiviert gleichzeitig auch die AHCI-Funktionen.

- Der IDE-Modus ist der einfachste Modus. Im IDE-Modus wird die Festplatte als IDE- oder Parallel-ATA- (PATA-)Festplatte betrieben.
- Der Advanced-Host-Controller-Interface- (AHCI-)Modus ermöglicht die Verwendung von erweiterten Funktionen auf SATA-Festplatten, z. B. Hot-Swapping und Native Command Queuing (NCQ ; übersetzt: integrierte Befehlsreihung; die HDD entscheidet selbst, über die Reihenfolge der Abarbeitung von mehreren Anfrage; NCQ kann die Bewegung des Lese/Schreibkopfes verringern).
- Im RAID-Modus können verschiedene Festplatten als ein Speicherbereich (die Matrix) fungieren. Ziel ist es dabei, entweder die Daten durch Redundanz zu sichern oder die Transferraten zu steigern (durch parallele Schreib- und Lesevorgänge von den bzw. auf die Platten).

Hinweis: Die Einrichtung des SATA-Controller-Modus sollte **vor** der Installation des Betriebssystems erfolgen. Das Ändern des Modus nach der Installation des Betriebssystems kann das System am Starten hindern. Alle SATA-Festplatten können per Definition im laufenden Betrieb (Hot Swapping) ausgetauscht werden.

Hot-Spare-Festplatten

Eine Hot-Spare-Festplatte ist eine in einem System in Reserve (spare) gehaltene (normalerweise nicht verwendete) Festplatte. Fällt eine andere Platte aus, wird die Hot-Spare-Platte im laufenden Betrieb (hot) automatisch anstelle der defekten eingebunden.

Die Festplatte ist im fehlerfreien Betrieb abgeschaltet und wird erst bei Bedarf per Software angeschaltet. Dies dient zur Schonung der mechanischen Bestandteile der Festplatte. Dies ist insbesondere in einem RAID sinnvoll, in dem die Daten der defekten Festplatte automatisch rekonstruiert werden können (Rebuild).

Während des Rebuilds auf die Hotspare-Platte lässt die Performance des RAID deutlich nach. Der Rebuild benötigt bei RAID 1 weniger Zeit als bei RAID 5, da bei RAID 5 zusätzlich Paritätsinformationen rekonstruiert werden müssen. Je mehr Festplatten in einem RAID-5-Verbund sind, desto länger dauert der Rebuild bzw. desto schlechter ist die Performance während eines Defekts einer Festplatte.

Hot Swapping

Mit Hot Swapping bietet sich die Möglichkeit, Speichermedien im laufenden Betrieb auszutauschen. Dazu muss der Bus-Controller Hot-Plugging unterstützen (i. d. R. nur SCSI, SAS oder SATA). Damit es nicht zu einem Ausfall des Systems führt, ist ein Austausch nur in Arrays mit redundanter Datenhaltung möglich – bei einem RAID-0-System würde das Ersetzen (bzw. Entfernen) eines Mediums unweigerlich zum Ausfall führen.

Hardware-RAID

Sind die Festplatten an einen RAID-Adapter angeschlossen, lässt sich auch das Betriebssystem auf einem RAID-System installieren. Beachte: Wenn man ein RAID-0-Verbund einrichtet, gehen alle bisher auf der Festplatte gespeicherten Daten verloren.

1. Falls der RAID-Adapter als Chip auf der Hauptplatine sitzt, muss die RAID-Funktion zunächst über die BIOS-Einstellungen einschaltet werden. Wie das geht, steht in der Bedienungsanleitung der Hauptplatine. Bei RAID-Steckkarten ist die RAID-Funktion immer eingeschaltet.
2. Praktisch alle RAID-Adapter haben ein eigenes BIOS. Über dessen Einstellungen lassen sich die Festplatten zu einem RAID-Verbund zusammenfassen und die Betriebsart (RAID-Level 1, 5, ...) festlegen. Da jeder Hersteller sein eigenes RAID-BIOS hat, unterscheidet sich die genaue Vorgehensweise von Adapter zu Adapter (siehe: Bedienungsanleitung).
3. Installieren Sie Windows. **Achtung:** Damit das Betriebssystem die RAID-Funktion nutzen kann, muss schon bei der Installation ein Treiber für den RAID-Adapter eingerichtet werden. Für ältere RAID-Adapter ist oft ein Treiber auf der Windows-Installations-CD enthalten. Dieser wird dann automatisch eingerichtet. Bei neueren RAID-Adaptoren muss man den Treiber extra installieren.

Wie sicher ist Hardware-RAID?

Mehr Datensicherheit bieten alle RAID-Betriebsarten mit Ausnahme von RAID 0. Ein RAID-System kann jedoch keine regelmäßige Datensicherung ersetzen! Denn die automatische Spiegelung der Daten schützt nur vor Festplattenausfällen. Geht eine Festplatte kaputt, kann sie einfach ersetzt werden.

Vor Bedienungsfehlern und vor Schadprogrammen bietet ein RAID-System dagegen keinen Schutz: Wird eine Datei auf einer Festplatte gelöscht, wird sie automatisch auch von den anderen Festplatte entfernt. Davor schützen nur regelmäßige Backups und Sicherheitskopien.

Was sollte man, bei einem Festplattenausfall beachten?

Für den Austausch einer defekten Festplatte, sollte am besten identische Festplatte gewählt werden.

- gleiche oder größere Speicherkapazität
- Festplatten vom gleichen Hersteller
- gleiche technische Eigenschaften (Umdrehungszahl, Zugriffszeiten, ...)
- Festplatten sollten am besten Fabrikneu sein; bei einer bereits partitionierte und formatierte Festplatte, sollte die Partition unbedingt gelöscht werden; für das BIOS ist eine Festplatte mit gelöschter Partition eine fabrikneue Festplatte

Bei einem Festplattenausfall, kann diese im laufenden Betrieb durch eine identische Festplatte ausgetauscht werden (Hot Swapping, defekte Festplatte entfernen → kurz abwarten → neue Festplatte einbauen). Der Rebuild-Vorgang sollte sofort automatisch starten. Der Rebuild-Vorgang kann bei RAID 1 einige Minuten bis mehrere Stunden dauern. Bei RAID 5 (bedingt durch die umfangreiche Berechnung, XOR-Verknüpfung) kann der Vorgang mehrere Stunden bis Tage dauern.

Anmerkung: Ein automatisch startendes Backup oder andere automatisch startende Vorgänge, sollten während eines Rebuilds deaktiviert werden.

Memtest86 ist eine Software, mit der man den Arbeitsspeicher eines Computers auf Fehler überprüfen kann. Das Programm überprüft Arbeitsspeicher mittels eines Stresstests auf Fehler und zeigt gegebenenfalls die Speicheradresse von fehlerhaften Speicherzellen in einer Liste an.

Aufgrund der Arbeitsweise von Memtest bedeuten gefundene Defekte nicht zwangsläufig einen defekten Arbeitsspeicher. Es kann sich auch um einen Defekt der CPU oder des Mainboards handeln, wobei der Arbeitsspeicher die bei weitem häufigste Fehlerquelle darstellt.

Memtest86 kann von CD gestartet werden, es stehen aber auch Versionen für USB-Stick zur Verfügung.

Memtest86+, geschrieben von Samuel Demeulemeester, ist eine Abspaltung auf Basis der Version 3.0 von Chris Bradys Memtest86. Das Projekt entstand, da das Original von Mai 2002 bis März 2004 nicht aktualisiert wurde.

Mittlerweile wird das ursprüngliche Memtest86 von der australischen Firma PassMark weiterentwickelt.

Download: <https://www.heise.de/download/product/memtest86-15466>; www.memtest.org/#downiso

1. Bootfähiger USB-Stick mit Auto-Installer erstellen

USB-Stick (Dateisystem: FAT32) in einen Port eines Rechners stecken. **Vorsicht!** Alle Daten auf dem Speicherträger werden gelöscht.

- ZIP-Datei entpacken und die enthaltene Datei anklicken
- Lizenzbestimmungen zustimmen
- Laufwerkbezeichnung des USB-Sticks auswählen
- Button »**Create**« anwählen, um ein mit Memtest86 bootfähigen USB-Stick zu erstellen

2. Bootreihenfolge im BIOS überprüfen, ändern

Bei den meisten Rechnern gelangt man in die BIOS-Einstellungen durch Drücken der Tasten [Entf] oder [F2] oder [F12] direkt nach dem Einschalten des Computers. Bei vielen Mainboards kommt man mit dem Drücken der Taste [F8] direkt in ein Bootauswahlmenu.

- Bei aktivierten **Secure Boot** (bei aktivierten Secure-Boot werden nur digital signierte Bootloader geladen) ist ein Setup-Passwort zu vergeben und anschließend **Secure Boot** zu deaktivieren.
- Bei aktivierten **Fast Boot** oder **Quick Boot** (verkürzter Hardware-Test) ist der Fast Boot zu deaktivieren. Bei aktivierten Fast Boot wird ein bootfähiger USB-Stick oder CD/DVD nicht erkannt.
- **Hinweis:** Nicht alle USB-Ports sind bootfähig (Port wechseln). Dies gilt auch für einige wenige USB-Sticks.

3. Memtest86 ausführen

Wenn im USB-Modus gebootet wird, muss man bei einer eventuell erscheinenden Eingabeaufforderung **mt501** eingeben und mit **[Enter]** bestätigen. **501** steht für die jeweilige Versionsnummer, hier 5.01. (eine bootfähige CD sollte auf jeden Fall automatisch starten).

Der Speichertest beginnt automatisch und es werden sofort Werte in die jeweiligen Speicheradressen des Hauptspeichers ein- und ausgelesen und miteinander abgeglichen.

Es werden jeweils 8 Testläufe durchgeführt. Wieweit der Speichertest fortgeschritten ist, lässt sich rechts oben unter dem Wert **Pass** erkennen.

Mit der Taste **[ESC]** kann der Speichertest jederzeit abgebrochen werden.

Mit der Taste **[C]** kann man die Standard-Konfigurationseinstellungen anpassen oder den Test neu starten.

Ob Fehler und wie viele Fehler aufgetreten sind, erfährt man in der Ergebnis-Tabelle unter den Spalten **Errors** und **ECC Errs**. Steht dort auch nach mehreren Durchgängen eine Null, ist der Arbeitsspeicher in Ordnung.

Erkennt Memtest86 einen Fehler wird die Tabellenzeile rot markiert.

Um die Fehlersuche im Vorfeld einzuschränken, wird empfohlen, die Speichermodule auf dem Mainboard einzeln zu testen. **Achtung:** Ein Test kann mehrere Stunden andauern.

Hinweise und Arbeitsweise von Memtest

Aufgrund der Arbeitsweise von Memtest bedeuten gefundene Defekte nicht zwangsläufig einen defekten Arbeitsspeicher. Es kann sich auch um einen Defekt der **CPU** (z.B. verbogene Pins) oder des **Mainboards** handeln, wobei der Arbeitsspeicher die bei weitem häufigste Fehlerquelle darstellt.

WallTime: die gesamte Laufzeit von Memtest im H:MM:SS; **Pass**: Anzahl der Testdurchläufe; **Errors**: Fehleranzahl

```

Memtest86+ v4.20 | Pass 33% #####
Intel Core Gen2 3398 MHz | Test 10% ###
L1 Cache: 32K 135923 MB/s | Test #6 [Moving inversions, 32 bit pattern]
L2 Cache: 6144K 55706 MB/s | Testing: 184K - 512M 512M
L3 Cache: None | Pattern: 00000010
Memory : 512M 16657 MB/s |-----
IMC : Intel(R) Core(TM) i7-2600 CPU @ 3.40GHz / BCLK : 0 MHz
Settings: RAM : 0 MHz (DDR3- 0) / CAS : 12-4-12-91 / Dual Channel

WallTime  Cached  RsvdMem  MemMap  Cache  ECC  Test  Pass  Errors  ECC Errs
-----
0:00:21  512M      0K      e820    on   off  Std    0      0

(Esc)Reboot  (c)configuration  (SP)scroll_lock  (CR)scroll_unlock

```

BIOS/UEFI

Das BIOS (Basic Input Output System) oder UEFI (Unified Extensible Firmware Interface) sitzt auf einem eigenen speziellen Speicherbaustein.

Dieser hat die Eigenschaft, dass er mehrmals neu programmiert, also mit neuen Daten beschrieben werden kann, die auch bestehen bleiben, wenn der Computer nicht mit Strom versorgt wird.

Hinweis: Ändere nie ein gut funktionierendes technisches System. Es sei denn, es gibt gute Gründe für diese Änderung.

Wann ist ein BIOS/UEFI-Update empfehlenswert?

- Fehlermeldungen, die vom BIOS verursacht werden
- durch ein BIOS-Update wird die Unterstützung von neuer Hardware (Prozessor, Hauptspeicher) installiert
- Entfernung von Schadsoftware, die sich im BIOS eingenistet hat

Voraussetzung: Das BIOS-Update (vom Hersteller des Mainboards) muss explizit mit dem verbauten Chip auf dem Mainboard kompatibel sein.

Bei einem Firmware-Update werden Software und Treiber des gesamten Mainboards, einschließlich des BIOS, aktualisiert.

Informationen über Mainboard und BIOS ermitteln:

[W] + [R] → systeminfo

Windows-Programme: CPU-Z, Hwinfo, Mainboard-Manual

Arten von BIOS-Update-Installationen

Für das Update gibt es kein einheitliches Prozedere. Das Update unterscheidet sich je nach Hersteller oder Computer-Modell.

- ein komplettes Update-Paket mit den Installationshinweisen, das unter Windows installiert wird; **Hinweis:** Virens Scanner und alle anderen offenen Anwendungen sind vor dem Update zu schließen; die Hersteller bieten mitunter die Aktualisierung der gesamten Firmware an (ratsam oder nicht, das muss jeder selbst entscheiden)
- Update über eine im BIOS integrierte Shelloberfläche (Menü: Flash, Update, in der erweiterten Ansicht oder über ein Bootmenü); die Update-Datei befindet sich auf einen FAT/FAT32-formatierten USB-Stick
- Update über ein bootfähigen USB-Stick, einschließlich mit der auf dem Datenträger befindlichen Update- (Binär-Datei) und Steuerungsdatei.

Im nachfolgenden, wird das Update über ein bootfähigen USB-Stick und über eine im BIOS integrierte Shelloberfläche behandelt.

1. Update über ein bootfähigen USB-Stick

Einige Hersteller stellen ZIP-Archive zur Verfügung, die beim Entpacken ein USB-Stick bootfähig machen und mit den entsprechenden Update-Dateien versorgen.

Im nachfolgenden Beispiel wird ein USB-Stick manuell bootfähig gemacht, mit einem Mini-Betriebssystem und den Update-Dateien bestückt.

A: Bootfähigen DOS USB-Stick erstellen

i. Bootfähigen DOS USB-Stick unter Windows erstellen

Rufus ist ein Open Source Programm lizenziert unter der GPL.

- Download von der Rufus Webseite (rufus.akeo.ie)
- Rufus muss nicht installiert werden. Nach dem Download muss das Programm mit Administratorrechten ausgeführt werden.
- Ein Download von FreeDOS ist nicht erforderlich, da es via Rufus per Vorlage direkt installiert wird.

Um mit Rufus einen bootfähigen DOS-USB-Stick erstellen zu können, muss man nach dem Start des Programmes folgende Einstellungen vornehmen:

- **Laufwerk:** Auswahl des entsprechenden USB-Sticks
- **Startart:** im Dropdown-Menü »FreeDOS« auswählen
- **Partitionsschema:** hier sollte man »MBR« auswählen
- **Zielsystem:** »BIOS (bzw. UEFI-CSM)« auswählen
- **Dateisystem:** »FAT32 (Standard)« auswählen

Mit einem anschließenden Klick auf START wird der DOS-USB-Stick automatisch erstellt.

ii. Bootfähigen DOS USB-Stick unter Linux erstellen

Eine weitere Möglichkeit, um FreeDOS auf einen USB Stick zu installieren, bietet sich mit UNetbootin an. Es ist für alle gängigen Betriebssysteme - auch für Linux - verfügbar.

Voraussetzung für die Installation ist ein FAT/FAT32 formatierter USB-Stick. Unter Ubuntu und ähnlichen Linux-Distributionen ist folgendes Kommando auszuführen:

- USB-Stick ist z.B. das Device `/dev/sdb`
- `sudo umount /dev/sdb1`
- `sudo mkfs.vfat -F 32 /dev/sdb1`

DOS-Stick mit UNetbootin erstellen

- Unter Ubuntu wird es über **apt-get install unetbootin** installiert; UNetbootin ist in vielen **Linux-Live-Distributionen** bereits enthalten
- Ein Download von FreeDOS ist nicht erforderlich, da UNetbootin FreeDOS und andere Distributionen selbstständig herunterladen und installieren kann.
- USB-Stick in ein USB-Port stecken
- UNetbootin aufrufen und im Dropdown-Menü FreeDOS auswählen
- den bootfähig zu machenden USB-Stick auswählen und die Auswahl bestätigen; erscheint der USB-Stick nicht in der Liste, so ist er erst einzuhängen/mounten
- FreeDOS wird von UNetbootin heruntergeladen, extrahiert und installiert
- Nach einem Neustart des Rechners steht FreeDOS zur Verfügung.

B: BIOS-Update mit einem bootfähigen USB-Stick

Die Update-Datei - meist eine EXE- oder ZIP-Datei – ist von der Webseite des Herstellers herunterzuladen. Die ZIP-Datei ist zu entpacken. Neben dem Flash-Programm sollte sich mindestens eine binäre Datei im entpackten Verzeichnis befinden.

Befindet sich in den entpackten Dateien auch eine Datei namens »Autoexec.bat« oder »Update.bat«, ist das Update besonders leicht zu handhaben. Die Batch-Datei startet das Flash-Programm automatisch mit den entsprechenden Parametern. Die Update-Dateien, das Flash-Programm, die EXE-Datei oder ähnliche Dateien, sind auf dem bootfähigen USB-Stick zu speichern.

A: bootfähiger USB-Stick mit den Update-Dateien in ein USB-Port stecken und den Rechner neu starten

B: am DOS-Prompt den Namen des Flash-Programmes oder der Batch-Datei eingeben und mit [Enter] bestätigen

C: einige Flash-Programme bieten die Erstellung eines Backups des alten BIOS an

D: es ist den Anweisungen des Flash-Programmes zu folgen

E: mit einem Neustart des Rechners wird das BIOS-Update abgeschlossen

Was kann man tun, falls nach dem BIOS-Update Probleme auftauchen?

- Eventuell legt das neue BIOS bestimmte Einstellungen in einem anderen CMOS-Register ab – so können Konflikte entstehen. In diesem Fall, kann man am ausgeschalteten Rechner versuchen, das CMOS zu löschen. **Hinweis:** Mit dem Löschen des CMOS, wird nicht das BIOS gelöscht.
- Herstellen des alten Zustandes, durch die Installation der Backup-Datei oder eines älteren BIOS-Update (siehe: Webseite des Herstellers). Vor dem Neustart des Rechners, sollte auch hier eventuell das CMOS gelöscht werden.

2. Update über eine im BIOS Integrierte Shelloberfläche

Das aktuelle BIOS/UEFI-Update ist vom Hersteller des Mainboards herunterzuladen und auf ein USB-Stick mit FAT/FAT32 Formatierung gespeichert. Die ausführbare Datei, die den BIOS-Update initiiert und durchführt, sollte sich im Wurzelverzeichnis des USB-Stick befinden. Der USB-Stick muss **nicht** bootfähig sein.

Das Update wird am Beispiel eines Supermicro Mainboard beschrieben.

A: USB-Stick mit den BIOS/UEFI-Dateien in ein USB-Port stecken

B: Rechner neu starten und über die Funktionstaste **[F11]** das Bootmenü aufrufen

C: im Bootmenü die Auswahl »**UEFI: Built-in EFI Shell**« mit den Pfeiltasten auswählen und mit **[Enter]** bestätigen

D: Die Hinweise der Shelloberfläche sollte man sehr genau lesen. Der USB-Stick wird im Beispiel mit **fs0:** (Doppelpunkt nicht vergessen) angesprochen. Falls sich die ausführbare Datei nicht Wurzelverzeichnis des USB-Stick befindet, wechselt man über **cd <VERZEICHNIS>** in das entsprechende Verzeichnis.

E: mit **flash.nsh <MAINBOARD-ORDNER>** (z.B. flash.nsh x10dri16.913) wird das BIOS-Update initiiert; im Mainboard-Ordner befinden sich die eigentlichen Update-Dateien

F: mit einem Neustart des Rechners wird das BIOS-Update abgeschlossen

Anmerkung: Bei einigen Mainboards kann die Vorgehensweise (Pkt. 1 und 2) von der hier beschriebenen Art und Weise ein wenig abweichen.

CMOS-Reset oder BIOS-Passwort zurücksetzen

Wann sollte ein CMOS-Reset durchgeführt werden?

Bei BIOS-Fehlermeldungen wie z.B. "CMOS Checksum Error", um ein vergessenes BIOS-Passwort zurückzusetzen oder möglicherweise nach einem BIOS-Update.

Hinweis: Das CMOS ist nicht das BIOS. CMOS (Complementary Metal-Oxide Semiconductor) ist vielmehr ein batteriegepufferter, statischer, also flüchtiger Speicherbaustein (SRAM), in dem die BIOS-Parameter gespeichert werden.

Bei einigen Notebooks wird das Passwort in einem integrierten IC-Baustein (Diebstahlschutz) gespeichert. Hier hilft es wenig, wenn man das CMOS löscht. Abhilfe schafft hier meistens nur ein direkter Kontakt zum Herstellersupport.

Der Speicher verliert seinen Inhalt, wenn die Stützbatterie (CMOS-Batterie) entfernt wird. Die Zeitdauer bis zum kompletten Datenverlust kann aber, je nach CMOS-Typ, zwischen **wenigen Sekunden, einigen Stunden**, oder **mehreren Tagen** liegen.

Somit hilft es meistens nichts, wenn man die CMOS-Batterie nur für kurze Zeit entfernt!

Aus diesem Grund besitzen die meisten PC-Mainboards einen Jumper (Steckbrücke) oder 2 Lötunkte die man mit einem geeigneten Werkzeug überbrücken kann (siehe: Manual des Motherboards), mit dem das CMOS sofort gelöscht wird. Der Jumper (Steckbrücke) befindet sich häufig in der Nähe der CMOS-Batterie. Bei Notebooks fehlt dieser Jumper häufig.

Einige Hersteller benutzen einfache Tastschalter für Power, Reset und CMOS-Reset auf ihren Mainboards, wobei die Arbeitsweise des CMOS-Reset-Tastschalters die gleiche ist wie die eines CMOS-Reset-Jumpers.

Die meisten Mainboardhersteller bieten auf ihren Webseiten im Downloadbereich ein Handbuch (Manual) für das jeweilige Mainboardmodell an, in dem sich eine Layoutzeichnung befindet, auf der die Position des Jumpers eingezeichnet ist.








Achtung: Starte niemals das Mainboard, wenn der CMOS-Jumper auf der Löschposition sitzt! Dadurch kann ein Kurzschluss entstehen, der das Mainboard zerstört!

Hinweis: Falls kein Jumper vorhanden ist oder wenn man nicht tagelang warten möchte, kann man als letzte Möglichkeit (auf eigene Gefahr) mit einer 10 Euro-Cent-Münze in den Batteriesockel, die Plus-/Minuskontakte des Batteriesockels überbrücken (wirkt wie ein Jumper). **Voraussetzung:** Der PC ist stromlos (Netzstecker ziehen) und bei Notebooks sind alle Akkus zu entfernen.

Achtung: Starte niemals das Mainboard, wenn die Münze noch im Batteriesockel liegt! Dadurch kann ein Kurzschluss entstehen, der das Mainboard zerstört!

Falls das erste CMOS-Reset erfolglos war, kann man den Reset-Versuch mehrmals wiederholen.

Schirmungskonzepte

Abkürzung	Bedeutung	Verwendung	
UTP*	„Unshielded Twisted Pair“ – ungeschirmtes, paarverseiltes, symmetrisches Kupferdatenkabel mit 2 oder 4 Adernpaaren	– lokale Netzwerke im arbeitsplatznahen Bereich, Anschluss- oder Installationskabel	
S/UTP	„Screened Unshielded Twisted Pair“ – 2- oder 4-paariges, paarverseiltes, symmetrisches Kupferdatenkabel mit einem zusätzlichen Gesamtschirm	– Installationskabel für Etagenverkabelung	
FTP	„Foil Twisted Pair“ – foliengeschirmtes, paarverseiltes, symmetrisches Kupferdatenkabel	– Installationskabel für Etagenverkabelung	
S/FTP	„Screened Foil Twisted Pair“ – geflecht- und foliengeschirmtes, paarverseiltes, symmetrisches Kupferdatenkabel	– Installationskabel für Etagenverkabelung	
STP	„Shielded Twisted Pair“ – 2- oder 4paariges, symmetrisches Kupferdatenkabel mit einzeln abgeschirmten Adernpaaren	– für Datenübertragungsraten bis 100 MBit/s – für den arbeitsplatznahen Bereich, z. B. zwischen Etagenverteiler und informations-technischem Anschluss	
S/STP	„Screened Shielded Twisted Pair“ – 2- oder 4paariges Kupferdatenkabel mit einzeln abgeschirmten Adernpaaren und zusätzlichem Gesamtschirm	– Installationskabel für Etagenverkabelung	
PiMf	„Paar in Metallfolie“ – mit Metallfolie geschirmtes, verdrehtes Paar eines Kupferdatenkabels mit hoher Nahnebensprechdämpfung	– Verkabelung großtechnischer Anlagen – Übertragung hoher Bitraten – Installationskabel für Etagenverkabelung	
ViMf	„Vierer in Metallfolie“ – mit Metallfolie geschirmter Vierer aus vier Adern eines Kupferdatenkabels	– Installationskabel für Etagenverkabelung	

Alternativer Weg ins BIOS bei Windows-Rechner

Wenn man partout nicht per Tastenkombination ins BIOS kommt, dann gibt es bei Windows 10 Systeme auch einen Weg über das Betriebssystem zur Firmware des Computers (Windows Boot Optionen Menü).

Ins Boot Optionen Menü kommt man am einfachsten, indem man den Computer mit gedrückter Shift-Taste bzw. Hochstelltaste aus Windows heraus neu startet. Den Aufruf des BIOS beim nächsten Computerstart lässt sich dann über die Schaltfläche »Problembehandlung« im Hauptmenü der Windows Boot Optionen aktivieren. **Hinweis:** Diese Möglichkeit wird nicht von allen Systemen unterstützt.

BIOS

Das BIOS – BIOS steht für Basic Input/Output System – 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.

Bei vielen PCs oder Notebooks wird heutzutage kein separates Installationsmedium in Form einer DVD oder CD mehr mitgeliefert. Um dem Nutzer trotzdem die Möglichkeit einer Neuinstallation des Betriebssystems zu geben, findet sich auf den verbauten Festplatten häufig eine sogenannte Recovery Partition (die Recovery-Partition kann mit einer Tastenkombination aufgerufen werden – siehe: Manual).

Anbieter	Modell	Aufruf des BIOS	Aufruf des Boot-Menüs	Weitere Tastenkombination
ASRock	Deskmini	F2 oder Entf	F11	F12: Diagnostics; Tab: Monitorwechsel
Asus	X Series, Zenbook	F2 oder Entf	Esc oder keine Taste	Asus empfiehlt, die Tasten bei Druck des Start-Knopfes zu drücken und so lange gedrückt zu halten, bis das Menü erscheint.
Dell	Inspiron, Latitude, Optiplex	F2	F12	
Intel	NUC	F2	F10	F7: BIOS Update
Lenovo	ThinkPad	F1	F12	F10: Lenovo Diagnostics - nicht bei allen Modellen
Medion	Akoya Exxx	F2	F10	
Samsung	R510	F2	Esc	
terra	Ultrabook	F2	F7	
Toshiba		Esc		die Taste ist vor dem Druck des Start Knopfes gedrückt zu halten

Die Recovery-Partition ist versteckt und damit im Dateimanager des Betriebssystems nicht sichtbar.

UEFI: 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.

Übersicht der Pieptöne: AWARD/PHOENIX-BIOS		
Tonfolge	Betroffene Komponente	Problemlösung
1 kurzer Ton	keine	Startkontrolle erfolgreich durchlaufen
2 kurze Töne	unkritischer Fehler, Anzeige auf dem Bildschirm (z.B. »Keyboard Error«)	mit Druck auf F1 lässt sich der Startvorgang meist fortsetzen.
kurze, wiederholende Töne	Stromversorgung Mainboard	Stromanschlüsse vom Netzteil an der Hauptplatine prüfen
kurze und lange Töne im Wechsel, wiederholend	fehlerhafte Prozessorspannung	Stromversorgung der CPU auf der Hauptplatine prüfen
1 langer Ton	Arbeitsspeicher	Taktfrequenzen der Speichermodule im Bios/Uefi sowie den Sitz im Steckplatz prüfen
3 lange Töne	Tastaturbaustein auf dem Mainboard	Tastatur wechseln, ansonsten Mainboard austauschen
4 lange Töne	CPU-Kühler	Sitz und Stromversorgung des Kühlers prüfen
1 langer Ton + 1 kurzer Ton	Mainboard	Prozessortakt im Bios/Uefi prüfen und Standard wiederherstellen, ansonsten Mainboard austauschen
1 langer Ton + 2 kurze Töne	Grafikkarte	Taktfrequenzen in Bios/Uefi prüfen und Standard wiederherstellen, festen Sitz im Steckplatz sicherstellen, ansonsten Grafikkarte austauschen
1 langer Ton + 3 kurze Töne	Tastatur oder Grafikkarte	Tastatur austauschen, Frequenzen der Grafikkarte prüfen und Standard wiederherstellen, Sitz im Steckplatz überprüfen
1 langer Ton + 9 kurze Töne	Bios/Uefi	alle Steckkarten entfernen und nochmals prüfen, Mainboard-Batterie wechseln
Dauerton (10 Sekunden) mit anschließender Selbstabschaltung	CPU-Kühler	Überhitzungsgefahr der CPU, Kühler prüfen
Dauerton	Arbeitsspeicher oder Grafikkarte	Stromversorgung kappen, Sitz der beiden Komponenten prüfen. Bei bleibendem Fehler: neues Netzteil, neue Grafikkarte oder neuen Arbeitsspeicher einbauen

Bootmenü aufrufen: Während des Bootvorganges die Taste [F12] mehrfach betätigen und anschließend den entsprechenden Datenträger auswählen und bestätigen. Alternative Tasten: [F8] ... [F12], [F2], [Tab], [Alt] und [Esc]; **Hinweis:** Die Pieptöne werden i.d.R. nur von Tower- und Tischcomputern unterstützt.

Übersicht der Pieptöne: AMI-BIOS

Tonfolge	Betroffene Komponente	Problemlösung
1 kurzer Ton	keine	Startkontrolle erfolgreich durchlaufen
1, 2 oder 3 kurze Töne oder 3 kurze Töne + 3 lange Töne + 3 kurze Töne	Arbeitsspeicher	Die Taktfrequenz der Speicherbausteine im Bios/Uefi prüfen und Standardwerte einstellen, den Sitz der Speicherriegel auf der Hauptplatine überprüfen. Bei bleibendem Fehler: Arbeitsspeicher austauschen
4 kurze Töne	Arbeitsspeicher oder Systemuhr	Arbeitsspeicher prüfen (siehe oben), Batterie auf der Hauptplatine wechseln
3 kurze Töne	Prozessor oder Grafikkarte	Prozessortaktfrequenz im Bios/Uefi überprüfen und Standardwerte einstellen. Sitz und Funktion des Prozessorlüfters überprüfen
6 kurze Töne	Tastaturbaustein auf dem Hauptplatine	Andere Tastatur anschließen. Bei bleibendem Fehler: Hauptplatine auswechseln
7 kurze Töne	Prozessor	Prozessortaktfrequenz im Bios/Uefi überprüfen und Standardwerte einstellen. Sitz des Prozessors auf der Hauptplatine überprüfen
8 kurze Töne oder 1 langer Ton + 2 kurze Töne oder 2 lange Töne + 2 kurze Töne	Grafikkarte	Taktfrequenz der Grafikkarte im Bios überprüfen und Standardwerte einstellen, Sitz der Grafikkarte auf der Hauptplatine überprüfen. Bei bleibendem Fehler: Grafikkarte auswechseln
9 kurze Töne	Bios/Uefi	Steckkarten ausbauen, um sicherzustellen, dass keine Controller-Chipsätze den Fehler verursachen, Batterie auf der Hauptplatine wechseln. Bei bleibendem Fehler: PC- oder Notebook-Hersteller kontaktieren
10 oder 11 kurze Töne oder 1 langer Ton + 1 kurzer Ton	Hauptplatine	Prozessortaktfrequenz im Bios/Uefi überprüfen und Standardwerte einstellen. Bei bleibendem Fehler: Hauptplatine auswechseln
1 langer Ton + 3 kurze Töne	Grafiksignal	Bildschirmanschluss überprüfen, Monitorkabel wechseln. Bei bleibendem Fehler: Grafikkarte tauschen
Dauerton	Netzteil	Stromversorgung trennen, wieder verbinden und erneut einschalten. Bei bleibendem Fehler: Netzteil austauschen

Bootmenü aufrufen: Während des Bootvorganges die Taste [F12] mehrfach betätigen und anschließend den entsprechenden Datenträger auswählen und bestätigen. Alternative Tasten: [F8] ... [F12], [F2], [Tab], [Alt] und [Esc]

Das Administrator-Passwort eines Windows-Benutzers (Gruppe: Administrator), kann durch die Ausnutzung einer seit Jahrzehnten bestehenden Lücke (seit Windows NT 3.5, Mitte der 90-iger Jahre) neu gesetzt werden.

Ziel bei dieser Methode ist es, das Dienstprogramm **utilman.exe** durch die **cmd.exe** zu ersetzen.

- A) CD oder ein USB-Stick mit Windows 10; USB-Stick muss mit spezieller Software bootbar (Windows ISO-Image auf USB-Stick übertragen) gemacht werden

Hinweis: nicht alle USB-Ports am Rechner sind bootbar (Port einfach wechseln); einige wenige USB-Sticks sind nicht bootbar

- B) die Bootreihenfolge im BIOS ist gegebenenfalls zu ändern; ein im BIOS aktiviertes **Fast Boot** oder **Quick Boot** ist zu deaktivieren; ein bootbares Medium wird bei aktivierten **Fast Boot** oder **Quick Boot** nicht erkannt

- C) eine evtl. bestehende Internetverbindung ist zu unterbrechen

- D) Nach dem Booten des Windows 10 ISO-Images von USB-Stick oder CD, ist die **Computerreparaturoption** aufzurufen. Startbildschirm (Windows 10 Setup) → weiter (**Achtung:** keine Installation) → Computerreparaturoption → Problembehandlung → Erweiterte Optionen → Eingabeaufforderung

- E) Ermittlung der Partition mit dem Windows-Verzeichnis
Beispiel: c: → dir; d: → dir ...

- F) Wechsel in das Verzeichnis System32 bzw. SysWOW64
Beispiel: cd Windows → cd System32 → dir utilman.exe

- G) Umbenennung der Programme utilman.exe und cmd.exe
rename utilman.exe utilman.exe.original
copy cmd.exe utilman.exe
exit

- H) Neustart des Rechners (ohne bootbares Medium) und Aufruf der **Erweiterten Bedienung** (Icon, Anmeldebildschirm – unten rechts); Statt des Dienstprogramms **utilman.exe** wird die **cmd.exe** mit den Rechten eines System-Benutzers (die Rechte des Benutzers **system** sind höher als die des Administrators) aufgerufen.

whoami
net user
net user <Benutzername> neues_Passwort

- I) Anschließend kann man sich mit dem neuen Passwort sofort anmelden. Die Umbenennung der beiden Programme ist mit derselben Methode wieder rückgängig zu machen.

Hinweis: Wird statt Windows 10 ein Fremdsystem (Linux, Unix) verwendet, muss das Fremdsystem mit dem aktuellen Dateisystem (NTFS) umgehen können.

Im BIOS ist ein aktiviertes **Secure Boot** zu deaktivieren. Die Deaktivierung von **Secure Boot** ist nur möglich, wenn vorher ein BIOS-Setup Passwort vergeben wird. Ansonsten ist die Vorgehensweise für Vergabe eines neuen Administrator-Passwortes relativ ähnlich.

Bei einem verschlüsselten Dateisystem, ist das Setzen eines neuen Passwortes für einen Benutzer mit Administratorrechten, mit dieser Methode **nicht** möglich.

Alternative Methoden:

Im Internet gibt es spezialisierte ISO-Images für CDROM's, USB-Sticks oder Windows-Programme. Diese alternativen Methoden sind mitunter nicht für aktuelle Windows-Betriebssysteme geeignet.

1. Offline NT Passwort und Registrierung bzw. NT Password Changer

Das ISO-Image kann auf der Webseite des Entwicklers Petter Nordahl-Hagen <http://home.eunet.no/~pnordahl/ntpasswd/> oder <http://pogostick.net/~pnh/ntpasswd/> oder aus dem Internet heruntergeladen werden (Suchmaschine: NT Password Changer). Die Bedienungsoberfläche des NT Password Changer ist ein wenig gewöhnungsbedürftig (**Hinweis:** Testdurchläufe sind erforderlich). Bei der Neuvergabe eines Passwortes für einen Benutzer mit Administrator-Rechten (nicht vom Benutzer »Administrator«; **siehe auch:** Nützliche CMD- oder Powershell-Befehle) ist zu beachten, dass dieser Benutzer ein leeres Passwort erhält (einfach die Enter-Taste betätigen).

2. LessLinux Search and Rescue

»LessLinux Search and Rescue« (<http://blog.lesslinux.org/>) ist ein bootfähiges System, dass von Matthias Schlenker entwickelt wurde. »LessLinux Search and Rescue« ist hilfreich bei vielen Wartungs- und Rettungsarbeiten an Windows- und Linux-Rechnern. Der Start ist sowohl von USB-Stick oder Festplatte, als auch von einer bootfähigen CD/DVD möglich.

3. Windows-Programm: grantAdminPriv (gAP)

Das Tool grantAdminPriv (gAP) kann sogar dem Benutzer »Gast« Administrator-Rechte zuweisen. Für die Änderung des Passwortes ist nur die Benutzerkontrolle aufzurufen (siehe auch: www.youtube.com).

4. Sala Password Renew

Das Tool ist mitunter Bestandteil von Rettungs- oder Notfallsysteme auf CD/DVD. **Hinweis:** Die Passwörter auf einer verschlüsselten Festplatte lassen sich nicht zurücksetzen. Start des Tools »Sala Password Renew« → »Select a target« (rechts unten) → c:/Windows → »Renew existing user password« (linke Seite) → »Account« (Benutzer) auswählen → hinter »New Password« und »Confirm Password« ein neues Passwort eingeben → »Install« (Menü auf der linken Seite)

5. Kon-Boot

»Kon-Boot« ist kostenpflichtig (27 Dollar, Englisch, Internet: <https://www.piotrbania.com>).

Mit »Kon-Boot« ist ein bootfähiger USB-Stick zu erstellen und anschließend der Windows-Rechner mit dem USB-Stick neu zu starten. »Kon-Boot« verändert den Windows-Code direkt im Arbeitsspeicher. Dadurch ist es möglich, Windows mit Administrator-Rechte ohne die Eingabe eines Passwortes zu starten. Anschließend kann wie gewohnt das vergessene Passwort eines beliebigen Benutzers neu gesetzt werden.

6. Microsoft-Online-Benutzerkonto neu setzen

Passwörter für die Benutzeranmeldung, werden bei einem Online-Benutzerkonto über ein Microsoft-Server verifiziert. Ein vergessenes Passwort kann dann über jeden beliebigen Windows-Rechner online zurückgesetzt werden. Mit Hilfe eines Webseiten-Assistenten auf der Seite <https://account.live.com/resetpassword.aspx> kann das Anmelde-Passwort zurückgesetzt werden.

Basisdaten: Mailadresse oder Handynummer, die bei der Einrichtung des Microsoft-Kontos hinterlegt wurde. Microsoft übermittelt anschließend einen Sicherheitscode. Nach der Eingabe des Sicherheitscodes kann ein neues Passwort vergeben werden.

Die Verwendungen von USB-Geräten wird an verschiedenen Stellen im System protokolliert, dies kann sich jedoch mit jedem Update ändern.

USB-Protokolle für den Datentransfer

Für den Datentransfer nutzt Windows drei Protokolle.

- Das Media Transfer Protocol (MTP) wird z.B. bei Smartphones oder Kameras verwendet.
- Das Picture Transfer Protocol (PTP) wird von mobilen Apple-Geräten zur Übertragung verwendet.
- Das Mass Storage Class (MSC) Protokoll wird von USB-Sticks, externen Festplatte, Smartphones und anderen Datenspeichern verwendet. MSC-Geräte bekommen als einzige einen Laufwerksbuchstaben von Windows zugewiesen.

Speicherorte in der Registry

Windows 10 speichert die angeschlossenen Geräte in der Registry an zwei verschiedenen Orten.

Für alle MTP- und PTP-Geräte wird ein Eintrag unter dem Registry-Subkey **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB** angelegt.

MSC-Geräte finden sich unter **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR** wieder.



Für jedes MSC-Gerät wird ein Subkey unter **USBSTOR** angelegt. Dieser enthält die Seriennummer, die Hersteller ID und Produkt ID.

Für alle USB-Geräte, welche eines der drei Protokolle verwenden, wird ein Subkey unter **USB** angelegt. Hier werden die Hersteller und Produkt ID (VID & PID) gespeichert, sowie falls vorhanden die Seriennummer. Die IDs können in dieser Liste den Herstellern zugeordnet werden.

In der Vergangenheit hat Windows diese Einträge einmal angelegt und nie wieder vergessen, das heißt jedes USB-Gerät, das jemals an einen Rechner angeschlossen wurde, war bis zur Löschung des Systems gespeichert. Microsoft hat dies durch ein Update geändert, möglicherweise um den gestiegenen Datenschutzanforderungen Rechnung zu tragen. Allerdings wurde dies von Microsoft nicht konsequent umgesetzt.

Trotz ggf. aktiver Löschautomatik, kann die Nutzung von USB-Geräten an einem Windows-System nachvollzogen werden. Es gibt noch eine Reihe weitere Einträge in der Registry und andere Bereiche von Windows, die die Nutzung von Speichergeräten protokollieren. Admins können anhand der Einträge z.B prüfen, an welchen Rechner ein mit Malware infizierter Stick angeschlossen war und so die betroffenen Geräte schnell vom Netzwerk trennen.

Das ReFS-Dateisystem (Resilient File System, robustes Dateisystem) ist die neueste Version des Dateisystems von Microsoft (seit Windows Server 2012, Windows 10 Enterprise verfügbar), das entwickelt wurde, um die Datenverfügbarkeit zu optimieren, die Skalierbarkeit für große Datenmengen effizient zu verwalten und die Datenintegrität durch Widerstandsfähigkeit gegen Dateikorruption zu gewährleisten.

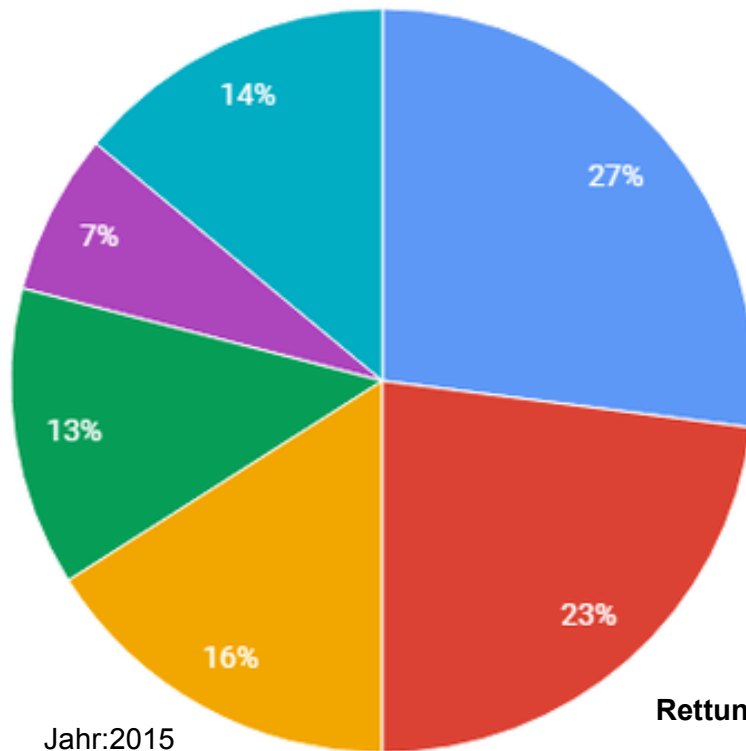
ReFS wird von Microsoft nur für spezielle Szenarien empfohlen. Die Vorteile von ReFS kommen wahrscheinlich nur in einer reinen Windows-Umgebung zum tragen.

1. Storage Spaces ist eine Technologie in Windows und Windows Server, die dazu beitragen kann, Daten vor Laufwerksausfällen zu schützen. Es ist konzeptionell ähnlich wie RAID, aber auf Softwareebene implementiert.
2. Gemeinsame Festplatten und Backup-Ziele. Diese Nutzung profitiert im Allgemeinen von der Verwendung spezifischer Anwendungen, die Zuverlässigkeit und Ausfallsicherheit bei der Verwaltung ihrer Daten benötigen und die die ReFS-Funktionen intern implementieren können. Ein mit ReFS formatiertes Backup-Ziel garantiert natürlich große Vorteile bei der Datensicherheit gegen mögliche Beschädigungen.

NTFS ist ein proprietäres Dateisystem von Microsoft für alle Betriebssysteme der Windows-NT-Reihe. Die Abkürzung steht für New Technology File System. Im Vergleich zum Dateisystem FAT bietet NTFS unter anderem einen gezielten Zugriffsschutz auf Dateiebene, sowie größere Datensicherheit durch Journaling. Allerdings ist keine so breite Kompatibilität gegeben wie bei FAT. Ein weiterer Vorteil von NTFS ist, dass die Dateigröße nicht wie bei FAT auf 4 GiB beschränkt ist.

Funktion	ReFS	NTFS
Max Länge Dateiname	255 Unicode characters	255 Unicode characters
Max Länge Dateipfad	32K Unicode characters	32K Unicode characters
Max Dateigrösse	35 PB (petabytes)	256 TB
Max Datenträgergröße	35 PB	256 TB

Eingesetzte Backup-Medien



Jahr:2015

- Datensicherungsbänder
- externe Festplatten
- Cloud Speicher
- NAS Server (network attached storage oder Speicher mit Netzwerkanschluss)
- HDD Cartridges - Festplattenkassette
- andere Datenträger



Rettungsschirm: Backup

- Für die Wahl der optimalen Hard- und Softwarelösung (Backup-System), sollten sich Freiberufler, Unternehmen und Privatpersonen ausreichend Zeit nehmen und sich nicht vom Preis leiten lassen. Mit dem Verlust wichtiger Daten, kann man sich schon auf den Besuch des Insolvenzverwalters »freuen« oder auch nicht.
- Ob privat oder geschäftlich, Daten sind wertvoll und müssen gesichert werden.
- Für die Datensicherung gibt es verschiedene Backup-Methoden und Backup-Strategien.
- Die meisten Backup-Lösungen stellen dafür drei Methoden zur Verfügung: Die vollständige, die differenzielle und die inkrementelle Datensicherung.

Backup-Ratgeber: Welche Methode ist die richtige für mich?

Vollsicherung: Mit der Vollsicherung, wird eine tägliche System-Sicherung mit steigendem Speicherbedarf erstellt.

Die Vollsicherung ist nicht nur die einfachste Art der Datensicherung, sondern auch die wohl effektivste Backup-Methode. Bei der Vollsicherung werden alle Daten gesichert. Bei Bedarf wird das System aus einer einzigen Datei wiederhergestellt.

Vorteile: Eine einfache Sicherung und Wiederherstellung mit nur einer Backup-Datei.

Nachteile: Zeitaufwendiger Backup-Prozess mit einem sehr hohen Speicherbedarf.

Differenzielle Datensicherung: Bei der differenziellen Datensicherung wird zunächst eine Vollsicherung erstellt und danach - etwa einmal die Woche - eine Teilsicherung. Bei der Teilsicherung werden dann nur die Daten gesichert, die seit der letzten Vollsicherung verändert oder neu erstellt wurden.

Die differenziellen Backups werden Tag für Tag größer und umfangreicher, da mit jeder differenziellen Datensicherung die in einer vorherigen differenziellen Datensicherung bereits abgesicherten Daten, erneut gesichert werden.

Vorteile: Die differenzielle Sicherung benötigt weniger Speicherplatz – im Vergleich zu einer Vollsicherung, kann aber deutlich schneller als eine Vollsicherung durchgeführt werden.

Nachteile: Dateien, die nach der Vollsicherung nur einmal verändert wurden, werden mit jedem differenziellen Backup erneut gesichert.

Inkrementelle Datensicherung: Die inkrementelle Datensicherung ähnelt der differenziellen Datensicherung - mit einem entscheidenden Unterschied. Zwar geht dem inkrementellen Backup auch eine Vollsicherung voraus, danach werden mit jeder Sicherung aber nur die Daten gesichert, die seit der letzten inkrementellen Sicherung erstellt oder verändert wurden.

Dadurch sind die einzelnen Datensätze alle miteinander verknüpft und zur Wiederherstellung der Daten benötigt man die erste Vollsicherung sowie alle nachfolgenden inkrementellen Sicherungen.

Vorteile: Inkrementelle Sicherungen haben einen geringen Speicherbedarf und können schnell angefertigt werden.

Nachteile: Zur Wiederherstellung wird die Vollsicherung inklusive **aller** inkrementellen Sicherungen benötigt.



Hinweis: Wichtige Backup-Datenträger oder dessen Kopien sollte man an einem sicheren, externen Ort lagern.

Local Storage ... lokale Festplatte, SSD

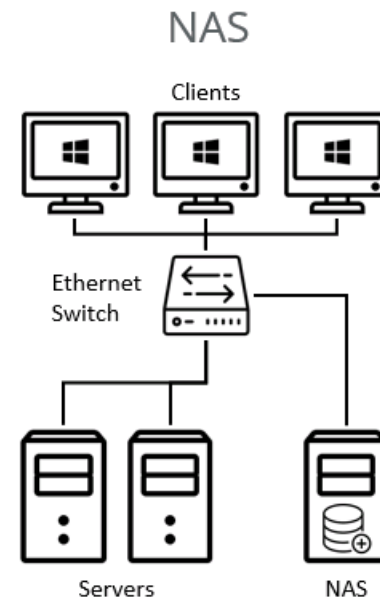
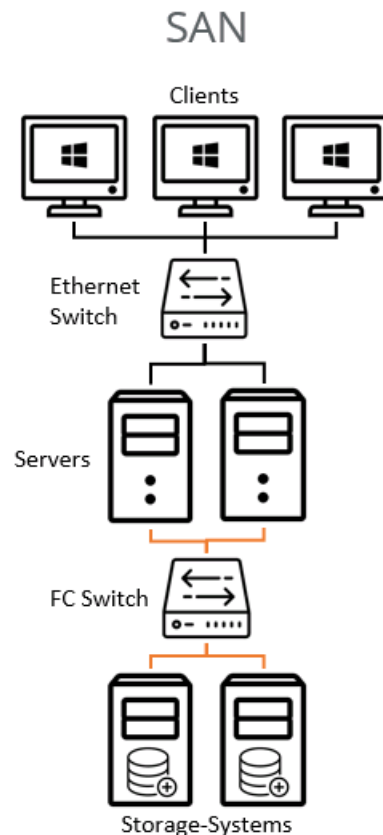
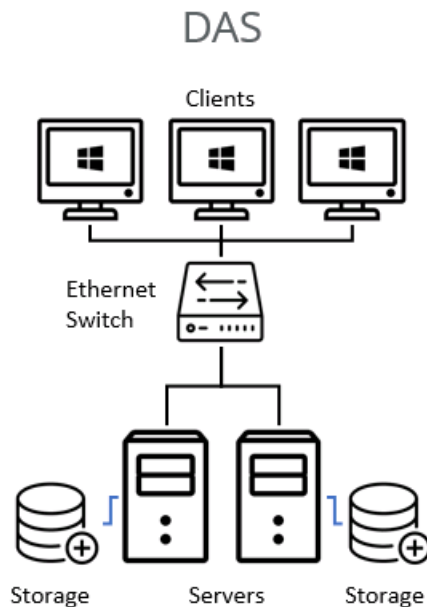
DAS ... Direct Attached Storage bezeichnet an einen einzelnen Host angeschlossene Festplatten, die sich in einem separaten Gehäuse befinden.

NAS ... Network Attached Storage ist eine Speicherarchitektur auf Dateiebene, bei der ein oder mehrere Server mit dedizierten Festplatten (dediziert/dedicated für eine bestimmte Anwendung) für die Speicherung von Daten sowie ihre Teilung mit vielen Clients in einem Netzwerk verwendet werden.

SAN ... Storage Area Network ist ein blockbasierter Storage, der Server mit ihren logischen Festplatteneinheiten verbindet.

SDS ... Software Defined Storage ist eine Storage Management-Software, die unabhängig von der zugrundeliegenden Hardware fungiert.

vSAN ... Virtual Storage Network, Virtual SAN, vSAN ist ein von VMware entwickeltes Software Defined Storage (SDS).



Fabric ... Als Fabric (engl. für »Gewebe«) bezeichnet man in Computernetzwerken im Gegensatz zu einer einfachen Punkt-zu-Punkt-Verbindung ein Netzwerk von Leitungen, Routern und Switches, das eine gewisse Redundanz und Quervernetzung besitzt und darauf ausgelegt ist. Beispiel: Werden Switches kaskadiert spricht man schon von einer Fabric. Innerhalb der Fabric können die Endgeräte beliebig miteinander verbunden werden und aufeinander zugreifen. Die Fabric-Technik erlaubt den Anschluss von 16 Millionen Geräten. Über FC-Switches (FC ... Fibre-Channel) werden die Geräte miteinander verbunden. So können alle Geräte parallel untereinander Daten austauschen.

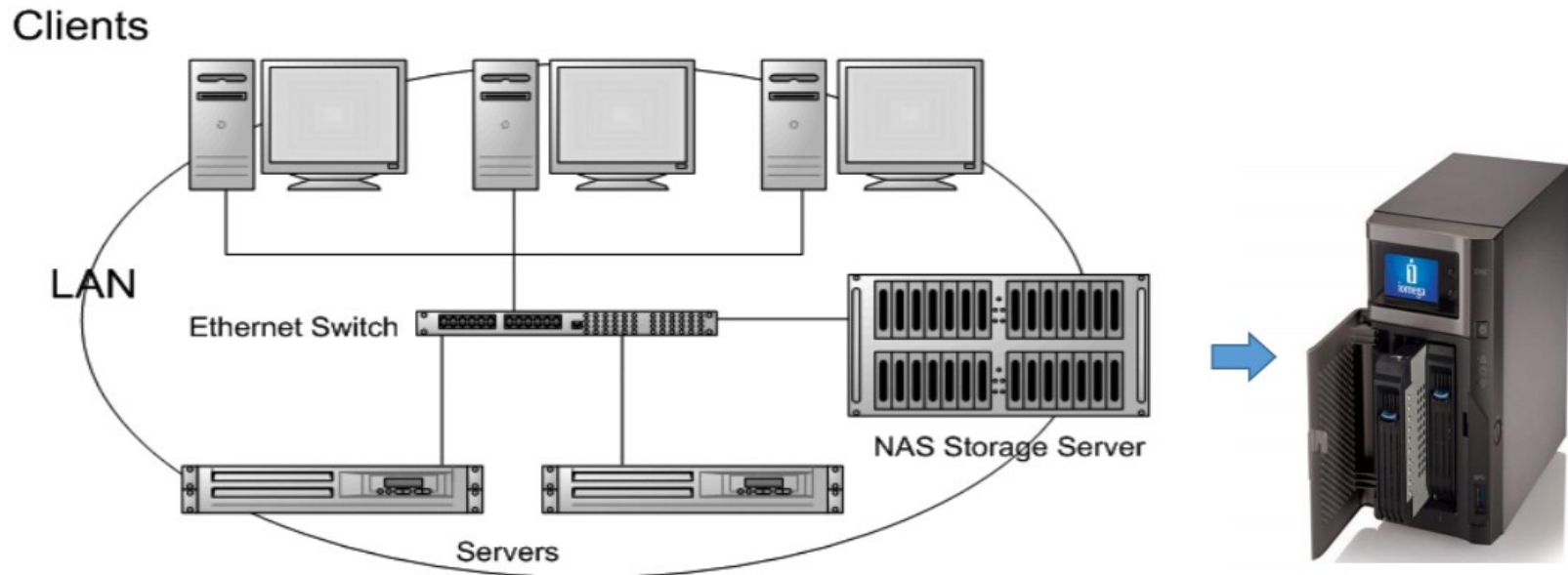
DAS: Als kostengünstiger Einstieg in den Storage-Bereich eignet sich das sogenannte Direct Attached Storage (DAS). Hier wird der Speicher über eine Punkt zu Punkt-Verbindung direkt an den jeweiligen Server angeschlossen. Mögliche Anschlussarten sind Serial Attached SCSI (SAS), seltener FibreChannel Point to Point (FC-P2P) sowie alle blockorientierten Übertragungsprotokolle von ATA/ATAPI über FireWire oder eSATA bis hin zu USB mit UAS (USB Attached SCSI Protocol).

Dank Direct Attached Storage minimiert sich der Hardware-Aufwand für das Unternehmen: Es sind keine zusätzlichen Switches oder Verwaltungseinheiten neben dem Server nötig.

NAS: Hierbei handelt es sich um Storage, das über ein Ethernet-Switch an die bestehende IT-Infrastruktur angeschlossen wird. NAS-Einheiten sind auf die Bereitstellung von Daten in Dateiform konzipiert. Einer der Vorteile von Network Attached Storage liegt eben in dieser einfachen Anbindung an das bestehende Netz bzw. an die jeweiligen Clients. Das NAS wird dabei über Standard-Interfaces für Netzwerk-Controller angeschlossen.

Die Anzeige der Dateien erfolgt mit standardmäßigen dateibasierten Protokollen, wie Network File System (NFS), Server Message Block (SMB), Common Internet File System (CIFS) bzw. Apple Filing Protocol (AFP), also Protokollen zur Kommunikation mit Linux und UNIX, Microsoft Windows und Apple Geräten.

Network Attached Storage

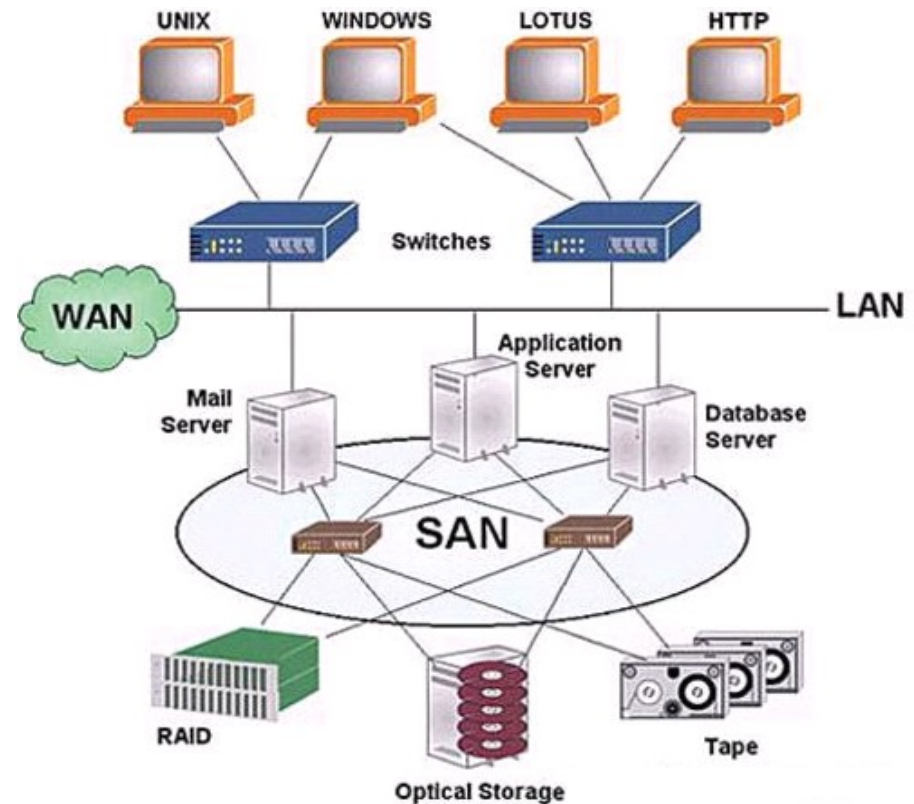


SAN – ein effizienter Speicherverbund

Prinzipiell ähnelt der Aufbau eines SANs dem eines LANs. Es existieren Komponenten wie Router, Switches oder Hubs. Über das Netzwerk sind die Server von ihren Massenspeichern entkoppelt. Das Storage Area Network wird parallel zum LAN betrieben und ist für die schnelle Übertragung der Daten der Massenspeicher optimiert. Durch die Auslagerung dieser Vorgänge verringert sich die Auslastung des LANs (Local Area Networks). Über redundante Verbindungen innerhalb des Speichernetzwerks sind hohe Verfügbarkeiten realisierbar. Neben Fibre Channel können Protokolle und Übertragungsmedien wie Gigabit-Ethernet, iSCSI oder Infiniband zum Einsatz kommen. Obwohl Fibre Channel (FC) sich als Übertragungsmedium für SAN durchgesetzt hat, kommen auch andere Techniken in Frage. Fibre Channel hat jedoch eine Nutzdatenauslastung von 90%, während z. B. Ethernet nur zwischen 20 und 60% der maximal möglichen Übertragungsrate mit Nutzlast belegen kann. In einem SAN werden die Daten blockbasiert übertragen. Bei einem Blockzugriff fordert der Rechner einzelne Datenblöcke von einer Festplatte an. Bei der dateibasierten Datenabfrage wie sie NAS nutzt, fordert der Rechner ganze Dateien an. FC-AL (Fibre-Channel-Arbitrated-Loop) ist eine Bus-Topologie. Server und Speichergeräte sind über einen virtuellen Ring miteinander verbunden. Fibre-Channel-Arbitrated-Loop ist die am häufigsten eingesetzten Ring-Topologien (Ähnlichkeit mit einem Token-Ring) für FC-Netzwerke. Der Datenaustausch ist in einem solchen Ring nur in eine Richtung möglich und auch nur zwischen zwei Komponenten. Wenn zwei Geräte Daten über einen solchen Ring austauschen, müssen die anderen angeschlossenen Geräte warten, bis der Bus wieder frei ist. In einem dieser Ringe lassen sich bis zu 128 Geräte zusammenschließen, die angeschlossenen Geräte teilen sich die vorhandene Bandbreite.

Die weitaus gängigere Methode, ein SAN aufzusetzen, ist die Switched-Fabric-Technik (ein Switched-Fabric besteht aus einer vermaschten Switch-Architektur).

Im SAN wird die gesamte Speicherkapazität, die Speichermedien wie HDDs, SSDs, Disk-Arrays (Festplattensubsysteme) oder Tape-Libraries (Bandbibliotheken) bereithalten, zu einer virtuellen Speichereinheit zusammengefasst und zentral verwaltet. Der Zugriff auf den SAN-Speicher erfolgt durch entsprechend konfigurierte Server.



Virtual SAN

Virtual SAN (VMware VSAN, vSAN ist ein von VMware entwickeltes Software Defined Storage) ist eine Storage-Funktion, die in vSphere 5.5 enthalten ist und den Speicherplatz von verschiedenen ESXi-Hosts vereint. Ein VSAN (Virtual Storage Area Network) ist eine logische Partition in einem SAN (Storage Area Network).

Die Administration der Cluster und die Implementierung der Storage-Richtlinien wird im vSphere 5.5 Web Client vorgenommen.

Jeder Host in einem VMware VSAN Cluster erfordert mindestens eine SSD als Cache sowie Zwischenspeicher und mindestens eine Festplatte (HDD) für die Datenspeicherung. Zusätzlicher Storage lässt sich zur Verfügung stellen, indem man HDDs zu den verfügbaren ESXi-Hosts hinzufügt.

Die Robustheit bzw. Ausfallsicherheit ist beim Storage-Pool dadurch gegeben, dass vSAN je nach Lizenz und Größe des Clusters ein integriertes und verteiltes RAID darstellt, allerdings auf Software-Ebene. Ein RAID-System zum Anschluss der Platten im Host ist nicht erforderlich, vielmehr arbeiten vorhandene RAID-Controller im Passthrough/HBA-Modus (HBA ... Host Bus Adapter-Modus, HBA ist ein Nicht-RAID-Modus, d.h. virtuelle Festplatten oder Hotspares sind nicht verfügbar).

Mit der Standardlizenz (VMware) bietet vSAN bei einem 3-Node-Cluster (der minimal möglichen Startgröße) Ausfallsicherheit für einzelne Hosts per Spiegelung, was bei der Analogie mit Platten-RAIDs einem RAID-1 entspricht. Ein 3-Node-vSAN-Cluster kann also maximal den Ausfall eines kompletten Nodes verkraften, ohne dass das Storage ausfällt.

Hinweis: Nicht initialisierte Laufwerke werden im RAID Modus automatisch als »Pass Through«- (oder RAW-) Laufwerke durchgereicht. Ist der Controller im HBA Mode, werden angeschlossene Laufwerke wie »Pass Through« (oder »Raw«) - Geräte behandelt.

Quelle: <https://www.windowspro.de/thomas-drilling/vmware-virtual-san-66-funktionsweise-installation>

SDS

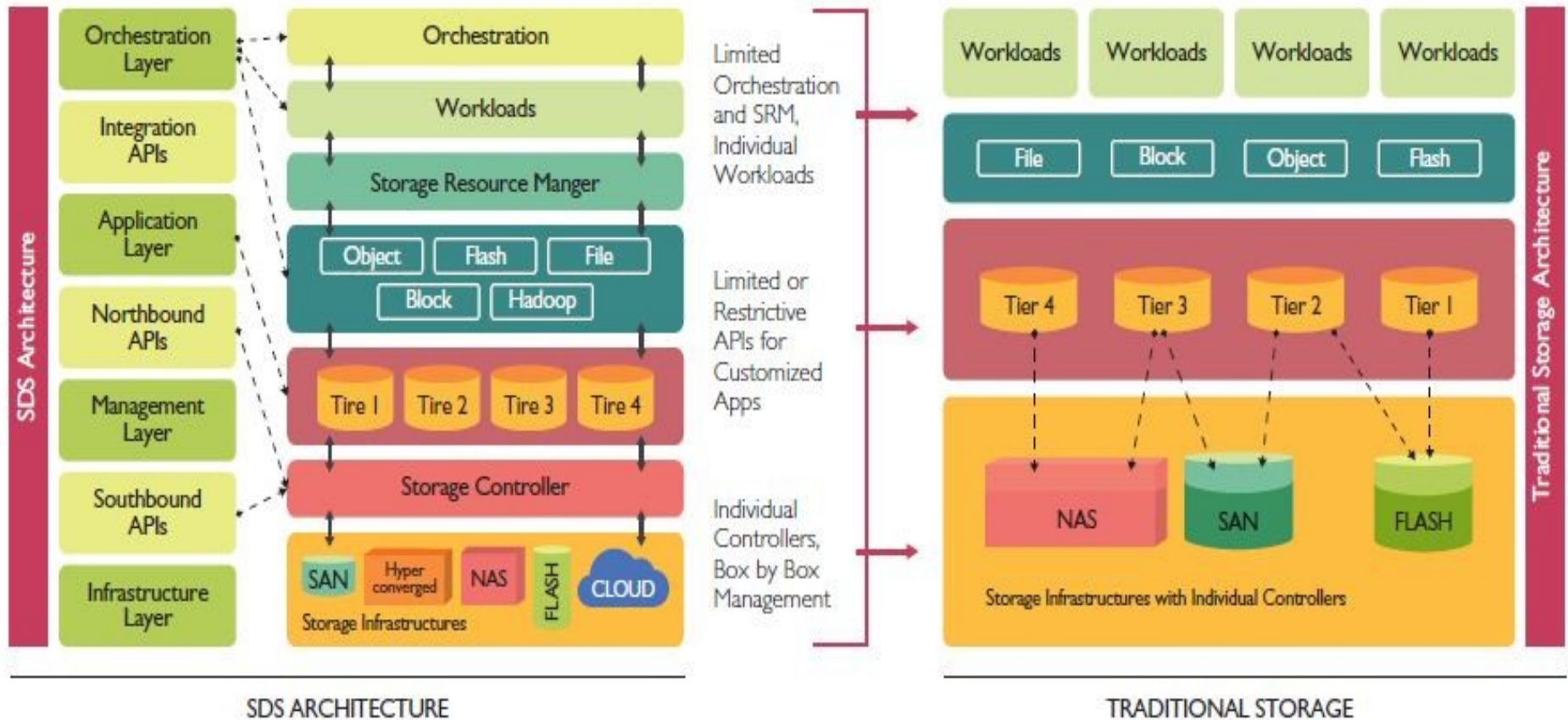
Software-defined Storage (SDS) ist eine Storage Management-Software, die unabhängig von der zugrundeliegenden Hardware fungiert. Das heißt, man kann SDS auf einer NAS-Box installieren und die Hardware an spezifische Workloads anpassen. Mit installierter SDS kann die Storage-Hardware so gruppiert werden, dass mehrere Server als einzelnes System und für einen bestimmten Zweck fungieren können.

Hinweis: Der Begriff Workload bezeichnet die Arbeitsbelastung an einem Arbeitsplatz, einen Arbeitsauftrag in einem verteilten Computersystem oder die Auslastung eines Prozesses.

Storage Tiering (Abstufen, Staffellung) ist eine Methode, Daten entsprechend nach ihren Zugriffen auf unterschiedliche Speichermedien – so genannten Storage Tiers – abzulegen. Da viele Speichersysteme mittlerweile mehr als ein Festplattenformat enthalten, lässt sich dies bereits in kleineren Systemen umsetzen. Dabei werden die Daten auf ihre Zugriffe überwacht und je nach Anzahl dieser Zugriffe verschoben. Die I/O-intensiven Informationen liegen auf Tier-1 (Tier-1 ... Performance Tier - für etwa 5 % der Datenbestände, schneller Speicher, SSD, Flash-basierte Cache Speicher; Tier-2 ... Capacity Tier - für etwa 35 % der Datenbestände, SAS-Harddisks; Tier-3 ... Archiving Tier - für etwa 60 % der Datenbestände, SATA-Platten, Bandlaufwerke, optische Speichermedien), oftmals kommen hier SSDs (Solid State Drive) oder SAS-Platten (Serial Attached SCSI, Server-Festplatten) zum Einsatz. Weniger oft angeforderte Daten verschiebt das System dann auf weniger teure Medien wie SATA-Drives. Das Tiering erfolgt bei fast allen Herstellern automatisch und soll künftig auf externe Ressourcen wie zum Beispiel Server und Bandsysteme erweitert werden.

Dieses Modell ist jedoch nach Ansicht einiger Fachleute überholt. Sie empfehlen eine feingliedrigere Struktur, die vier (zusätzlich Tier-0) bis fünf Ebenen vorsieht.

Software-defined Storage (SDS)



Siehe auch: http://openbook.rheinwerk-verlag.de/windows_server_2012r2/03_002.html

VEEAM - Backup für virtuelle Infrastrukturen

VEEAM ist seit vielen Jahren Marktführer beim Backup von virtuellen Servern und Datacenter Infrastrukturen (VMware). Insbesondere die Unterstützung aller marktgängigen Speichermedien als Backupziel ist der große Vorteil von VEEAM. Es werden Bandlaufwerke, NAS, SAN, lokale HDD, Tape-Libraries und Cloud-Speicher unterstützt, ohne das weitere Zusatztools oder zusätzliche Lizenzen nötig wären. Noch dazu ist VEEAM sehr schnell beim Speichern großer Datenmengen und dabei einfach und übersichtlich in der Bedienung. Eine Wiederherstellung von ganzen VMs oder einzelnen Dateien ist unkompliziert und zügig erledigt. Die Veeam Availability Suite ist in drei Editionen (Standard Edition, Enterprise Edition, Enterprise Plus Edition) erhältlich, die auf unterschiedliche Anforderungen ausgerichtet sind.

VEEAM - Backup für virtuelle Infrastrukturen

VEEAM ist seit vielen Jahren Marktführer beim Backup von virtuellen Servern und Datacenter Infrastrukturen (VMware). Insbesondere die Unterstützung aller marktgängigen Speichermedien als Backupziel ist der große Vorteil von VEEAM.

Es werden Bandlaufwerke, NAS, SAN, lokale HDD, Tape-Libraries und Cloud-Speicher unterstützt, ohne das weitere Zusatztools oder zusätzliche Lizenzen nötig wären. Noch dazu ist VEEAM sehr schnell beim Speichern großer Datenmengen und dabei einfach und übersichtlich in der Bedienung.

Eine Wiederherstellung von ganzen VMs oder einzelnen Dateien ist unkompliziert und zügig erledigt. Die Veeam Availability Suite ist in drei Editionen (Standard Edition, Enterprise Edition, Enterprise Plus Edition) erhältlich, die auf unterschiedliche Anforderungen ausgerichtet sind.

VEEAM-Backup

Aufgrund der entstehenden Herausforderung, aus der Virtualisierung riesiger Datenmengen und eine große Anzahl von Servern zu sichern zu müssen, ist es essentiell notwendig, das beste Backup- und Wiederherstellungstool einzusetzen, welches auf dem Markt existiert.

Veeam Software bietet mit seinen im Virtualisierungs-Backupmarkt herausragenden Funktionen genau die dafür notwendigen Mehrwerte und Alleinstellungsmerkmale.

Ein Highlight ist z.B. die Möglichkeit einen Server und Benutzer-Dienst unabhängig von der Datenmenge innerhalb von einer Minute plus Betriebssystemstart wieder zur Verfügung zu stellen.

VEEAM kann die gesicherten Daten in verschiedenen organisierten Backupdateien ablegen. Eine der Speichermethoden ist das klassische Full- und Incremental-Backup Verfahren.

Mit Veeam Backup & Replication lassen sich einzelne Files, ganze VMs, einzelne VMware Files, einzelne VM Volumes und Applikationsobjekte (z.B. einzelne Mails oder Active Directory Benutzer) wiederherstellen.

Alle Backups werden vor der Wiederherstellung automatisch auf die Wiederherstellbarkeit geprüft.

Die Replikationsmöglichkeiten von VEEAM bieten beste Disaster Recovery Möglichkeiten für verteilte Standorte. Ebenso sind Sie erste Wahl wenn im Fehlerfall ein Server sofort mit voller Leistung wieder zur Verfügung stehen muss.

Einige Begriffe:

Change-Block-Tracking

VEEAM hat für Hyper-V ein eigenes Hyper-V Clusterfähiges Change-Block-Tracking entwickelt, um auch hier nur die geänderten Blöcke mit Backup & Replication sichern zu können.

Ein Beispiel für den Nutzen von Change-Block-Tracking: Sie haben eine große Filmdatei mit 8GB in einer Datei. Jetzt öffnen und speichern Sie die Datei ohne wirklich Änderungen vorzunehmen.

Auf herkömmliche Agenten basierte Backup-Software würde erkennen, dass die Datei sich geändert hat und die vollen 8 GByte sichern.

Jedoch auf Blockebene betrachtet, wird nur die Information mit dem Zeitstempel in neuen Blöcken auf das Disk-System übertragen und im Change-Block-Tracking festgehalten. Dies sind in diesem Fall nur wenige KByte, die dann als Backup mit minimaler Datenübertragung gesichert werden können.

Nachteil dieses Backupverfahrens innerhalb von VMware ist, dass solange der VM-Snapshot besteht, die Änderungen die sich seither ergeben haben in einen separaten Bereich abgelegt werden.

VEEAM löst dieses Problem elegant, in dem nur einmalig die Daten als Full-Backup gesichert werden und zukünftig immer nur die geänderten Blöcke.

Somit kann bei hoch belasteten Systemen innerhalb eines Wartungsfensters der Full-Datenbestand übertragen werden und anschließend während des normalen Betriebes nur die Änderungen.

Oftmals können mit Veeam Backup & Replication dadurch Systeme gesichert werden, die sonst gar nicht mit Standard Virtualisierungsbackup-Methoden gesichert werden können.

VMware vSphere

VMware vSphere stellt Rechenzentrumsvirtualisierung für x86-64 basierte Serversysteme zur Verfügung. Sie versetzt Anwender in der Lage, geschäftskritische Anwendungen zuverlässig auszuführen und schneller auf geschäftliche Anforderungen zu reagieren.

IBM® Tivoli® Storage Manager (TSM)

Mit dem IBM® Tivoli® Storage Manager (TSM) bietet IBM® eine ganze Suite von Dataprotection Lösungen für fast alle Systeme in einem Rechenzentrum.

Unter anderem werden die Backupdaten auf Tape-Systeme vorgehalten und das Verbringen einzelner Tapes zu Offsite-Location organisiert.

Mit dem TSM Client können Full Sicherungen von VMware VMs erstellt werden. Der IBM® Tivoli® Storage Manager für Virtual Environments (TSM VE) stellt darüber hinaus inkrementelle Sicherungen von VMs zur Verfügung.

Backup-Alternative: RSync

RSync versucht nur Änderungen zu übertragen, indem Rsync nur die Unterschiede ermittelt. Ferner komprimiert RSync die zu übertragenden Daten und bemüht sich, eventuell schmalbandige Leitungen möglichst optimal auszulasten.

Damit eignet sich RSync zum Beispiel für den Einsatz im Internet, etwa fürs Spiegeln von Änderungen an einem Web-Server, oder bei der Software-Entwicklung, wo Quelltextänderungen an einen sicheren zweiten Server zu übermitteln sind.

Aufgrund seiner Funktionsweise muss RSync sowohl auf dem Quell- als auch dem Zielrechner laufen. Es bedient sich normalerweise der ohnehin vorhandenen Infrastruktur für Remote-Kommandos (rsh, rcp, rlogin), kann aber auch auf einer sicheren Verbindung wie SSH aufsetzen.

Neben der klassischen Arbeitsweise über die R-Kommandos kann RSync inzwischen als Server arbeiten: RSyncD lauscht wie andere Dienste, etwa ein FTP-Server, an einem Port auf eingehende Verbindungen. In dieser Betriebsart kümmert sich RSync selbst um die Authentifizierung; anonyme Zugriffe etwa für FTP-Spiegel sind möglich.

Hinweis: RSync ist für alle gängigen Unix- und Linux-Betriebssysteme verfügbar; auf der Basis von Cygwin ist es auch auf Windows-Systemen lauffähig.

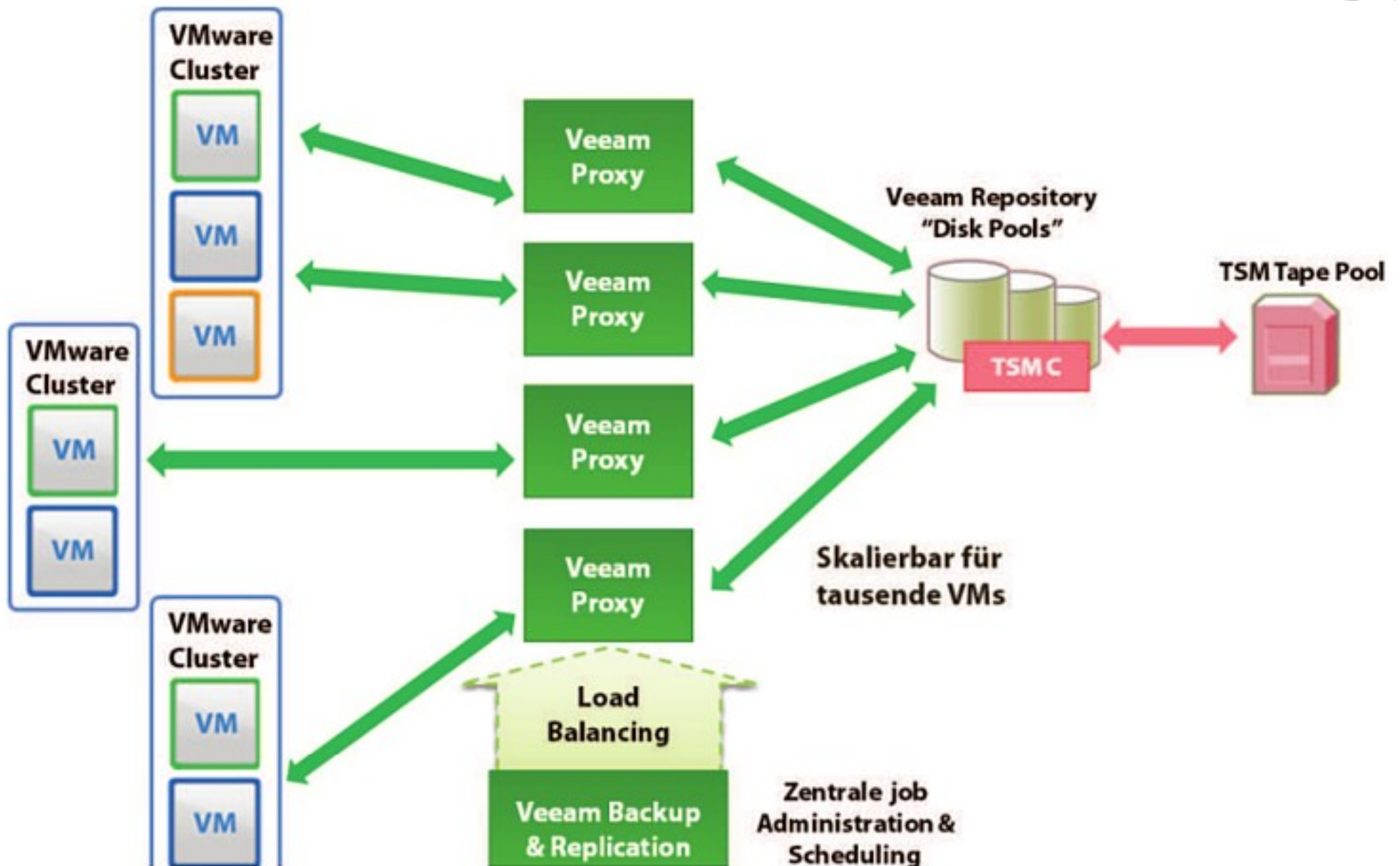


Bild: Backup Infrastruktur

Software: mention v.2018 Warenwirtschaft

Funktionen:

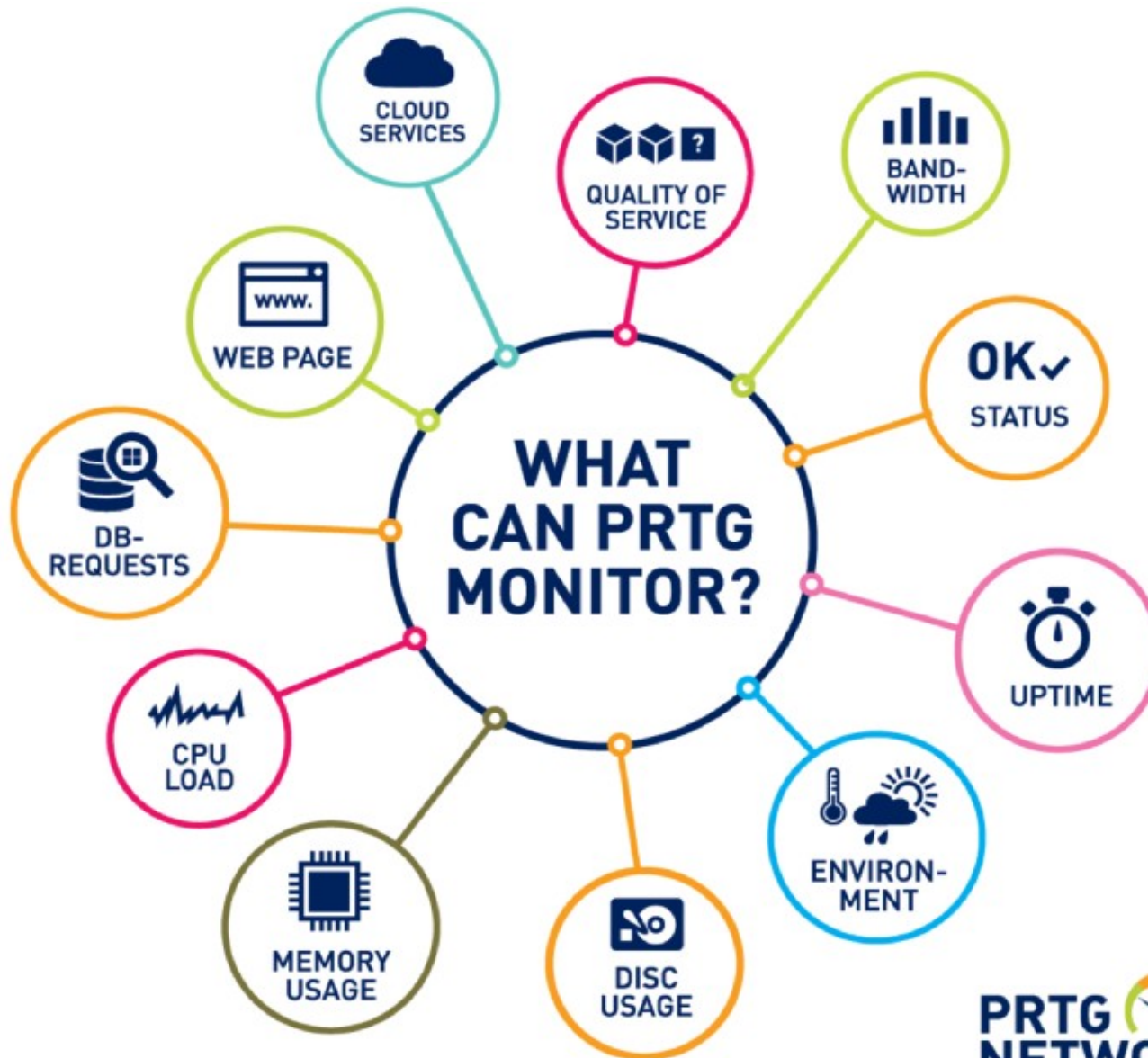
- **Stammdatenverwaltung**
Adressen, Interessenten, Kunden, Lieferanten, Artikel, Stücklisten, Leistungen, Ersatzteile
- **Abwicklung: Verkauf**
Angebote, Bestellungen, Auftragsbestätigungen, Lieferscheine, Rechnungen, Gutschriften inkl. Leih- und Teststellung, Kommissionsware, Reparaturabwicklung, Werkstattmontagen
- **Abwicklung: Einkauf**
automatische Bedarfsermittlung, Anfragen, Bestellungen, Wareneingang, Rücksendung
- **Abwicklung: Versand**
Schnittstellen zur Datenübergabe für alle gängigen Logistiksysteme, z.B. MHP.
- **Seriennummer und Chargenverwaltung**
Jetzt kommt nichts mehr weg. Einmal die Seriennummer gescannt und Sie haben die perfekte Übersicht über alle Warenbewegungen.
- **Informations- und Auswertungssystem**
Erfahren Sie mehr über Ihr Unternehmen. Die umfangreichen Informations- und Auswertungsfunktionen von mention halten Sie auf dem laufenden. Mit individuellen Provisionierungsmodellen fördern Sie die Motivation Ihrer Mitarbeiter.
- **Kassensysteme**
Damit die Kasse stimmt. Alle Funktionalitäten eines kompletten Kassensystems in mention: Bondrucker und Schublade ansteuern, verschiedene Zahlungsmittel verwalten, Brutto- und Nettopreise ausweisen.
- **Wiedervorlagen**
Erinnern Sie sich selbst oder Ihre Mitarbeiter an wichtige Termine, Aufgaben und Projekte. Minutengenau und mit allen dazugehörigen Daten.
- **Controlling**
So haben Sie Ihr Unternehmen im Griff: Auswertungstools, Statistiken und alle Kennzahlen für den Geschäftsführer auf einen Blick.

Der Wechsel bisheriger Datenformate von SMS, EPF, KHK oder OMS ist ohne Ausfallzeiten möglich. Ein sofortiges Weiterarbeiten ist somit gewährleistet. Alle relevanten Kundendaten, angefangen bei den Einkaufsgewohnheiten bis hin zur Kontakthistorie, erscheinen übersichtlich aufgelistet, wodurch der Vertrieb unschlagbar in den Verkaufsgesprächen sein wird.

Mention wurde speziell für die IT-Branche entwickelt und optimiert.

Hersteller: mention Software GmbH

PRTG: Ungewöhnliche Zugriffsmuster entlarven 1/3



Monitoring und Grafisches Intrusion Detection System (IDS)

PRTG ... Passler Routing Tracking Grapher

PRTG überwacht die IT-Infrastruktur

PRTG Network Monitor ist eine intelligente Monitoring-Lösung für die IT-Infrastruktur. Mit der Software PRTG kann man ein gesamtes Netzwerk, deren Systeme und Anwendungen auf einer einzigen Oberfläche vereinen.

Traffic, Pakete, Anwendungen, Bandbreite, Cloud-Dienste, Datenbanken, virtuelle Umgebungen, Betriebszeit, Ports, IPs, Hardware, Sicherheit, Webdienste, Nutzung von Festplatten, physische Umgebungen und IoT-Geräte können mit PRTG überwacht werden.

Weltweit vertrauen mehr 200.000 Administratoren (2019) auf die Monitoring-Software PRTG.

In der kostenfreien Version von PRTG kann man dauerhaft auf 100 Sensoren zugreifen. In der Regel benötigt man 10 Sensoren pro Netzwerkgerät. Aber es ist auch möglich nur mit einem SNMP-Sensor, um den Traffic zu überwachen oder einen Ping-Sensor für die Erreichbarkeit zu arbeiten.

PRTG: Ungewöhnliche Zugriffsmuster entlarven 2/3

PRTG Network Monitor aus dem Hause Paessler ist eine Netzwerk-Monitoring-Lösung zur umfassenden Überwachung des Datenverkehrs sowie der Verfügbarkeit und Leistung von Geräten und Applikationen in IT-Infrastrukturen. Dies beinhaltet klassische Netzwerk-Geräte wie Router, Switches und Firewalls, aber auch virtuelle Umgebungen, Applikation.

Funktionsumfang und Lizenzierung

Als Netzwerk-Monitoring-Programm überwacht PRTG Network Monitor verschiedene Systemzustände. Beim Erreichen oder Überschreiten von selbst definierten Grenzwerten ist eine Benachrichtigung per SMS, E-Mail oder Push-Nachricht möglich. Ziel ist es, Ausfälle von Systemen und Computern auf ein Minimum zu reduzieren. PRTG ist ausschließlich für Windows-Systeme verfügbar. Zusätzlich zur Desktop-Variante ist die cloudbasierte Lösung »PRTG hosted by Paessler« erhältlich.

Sensoren

Die Software basiert auf sogenannten Sensoren, die für einen bestimmten Zweck konfiguriert werden können. Beispielsweise gibt es Sensoren für SNMP, ReST API, WMI, Flow-Protokolle wie NetFlow sowie hardware-spezifische Sensoren für Switches, Router und Server. PRTG Network Monitor verfügt über mehr als 200 verschiedene vordefinierte Sensoren, die Statistiken von den überwachten Instanzen abfragen (z.B. Antwortzeiten, Prozessorauslastung, Speicherplatz, Datenbank-Informationen, Systemzustände oder Daten über APIs).

Bedienung

Die Software kann komplett über ein Webinterface bedient werden. Das Webinterface eignet sich sowohl für die Fehlerbehebung in Echtzeit als auch für den Datenaustausch mit nicht-technischen Mitarbeitern über sogenannte Maps (Dashboards) und benutzerdefinierte Berichte.

Ein zusätzliches Desktop-Interface für Windows und macOS ist aktuell im Beta-Status.

Lizenzierung

Die Lizenzierung von PRTG richtet sich nach der Anzahl der benötigten Sensoren. Größere Netzwerke benötigen zur umfassenden Überwachung mehr Sensoren und damit eine größere Lizenz. Eine Version mit 100 integrierten Sensoren steht kostenfrei zur Verfügung.

Verbreitung

Zielgruppe von PRTG Network Monitor sind Netzwerk-Administratoren von kleineren und mittelständischen Unternehmen. Laut eigenen Angaben zählt PRTG weltweit 200.000 Kunden.



PRTG: Ungewöhnliche Zugriffsmuster entlarven 3/3

Bandbreiten-Monitoring – Fünf Ursachen für plötzliche Traffic-Spitzen

Die fünf häufigsten Gründe für plötzliche Traffic-Spitzen sind:

1. Backups über das LAN: Viele Backup-Lösungen können so eingestellt werden, dass sie zu einer bestimmten Zeit ihre Arbeit verrichten.

Allerdings können sie auch enorme Lastspitzen verursachen, sodass deren Einsatzzeitpunkt clever gewählt werden sollte.

2. Remote Backup-Lösungen: In vielen Netzwerken kommen Cloud-basierte Backup-Lösungen zum Einsatz. Große Backups hochzuladen, kann jedoch die Internet-Verbindung enorm belasten und verlangsamen.

3. Virens Scanner- oder andere Software-Updates, die im Netzwerk stattfinden, sind ein häufiger Grund für plötzliche Traffic-Spitzen.

4. Probleme mit dem Mail-Server: Es wurde schon oft beobachtet, dass ein fremder Mail-Server versucht, eine E-Mail mit einem z.B. 15 Megabyte großen Anhang an den Mail-Server eines Unternehmens zu senden – wieder und wieder. Selbst wenn der Ziel-Server die Annahme verweigerte und die E-Mail löschte, hörten die Versuche des fremden Mail-Servers nicht auf. Die Ursache in diesem Szenario: Die beiden vorhandenen SMTP-Implementierungen waren schlicht inkompatibel. Um das Problem zu lösen, musste der Mail-Server des Unternehmens so eingestellt werden, dass er die IP-Adresse des fremden Mail-Servers blockierte.

5. Infektionen mit Malware und Versuche, ein Netzwerk zu hacken, können ebenfalls plötzliche Spitzen im Traffic eines Netzwerkes verursachen. Dies kann aber auch dabei helfen, Hackerangriffe zu identifizieren und Gegenmaßnahmen zu ergreifen. So wird Netzwerk Monitoring auch zu einem wichtigen Bestandteil des IT-Security-Konzeptes.

Gründe für Traffic-Spitzen identifizieren:

1. Versuchen Sie innerhalb der Spitzen ein Muster zu finden. Treten sie in einigermaßen gleichmäßigen Intervallen auf? Treten sie nur während der Geschäftszeiten auf, (Dann ist es wahrscheinlicher, dass ein Nutzer die Probleme verursacht), oder später? (Dann ist es wahrscheinlich ein Terminierungsproblem).

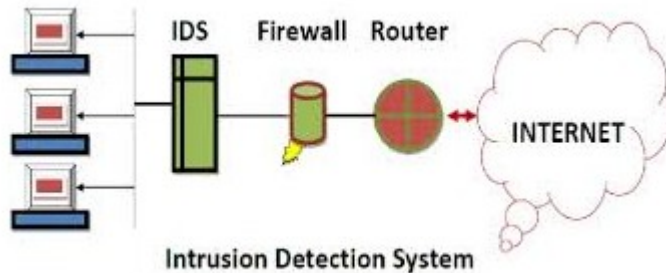
2. Wenn Sie ein Muster identifiziert haben, versuchen Sie weitere Monitoring-Punkte zu finden, die ähnliche Muster aufweisen. Vergleichen Sie die Muster mit Prozessen in Ihrem Netzwerk. (tritt beispielsweise zusammen mit den Traffic-Spitzen häufig eine hohe CPU-Auslastung auf?). PRTG Network Monitor verfügt über die Funktion »Sensor Similarity«. Damit lassen sich alle an PRTG angeschlossenen Sensoren auf solche Muster hin überprüfen. Diese Funktion kann sehr hilfreich dabei sein, versteckte Korrelationen zu entdecken.

3. Analysieren Sie den Traffic mit einem Packet Sniffer oder einem Flow Management Tool. In Netzwerken mit modernen Switches ist das vielleicht nicht so einfach, aber es ist die beste Möglichkeit, herauszufinden, welches Computersystem die Probleme verursacht.

Vorsicht vor »falschen« Traffic-Spitzen

Es gibt auch immer noch die Möglichkeit, dass die Traffic-Spitzen, die ein Bandbreiten-Monitoring anzeigt, gar nicht real sind. Sie könnten beispielsweise auch auf fehlerhafte Soft- oder Hardware zurückgehen.

Snort: Intrusion Detection System (IDS) 1/6



Aufbau der Regeln

Die Regeln bestehen aus dem **Rule Header** und den optionalen **Rule Options**, dabei müssen alle Angaben der Regel zutreffen.

IDS ... Intrusion Detection System

NIDS ... Network Intrusion Detection System; NIDS ist keine Firewall und eine Firewall ist kein NIDS. Analogie: Firewall ist der Türsteher, NIDS ist die Überwachungskamera. Sie unterstützen die Firewall und installierte Schutzsoftware (Schutz vor Malware) beim Erkennen von Angriffen oder schädlichen Aktivitäten.

IDPS ... Intrusion Detection and Prevention System; sie blockieren schädliche Netzaktivitäten und machen durch Änderungen diese Aktivitäten unschädlich

IDS - Erkennung von Angriffen

Intrusion Detection Systeme (IDS) versuchen Angriffsmustern zu entdecken und zu erkennen. Die Erkennung erfolgt auf Grund von Abweichungen des Normalverhalten von Benutzern und des Netzwerkes (Protokollanalyse und Anomalie-Erkennung).

Erkennung der Angriffe an Hand bekannter Angriffssignaturen:

- viele Datenpakete vom gleichen Host an unterschiedliche Ports -> Portscan
- ungewöhnlich hohe Anzahl an Datenpaketen in kurzer Zeit -> DDos
- mehrere fehlerhafte Loginversuche

Snort (erste Version wurde 1998 veröffentlicht) ist ein Open Source NIDS, dass für Windows, Linux und Mac verfügbar ist. Snort arbeitet signaturbasierend mit einer Kombination von Regeln und Präprozessoren. Es kann Pakete defragmentieren und Streams untersuchen. Snort kann sowohl als aktives (Inline-NIDS) als auch als passives NIDS betrieben werden.

Die Konfigurationsdatei von Snort befindet sich unter Linux im Verzeichnis /etc/snort/snort.conf (HOME_NET, INTERFACE, LOGDIR, DAEMON, ...).

Snort Regeln

Die Standardregeln von Snort findet man im Verzeichnis /etc/snort/rules. Die Regeln können angepasst und es können Regeln hinzugefügt werden (**siehe auch:** aktuelle Regeln unter snort.org). **Hinweis:** Die Regeln werden nacheinander abgearbeitet und die erste zutreffende Regel wird angewendet.

Action Field

Protocol Field

Source und Destination IP Field

alert tcp !10.1.1.0/24 any -> 10.1.1.0/24 any (flags: SF; msg: "SYN-FIN-scan"; sid: 12345;)

Rule Header

Rule Options

Regelaufbau

alert tcp ![130.83.0.0/16,\$HOME_NET] any -> \$HOME_NET 135:139

↑ ↑ ↑ ↑ ↑ ↑
Aktion Protokoll Quelle Quellport Ziel Zielport

(msg:"Samba file info";flow:to_server, established; content „|32|“; content:"|05 00|";

↑ ↑ ↑ ↑ ↑
Beschreibung Flussrichtung Status Inhalt in Hex (Mehrfach möglich)

classtype:not-suspicious; logto:"/var/log/MyFile"rev:4;)

↑ ↑ ↑
Klassenidentifikation
nach
classification.config Optional:
anderes Logfile
für spezielle
Alarme Revisionsnum-
mer der Regel

Snort 3/6

Aktions-Feld

Das Aktions-Feld legt die Ausführung fest:

- **alert** -> erstellt Einträge im Alert-File und logt Pakete
- **log** -> logt die geschnitten (mitgelauchten) Datenpakete
- **pass** -> Passiv-Modus - Pakete werden nicht verarbeitet
- **activate** -> löst Alert (Alarm) aus und aktiviert die dynamischen Rules (Regeln)
- **dynamic** -> Aktion ist inaktiv bis es durch ein Activate-Event getriggert wurde

Im Inline-Modus (aktiver Modus) ist auch **drop**, **reject** und **sdrop** möglich.

Protokoll-Feld

Das Protokoll-Feld bestimmt das Protokoll, welches untersucht werden soll (TCP, UDP, ICMP, IP).

Quell- und Ziel-Adressfeld

Das Quell- und Ziel-Adressfeld legt den Quell- und Ziel-Adressbereich und den Port für die Pakete fest.

- **Format:** Adresse/Netzmaske Port
- **192.168.0.2/24** -> einzelner Host
- **192.168.0.0/24** -> komplettes Subnetz
- durch Komma getrennt, können mehrere Adressen eingetragen werden
- Flussrichtung wird durch einen Pfeil angegeben (-> bzw. <-)
- Verwendung von Variablen wie **\$HOME_NET** sind möglich

Sonderzeichen

- **any:** -> beliebige IPs oder Ports
- **!** -> Adresse oder Port negieren
- **20:22** -> Port-Bereich
- **:1023** -> 'kleiner als'
- **1023:** -> 'größer als'
- **Hinweis:** ICMP benötigt die Angabe eines Ports, in diesem Fall wird **any** verwendet.

Optional beliebig viele Optionen

Beispiele:

- **msg** -> Nachricht, die im Log angezeigt wird
- **dsiz** -> Größe des Payloads eines Paketes
Als **Payload** werden die eigentlichen Nutzdaten einer Datenübertragung beschrieben.
- **ags** -> gesetzte TCP-Flags (Flags sind verschiedene Werte, Marker im Header eines Datenpaketes)
- **content** -> String (Zeichenkette) im Payload

```
alert tcp !10.1.1.0/24 any -> 10.1.1.0/24 any /
( flags : SF ; msg : "SYN-FIN-scan" ; sid : 12345 ; )
```

- ▶ TCP-Traffic von ausserhalb 10.1.1.0/24 nach 10.1.1.0/24
- ▶ beliebiger Port
- ▶ Gesetzte Flags SYN und FIN
- ▶ Nachricht im Log-File: *SYN-FIN-scan*

Präprozessoren

- der Funktionsumfang von Snort kann durch verschiedene Präprozessoren erweitert werden
- Verarbeitung der Pakete vor der eigentlichen Untersuchung durch die Regeln
- Pakete können analysiert oder verändert werden
- Aktivierung der Präprozessoren in der Konfigurationsdatei `snort.conf`
`PREPROCESSOR [NAME]: [OPTION]`

Snort 4/6

Bekannte Präprozessoren

- **Stream5** -> setzt TCP-Verkehr zusammen
- **Arpspoof** -> erkennt Arp-Spoofing
- **sfPortscan** -> erkennt TCP-, UDP-, IP-Portscans
- **Reputation** -> Black/Whitelist
- **SSL/TLS** -> erkennt verschlüsselten Verkehr

Denial of Service (DoS)

- IDS lassen bei Überlast den Verkehr ungefiltert passieren
- Angreifer kann durch gezielten Datenverkehr Speicher vollladen lassen
- Überlauf des Speichers, kann auch bei hoher Netzlast ungewollt vorkommen

Session Splicing

Eine Möglichkeit einen Angriff auf ein Netzwerk auszuführen, der von einem Network Intrusion Detection System unerkannt bleibt, ist das sogenannte Session Splicing. Grundlage hierfür ist, dass das Payload-Feld eines TCP-Paketes keine feste Größe hat, sondern sich über die sogenannte Maximum Transmission Unit (MTU) festlegen lässt. Die MTU gibt an, wie groß ein TCP-Frame maximal sein darf - ist die zu übertragende Datenmenge zu groß für ein einzelnes Paket, so wird sie auf mehrere Pakete aufgeteilt. Da Snort in der Standard-Einstellung den Datenverkehr, Paket für Paket bearbeitet und somit keine Informationen über vorhergegangene Pakete zur Verfügung stehen, kann dieser Umstand dazu ausgenutzt werden um auf einfache Weise einen Angriff unbemerkt an einem Network Intrusion Detection System vorbei zu schleusen.

Die im Beispiel dargestellte Regel durchsucht den Datenverkehr nach Paketen, die den String **www.evil.com** enthalten. Da bei einem Aufruf einer Internetseite die aufgerufene Adresse an den Client übertragen werden muss, würde die dargestellte Snort-Regel im Normalfall bei einem Aufruf der Internetseite **www.evil.com** einen Alert auslösen.

Wird die MTU der zu übertragenden Pakete jetzt jedoch soweit verringert, dass die Adresse nicht mehr als zusammenhängender String übertragen werden kann sondern aufgeteilt werden muss, so schlägt das NIDS nicht mehr an.

ALERT TCP !10.1.1.0/24 ANY -> 10.1.1.0/24 ANY /
(CONTENT: "www.evil.com"; MSG: "AUFRUF VON EVIL.COM"; SID: 123456;)



Probleme und Schwächen

Schwächen des eingesetzten Erkennungssystems:

- NIDS kann etwa durch Fragmentation umgangen werden
- bei falscher oder schlechter Konfiguration können viele Fehlalarme ausgelöst werden
- Beeinträchtigungen durch falsche Reaktionen auf angebliche Angriffe (Angriffe mit gefälschter IP)
- NIDS alleine bietet keinen vollständigen Schutz

Snort 5/6

Zusatz-Tools

Um das Arbeiten mit Snort zu vereinfachen, gibt es diverse Zusatzsoftware. Einige Programme werten die Logdateien aus und stellen die Meldungen übersichtlich dar. Andere erlauben das Management der Snort-Regeln.

ACID: Zu den beliebtesten Analyse-Tools zählt **ACID** (Analyse Console for Intrusion Database). Die PHP-basierte Analysesoftware bietet einfache und interaktive Funktionen zur Filterung der Daten und erlaubt auch die grafische Darstellung der Ergebnisse. Keywords für die Suchmaschine: ACID
snort

Snortreport: Snortreport ein Analyse-Tool um die Datenanalyse zu vereinfachen. Auf Snortreport greift man ebenfalls über einen Internet-Browser zu. Snortreport arbeitet etwas performanter als ACID.

Snort Alert Monitor (SAM): Snort Alert Monitor ist ein Zusatztool für Snort, welches Alarme in Echtzeit grafisch darstellt. SAM greift wie ACID auf die Datenbank zu und verarbeitet die von Snort generierten Daten. Weiterhin hat SAM die Möglichkeit eine Alarmierung per Mail auszulösen, wenn eine vom Benutzer definierte Anzahl von Alarmen überschritten ist.

Graylog2: Graylog (Linux) ist ein kostenloses und quelloffenes Protokollverwaltungstool auf Basis von Java, Elasticsearch und MongoDB, mit dem Sie jedes Serverprotokoll von einem zentralen Standort aus sammeln, indizieren und analysieren können. Sie können die SSH-Logins und ungewöhnliche Aktivitäten zum Debuggen von Anwendungen und Protokollen mit Graylog einfach überwachen. Graylog bietet eine leistungsstarke Abfragesprache und Alarmierungsfunktionen.

BASE: Snort ist ein gutes Tool, um unerwünschte Aktivitäten - etwa Port-Scans, heimliche Attacken, Pufferüberläufe oder andere böswillige Aktionen im Netz - zu erkennen. In Kombination mit BASE (Basic Analysis and Security Engine) erhält man ein Web-gestütztes Frontend, das Snort-Alerts abfragen und analysieren kann, sowie ein rollenbasierendes Authentifizierungssystem, mit dem sich der Nutzerzugriff auf Snort-Daten kontrollieren lässt.

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.

FireEye: Die Produkte von FireEye sind besonders gut beim Erkennen bekannter und unbekannter Exploits. Eine ebenfalls sehr wichtige Funktion ist die Fähigkeit, die gesammelten Daten klar zu visualisieren und eine leistungsfähige Suchfunktion zur Verfügung zu stellen.

SGUIL: Sguil ist eine Sammlung kostenloser Softwarekomponenten für die Überwachung der Netzwerksicherheit und die ereignisgesteuerte Analyse von IDS-Warnungen. Der sguil-Client ist in Tcl / Tk geschrieben und kann auf jedem Betriebssystem ausgeführt werden, das Tcl/Tk unterstützt.

Samhain: Samhain ist ein Host-basierendes System, das auf vielen Plattformen läuft. Viele Linux-Distributionen enthalten bereits vorgefertigte Pakete dieser Software. Durch kryptographische Signaturen können Verfälschungen an Konfigurations-Dateien und der Kommunikation über das Netzwerk aufgedeckt werden.

Snort 6/6

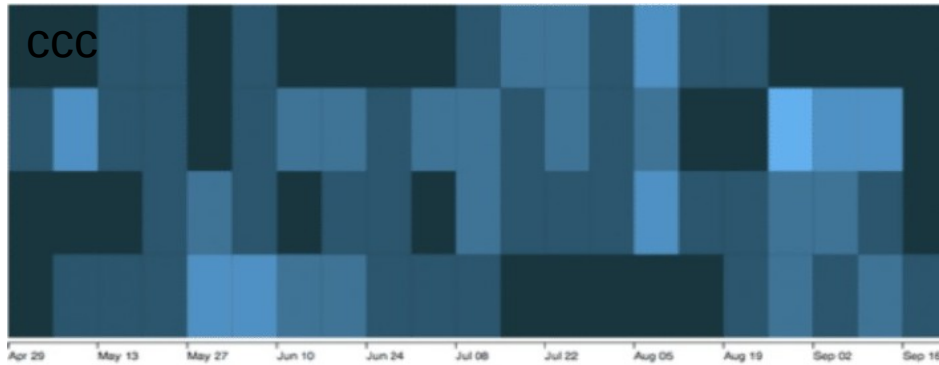


Abbildung 1

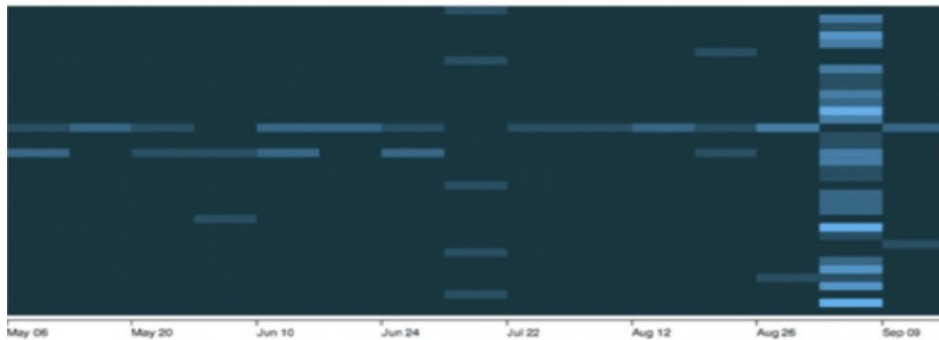


Abbildung 2

Die Protokolldaten von Snort können mithilfe statistischer Methoden und der Programmiersprache PHP in dynamische Grafiken umgewandelt werden, die leichter auswertbar sind als große Mengen an Protokolldaten. Inspiration kann man sich vom Analyse-Tool (Marketing- und Überwachungstool zur Auswertung großer Datenmengen) von Pivotal (<https://pivotal.io/de/data-science>) holen.

Abbildung 1: typisches Zugriffsmuster für eine bestimmte Gruppe an Nutzern

Abbildung 2: Nutzer verhalten sich nicht normal im Sinne ihrer Zugriffsberechtigungen

Micos: Software für soziale Einrichtungen

MICOS-Konzept: Die integrierte Software-Lösung für soziale Einrichtungen

Größere sozialwirtschaftliche Organisation liefern nur dann erfolgreiche Ergebnisse, wenn jedes Mitglied seine Aufgaben und Befugnisse kennt, Zugang zu allen relevanten Informationen hat und der Informationsaustausch einfach, schnell und sicher möglich ist.

BASIS-Funktionalitäten von MICOS

- **Datenmanagement mittels Baumstrukturen** - Organisationsmethode für Daten, Aufbauorganisation, Berechtigungen, strukturierte Suche nach Daten u.v.m.
- **Berechtigungssystem** - Das ausgesprochen detaillierte Berechtigungssystem erlaubt Berechtigungen auf Funktionen sowie Daten zu vergeben, über konfigurierbare, wiederverwendbarer Rollen, Schablonen sowie personenbezogene Rechte.
- **Adressmanagement** - Die zentrale Datenhaltung von Stammdaten für alle Nutzer eröffnet den Benutzern große Qualitäts- und Zeitvorteile in allen Organisationsbereichen. Weitere Pluspunkte: Die Konsistenzprüfung von Adressen (Dubletten), die Pflege von Verbindungen zwischen Adressen sowie Import- und Exportfunktionen.
- **Nachrichtensystem** - Medienbruchlose Kommunikation zwischen allen MICOS-Anwendern. Durch Aufruf aus den Masken gibt man Empfängern direkt den Verweis auf relevante Daten mit. Sehr praktisch gestaltet sich auch der elektronische Belegversand mit externen Partnern mit konfigurierbaren Inhalten aus einer Datenbank.
- **Terminmanagement** - Das Terminmanagement verwaltet manuell sowie systemseitig erzeugte Termine. MICOS ermöglicht eine Vielzahl von Ansichten (Tag, Woche, Monat, Terminliste) sowie Filterungsoptionen. Praktisch: die Erinnerungsfunktion.
- **Digitale Akte (DMS)** - Aktenberge gehören mit MICOS der Vergangenheit an. Die vollständig in die MICOS-Oberfläche integrierten elektronischen Akten sorgen für eine strukturierte, langfristige und sichere Aufbewahrung der Dokumente, von Rechnungen über E-Mails bis zu Handbüchern (Akten für Kunden, Mitarbeiter, Lieferanten, Gebäude oder Ärzte).
- **Auswertungscenter** - In diesem Bereich werden umfassend konfigurierbare Standardberichte und persönliche Berichte zur Verfügung gestellt. Mit einer umfangreichen Sortierungs-, Filterungs- und Gruppierungs- und Rechenfunktionen können aussagefähige Auswertungen erstellt werden.
- **Zeitsteuerung von Aufgaben** - Automatisierung von regelmäßigen Tätigkeiten durch zeitgesteuerte Aufgaben bis hin zu komplexen Aufgabenketten.
- **Benutzerspezifische Navigation** - Die Funktionen in MICOS können entsprechend der persönlichen Prozessabläufe einfach per Drag & Drop mit Favoriten in die für die Anwender optimale Reihenfolge und Gruppierung gebracht werden.
- **Individuelle Erweiterung von Maskenfunktionen** - Ohne aufwendige Individualprogrammierung kann das MICOS-Konzept erweitert werden. Mit dem Maskeneditor können ohne Programmierkenntnisse zusätzliche Reiter mit individuellen Inhalten angelegt werden.
- **Kundenindividuelle Hilfefunktion** - Keine Standard-Hilfefunktion kann die individuelle Konfiguration der Anwendung und deren Nutzungsrichtlinien abbilden. Deshalb lassen sich in MICOS eigenen Leitfäden (Hilfe-Hinweise) direkt in den Masken der Anwender hinterlegen. So sind die Richtlinien der Organisation immer aktuell und wirken dort wo sie auch wirken sollen: am Arbeitsplatz der Anwender!

Quelle: <https://micos-VRg-gruppe.de>

VDI: Virtual Desktop Infrastruktur

Virtual Desktop Infrastruktur (VDI)

Eine Infrastruktur virtueller Desktops (Virtual Desktop Infrastructure, VDI) ist das Bereitstellen von Desktop-Umgebungen auf einem zentralen Server. Es handelt sich dabei um eine Form der Desktop-Virtualisierung, da die spezifischen Desktop-Images von virtuellen Maschinen (VMs) ausgeführt werden und per Netzwerk auf Endgeräten bereitgestellt werden.

VDI ermöglicht personalisierte Desktops. Dies ist mit Terminalserver, Rembo (RemoteBoot) nicht möglich, die nur gleiche Desktops für größere Benutzergruppen zur Verfügung stellen kann.

Die Virtual Desktop Infrastructure entstand aus dem Gedanken, dass der Einsatz von herkömmlichen PCs einen erheblichen Aufwand erfordert und daher sinnvoll reduziert werden sollte. Statt in teure Hardware-Ersatz-Zyklen, Sicherheits-Anforderungen der Desktops und Notebooks, umfassende Helpdesks sowie zahlreiche IT-Mitarbeiter zu investieren, sollten moderne VDI-Lösungen implementiert werden.

Die VDI-Technologie eignet sich besonders für umfassende, sich wiederholende Anwendungsfälle wie sie zum Beispiel in Finanz- und Buchhaltungsabteilungen, Krankenhäusern oder bei der Bearbeitung von Versicherungsansprüchen vorkommen. Der Nutzer braucht dafür keinen dedizierten PC, sondern nur ein Basis-Betriebssystem sowie ein paar voreingestellte Anwendungs-Tools.

Anbieter von VDI-Lösungen: Als einer der Marktführer gilt der Anbieter VMware mit dem Produkt »VMware View«. Danach folgt »Xen Desktop« von Citrix. Das Produkt »Xen Desktop« gilt zu »VMware View« als technisch ebenbürtig, wobei »Xen Desktop« mit verschiedenen Hypervisoren zusammenarbeiten kann. »VMware View« hingegen ist an den firmeneigenen »ESXi-Server« gebunden. Einen deutlich geringeren Marktanteil kann die »Microsoft VDI-Suite« für sich verbuchen. Darüber hinaus gibt es ein paar kleinere Anbieter, die um ein paar Prozent Marktanteile kämpfen.

Dazu zählt »Quest vWorkspace« und »Pano Logic«. Zu den frei verfügbaren VDI-Systemen gehören »Linux Terminal Server Project« und »QVD Community Edition«.

Wie funktioniert VDI?

Für alle VDI-Bereitstellungen gilt Folgendes:

- Die virtuellen Desktops befinden sich in VMs (virtuelle Maschinen) auf einem zentralisierten Server (Unternehmens-Rechenzentrum).
- Jeder virtuelle Desktop enthält das Image eines Betriebssystems, meist Microsoft Windows.
- Die VMs sind hostbasiert, es können sich also mehrere Instanzen von ihnen auf dem gleichen Server im Rechenzentrum befinden.
- VDI benutzt das RDP-Protokoll (Remote Desktop Protokoll).
- Die Endgeräte müssen über eine konstante Verbindung zum zentral verwalteten Server verfügen, damit der Zugang zu den virtualisierten Desktops erhalten bleibt.
- Der Verbindungsbroker der VDI-Implementierung findet für jedes Gerät einen virtuellen Desktop im Ressourcenpool, um beim erfolgreichen Zugriff der VDI-Umgebung eine Verbindung herzustellen.
- Währenddessen erstellt, verwendet und verwaltet ein Hypervisor die verschiedenen Host-VMs, die die individuellen Umgebungen der virtuellen Desktops bilden.
- In einer VDI-Umgebung können verschiedene Arten von Clients (Rechner) zum Einsatz kommen: Thin, Thick und Zero Clients.

Bei modernen digitalen Arbeitsplätzen, wo zahlreiche Anwendungen nach Bedarf geöffnet werden, sorgt VDI für einen sicheren und einfachen Remote-Zugriff, der die Mitarbeiterproduktivität steigert. Zudem wird dadurch eine konsistente Erfahrung auf allen Geräten erreicht.

siehe auch: www.citrix.de/glossary/vdi.html

Projekt FIDO2 – Authentifizierungslösung 1/5

Das Projekt FIDO2 ist eine gemeinsame Unternehmung zwischen der FIDO-Allianz (besteht aus etwa 250 Firmen) und dem W3C, mit dem Ziel eine starke Authentifizierungslösung für das Web zu entwickeln.

FIDO 2 - Worum geht es?

Passwörter zur Anmeldung an Webseiten bieten die Gefahr, dass diese gehackt oder vom Benutzer vergessen werden. Daher ist es das Ziel, die Anmeldung ohne ein Kennwort, über andere Identifikationsverfahren, zu ermöglichen.

Im Kern besteht FIDO2 aus dem W3C Web-Authentication-Standard (WebAuthn) und dem FIDO Client-to-Authenticator-Protocol (CTAP). FIDO2 basiert auf früheren Arbeiten der FIDO-Allianz, insbesondere dem Universal 2nd Factor (U2F) Authentifizierungsstandard. Mit dem Release von FIDO2 wurde U2F in CTAP1 umbenannt.

WebAuthn ist ein vom World Wide Web Consortium (W3C) veröffentlichter Standard für eine Programmierschnittstelle mit Webanwendungen und Websites. Sie erlaubt ihren Benutzern eine direkte Authentifikation mittels Public-Key-Verfahren im Webbrowser anbieten zu können.

Die Voraussetzung ist, dass der Webbrowser sicher auf einen Authentifikator (z.B. USB-Stick, FIDO Security Keys) im oder am Gerät des Benutzers zugreifen kann. Viele moderne Smartphones oder Laptops bieten diese in Form von Fingerabdrucksensoren oder Gesichtserkennung.

Wie der Name bereits andeutet ermöglicht das Client-to-Authenticator-Protocol (CTAP) einem kompatiblen kryptografischen Authentifizierer mit dem WebAuthn-Client (z.B. Browser) interagieren zu können.

Die CTAP-Spezifikation verweist auf zwei Protokollversionen: CTAP/U2F und CTAP2. Ein Authentifizierer, der eines dieser Protokolle implementiert hat, wird entweder U2F-Authentifizierer oder FIDO2-Authentifizierer genannt.

Abkürzungen:

CTAP ... CTAP (Client to Authenticator Protocol) ist ein Protokoll auf Anwendungsebene und dient zur Kommunikation zwischen einem Client (Desktop) oder einer Plattform (Betriebssystem) und einem externen Authentifikator (z.B. Security Key, Token).

FIDO ... FIDO (Fast IDentity Online Alliance, 2013, FIDO2 seit März 2019) ist ein Satz an plattformunabhängigen Security-Spezifikationen, um starke Authentifizierung zu ermöglichen.

FIDO-U2F ... FIDO - Universal Second Factor ist ein kryptografisches Public Key Verfahren zur Authentifizierung mit einem kleinen USB-Stick.

NFC ... Die Near Field Communication ist ein auf der RFID-Technik basierender internationaler Übertragungsstandard zum kontaktlosen Austausch von Daten per elektromagnetischer Induktion mittels loser gekoppelter Spulen über kurze Strecken von wenigen Zentimetern.

Projekt FIDO2 – Authentifizierungslösung 2/5

OTP ... Unter der Abkürzung OTP versteht man in der IT-Sicherheit entweder das One-Time-Pad (Einmalverschlüsselung) oder ein One-Time Password (Einmalkenntwort).

SSO ... Single Sign-on (Einmalanmeldung) bedeutet, dass ein Benutzer nach einer einmaligen Authentifizierung an einem Arbeitsplatz auf alle Rechner und Dienste, für die er lokal berechtigt (autorisiert) ist, vom selben Arbeitsplatz aus zugreifen kann, ohne sich an den einzelnen Diensten jedes Mal zusätzlich anmelden zu müssen.

U2F ... Universal Second Factor (U2F, 2FA, Zwei-Faktor-Authentifizierung) ist ein Standardprotokoll für die Authentifizierung, das auf der Two-Factor-Authentication (2FA) basiert.

WebAuthn/FIDO2 ... WebAuthn/FIDO2 ist ein Standard des W3C, der im März 2019 verabschiedet wurde und von den Großen der IT-Branche unterstützt wird. WebAuthn ist eine Weiterentwicklung von FIDO-U2F und soll den Login mit Username / Passwort Kombinationen komplett ersetzen können.

YubiKey intern

Der YubiKey wird von Windows als Tastatur erkannt und die nötigen Treiber werden automatisch installiert. Für den ersten Funktionstest, kann man einfach ein Textprogramm (Editor, Notepad) öffnen und den Knopf (Sensorfeld, Leuchtdiode) kurz drücken. Es wird eine Zeichenkette mit 44 Zeichen eingefügt, wovon die ersten 12 Zeichen den Public Key des Sticks darstellen. Dieser bleibt bei jedem Passwort gleich. Die übrigen 32 Zeichen sind ein eindeutiger Passcode sowie ein Zähler. Letzterer ist wichtig, um aus dem Passwort viele Einmalpasswörter zu generieren (Voreinstellung), denn der Server (die Gegenstelle) speichert den zuletzt benutzten Zählerwert und für jede weitere Anfrage wird ein höherer Wert benötigt. Nur wenn Public Key und Zählerwert übereinstimmen, wird Zugriff gewährt. Über einen integrierten USB-Hub am USB-Token melden sich mehrere USB-Geräte am PC an.

Eines der Geräte ist der Smartcard-Reader, ein anderes ist eine USB-Tastatur über die die OTP-Token und auch das statische Passwort als Tastatureingabe zurück an die (Web-)Anwendungen gesendet werden. Man kann davon ausgehen, dass eines der USB-Eingabegeräte die U2F-Schnittstelle darstellt und ein weiteres USB-Eingabegerät eine interne Funktion hat.

Über die USB-Schnittstelle können Yubikeys drei verschiedenartige, virtuelle USB-Geräte emulieren und damit vielfältige Funktionen anbieten: OTP, FIDO und CCID. Die drei USB-Protokolle lassen sich miteinander kombinieren oder wenn nicht benötigt, auch deaktivieren.

Das USB-Protokoll OTP, abgeleitet vom Begriff One-Time-Pad, stellt das ursprüngliche USB-Protokoll für Security-Token dar. Es erlaubt am Yubikey die Konfiguration von zwei sogenannten Slots (Speicherpositionen). Jeder Slot kann unabhängig eine Funktion und der dafür notwendigen Daten, wie geheime Schlüssel, aufnehmen.

- Yubico OTP, ein proprietäres One-Time-Pad Verfahren von Yubico
- Challenge-Response-Authentifizierung mittels HMAC-SHA1
- Statisches Passwort. Dabei wird vom Yubikey eine virtuelle USB-Tastatur emuliert und gestattet es so direkt das Passwort ohne zusätzliche Software in der jeweiligen Anwendung in das Passwortfeld direkt einzugeben.
- HOTP - benannt nach der Initiative »For Open Authentication« (OATH)

Die jeweilige OTP-Funktion kann oder muss mit der Sensortaste verknüpft werden, d. h. man drückt zur Auslösung sein Einverständnis durch Tasten-Betätigung aus. Je nachdem wie lange man die Taste drückt, löst man die Funktion vom Slot 1 (kurze Tasten-Betätigung) oder Slot 2 (Tasten-Betätigung für 3 bis 4 Sekunden) aus.

Projekt FIDO2 – Authentifizierungslösung 3/5



Yubico Security Key - U2F and FIDO2, USB-A, Two-Factor Authentication

- der Security Key ersetzt die Anmeldung mit einem Passwort bei Windows 10 (ab Version 1809)
- der Security Key generiert Einmal-Passwörter, die sich nach jeder Benutzung automatisch ändern
- unterstützt Google, Dropbox, Facebook, Twitter, Gmail, Microsoft Konto, Skype
- wasserdicht und robust



YubiKey 5 Nano

- Unterstützung für Single-Faktor-, Zwei-Faktor-Hardware- und Multi-Faktor-Authentifizierung
- Authentifizierung mit Unterstützung für mehrere Protokolle (Yubico OTP, OATH HOTP, OATH TOTP, U2F, sicheres statisches Passwort, PIV und Open PGP) und FIDO2

Projekt FIDO2 – Authentifizierungslösung 4/5



OnlyKey mit Stealth Black Case - Hardware Passwort-Manager mit 2-Faktor-Authentifizierung (U2F, YubiKey OTP (One-Time Password), Google Auth, SSH, PGP/GPG)

- Um das Gerät nutzen zu können, muss eine PIN (Master-PIN) eingegeben werden. Die PIN wird auf dem OnlyKey eingegeben.
- Passwortverwaltung und zwei-Faktoren-Authentifizierung und Offline-Speicherung.
- Universelle Unterstützung: Identifiziert sich als reguläre Tastatur (USB HID), keine speziellen Treiber erforderlich.
- Unterstützt den Chrome-Browser unter Windows, Mac und Linux.
- Der OnlyKey gibt per Knopfdruck die Website-URL aus und gibt dann den gespeicherten Benutzernamen und das Passwort automatisch ein.
- Passwörter, URLs und Usernamen dürfen max. 56 Zeichen lang sein
- Der OnlyKey ist langlebig und wasserdicht (robustes Silikongehäuse).

Der OnlyKey ist derzeit eher etwas für Entwickler. Er ist eigentlich ein frei programmierbarer Micro-Controller mit 6 Sensortasten und einer Vielfarb-LED im Format eines USB-Sticks.

Er ist so aufgebaut, dass die in ihm gespeicherten geheimen Schlüssel (SSH/PGP) oder shared Secrets (HOTP/Yubikey TOTP/Google-Auth-Secret) niemals das Gerät unverschlüsselt verlassen können. Zusätzlich funktioniert er auch als portabler Passwortsafe.

Wer die (mindestens 6-stellige) PIN nicht kennt, kann den Key nicht verwenden.

Nach 10 Falscheingaben löscht sich der Key. Zusätzlich gibt es eine Lösch-PIN, die das sofort auslöst.

Projekt FIDO2 – Authentifizierungslösung 5/5

Anmeldung unter Windows 10

Beim ersten Einstecken des YubiKeys installiert Windows 10 automatisch den passenden Treiber. Danach startet man die App »YubiKey for Windows Hello« (Microsoft Store) und klickt sich in wenigen Schritten durch die Einrichtung.

Mit der App »YubiKey for Windows Hello« muss der Nutzer zunächst eine Registrierung des Keys durchführen. Hierzu ist es erforderlich, zunächst eine PIN auf dem Windows-10-Rechner einzurichten. Danach kann der Anwender den gesperrten PC durch Anstecken des Keys und – wenn man es entsprechend konfiguriert hat – auch per Fingerkontakt auf der entsprechende Fläche des Keys entsperren.

Dabei ist es wichtig zu wissen, dass dieser kleine Punkt auf dem Key, der auch entsprechend blinkt, nicht etwa einen Fingerabdrucksensor beinhaltet, sondern einfach aufgrund des Hautwiderstandes einen Impuls sendet.

Zieht man den YubiKey ab, muss man wieder wie gewohnt Passwort oder PIN eingeben. Bei einem Neustart des Systems erfolgt allerdings keine automatische Anmeldung mittels YubiKey – das soll verhindern, dass ein Dieb uneingeschränkter Zugriff bekommt, wenn er beispielsweise ein Notebook mit eingestecktem YubiKey stiehlt.

Achtung: Wenn der Key im Rechner steckt, kann jeder, der Zugang zum Gerät hat, einfach durch ein Berühren des Feldes am Token den PC entsperren.

Hinweis: Die YubiKeys unterstützen auch andere Betriebssysteme. Darüber hinaus können die Hardware-Token auch zur Authentifizierung bei einer Vielzahl von Online-Diensten und Services genutzt werden.

Schlussbetrachtungen

- Die Firma Yubico stellt auf ihrer Webseite einige Tools (Download: <https://www.yubico.com/support/download/>) für die Einrichtung und Konfiguration zur Verfügung (Beispiel: »YubiKey Manager«, »Yubikey Personalization Tools«).
- Nur wenn der YubiKey im System (als Tastatur) ist, kann die Hello-App von Windows 10 ihn auch finden. Ist er als Smartcard mit den entsprechenden Treibern installiert, findet ihn die Hello-App nicht. **Siehe auch:** Windows »Einstellungen« -> »Bluetooth- und andere Geräte«
- **Empfehlung:** Zur Sicherheit sollte ein zusätzlicher YubiKey als Backup für alle Web-Dienste eingerichtet werden.
- Alle Kennnamen und Passwörter sollten zusätzlich sicher aufbewahrt werden (verschlüsselte Datei). Nach einigen Monaten der Benutzung der Security-Keys, kann sich keiner mehr an die Anmeldenamen und Passwörter erinnern.
- Aus Sicherheitsgründen kann die Software auf den Yubikey weder ausgelesen noch verändert werden. Bei einem Update muss das Gerät durch ein neues Modell ersetzt werden. Geheime private Schlüsseldaten können am Token erzeugt oder auf dem Token geschrieben werden, aber nachfolgend nicht ausgelesen werden.
- Bei Einrichtung des Zugangs zu einem Webdienst über ein Schlüssel (Token), sollte man sich unbedingt schon über die Deaktivierung oder Löschung eines verloren gegangenen Schlüssels erkundigen.

Siehe auch:

Wissensdatenbank – Yubico:

<https://www.mtrix.de/support/index.php?/Knowledgebase/List/Index/3/>
Yubico

Yubico-Download: <https://www.yubico.com/support/download/>

Gefahrloser Test eines neuen YubiKey: <https://webauthn.io/>

MySQL

In der MySQL-Abfrage ist das einfache Hochkomma (') innerhalb von Strings, Texten nicht zu verwenden - bedingt durch die MySQL-Syntax.

Der Backslash (\) innerhalb von Strings, Texten ist durch einen zweiten Backslash zu schützen (\\).

Alle MySQL-Befehle sind mit einem Semikolon (;) abzuschließen.

Beispiel: Erstellung einer neuen Tabelle

```
CREATE TABLE `name_tabelle` (
  `id` SMALLINT(6) UNSIGNED NOT NULL
  AUTO_INCREMENT PRIMARY KEY,
  `date` DATE NOT NULL,
  `zaehler` INT(10) UNSIGNED NOT NULL,
  `kommentar` TEXT NOT NULL,
  `status` TINYINT(3) UNSIGNED NOT NULL, `ciao`
  VARCHAR(255) NOT NULL
)
COMMENT = 'Kommentar zur Tabelle';
```

Beispiele:

Einfügen eines neuen Datensatzes:

```
INSERT INTO name_tabelle (zaehler,ciao) VALUES (7,'hier steht
Text');
```

Aktualisierung eines bestehenden Datensatzes:

```
UPDATE name_tabelle SET zaehler=8, ciao='hier steht noch ein
Text' WHERE id=3;
SELECT * FROM name_tabelle WHERE id>100 ORDER BY
zaehler;
```

Löschung eines Datensatzes:

```
DELETE FROM name_tabelle WHERE id>50;
```

Einfügen eines Feldes in einer Tabelle:

```
ALTER TABLE name_tabelle ADD zaehler_ganz_neu
VARCHAR(255);
```

```
ALTER TABLE name_tabelle ADD zaehler_ganz_neu_nr2
VARCHAR(30) AFTER ciao;
```

Entfernung eines Feldes in einer Tabelle:

```
ALTER TABLE name_tabelle DROP zaehler_ganz_neu;
```

Änderung eines Tabellennamen:

```
ALTER TABLE name_tabelle RENAME name_tabelle_a;
```

Feldeigenschaften von Tabellenfelder ändern:

```
ALTER TABLE name_tabelle_a CHANGE ciao servus
VARCHAR(255);
```

```
ALTER TABLE name_tabelle_a CHANGE servus servus
VARCHAR(128);
```

SQL - SAP Datenbanken

OpenSQL

OpenSQL ist ein proprietäres SQL-Derivat, das vom Unternehmen SAP stammt. SAP beabsichtigt damit, einen einheitlichen SQL-Dialekt für alle von SAP unterstützten Datenbanken anzubieten. OpenSQL ist Bestandteil der Programmiersprache ABAP (Advanced Business Application Programming Language, Programmiersprache von SAP).

Das Modifizieren von Tabelleninhalten auf der Datenbankebene erfolgt durch OpenSQL-Anweisungen. Dabei handelt es sich um spezielle ABAP Befehle, die eine einheitliche Syntax für alle Datenbanksysteme sicherstellen (www.dbs.ethz.ch/sapr3).

Die häufigsten OpenSQL-Befehle sind SELECT, INSERT, MODIFY, UPDATE und DELETE.

In der FROM-Klausel sind pro Open-SQL-Select-Statement nur maximal zwei Tabellen erlaubt - Beispiel 1:

TABLES: zautor, zwerk. " zautor und zwerk nicht transparent
SELECT * FROM zautor.

SELECT * FROM zwerk

WHERE autorid = zautor-autorid.

WRITE: / zautor-nachname, zwerk-titel.

ENDSELECT. " zwerk

ENDSELECT. " zautor

Schlüsselwort »Parameters« deklariert Eingabeparameter eines Berichts - Beispiel 2:

PARAMETERS: name LIKE zautor-nachname.

SELECT * FROM zautor

WHERE nachname = name.

[...]

ENDSELECT.

Die OpenSQL-Syntax ist mit der Syntax der anderen SQL-Sprachen vergleichbar, aber nicht identisch.

OpenSQL-Kommentare

Kommentare sind Texte, die zur Erläuterung zwischen die Anweisungen eines ABAP-Programms geschrieben werden können. Kommentare unterscheiden sich durch die voranstehenden Zeichen * (am Zeilenanfang) und " (an beliebiger Zeilenposition) von den ABAP-Anweisungen. Wenn die ganze Zeile Kommentar ist, wird am Anfang der Zeile ein Stern (*) eingegeben. Das System ignoriert die gesamte Zeile bei der Programmgenerierung. Wenn nur ein Teil der Zeile Kommentar sein soll, wird vor dem Kommentar ein Anführungszeichen eingegeben. Das System interpretiert Kommentare, die durch das Anführungszeichen gekennzeichnet sind, als Leerzeichen.

Beispiele:

SQL-Kommentarindikator: **Stern (*)**

```
*****
* PROGRAM SAPMTEST                      *
* WRITTEN BY KARL BYTE - 06/27/1995      *
* LAST CHANGED BY RITA DIGIT, 10/01/1995 *
*****
```

SQL-Kommentarindikator: **doppeltes Hochkamma (")** an beliebiger Stelle - der Datenbankserver ignoriert alle restlichen Zeichen in der Zeile
select ... " Diverse Felder

Weitere von SQL unterstützte Kommentarindikatoren:

Doppel-Bindestrich (--) am Anfang oder an beliebiger Stelle - der

Datenbankserver ignoriert alle restlichen Zeichen in der Zeile; **Doppel-Schrägstrich (//)** - Doppel-Schrägstrich hat dieselbe Bedeutung wie der Doppel-Bindestrich; **Schrägstrich-Stern (/ * ... */)** - alle Zeichen zwischen den beiden Kommentarmarkierungen werden ignoriert

select ... -- Diverse Felder

order by ... // Sort

/* dieser Text ist ein Kommentar */

Erweiterte Excel-Hinweise

=WENN(ISTLEER(D9);"FEHLER-HINWEIS";WENN((D9+E9)>10;10;D9+E9))

=WENN(ODER(ISTLEER(D9);ISTLEER(E9));"FEHLER-HINWEIS";WENN((D9+E9)>10;10;D9+E9))

=HEUTE() -> aktuelles Datum

=JETZT() -> aktuelles Datum und Uhrzeit

Hinweis: Bei Datumsberechnungen ist auch auf die Formatierung der Felder zu achten.

=DATUM(2019;9;2) -> formatierte Datumsausgabe

=DATUM(G1;H1;I1) -> formatierte Datumsausgabe

=VERKETTEN(TAG(H5+1);".";MONAT(H5);".";JAHR(H5))

HINWEIS: in H5 befindet sich ein Datum

=JAHR(HEUTE()) -> I1

=MONAT(HEUTE()) -> H1

=TAG(HEUTE()) -> G1

=VERKETTEN(G1;".";H1;".";I1)

=WENN((TAG(HEUTE())<10;VERKETTEN("0";TAG(HEUTE()));TAG(HEUTE()))

=WENN(ISTFEHL(H11)=WAHR;"HINWEIS-TEXT";H11)

=WENN(ISTFEHLER(H11)=WAHR;"HINWEIS-TEXT";H11)

Fehlermeldungen ausblenden - #NAME, #WERT, ...

ZAHLEN IN FARBE:

bedingte Formatierung -> neue Regel -> nur Zellen formatieren, die enthalten

Unbeaufsichtigten Installation

Bei einer unbeaufsichtigten Installation (englisch: unattended installation) wird das komplette Setup eines Programms oder einer Installationsroutine durchlaufen, so dass nur wenige Eingaben des Benutzers erforderlich sind.

Eingaben während der Installation entfallen bei einer unbeaufsichtigten Installation, da diese Einstellungen zuvor in einem Skript (einer sogenannten Antwortdatei, Dateiformat: XML) oder mit einem bestimmten Kommandozeilenparameter festgelegt werden.

Die Windows-Setup-Datei »setup.exe« und die Autounattend-Datei »Unattend.xml«, müssen sich auf derselben Verzeichnisebene befinden.

Die Autounattend-Datei »Unattend.xml«, wird von der setup.exe erkannt und automatisch ausgewertet. Der Dateiname Unattend.xml darf nicht geändert werden, ansonsten kann die Installationsroutine die XML-Datei nicht mehr so einfach erkennen und auswerten.

Programme - Unbeaufsichtigte Installation (Windows 10)

1. Windows Answer File Generator

Der »Windows Answer File Generator« ist auf der Webseite https://windowsafg.com/win10x86_x64_uefi.html zu erreichen. Der »Windows Answer File Generator« verwendet noch einige Einstellungen die von Microsoft als deprecated (veraltet) gekennzeichnet wurden.

Die Textdatei ist dann entsprechend noch manuell zu bearbeiten und anschließend in das XML-Format zu konvertieren (Textdatei mit den Internet-Explorer öffnen -> Seitenquelltext anzeigen -> Bearbeiten aufrufen -> »Alle Dateien anzeigen« und anschließend die Textdatei mit der Dateierweiterung .xml versehen und speichern).

2. Windows Assessment and Deployment Kit (ADK)

Das frei erhältliche Windows ADK (Assessment and Deployment Kit) von Microsoft enthält Tools die eine angepasste und automatisierte Windows-Installation ermöglichen.

Der **Windows System Image Manager** aus dem Windows Assessment and Deployment Kit (ADK) hilft bei der Erstellung einer Unattend.xml.

3. Ergänzungen

DISM: Deployment Image Servicing and Management tool ist ein Befehlszeilenprogramm (Administratorrechte erforderlich). Der Befehl dient zur Reparatur und Administration verschiedener Windows Komponenten und der Vorbereitung und Bereitstellung von Windows PE-Images (Windows Preinstallation Environment).
DISM-Befehle oder andere CMD-Befehle können am Schluss in der Unattend.xml eingefügt werden.

PlainText: Bei PlainText false, ist der Wert verschlüsselt einzutragen.

Computernamen korrigieren: Wenn kein Computernamen in der Autounattend.xml angegeben wird, generiert das Setup den Namen automatisch. Der Administrator sollte den Namen nach Abschluss des Setup's entsprechend ändern.

Hinweis: Alle Autounattend.xml oder Unattend.xml die im Internet kursieren, haben eines gemeinsam. Sie funktionieren entweder nicht oder erst nach einer deutlichen Bearbeitung.

Hinweise: spezielle Google-Suche

Google bietet eine Reihe spezieller Operatoren, mit denen man besondere Inhalte suchen, oder die Treffer auf ganz spezielle Bereiche begrenzen kann. Google wertet bis zu 32 Wörter aus, alle weiteren Wörter werden ignoriert (Stand: 2019). Alle Begriffe werden durch ein logisches UND verbunden. Für eine qualifizierte Anfrage reichen 2 bis 4 gut ausgewählte Worte, Begriffe aus.

related: dresden.de

Verwandte Webseiten und Webseiten mit ähnlichen Inhalten finden.

cache: möglicher Suchtext von gelöschten Inhalten

Viele Webseiten werden in regelmäßigen Abständen aktualisiert. Mit dem Schlüsselwort "cache:" kann man den Zwischenspeicher von Google durchsuchen und bereits gelöschte Inhalte finden.

inanchor: Suchworte in einem Link
Suche nach Texten in einem Link.

inurl: Suchwort

Liefert Internetadressen, die das Suchwort enthalten.

allinurl: Suchausdruck.

Der Operator allinurl: listet nur Webseiten auf, deren Adresse alle eingegebenen Suchwörter enthalten.

intitle: Suchworte

Begrenzt die Suche auf den Titel der Seite.

intext: Suchtext

Durchsucht den Webseiten-Text nach dem eingegebenen Ausdruck.

filetype:pdf bilanz firmenname

Für die gezielte Suche nach einem bestimmten Dateityp ist der filetype-Operator hilfreich.

"berühmte Zitate"

Bei der Suche nach einer genauen Wortgruppe (Zitate, etc.) sind die Worte in Anführungsstriche zusetzen. **Anmerkung:** Für populäre, allgemein bekannte Suchbegriffe können die Anführungszeichen entfallen.

site:de.wikipedia.org Suchwort

Bei der Domain-Suche mit dem site-Operator, wird die Suche auf die Webseiten einer Domain beschränkt.

site:org Medizin

Der Operator arbeitet für die Suche mit der Top Level Domain (z.B. .de .edu .com, .org, .net).

location:Stadt Suchwort

Mit dem location-Operator kann man die Suche auf eine Stadt, Region oder Land eingrenzen.

d:1 börsenbericht

Für die Suche kann der Zeitraum eingegrenzt werden.

h: Stunden, hours; d: Tage, days; w: Wochen, weeks; m: Monate, month, y: Jahre, years

Internet-Browser (about-Befehle) 1/2

Firefox:

about:

Ohne weiteren Zusatz zeigt dieser Befehl Informationen zur verwendeten Version von Firefox, ergänzt um Links zu den Seiten von about:license, about:credits und about:buildconfig.

about:config

Listet die Einstellungsoptionen von Firefox auf. Die Benutzeränderungen werden in gefetteter Schrift dargestellt. Sie können die Werte durch Doppelklick auf einen Eintrag verändern.

about:telemetry

Diese Seite zeigt durch Telemetrie gesammelte Informationen über Performance, Hardware, Benutzung und vom Benutzer gemachte Änderungen an.

about:cache

Zeigt eine Statistik, wie viel Speicher die Cache-Devices (Memory, Disk und Offline) von Firefox beanspruchen. Die Werte sind übrigens in Kilobyte (KiB) angegeben.

about:plugins

Listet übersichtlich alle im Browser installierten Plugins auf. Im Gegensatz zu Google Chrome haben Sie hier keine Möglichkeit, die Einstellungen der Add-ons zu verändern.

about:crashes

Zeigt, welche Informationen über Abstürze an Mozilla gesendet wurden. Sie können neuere Crash-Reports und die dabei übertragenen Informationen auch über Links auf der Mozilla-Webseite direkt ansehen.

about:memory

Informiert detailliert über den Speicherverbrauch des Browsers.

about:support → Firefox bereinigen...

Setzt die Einstellungen von Firefox zurück.

Firefox: about:config komplett zurücksetzen:

Firefox: Abgesicherter Modus

Wurden viele Werte geändert und man kann sich nicht mehr an jeden geänderten Wert erinnern, so kann man about:config auch vollständig zurücksetzen.

1. Schließen Sie als erstes Firefox. Dann halten Sie die [Umschalt]-Taste gedrückt und öffnen Firefox erneut.
2. Nun können Sie auswählen, dass Sie Firefox im abgesicherten Modus starten möchten.
3. Um about:config vollständig zurückzusetzen, aktivieren Sie als nächstes die Checkbox "Alle Benutzereinstellungen zurücksetzen".
4. Abschließend klicken Sie auf "Änderungen ausführen und neustarten".

Firefox-Referer (gespeicherte Seitenaufrufe) abschalten:

Adresszeile: about:config → Suchenfeld: referer → network.http.sendRefererHeader → Wert 2 in 0 (Null) ändern

Adresszeile: javascript.alert(document.referer) oder
Firefox Einstellungen: Datenschutz & Sicherheit → Chronik → niemals anlegen oder Chronik leeren

Firefox Add-ons:

Cookie-Editor → die von Firefox akzeptierten Cookies auslesen und bearbeiten

Cookie Quick Manager → die von Firefox akzeptierten Cookies auslesen und bearbeiten

Chrome:

about: bzw. about:version

Gibt Informationen zur Version von Google Chrome heraus.

about:memory

Liefert Informationen um den verwendeten Speicher, sortiert nach einzelnen Tabs und Plugins.

about:downloads → Listet alle Downloads auf.

about:dns → Zeigt die zwischengespeicherten DNS-Einträge.

about:histograms → Zeigt die Chrome-internen Messungen.

about:bookmarks → Bringt uns zur Lesezeichenverwaltung.

about:settings → Ruft den Standard-Einstellungsdialog auf.

about:cache → Zeigt die im Cache gespeicherten URLs.

about:plugins

Listet die installierten Plug-ins, diese können an dieser Stelle auch deaktiviert werden.

chrome:flags

Design von Chrome zurücksetzen; Default → Normal

about:about

Listet fast alle about-Befehle auf, die von der aktuell verwendete Version von Google Chrome unterstützt wird.

about:sync

Zeigt eine Zusammenfassung zur letzten Chrome-Synchronisation.

chrome://downloads/

Zeigt eine Seite mit allen durchgeführten Downloads an.

chrome://history

Listet den Browser-Verlauf auf, also die zuletzt besuchten Webseiten.

chrome://extensions

Zeigt alle installierten Browser-Erweiterungen inklusive Zugriff auf Deinstallieren, Deaktivieren und Optionen der Plugins.

chrome://plugins/ (bzw. about:plugins)

Liefert alle Plugins auf, die Chrome erkannt hat (etwa Java, Medien-Plugins, Flash, Adobe Reader, interne PDF- und Flash-Plugins etc.).

chrome://bookmarks

Aktiviert den Lesezeichen-Manager von Google Chrome.

chrome://about/gpu/ (bzw. about:gpu)

Grafikkarten-Informationen - wird erst dann relevant, wenn die Grafikkartenbeschleunigung von Chrome aktiviert ist.

chrome://about/sync/ (bzw. about:sync)

Aktueller Status von Chrome Sync (Lesezeichen, Autofill, Einstellungen etc..).

chrome://print/[derzeit unbekannte Argumente, etwa URL]

Bietet in Zukunft Zugriff auf die Druckvorschau von Webseiten und Dokumente.

Hinweise für die Fehlerbeseitigung 1/16

Frage: Speicher, Mainboard oder Prozessor defekt?

- ❖ ein Speicherriegel nach dem anderen entfernen
- ❖ Speicherplatz der RAM-Speicherriegel wechseln
- ❖ PINs des Prozessors überprüfen -> verbogene PINs können eine Speicherfehler-Meldung generieren
- ❖ alle Befestigungsschrauben entfernen (defekte Leiterbahnen)

Frage: Woher kommt ein ungewöhnliches Fenster nach einer Standardinstallation des Betriebssystems (Motherboard: Asus)?

- ❖ Meldung: kein DVD-LW, bei einer Workstation die standardmäßig ohne DVD-LW ausgeliefert werden soll.
- ❖ alle Hardware-Geräte wurden vom Betriebssystem erkannt und mit den Standardtreibern versorgt
- ❖ **Lösung:** nach der Installation der Gerätetreiber vom Motherboard-Hersteller ist das Fenster endgültig verschwunden

Frage: Warum funktioniert ein Kleindrucker für Unterwegs (Notebook) von Brother nicht oder nicht wie erwartet?

- ❖ Der Kleindrucker hat nach der Erstinbetriebnahme wie erwartet funktioniert.
 - ❖ Der Kleindrucker wurde relativ selten im Außendienst benutzt, so dass der Fehler erst nach mehr als einem Jahr bemerkt wurde. Möglicherweise wurden im Außendienst einige Drucker dem Notebook temporär hinzugefügt.
 - ❖ **Lösung:** Alle nicht mehr benötigte Druckertreiber (Inkompatibilität mit Druckertreiber anderer Hersteller) sind zu entfernen.
[W] + [I] -> Geräte -> Drucker und Scanner -> [...]
- Hinweis:** virtuelle Drucker bitte nicht entfernen (z.B. PDF-Drucker, drucken in eine Datei)

Frage: Was kann man gegen deutlich störende Lüftergeräusche tun?

- ❖ Eigentlich hilft nur ein Austausch des Lüfters. Lüfter mit Pulsweitenmodulations-Steuerung (PWM) sind deutlich leiser, als Lüfter die mittels variabler Spannung den Lüfter steuern. Zusätzlich kann man die Lüftersteuerung im BIOS beeinflussen (Einstellung: Silent)
- Beispiel:** ARCTIC - Alpine 64 GT (PWM-Steuerung)

Frage: Warum funktioniert der Windows 10 – Startbutton für den Benutzer Gast nicht?

- ❖ Für einen aktivierten Gast-Benutzer verweigert das Betriebssystem standardmäßig die Benutzung des Start-Buttons (gilt auch für die Tastatur [W]).
 - ❖ Die Aktivierung des vorinstallierten Benutzer Gast, sollte bevorzugt über Kommandozeile erfolgen. Ein evtl. vorhandenes Passwort wird durch den 2. Befehl gelöscht.
- ```
net user Gast active:yes
net user Gast ""
```

## Frage: Warum kann ein einzelner Rechner in einem WLAN den WLAN-Netzwerkdrucker nicht erreichen?

- ❖ **Hinweis:** Der Rechner hat einen funktionierenden Zugang zum Internet. Alle anderen Rechner im WLAN können problemlos drucken.
- ❖ Im Haus existieren mehrere Netze und WLAN-Netze - versorgt über mehrere Access Points (AP).
- ❖ **Lösung:** Der Rechner wurde fälschlicherweise mit einem anderen WLAN-Netz verbunden (Eintrag eines anderen Access Point). Der Name des zuständigen Access Point ist einzutragen.

# Hinweise für die Fehlerbeseitigung 2/16

## Laufwerksbuchstaben in Windows ändern

Die Erkennungsbuchstaben der verschiedenen Laufwerke (USB-Sticks, externe Laufwerke, ...) lassen sich in der

**Datenträgerverwaltung** (Disk Management, Administratorrechte erforderlich) ändern.

Manche Programme können **Probleme** mit einer Änderung des Laufwerksbuchstaben bekommen. Diese Probleme können in der Regel in den Einstellungen der jeweiligen Programme oder über eine Neuinstallation der betroffenen Programme gelöst werden.

## Kurzanleitung

1. Datenträgerverwaltung durch die Tastenkombination **[Windows] + [R]** und anschließender Eingabe von **diskmgmt.msc** öffnen (Administratorrechte erforderlich, Alternativ: [W] + [X] ... ExpertModus).
2. Auswahl des Laufwerkes durch einen Rechtsklick mit der Maus und die Auswahl der Option »**Laufwerksbuchstaben und -Pfade ändern...**«.
3. Auf »**Ändern**« klicken und einen **neuen Laufwerksbuchstaben** vergeben. Bestätigung mit »**OK**« und den Warndialog mit »**Ja**« beantworten.

Damit wurde der Laufwerksbuchstabe des gewählten Laufwerkes erfolgreich geändert.

**Hinweis:** Der Laufwerksbuchstabe X sollte nicht verwendet werden, da dieser Laufwerksbuchstabe für Windows PE reserviert ist. Windows Preinstallation Environment (Windows PE) ist ein minimiertes Windows-Betriebssystem das von einer CD/DVD, einem USB-Stick oder von einer Festplatte an jedem beliebigen Computer gestartet werden kann.

## Frage: Keinen Zugriff auf USB-Stick oder SD-Karte, was kann ich tun?

USB-Stick oder die SD-Karte sind am Rechner angeschlossen, aber sie werden nicht erkannt oder sie werden erkannt, aber es lässt sich nicht auf das entsprechende Laufwerk zugreifen.

- ❖ Teilweise können die Dateien auf den Speichermedien schlicht nicht erkannt werden, da ein äußerer Defekt oder im Fall von externen Festplatten ein Defekt der Steckkontakte oder des Verbindungskabeln vorliegt.

**Lösung:** Steckkontakte und Verbindungskabel überprüfen.

- ❖ **Hinweis:** SD-Karten haben möglicherweise auch einen eingebauten Schreibschutz, durch den die Lesbarkeit der Daten verhindert wird. Somit sollte bei auftretenden Problemen zunächst getestet werden, ob die Schwierigkeiten nach Umlegen des Schalters zur Entfernung des Schreibschutzes weiterhin bestehen.
- ❖ Werden USB-Laufwerke an verschiedene Rechner benutzt, so kann es vorkommen, das Windows 10 den aktuellen Laufwerksbuchstaben ändert. Ist dieser Laufwerksbuchstabe an einen anderen Rechner bereits vergeben, kommt es zu einem Konflikt. Das USB-Laufwerk (USB-Stick, externes Laufwerk) wird zwar vom Betriebssystem erkannt, aber es werden keine Dateien angezeigt (Zugriffsverweigerung).  
**Lösung:** Änderung des Laufwerksbuchstaben, mithilfe der Datenträgerverwaltung. In Zukunft, sollten die USB-Laufwerke aus dem Verzeichnisbaum, Ordnerstruktur sauber ausgegangen werden (siehe: Taskleiste – unten rechts).



# Hinweise für die Fehlerbeseitigung 3/16

## Laufwerksbuchstaben von Laufwerken ändern

### 1. Schritt:

Zuerst müssen Sie die Datenträgerverwaltung öffnen. Drücken Sie dazu die Tasten **[Windows] + [R]**. Am unteren linken Bildschirmrand sollte ein Fenster mit dem Titel "**Ausführen**" auftauchen. Geben Sie hier **diskmgmt.msc** (Disk Management oder Datenträgerverwaltung) ein und klicken Sie auf »**OK**«.

### 2. Schritt:

Rechtsklicken Sie nun auf das **Laufwerk**, dessen Laufwerksbuchstaben Sie ändern möchten. Im Kontextmenü wählen Sie nun den Eintrag »**Laufwerksbuchstaben und -Pfade ändern...**«.

### 3. Schritt:

In dem auftauchenden Fenster klicken Sie auf »**Ändern...**«, um zum nächsten Fenster zu gelangen.

### 4. Schritt:

In diesem Fenster können Sie den **neuen Laufwerksbuchstaben** festlegen. In der Liste stehen Ihnen alle Buchstaben von A bis Z zur Verfügung. Achten Sie allerdings darauf, dass der Laufwerksbuchstabe **noch nicht vergeben** ist. Klicken Sie auf »**OK**«, wenn Sie Ihre Auswahl getroffen haben.

### 5. Schritt:

Windows weist noch einmal auf die möglichen Probleme hin, die bei einer Änderung auftreten können. Wenn Sie den Buchstaben des Laufwerks ändern möchten, bestätigen Sie mit »**Ja**«.

### 6. Schritt:

Der Laufwerksbuchstabe sollte jetzt dem von Ihnen ausgewählten Buchstaben entsprechen. Sie können sich im **Hauptmenü der Datenträgerverwaltung** noch einmal davon überzeugen. Danach können Sie alle Fenster wieder schließen und die Änderung war erfolgreich.

**Hinweis:** Alternativ zur Eingabe von **diskmgmt.msc** (Datenträgerverwaltung) in der Ausführungszeile, kann man auch **compmgmt.msc** (Computerverwaltung) eingeben, um zu der Datenträgerverwaltung zu gelangen.

### Frage: Wie kann man Laufwerksbuchstaben mit Diskpart zuweisen?

Um einen Laufwerksbuchstaben zuzuweisen, zu ändern oder zu entfernen, kann man auf der Windows-Oberfläche das grafische Dienstprogramm **Datenträgerverwaltung** (diskmgmt.msc oder compmgmt.msc) oder mittels der Befehlszeile (cmd) das Kommandozeilenprogramm **Diskpart** verwenden.

### Laufwerksbuchstaben mit Diskpart zuweisen:

**Schritt 1.** Zur Verwendung der Befehlszeile, muss man erst die Befehlszeile (cmd) öffnen. Auf **Start** klicken, **cmd** in das Suchfeld eingeben, einen Rechtsklick auf das Programm ausführen und anschließend die Option **Als Administrator ausführen** auswählen.

Alternativ kann man die Tastenkombination **[W] + [R]** drücken, **cmd** eingeben, zur Bestätigung **[Strg] + [Shift]** und die Eingabetaste drücken (cmd wird mit Administratorrechten geöffnet) und anschließend **diskpart** eingeben, um das Dienstprogramm zu starten.

# Hinweise für die Fehlerbeseitigung 4/16

**Schritt 2.** Mit der Eingabe von **list volume**, werden alle von Windows 10 erkannten Laufwerke aufgelistet. An der Nummer des Laufwerks (USB-Stick, SD-Karte, ...) und an der Größe des Speicherplatzes kann man das entsprechende Laufwerk erkennen, dessen Laufwerksbuchstaben man zuweisen, ändern oder entfernen möchte.

**Schritt 3.** Das entsprechende Laufwerk mit **select volume n** (n ... Nummer des Laufwerkes) auswählen und mit der Eingabetaste die Auswahl bestätigen. An dieser Stelle kann man dem Laufwerk einen neuen Laufwerksbuchstaben zuweisen, ihn ändern oder entfernen.

**Schritt 4.** Mit dem Befehl **assign letter=x** (x ... neuer Laufwerksbuchstabe) wird dem Laufwerk ein neuer Laufwerksbuchstabe zugewiesen. Der Befehl wird mit einer entsprechenden Meldung bestätigt.

Mit dem Befehl **remove letter=g** (g ... aktueller Laufwerksbuchstabe) entfernt das Dienstprogramm Diskpart den Laufwerksbuchstaben.

Damit wurde der Laufwerksbuchstabe zugeordnet, geändert oder entfernt. Mit der Eingabe von **list volume**, können die Änderungen überprüft werden.

## Kurzanleitung:

**[W] + [R] -> cmd -> diskpart**

**select volume n** (n ... Nummer des Laufwerkes)

**assign letter=x** (x ... neuer Laufwerksbuchstabe) oder  
**remove letter=g** (g ... aktueller Laufwerksbuchstabe)

**list volume**

**Hinweis:** Der Laufwerksbuchstabe X sollte nicht verwendet werden, da dieser Laufwerksbuchstabe für Windows PE reserviert ist. Windows Preinstallation Environment (Windows PE) ist ein minimiertes Windows-Betriebssystem das von einer CD/DVD, einem USB-Stick oder von einer Festplatte an jedem beliebigen Computer gestartet werden kann.

## Passwort-Eingabe für CMD (Kommandozeile) aktivieren

Bei einigen Windows 10 Versionen, kann es vorkommen das die CMD mit Administratorrechten ohne Passwordeingabe aufgerufen werden kann. Dies kann man über die Registry ändern.

**[W] + [R] → regedit.exe**

**HKEY\_LOCAL\_MACHINE**

→ **SOFTWARE**

→ **Microsoft**

→ **Windows**

→ **CurrentVersion**

→ **Policies**

→ **System** → rechte Seite – Schlüssel →

→ **ConcertPromptBehaviorAdmin**

→ **Daten** → Wert 5 in 1 ändern

Von nun an, kann die CMD mit Administratorrechten nur mit Passwordeingabe aufgerufen werden.

## Hinweise für die Fehlerbeseitigung 5/16

### Frage: Wie können die Lautsprecher deaktiviert werden und der Kopfhörer-Ausgang gleichzeitig aktiviert bleiben?

- ❖ Um Personen im Raum nicht zu stören, sollen die Lautsprecher deaktiviert werden und der Audio-Ausgang für die Kopfhörer aktiviert bleiben.
- ❖ **Lösung 1:** Tastenkombination [W] + [R] → control → Sound → Audiogerät auswählen (Gerätename des Lautsprechers) → Eigenschaften → Geräteverwendung → deaktivieren oder aktivieren
- ❖ **Lösung 2:** Tastenkombination [W] + [I] (Einstellungen) → System → Sound → Audiogeräte verwalten → Audiogerät auswählen (Gerätename des Lautsprechers) → deaktivieren oder aktivieren
- ❖ **Lösung 3:** Das Symbol für den Lautsprecher in der Taskleiste (unten rechts) mit der Maus auswählen und anschließend den nach oben gerichteten Pfeil anklicken. In der angezeigten Liste, ist die Zeile mit dem Eintrag »Lautsprecher ... « auszuwählen. Um dies wieder rückgängig zu machen, ist die Zeile mit dem Eintrag für die Soundkarte auszuwählen.

### Frage: Wie kann ein scheinbar nicht funktionierender Lautsprecher-Ausgang aktiviert werden?

- ❖ Mitunter kann es nach einer Neu- oder Erstinstallation des Betriebssystems vorkommen, dass der Gerätename der Soundkarte nicht richtig ausgewählt oder er einfach nicht aktiviert wurde.
- ❖ Es besteht auch die Möglichkeit, dass ein anderer Benutzer des Rechners den Gerätenamen für das Audiogerät unabsichtlich geändert hat.
- ❖ **Lösung:** Das Symbol für den Lautsprecher in der Taskleiste (unten rechts) mit der Maus auswählen und anschließend den nach oben gerichteten Pfeil anklicken. In der angezeigten Liste befinden sich alle vom Windows-Betriebssystem erkannten Audiogeräte. Diese Audiogeräte sind nacheinander auszuprobieren, bis sich der gewünschte Erfolg einstellt.

### Frage: Warum funktioniert die Soundausgabe nicht?

- ❖ Mitunter hat ein Witzbold, im Geräte-Manager den Treiber für die Soundkarte nur deaktiviert.
- ❖ **Lösung 1:** [W] + [R] → control → Gerätemanager → Gerät auswählen → rechte Maustaste → Treiber aktivieren (Administratorrechte erforderlich)
- ❖ **Lösung 2:** [W] + [I] → Einstellungen → im Suchfeld »Geräte-Manager« eingeben → Gerät auswählen → rechte Maustaste → Treiber aktivieren (Administratorrechte erforderlich)

### Frage: Warum sind bestimmte Webseiten nicht erreichbar?

- ❖ Mitunter hat ein Witzbold, in der hosts-Datei (**Verzeichnis:** Windows\System32/drivers/etc) ein paar Eintragungen getätigt, die Webseiten auf **nicht** vorhandene IP-Adressen umleitet.
- ❖ **Lösung:** Die Eintragungen in der hosts-Datei sind zu entfernen (Administratorrechte erforderlich).

**Hinweise:** Die einfachsten Fehler oder fehlerbehafteten Einstellungen zu finden, sind häufig die zeitraubendsten Tätigkeiten.

## Hinweise für die Fehlerbeseitigung 6/16

**Frage: Warum können auf ein USB-Stick keine Dateien gespeichert oder geändert werden und weiterhin ist auch eine Formatierung des USB-Stick nicht möglich?**

- ❖ Der USB-Stick wurde möglicherweise mit einem Schreibschutz versehen.
- ❖ **Lösung:** Schreibschutz über die Registry aufheben.
- ❖ [W] + [R] → regedit.exe
- ❖ HKEY\_LOCAL\_MACHINE
  - SYSTEM
  - CurrentControlSet
  - Control
  - (**Hinweis:** Einträge **SafeBoot** und **SecurityProviders** kontrollieren)
  - StorageDevicePolicies → Name: WriteProtect → Wert 1 in 0 (Null) ändern
- ❖ Zum Schluss ist noch ein Neustart des Rechners erforderlich.

**Frage: Wie kann man einen durch Ransomware gesperrten Rechner (nicht verschlüsselten Rechner) wieder entsperren, zugänglich machen?**

- ❖ Windows-Installations-CD einlegen und den Rechner neu starten
- ❖ um die Wiederherstellungskonsole zu öffnen, ist bei Aufforderung der Buchstaben »R« einzugeben
- ❖ bei Aufforderung ist das Administrator-Kennwort einzugeben
- ❖ Wechsel zum Laufwerk, auf dem Windows installiert ist; in der Regel ist dies das Laufwerk C:
- ❖ an der Eingabeaufforderung den Befehl »fixmbr  
[Laufwerksbuchstabe]« eingeben  
**fixmbr c:**  
Nach erfolgreicher Ausführung des Befehls ist der Schalter »Exit« auszuwählen.
- ❖ Anschließend ist noch ein Neustart des Rechners von der Festplatte erforderlich.

- ❖ Zum Abschluss ist noch ein vollständigen Systemscan mit einer Sicherheitssoftware (Antivirus-Software) erforderlich, um sämtliche Komponenten der Malware zu entfernen.

**Frage: Wie kann man eine nicht entfernbare Linie in einer DOC-Datei am einfachsten löschen?**

- ❖ Auf dem Desktop über das Kontextmenü (rechte Maustaste) eine einfache neue Textdatei (.txt) erstellen und öffnen.
- ❖ In der Windows DOC-Datei sind 2 bis 3 Zeilen vor und nach der Linie zu markieren und auszuschneiden. Dieser Text ist in die geöffnete Text-Datei einzufügen.
- ❖ Die einfache Textdatei kann mit der speziellen DOC-Formatierung nichts anfangen und filtert diese. Anschließend kann man diesen bereinigten Text wieder in die DOC-Datei einfügen.
- ❖ Es gibt zwar noch weitere Möglichkeiten diese nicht entfernbare Linie zu löschen, aber die Vorgehensweise kann sich von Version zu Version ändern.

**Frage: Wie kann man eine beschädigte Datei und nicht löschbare Datei entfernen?**

- ❖ In den meisten Fällen reicht es aus sich abzumelden und wieder neu anzumelden.
- ❖ Falls dies nicht zum gewünschten Ergebnis führt, bleibt nur der bewährte Neustart oder der Neustart im abgesicherten Modus.

# Hinweise für die Fehlerbeseitigung 7/16

## Frage: Wie macht man versteckte Devices, Geräte wieder sichtbar?

- ❖ Mit dem Aufruf der Einstellungen für die Audiogeräte aus der Taskleiste heraus, kann es vorkommen, dass die Audiogeräte auf der entsprechenden Seite nicht angezeigt werden.
- ❖ Dies kann vorkommen, wenn man ein Headset (Kopfhörer, Mikrofon) benutzt hat und das Betriebssystem die externe Hardware automatisch erkannt hat.
- ❖ **Lösung:** Die Einstellungsseite aufrufen (Taskleiste → Lautsprechersymbol → Kontextmenü → Sounds) und zur Registerkarte »Playback« wechseln, auf der für gewöhnlich die Audiogeräte angezeigt werden. Den Mauszeiger über die leere Registerkarte bewegen und das Kontextmenü über die rechte Maustaste aufrufen. Nach der Auswahl des entsprechenden Eintrages, sollten die Audiogeräte wieder sichtbar sein.

## Windows 10 - Schwerwiegender Fehler: Das Menü Start und Cortana funktionieren nicht.

- ❖ **Problem:** Wenn man auf den Button »Jetzt abmelden« klickt, um den Rechner neu zu starten, taucht der Fehler beim nächsten Start wieder auf.
  - ❖ **Lösung:** Das Betriebssystem muss vollständig heruntergefahren werden und anschließend neu gestartet werden.
1. Sperrbildschirm aufrufen: Tastenkombination [Strg] + [Alt] + [Entf]
  2. Power-Button anklicken -> Wahlmöglichkeiten: Energie sparen, Herunterfahren, Neu Starten
  3. Shift-Taste gedrückt halten und auf »Herunterfahren« klicken
  4. Rechner fährt komplett herunter -> Rechner wieder hochfahren -> Fehlermeldung sollte jetzt nicht mehr auftauchen

Der Trick bei dieser Methode besteht darin, dass Windows 10 damit vollständig herunterfährt. Im Normalfall verwendet Windows 10 stattdessen den sogenannten Hybrid-Modus: Dabei werden Systeminformationen in der Datei **hiberfil.sys** gespeichert, so dass die Informationen in dieser Datei beim nächsten Systemstart direkt zur Verfügung stehen. Das ist wesentlich schneller und führt aber dazu, dass ein etwaiger Fehler im Systemcache verbleibt und beim nächsten Start wieder reproduziert wird.

## Frage: Wie kann man Windows 10 vollständig herunterfahren?

- ❖ Einige Notebooks fahren unter Windows 10 nicht vollständig herunter, sondern begeben sich in eine Art Ruhezustand. Microsoft wollte so schnellere Systemstarts einführen. Allerdings kann es dadurch vorkommen, dass Fehler bei einem Neustart nicht beseitigt werden und immer wieder erneut auftreten.
1. Startmenü öffnen
  2. auf den Ein/Aus-Button klicken
  3. Shift-Taste gedrückt halten und auf »Herunterfahren« klicken

## Frage: Wie kann man Windows 10 immer vollständig herunterfahren?

- ❖ **Lösung:** Der verantwortlichen Schnellstart von Windows 10 muss deaktiviert werden.
1. Tastenkombination [Windows] + [R]
  2. »cmd« eingeben -> [Strg] + [Shift] gedrückt halten und mit der Enter-Taste bestätigen
  3. Es öffnet sich eine Eingabeaufforderung mit Administratorrechten.
  4. Befehl eingeben: `powercfg.exe -h off`
  5. Windows startet jetzt neu

Den Schnellstart kann man mit der erneuten Eingabe des Befehls »`powercfg.exe -h on`« wieder aktivieren.

**Hinweis:** Beim normalen »Herunterfahren« fährt Windows 10 nicht vollständig herunter, sondern in eine Art von Ruhezustand, was irgendwann zu Windows-Fehlern führen kann - dies gilt insbesondere für Notebooks.



# Hinweise für die Fehlerbeseitigung 8/16

## Frage: Wie kann Windows 10 mit Verknüpfungen schneller herunterfahren?

Wenn man Windows 10 schneller herunterfahren möchte, so kann man folgende Verknüpfungen anlegen:

1. Mit der rechten Maustaste auf einen freien Bereich des Desktops klicken.
2. Neu -> Verknüpfung und folgende Zielpfade eingeben
- 2.1 **Vollständig herunterfahren:** %windir%\system32\shutdown.exe /s /t 0
- 2.2 **Neustarten:** %windir%\system32\shutdown.exe /r /t 0
- 2.3 **Im Hybridmodus herunterfahren:** %windir%\system32\shutdown.exe /s /hybrid /t 0
- 2.4 **In den Energiesparmodus wechseln:** %windir%\System32\rundll32.exe powrprof.dll,SetSuspendState Sleep

Der Verknüpfung noch einen Namen geben: »Windows komplett herunterfahren«. Um herunterzufahren, genügt jetzt ein Doppelklick auf die Verknüpfung.

**Hinweis:** Ein/Aus-Button - drei Optionen:

1. **Herunterfahren:** Windows fährt im sogenannten Hybridmodus herunter, dabei werden alle wichtigen Systeminformationen standardmäßig in der Datei **hiberfil.sys** gespeichert und stehen beim nächsten Systemstart direkt zur Verfügung. Dadurch startet Windows 10 wesentlich schneller als die Vorgängerversionen.
2. **Neu starten:** Mit dieser Option fährt Windows 10 komplett herunter und wird anschließend wieder hochgefahren. Die gespeicherten Systeminformationen aus der Datei hiberfil.sys werden dabei in der Regel nicht eingelesen.
3. **Energie sparen:** Windows 10 wechselt in den Energiesparmodus. Alle offenen Dateien und Programme werden im RAM gespeichert. Wird der Rechner in diesem Modus ausgeschaltet, gehen alle im RAM zwischengespeicherten Daten verloren. Um den Energiesparmodus zu verlassen, muss man nur eine Taste drücken.

## Frage: Wie kann man in Windows 10 die WLAN-Netze zurücksetzen?

❖ Bei WLAN-Problemen kann man versuchen die Verbindung zum aktuellen WLAN-Netz zu löschen und wieder neu einzurichten.

1. Windows-Einstellungen aufrufen: [Windows] + [I]
2. Kategorie »Netzwerk und Internet« -> WLAN
3. »Bekannte Netzwerke verwalten« -> aktuelles WLAN-Netz auswählen
4. Mit einem Klick auf den Button »Nicht speichern« wird das ausgewählte WLAN gelöscht.
5. Anschließend kann man versuchen, sich mit dem WLAN erneut zu verbinden.

## Problem: Die Taskleiste geht über den Bildschirmrand hinaus.

- ❖ Bei einigen Nutzern geht die Taskleiste nach einem Neustart über den Bildschirmrand hinaus. Dieses Problem entsteht durch einen versehentlichen Wechsel in den Tablet-Modus von Windows 10.
- ❖ **Lösung:** Tastenkombination: [Windows] + [A] und anschließend auf »Tabletmodus« unten rechts klicken, um diesen zu deaktivieren. Sollte die Schaltfläche nicht blau sein, klickt man einmal auf diese um den Tablet-Modus zu aktivieren. Ist das geschehen, deaktiviert man diesen wieder. Die Taskleiste sollte nun wieder normal zu sehen sein.

## Problem: Startmenü funktioniert nicht richtig

- ❖ Arbeitet das Startmenü nicht wie gewohnt, ist der Zugriff auf viele Funktionen erschwert oder gar nicht mehr möglich. In den meisten Fällen lassen sich Probleme mit dem Windows 10-Startmenü aber schnell wieder beheben.
- ❖ **Lösung:** Probleme mit dem Windows-Startmenü behebt man unter Umständen bereits mit einem Neustart des PCs oder des Windows-Explorers.

# Hinweise für die Fehlerbeseitigung 9/16

## Frage: Wie kann man Windows 10 im abgesicherten Modus starten?

- ❖ Falls das System nicht mehr vernünftig hochfährt, sollte man Windows 10 im abgesicherten Modus starten und sich dort auf Fehlersuche begeben.
- ❖ Die einfachste Methode ist der Aufruf des Bootmenüs über die **Tastenkombination [Strg] + [F8]** während des Bootvorgangs. Im Boot-Menü findet man unter anderem den abgesicherten Modus.
- ❖ Doch leider funktioniert diese Methode nicht an jedem Rechner. Bootet der Rechner von einer SSD-Festplatte, fährt er so schnell hoch, dass man den richtigen Zeitpunkt für die Tastenkombination kaum treffen kann.
- ❖ **Lösung:** Mit »msconfig« den abgesicherten Modus aus Windows 10 heraus starten. Befinden man sich bereits in Windows 10, hilft die Systemkonfiguration beim Neustart im abgesicherten Modus.

1. Tastenkombination [Windows] + [R] und im Ausführen-Feld »msconfig« eingeben.
2. Es öffnet sich das Fenster »Systemkonfiguration«.
3. Reiter »Start« anklicken -> bei »Startoptionen« jeweils ein Häkchen vor »Abgesicherter Start« und »Netzwerk« eintragen

**Hinweis:** Beim nächsten Neustart fährt Windows 10 im abgesicherten Modus hoch. Doch Vorsicht: Auch bei weiteren Neustarts wird der abgesicherte Modus eingeleitet, da die Häkchen in der Systemkonfiguration gesetzt bleiben. Möchte man Windows 10 wieder normal starten, sind die Häkchen wieder zu entfernen.

## Problem: Windows 10: Abgesicherten Modus per Eingabeaufforderung starten

1. Tastenkombination [Windows] und [X]
2. Option "Eingabeaufforderung (Administrator)" und die anschließende Sicherheits-Abfrage bestätigen
3. Geben Sie anschließend den Befehl "bcdedit /set {current} safeboot network" ein, wird Windows im abgesicherten Modus gestartet.

## Problem: Windows 10: Verknüpfung zum abgesicherten Modus erstellen

- ❖ Müssen Sie sich in Zukunft häufiger in den abgesicherten Modus begeben, kann eine Verknüpfungen viele Klicks ersparen.
1. Klicken Sie mit der rechten Maustaste auf einen freien Bereich auf dem Desktop und wählen Sie unter "Neu" eine "Verknüpfung" aus.
  2. Geben Sie als Pfad "shutdown.exe /r /o /f /t 00" ohne die Anführungszeichen ein und klicken Sie auf "Weiter" und "Fertig stellen".
  3. Klicken Sie nun auf die Datei "shutdown.exe", wird Windows im abgesicherten Modus gestartet.

## Problem: Windows 10: letzte Chance zum abgesicherten Modus

- ❖ Können Sie gar nicht mehr auf Ihren Rechner zugreifen, gibt es auch in dieser Not noch eine Lösung für das Problem.
- ❖ **Lösung 1:** Haben Sie eine DVD mit Windows 10 zur Hand, legen Sie diese ein. Wird die DVD geladen, klicken Sie im Installations-Bildschirm unten rechts auf »Computerreparatur«.
- ❖ **Lösung 2:** Startet Windows so gut wie gar nicht mehr, gibt es noch eine letzte, aggressivere Methode: Starten Sie Ihren Rechner und halten Sie den Power-Button sofort wieder gedrückt, bis der Computer wieder ausgeht. Wiederholen Sie den Vorgang viermal. Damit gelangen Sie ins UEFI.

Wählen Sie als erstes die "Problembehandlung". Unter den "Erweiterten Optionen" finden Sie nun die "Windows-Starteinstellungen". Klicken Sie dort auf den Button "Neu starten". Warten Sie einen Moment, bis das System geladen wurde. Drücken Sie nun auf die Taste [4], wird Windows im abgesicherten Modus gestartet.

# Hinweise für die Fehlerbeseitigung 10/16

## Problem: Windows 10: Abgesicherten Modus per Start-Menü oder Sperrbildschirm öffnen

- ❖ Bei älteren Windows-Versionen konnte man den abgesicherten Modus bequem per Tastenkombination beim Start von Windows aufrufen. Das funktioniert bei Windows 10 immer noch, allerdings ist das Zeitfenster bei einigen Rechnern so klein, dass der Vorgang meist fehlschlägt. Je nach PC muss man beim Start die Tasten-Kombination [Umschalt] und [F8] drücken, oder eine andere Taste wie [Esc], [Tab], [Alt], [Entf], [F1], [F2], [F8] bis [F12] drücken.

Lässt sich Windows 10 noch ordnungsgemäß starten, geht es wie folgt meist leichter:

1. Klicken Sie unten links auf das Windows-Symbol, finden Sie ganz unten den Power-Button. Diesen Power-Button sehen Sie ebenfalls unten rechts im Sperrbildschirm, wenn Sie Windows starten.
2. Klicken Sie auf den Power-Button, erscheint unter anderem die Option "Neu starten".
3. Halten Sie die [Umschalt]-Taste gedrückt und klicken Sie mit der Maus auf "Neu starten". Windows startet jetzt neu und lädt das UEFI.
4. Alternativ können Sie das UEFI auch über die Einstellungen von Windows 10 öffnen. Klicken Sie im Start-Menü einfach auf das Zahnrad-Symbol (Einstellungen).
5. In der Kategorie "Update und Sicherheit" klicken Sie in der "Wiederherstellung" bei "Erweiterter Start" auf den Button "Jetzt neu starten". Ob Sie anschließend im UEFI angekommen sind, erkennen Sie an dem hellblauen Hintergrund.
6. Wählen Sie als erstes die "Problembehandlung".
7. Unter den "Erweiterten Optionen" finden Sie nun die "Windows-Starteinstellungen". Klicken Sie dort auf den Button "Neu starten".
8. Warten Sie einen Moment, bis das System geladen wurde.
9. Drücken Sie nun auf die Taste [4], wird Windows im abgesicherten Modus gestartet..

## Problem: Microsoft-Apps lassen sich nicht deinstallieren

- ❖ Mitunter lassen sich einige Apps nicht auf dem üblichen Weg deinstallieren. In diesen Fällen, kann man auf die Windows PowerShell-Konsole zurückgreifen, um die unerwünschten Programme zu entfernen.

- ❖ **Befehlssyntax:** Get-AppxPackage \*PROGRAMMNAME\* | Remove-AppxPackage

**Hinweis:** Die Sternchen vor und nach dem Namen des Programmes müssen beibehalten werden.

Einige Programm-Beispiele für die Windows PowerShell:

**3D Builder** → Get-AppxPackage \*3d\* | Remove-AppxPackage

**Fotos** → Get-AppxPackage \*photo\* | Remove-AppxPackage

**Kamera** → Get-AppxPackage \*camera\* | Remove-AppxPackage

**Kontakte** → Get-AppxPackage \*people\* | Remove-AppxPackage

**Mail und Kalender** → Get-AppxPackage \*communi\* | Remove-AppxPackage

**Microsoft Solitaire Collection** → Get-AppxPackage \*solit\* | Remove-AppxPackage

**Nachrichten** → Get-AppxPackage \*bing\* | Remove-AppxPackage

**Phone Companion** → Get-AppxPackage \*phone\* | Remove-AppxPackage

**Sprachrekorder** → Get-AppxPackage \*soundrec\* | Remove-AppxPackage

**XBOX** → Get-AppxPackage \*xbox\* | Remove-AppxPackage

# Hinweise für die Fehlerbeseitigung 11/16

## Frage: Was bedeutet der Fehlercode "8007003"?

- ❖ Sollte bei der Suche nach Updates der Fehlercode "8007003" angezeigt werden, müssen die temporären Dateien gelöscht und der Update-Prozess erneut gestartet werden. Hierfür müssen folgende Schritte als Administrator ausgeführt werden.

### 1. Windows Update-Dienst beenden

Zunächst muss der Windows Update-Dienst beendet werden, da sonst die temporären Dateien nicht gelöscht werden können.

- Systemsteuerung »Einstellungen« öffnen: [Windows] + [I]
- Im Suchfeld »Verwaltung« eingeben und diese öffnen
- Im sich öffnenden Dialog auf »Dienste« doppelklicken
- Dort nach »Windows Update« suchen mittels »Rechtsklick« im Kontextmenü die Option »Beenden« aufrufen

### 2. Temporäre Dateien löschen

Jetzt können die temporären Dateien von der Festplatte gelöscht werden. Das sind alle Dateien im Ordner

»C:\Windows\SoftwareDistribution\DataStore« und »C:\Windows\SoftwareDistribution\Download«.

Man kann das über die Kommandozeile machen oder alternativ kann man diesen Schritt auch über den »Explorer« ausführen.

- Über »Start« -> »Computer« den »Explorer« starten.
- Dort das Laufwerk "C:" und dort den Ordner »Windows« und den Unterordner »SoftwareDistribution« öffnen.

- Jetzt zunächst den Ordner »DataStore« öffnen und alle darin befindlichen Dateien löschen und anschließend den gleichen Schritt für den Ordner »Download« wiederholen.

### 3. Windows Update-Dienst wieder starten

Jetzt kann der Windows Update-Dienst wieder gestartet und danach der Update-Prozess von vorne begonnen werden.

- »Verwaltung« wie oben beschrieben öffnen und erneut nach dem Dienst »Windows Update« suchen und mit einem Rechtsklick auf den Dienst das Kontextmenü aufrufen und »Starten« anklicken.

# Hinweise für die Fehlerbeseitigung 12/16

## Problem: Windows 10 ohne Microsoft-Konto nutzen

### ❖ Einrichtung eines lokalen Kontos

Wenn man Windows 10 nutzt, wird meist automatisch ein Microsoft-Konto erstellt, bei dem man sich immer wieder anmelden muss.

### ❖ Account zum lokalen Benutzer umzuwandeln

Windows 10 ohne Microsoft-Konto nutzen, geht das? Mit Windows 10 rückt der Hersteller Microsoft die hauseigenen Nutzerkonten weiter in den Mittelpunkt.

Bereits bei der Anmeldung und beim Starten des Rechners soll man sich mit einer Microsoft-ID anmelden und den PC entsprechend mit dieser verknüpfen.

Zwar hat das auch Vorteile - automatisches einloggen bei Microsoft-Diensten wie OneDrive oder Skype. Doch viele Nutzer bevorzugen die lokale Verwaltung ihres Benutzerkontos.

Mit einigen Handgriffen kann man Windows 10 ohne Microsoft-Konto nutzen und sich wieder mit einem lokal gespeicherten Benutzerkonto anmelden.

### ❖ Ein neues lokales Benutzerkonto erstellen

- Systemsteuerung »Einstellungen« öffnen: [Windows] + [I] und in den Bereich »Konten« wechseln

- In der linken Navigationsleiste auf »Familie & weitere Kontakte« bzw. »Email & Konten« klicken, sowie anschließend auf »diesem PC eine andere Person hinzufügen« bzw. »Geschäfts- oder Schulkonto hinzufügen«.

- Da man den Nutzer ohne Microsoft-Konto anlegen will, wählt man im aufkommenden Dialogfenster »Ich kenne die Anmeldedaten dieser Person nicht« und im nächsten Schritt wählt man ohne die Eingabe von Daten - den Punkt »Benutzer ohne Microsoft-Konto hinzufügen«.

- Abschließend gibt man einen Benutzernamen, sowie optional ein Passwort ein. Damit ist die Einrichtung des lokalen Kontos abgeschlossen.

### ❖ Alten Benutzer zum lokalen Konto umwandeln

- Ein bestehendes Microsoft-Konto kann man nachträglich in ein lokales Konto umwandeln. Dafür muss man das Windows-Startmenü aufrufen und über einen Rechtsklick auf den Nutzernamen die Option »Kontoeinstellungen ändern« auswählen.

- Im geöffneten Fenster erscheint nun das aktuelle Benutzerkonto. Im nächsten Schritt, wird mit einem Klick auf den Schriftzug »Stattdessen mit einem lokalen Konto anmelden« und der Eingabe des aktuellen Passwortes fortgefahren.

- Nun kann man einen Benutzernamen sowie ein Passwort für das umgewandelte lokale Konto festlegen. Mit der Bestätigung auf »Abmelden und fertig stellen« wird der Vorgang abgeschlossen.

**Hinweis:** Bei der nächsten Anmeldung kann man nun das neu erstellte lokale Konto auswählen und sich bei Windows 10 anmelden - ohne Microsoft-Konto.



# Hinweise für die Fehlerbeseitigung 13/16

## Problem: Windows 10 - Fehler 0xc00000e9

- ❖ Der Fehler 0xc00000e9 deutet auf ein Problem mit Datenträgern hin. Er kann während des Bootvorganges, der Installation oder dem normalen Arbeiten mit Windows 10 auftauchen und meldet sich normalerweise mit der Fehlermeldung "0xc00000e9: unerwarteter Ein-/Ausgabefehler".
- ❖ Wenn unter Windows die Meldung "0xc00000e9: unexpected i/o error has occurred" oder "0xc00000e9: unerwarteter Ein-/Ausgabefehler" angezeigt wird, dann hat der PC ein Problem mit Schreib- oder Lesezugriffen auf einem Datenspeicher. Datenspeicher sind Festplatten, USB-Sticks, SD-Karten in entsprechenden Lesegeräten, CD/DVD-Laufwerke und andere Geräte auf denen Daten permanent abgelegt werden können.

# Hinweise für die Fehlerbeseitigung 14/16

**Problem:** Windows 10 - Fehlercode 0x80240FFF

- ❖ Der Fehlercode 0x80240FFF wird bei einem fehlgeschlagenen Windows-Update angezeigt.
- ❖ Oft hilft ein einfacher Neustart des Rechners oder das Deaktivieren von Antiviren-Programmen, Firewalls und speziellen Tuning-Tools.
- ❖ Schlägt das Update trotzdem fehl, hilft das Bereinigen der Updates und das Überprüfen der Systemdateien. Beides kann man bequem über die Eingabeaufforderung erledigen. Bereinigung des Updates durch die Eingabe von:

```
net stop wuauclt
```

```
ren C:\Windows\SoftwareDistribution C:\Windows\SoftwareDistribution.OLD
```

```
net start wuauclt
```

- ❖ Danach startet man eine Überprüfung der Systemdateien mit dem Befehl: `sfc /scannow`

## Hinweise für die Fehlerbeseitigung 15/16

**Problem:** Windows 10 - Fehlercodes 0x80070070 - 0x50011,  
0x80070070 - 0x50012 und 0x80070070 – 0x60000

- ❖ Die Fehlercodes 0x80070070 - 0x50011, 0x80070070 - 0x50012 und 0x80070070 - 0x60000 zeigen an, dass der Rechner für die Installation des Updates nicht genügend Speicherplatz bereithält.
- ❖ Tritt einer der genannten Fehler-Codes bei einem Update-Vorgang auf, muss man nur entsprechenden Speicherplatz auf dem System freigeben (integriertes Windows-Programm: »Disk Cleanup«-Tool).
- ❖ Aufruf über die Tastenkombination: [Windows] + [R] -> »cleanmgr« eingeben. Nach einer kurzen Analysezeit wird die Festplatte bereinigt.

## Hinweise für die Fehlerbeseitigung 16/16

**Problem:** Windows 10 - Fehler 8007003 beheben - Update von Windows 10 funktioniert nicht

- ❖ Neben diversen anderen Fehlern, kann es während dem Windows 10 Update zum Fehler "8007003" kommen. Der Fehler kann während oder nach dem Download der Dateien auftreten und ist in der Regel auf beschädigte Dateien zurückzuführen.

# Malware, Angriffe und Infektoren 1/5

## Arten von Malware, Infektoren

IT-Analytiker versuchen den Begriff »Virus« zu vermeiden und bevorzugen Malware, Threat, usw. Der Grund dafür ist, dass ein Virus eine bestimmte Art von Malware ist, die ein bestimmtes Verhalten zeigt: Sie infiziert saubere Dateien. Untereinander beziehen sich Analysten auf einen Virus deshalb mit dem Begriff Infektor.

### Spearfishing

Spearfishing-Angriffe sind **gezielte** Angriffe, Betrugsversuche auf Personen, Unternehmen und Organisationen.

### Phishing

Phishing sind **ungezielte** Angriffe, Betrugsversuche auf Personen, Unternehmen und Organisationen.

### Bootviren, Bootsektorviren

Bootviren oder Bootsektorviren verbreiten sich nicht über Programme, sondern über externe Datenträger. Sie infizieren den Startbereich eines Datenträgers. Beim Booten (Starten) des Rechners von einem infizierten Datenträger oder Festplatte lädt sich der Bootvirus unbemerkt in den Speicher.

### Trojanische Pferde

Der Sage nach belagerte Odysseus mit dem Athener Heer die Stadt Troja. Mit einem Trick schmuggelte er seine griechischen Soldaten im Innern eines als Geschenk getarnten Holzpferdes in die Stadt. Ähnlich die Viren-Trojaner: Die Programme geben vor, bestimmte Funktionen auszuführen (z.B. Entpacken von Programmen, Systemtuning, ...), in Wahrheit wird jedoch (anstelle der versprochenen Funktion oder unbemerkt als "Nebeneffekt") eine Schadensfunktion wie z.B. das Ausspähen und Versenden von Passwörtern ausgeführt.

### Polymorphe Viren

Antivirenprogramme erkennen Viren unter anderem anhand typischer Bytefolgen. Polymorphe Viren verändern ihren eigenen Programmcode bei jeder neuen Infektion, dadurch wird die Erkennung wesentlich erschwert.

### Makro-Viren

Makroviren befallen nicht Programme, sondern Dokumente! Sie verstecken sich in Word- oder Excel-Dokumenten (Endungen DOC bzw. XLS) oder in Dokumentvorlagen (Endung DOT). Sie werden durch das Öffnen des befallenen Dokuments aktiv. Da die dazugehörigen Programme Word bzw. Excel sehr weit verbreitet sind und außerdem für verschiedene Betriebssysteme zur Verfügung stehen, kommt dieser Virenart in letzter Zeit eine große Bedeutung zu. Für etwa 80% aller Schadensmeldungen sind Makro-Viren verantwortlich, obwohl sie zahlenmäßig nur etwa 13% aller bekannten Viren umfassen.

### Würmer

Als Würmer wird Maware bezeichnet, die sich selbständig in Rechnernetzen ausbreiten können. Ihre massenhafte Verbreitung hat wesentlich mit der zunehmenden Vernetzung von Rechnern sowohl innerhalb einer Firma als auch über das Internet zu tun. Bevorzugter Ausbreitungsmechanismus sind dabei email-Anhänge. Werden die Anhänge sorglos geöffnet, kann sich die Malware im System einnisten. Danach verschickt sich die Malware, vom Anwender unbemerkt, selbständig weiter. Die dazu notwendigen email-Adressen entnimmt die Malware aus dem Adressbuch von Outlook - andere email-Programme sind hiervon seltener betroffen! In der Vergangenheit mussten mehrere große Firmen (auch Microsoft) ihre email-Server schon öfter vom Netz trennen, da sie die lawinenartige Zunahme an (automatisch verschickten) Emails nicht verkrafteten.



## Malware, Angriffe und Infektoren 2/5

### Stealth-Viren, Tarnkappenviren

Tarnkappenviren oder auch Stealth-Viren sind Viren mit speziellen Mechanismen, sich vor Virensuchprogrammen zu verstecken. Sie können z.B. eine infizierte Datei vor der Überprüfung restaurieren und somit die Verseuchung unkenntlich machen. Oder anders: sie versuchen sich, durch die Ausgabe der ursprünglichen statt der aktuellen Dateigröße, einer Entdeckung durch den Virenschanner zu entziehen. Eine andere Strategie: Greift z.B. ein Antivirenprogramm auf die Datei zu, so entfernt sich der Virus zeitweilig und infiziert die Datei im Anschluss an die Prüfung durch das Antivirenprogramm erneut.

### Programmviren, Dateiviren

Programmviren infizieren - Programme, also ausführbare Dateien mit der Endungen EXE oder COM (z.T. auch SYS oder OVL). Beim Start eines infizierten Programmes wird zunächst (unbemerkt vom Nutzer) der Virus gestartet, es werden andere Dateien infiziert und anschließend das eigentliche Programm gestartet. Eine infizierte Datei ist etwas größer als die Originaldatei, sie vergrößert sich um die Länge des Virencodes. Außerdem verändert sich durch eine Infektion die Prüfsumme der Datei, so dass Antivirenprogramme diese Viren mit Hilfe von Prüfsummenverfahren entdecken können.

### Skriptviren

Ein Skript ist ein Programm, welches nicht durch einen Kompilierer in Maschinensprache übersetzt wird, sondern durch einen Interpreter Schritt für Schritt ausgeführt wird. Ein Skript wird häufig auf Webservern verwendet (z.B. Perl oder PHP) bzw. durch in Webseiten eingebettete Skriptsprachen (z.B. JavaScript).

Ein Skript wird gerne in Webseiten zusätzlich zu normalem HTML oder XML eingesetzt, um Funktionen zu realisieren, die sonst nur unter Zuhilfenahme ausführbarer Programme auf dem Server (CGI-Programme) realisierbar wären. Solche Funktionen sind zum Beispiel Gästebücher, Foren, dynamisch geladene Seiten oder Webmailer. Skriptsprachen sind meist vom Betriebssystem unabhängig.

Im Falle von HTML-Dateien fügt sich das Skriptvirus in einen speziellen Bereich, den Skriptbereich, einer HTML-Datei ein (oder erzeugt diesen). Die meisten Browser laden diesen Skriptbereich des HTML-Dokuments um ihn schließlich auszuführen. Diese speziellen Skriptviren verhalten sich also fast genauso wie die oben beschriebenen Makroviren.

### Banking-Trojaner sind lautlose Räuber

Während Erpresserviren sich sofort melden wenn sie einen PC infiziert haben, machen Banking-Trojaner das genaue Gegenteil: Sie verstecken sich und tun alles, damit der Nutzer bloß nicht merkt, dass sie da sind. Im Verborgenen warten die Viren dann darauf, dass der Nutzer seinen Kontostand abrufen oder per Online-Banking Überweisungen tätigt. Erst dann reagieren die Schadprogramme und versuchen, auf unterschiedlichste Art einzugreifen. Beispielsweise ändern einige die Überweisungsdaten im Arbeitsspeicher, nachdem der Nutzer auf »Abschicken« geklickt hat, aber bevor die Daten übermittelt werden. So landet das Geld dann nicht beim gewünschten Empfänger, sondern bei den Kriminellen.

Andere Schädlingvarianten blenden stattdessen täuschend echte Meldungen auf Internetseiten oder in Banking-Programmen ein. Und zwar so, dass die über den richtigen Feldern liegen und diese nicht mehr sichtbar sind. Wer das nicht bemerkt – und das ist mit bloßem Auge teilweise gar nicht möglich – trägt die nötigen Daten für die Überweisung nicht ins Banking-Programm ein, sondern übergibt sie direkt an die Kriminellen hinter dem Virus. Und treu nach dem Motto »Nach dem Raub ist vor dem Raub« versuchen die Trojaner auch nach geglücktem Diebstahl alles normal aussehen zu lassen. Die Opfer merken daher oft erst Wochen später, dass etwas auf dem Kontoauszug nicht stimmt.

## Malware, Angriffe und Infektoren 3/5

### Ransomware oder Kryptotrojaner

Ransomware sperrt Benutzer aus ihrem eigenen Computer oder von bestimmten Dateien aus und verlangt zur Freigabe ein Lösegeld.

**Verschlüsselnde Ransomware:** Diese Art bedient sich Verschlüsselungsmethoden, um Dateien bis zur Zahlung des Lösegelds (meist um die 100 bis 300 €) unzugänglich zu machen. 2013 tauchte eine neue Variante namens Cryptolocker auf, die alle privaten und beruflichen Dateien verschlüsselt und sie erst nach Begleichen einer Gebühr in Höhe von etwa 300 € wieder entschlüsselt. Die Verschlüsselung ist dabei so komplex, dass dem Opfer nichts anderes übrig bleibt, als das Lösegeld zu begleichen oder eine komplette Neuauflistung des Systems vorzunehmen.

**Nicht verschlüsselnde Ransomware:** Hier gibt es verschiedene Varianten, die den Benutzer aus seinem eigenen Computer aussperren und so Lösegeld erpressen. Eine Variante zeigt eine gefälschte Windows-Aktivierungsnachricht und eine Zahlungsoption an. Eine andere, noch arglistigere Version sperrt den Benutzer nicht nur aus, sondern zeigt auch eine gefälschte Meldung an, die vorgibt, von einer Strafverfolgungsbehörde zu stammen, und die Zahlung eines Bußgelds wegen des Besitzes illegaler Software oder Kinderpornografie einfordert. Diese neueren Ransomware-Varianten unternehmen große Anstrengungen, um seriös zu erscheinen, und sind in unterschiedlichsten Sprachen erhältlich, um möglichst viele Opfer zu erreichen.

**siehe auch:** Hinweise zur Fehlerbeseitigung

### Paralleluniversum ADS

Ein häufig vernachlässigter Speicherort für Schadsoftware sind die Alternate Data Streams (ADS). Es handelt sich dabei um eine Besonderheit des NTFS-Dateisystems, eine Datei mit Anhängseln zu versehen, die nicht Teil der eigentlichen Datei sind. Dabei kann es sich um Metadaten handeln, wie z.B. die Abspielhäufigkeit einer MP3-Datei. Alternate Data Streams sind im Dateisystem nicht sichtbar (auch für Antivirensoftware), werden aber über den per Doppelpunkt vom Dateinamen getrennten Namen des Streams angesprochen. Bei einem unter Linux gemounteten NTFS-Dateisystem mit: **cat datei.mp3:count**

Dieser Datastream kann beliebige Daten von wenigen Bytes bis zu ganzen Dateien enthalten. So kann eine EXE-Datei versteckt werden, indem sie einfach als ADS an eine vermeintlich harmlose Datei angehängt wird. Unter Windows (CMD) lässt sie sich trotzdem ausführen: **start datei.mp3:malware.exe**

Windows zeigt mit dem Befehl **getfatr** die Namen der Alternate Data Streams als sogenannte Extended Attributes an. Damit können die ADS ausgelesen oder in separate Dateien kopiert werden und anhand von file ermittelt werden, in welcher Form die Daten gespeichert sind. Anschließend kann ein ganz normaler Malware-Scan durchgeführt werden.

# Malware, Angriffe und Infektoren 4/5

## Infektionsarten

### Companion-Viren

Companion-Viren infizieren nicht die ausführbaren Dateien selbst, sondern benennen die ursprüngliche Datei um und erstellen eine Datei mit dem ursprünglichen Namen, die nur das Virus enthält, oder sie erstellen eine Datei mit ähnlichem Namen, die vor der ursprünglichen Datei ausgeführt wird.

Es handelt sich also nicht um ein Virus im eigentlichen Sinne, da kein Wirtsprogramm manipuliert wird. Der Schädling führt, nachdem er sich meist im Arbeitsspeicher festgesetzt hat, das ursprüngliche Programm aus, so dass der Benutzer oft nichts von der Infektion bemerkt.

### Überschreibende

Überschreibende Computerviren sind die einfachste Form von Viren, wegen ihrer stark zerstörenden Wirkung aber am leichtesten zu entdecken. Wenn ein infiziertes Programm ausgeführt wird, sucht das Virus nach neuen infizierbaren Dateien und überschreibt entweder die ganze Datei oder nur einen Teil derselben (meist den Anfang) mit einer benötigten Länge. Die Wirtsdatei wird dabei irreparabel beschädigt und funktioniert nicht mehr oder nicht mehr korrekt, wodurch eine Infektion praktisch sofort auffällt.

### Prepender

Diese Art von Computerviren fügt sich am Anfang der Wirtsdatei ein. Beim Ausführen der Wirtsdatei wird zuerst das Virus aktiv, das sich weiterverbreitet oder seine Schadwirkung entfaltet. Danach stellt das Virus im Arbeitsspeicher den Originalzustand des Wirtsprogramms her und führt dieses aus. Außer einem kleinen Zeitverlust merkt der Benutzer nicht, dass ein Virus gerade aktiv wurde, da die Wirtsdatei vollkommen arbeitsfähig ist.

### Appender

Ein Appender-Virus fügt sich an das Ende einer zu infizierenden Wirtsdatei an und manipuliert die Wirtsdatei derart, dass es vor dem Wirtsprogramm zur Ausführung kommt. Nachdem das Virus aktiv geworden ist, führt es das Wirtsprogramm aus, indem es an den ursprünglichen Programmeinstiegspunkt springt. Diese Virusform ist leichter zu schreiben als ein Prepender, da das Wirtsprogramm nur minimal verändert wird und es deshalb im Arbeitsspeicher nicht wieder hergestellt werden muss. Da Appender einfach zu implementieren sind, treten sie relativ häufig auf.

### Entry Point Obscuring

Der Fachbegriff »Entry Point Obscuring« (kurz: EPO) heißt übersetzt »Verschleierung des Einsprungpunktes«. Viren, die diese Technik benutzen, suchen sich zur Infektion einen bestimmten Punkt in der Wirtsdatei, der nicht am Anfang oder am Ende liegt. Da dieser Punkt von Wirt zu Wirt variiert, sind Viren dieses Typs relativ schwierig zu entwickeln, da unter anderem eine Routine zum Suchen eines geeigneten Infektionspunktes benötigt wird. Der Vorteil für diesen Virentyp besteht darin, dass Virens Scanner die gesamte Datei untersuchen müssten, um EPO-Viren zu finden – im Gegensatz zum Erkennen von Prepender- und Appender-Viren, bei denen der Virens Scanner nur gezielt Dateianfang und -ende untersuchen muss.

### Gefahren durch Botnetze

Durch Botnetze ist Ihr Rechner (infiziert mit einem Trojaner) nicht mehr nur Opfer, sondern er wird gleichzeitig auch zum Täter. Er erhält die entsprechenden Befehle und führt diese ohne Ihre Kontrolle aus. Auch Ihre, auf dem PC gespeicherten persönlichen Daten sind nun nicht mehr sicher. In den Medien taucht für Botnetze übrigens immer öfter der Begriff »Zombie-Rechner« auf, weil der Rechner wie ein Zombie – ein willenloses Werkzeug – zum Leben erweckt wird.

# Malware, Angriffe und Infektoren 5/5

## Schutz durch Live-Systeme

Live-Systeme wie Knoppix, die unabhängig vom installierten Betriebssystem von einer CD gestartet werden, bieten nahezu vollständigen Schutz, wenn keine Schreibgenehmigung für die Festplatten erteilt wird. Weil keine Veränderungen an Festplatten vorgenommen werden können, kann sich kein schädliches Programm auf der Festplatte einnisten. Speicherresidente Malware kann aber auch bei solchen Live-Systemen Schaden anrichten, indem diese Systeme als Zwischenwirt oder Infektionsherd für andere Computer dienen können. Malware, die direkt im Hauptspeicher residiert, wird erst bei einem Reboot unschädlich gemacht.

## Begriffe

**Payload:** Payload bezeichnet die eigentlichen Nutzdaten (Programme, Daten, Malware, ...), die innerhalb eines Paketes oder einer anderen Übertragungseinheit, übertragen werden.

**Signaturen:** Als Signaturen werden heutzutage alle Einträge in einer Antivirusdatenbank bezeichnet.

**Threat:** engl.: Drohung, Bedrohung, Gefahr

**APT:** Ein APT (Advanced Persistent Threat) ist ein Angriff auf das Firmen-Netzwerk, bei dem unautorisierte Personen so lange wie möglich unentdeckt bleiben möchten.

**PUA:** potentiell unerwünschte Anwendungen (Werbung, Ausspähung, Spionage)

# Schutzsoftware: FireEye und DLP

Die Schutzsoftware »FireEye« und DLP-Software (Data Loss Prevention) werden in einem größeren Firmennetzwerk häufig gemeinsam eingesetzt.

## FireEye

FireEye, Inc. ist ein börsennotiertes Unternehmen mit Sitz in Milpitas, Kalifornien, USA, das Netzwerksicherheits-Software und Dienstleistungen anbietet.

Das Hauptprodukt »FireEye Malware Protection System« ist eine Software zur Angriffserkennung. Sie arbeitet auf der Grundlage von Datenverkehrsanalyse mittels Signaturen und heuristischen Methoden, um verdächtiges Verhalten auszumachen und versucht dann mittels Wiedereinspielung gegen eine Sandbox eine Kompromittierung nachzuvollziehen. Sie wird als revolutionäre Lösung gegen fortschrittliche Schadprogramme wie Advanced Persistent Threats (APT) und Zero-Day-Exploits vermarktet.

## DLP (Data Loss Prevention)

Eigenständige DLP-Produkte können auf Spezialgeräten installiert oder als Software verkauft werden. Integrierte DLP-Produkte befinden sich in der Regel auf Sicherheit Gateways am Perimeter (engl.: Eingrenzung, Grenze) und sind nützlich, um sensible Daten im Ruhezustand und in Bewegung zu erkennen. Bei DLP-Produkten handelt es sich also entweder um Software oder Module aus Software und Hardware.

Data Loss Prevention (DLP) ist ein Marketingbegriff aus dem Bereich der Informationssicherheit. Auch Data Leak oder Leakage Prevention genannt, ist DLP aus der »Extrusion Prevention« Technik hervorgegangen. Klassisch gesehen gehört DLP zu den Schutzmaßnahmen, die direkt den Schutz der Vertraulichkeit von Daten unterstützt (Daten-Integrität).

»Data Loss Prevention« und »Data Leakage Prevention« werden meist synonym gebraucht. In Fachdiskussion werden sie aber unterschieden: »Data Loss Prevention« ist der Schutz gegen den

unerwünschten Abfluss (externer oder interner Datendiebstahl) von Daten. Während »Data Leakage Prevention« für den Schutz gegen ein vermutetes, aber nicht messbares und manchmal auch im Einzelfall gar nicht feststellbares Weitergeben von Informationen an unerwünschte Empfänger steht.

DLP-Module gibt es für das Netz und auch als Erweiterungen bestehender Sicherheitstechniken. Sie arbeiten als Proxy oder Sniffer, für bestehende Proxys oder Mailfilter. Diese Module haben zurzeit die geringste Erkennungsrate, unterstützen die wenigsten Dateiformate und lassen sich am einfachsten umgehen.

Eine wirksame DLP-Lösung kann nur agentenbasiert sein. Im Prinzip handelt es sich um eine intelligent gesteuerte Verschlüsselung. Neben der Verschlüsselung müssen zusätzliche Funktionen zur Verfügung stehen, die den Umgang bestimmter Anwender mit bestimmten Daten regulieren können.

DLP-Agenten auf Arbeitsplatzrechnern und Servern mit schützenswerten Daten werden immer zentral verwaltet. Auf dem Verwaltungscomputer werden für Benutzergruppen oder einzelne Benutzer bestimmte Rechte erteilt. Diese Rechte können aber bei den meisten Produkten nicht sehr fein justiert werden. Daher muss immer geprüft werden, ob ein Produkt den Anforderungen überhaupt entspricht.

**Beispiele:** Eine sehr einfache DLP-Lösung protokolliert Dateinamen, die von und zu allen USB-Geräten geschrieben werden. Eine umfassendere DLP-Lösung erkennt jede Änderung an vertraulichen Daten, besonders auch mit Hilfe von Drittsoftware, und kann je nach Sicherheitsrichtlinie beliebige Aktionen durchführen, die auch mit administrativen Rechten des Anwenders nicht abzuwenden sind.

**Hinweis:** Die Einführung von DLP in einem Unternehmen wirft erhebliche Datenschutzbedenken auf.

# BitLocker

Mit BitLocker können Daten verschlüsselt werden und damit vor unautorisierten Personen geschützt werden.

## Windows 10 mit BitLocker verschlüsseln

Voraussetzung für die Verschlüsselung ist das Vorhandensein des **TPM-Chip** (Trusted Platform Module) auf dem Motherboard.

1. Vorhandensein des TPM-Chip überprüfen; Tastenkombination [Windows] + [X] → Geräte manager → Sicherheitsgeräte
2. Im Windows 10 Suchenfeld »BitLocker« eingeben und das Programm starten (BitLocker nur für W10 Pro und W10 Enterprise verfügbar)
3. Der Rechner wird vor der Verschlüsselung kurz überprüft und das zu verschlüsselnde Laufwerk vorbereitet.  
**Achtung:** Dieser Schritt kann optional sein, falls das Laufwerk keine Vorbereitung benötigt. Nach abgeschlossener Überprüfung werden Sie gefragt, wie das Laufwerk beim Start entsperrt werden soll (z.B. Option: »Kennwort eingeben«).
4. Sie haben anschließend mehrere Möglichkeiten, wie der Wiederherstellungsschlüssel gesichert werden soll. Falls Sie Ihr Passwort vergessen haben, erhalten Sie auf diesem Wege wieder Zugriff auf Ihre Daten (z.B. Option: »Auf USB-Speicherstick speichern«).
5. Optionsauswahl: nur Speicher verschlüsseln (Speicherbereich der Benutzer) oder gesamte Festplatte; Beachten Sie aber, dass die Option »Gesamtes Laufwerk verschlüsseln« wesentlich langsamer ist.
6. Der Rechner wird zum Abschluss von BitLocker neu gestartet. Sie haben damit Ihr Laufwerk erfolgreich verschlüsselt und werden beim Neustart nach Ihrem festgelegten Kennwort gefragt.

## Hinweis:

- Auch wenn BitLocker ein integriertes Feature von Windows 10 Pro und Enterprise ist, sollten Sie ein komplettes Backup Ihres Systems vor der Verschlüsselung machen, um bei möglichen Komplikationen wieder zum Status quo zurückzukehren.
- Kurzhilfe für die BitLocker-Verschlüsselung aufrufen; Powershell → manage-bde
- »BitLocker Drive Preparation Tool« direkt aufrufen: BdeHdCfg.exe

## Kurzanleitung: BitLocker ohne kompatibles TPM zulassen

1. Drücken Sie [Windows] + [R] und geben Sie »gpedit.msc« ein, bestätigen Sie mit »OK«.
2. Klicken Sie auf »Administrative Vorlagen« → "Windows-Komponenten" → »BitLocker-Laufwerkverschlüsselung« → »Betriebssystemlaufwerke«.
3. Machen Sie einen Doppelklick auf den Eintrag »Zusätzliche Authentifizierung beim Start anfordern«.
4. Wählen Sie die Option »Aktiviert« aus und überprüfen Sie, dass die Checkbox »BitLocker ohne kompatibles TPM zulassen [...]« aktiviert ist. Abschließend drücken Sie »Übernehmen« und »OK«.



# Windows 10 reparieren 1/4

## Windows 10 reparieren

Wenn irgendwas nicht mit Windows 10 stimmt, sollte erst mal das **Allheilmittel Neustart** probiert werden.

- Mit der Tastenkombination **[W] + [R]** den Ausführen-Dialog öffnen.
- **shutdown -g -t 0** eingeben und Bestätigung mit der Eingabetaste.

Windows startet neu und nach dem Neustart auch alle registrierten Anwendungen.

## Windows 10 reparieren mit DISM, SFC und USB-Stick

Wenn Windows 10 nicht mehr richtig funktioniert und auch ein Neustart nicht weiterhilft, bleibt noch die Windows-10-Reperatur mit den Programmen DISM und SFC.

**DISM** ... Deployment Image Servicing and Management tool ( Befehlszeilenprogramm, Administratorrechte erforderlich); zu Deutsch: kann auch mit Abbildverwaltung für die Bereitstellung übersetzt werden

**SFC** ... System File Check

## Windows 10 Systemdateien reparieren mit SFC

Windows verwendet seit jeher viele tausende Systemdateien, die für den reibungslosen Betrieb vonnöten sind. Wenn diese Dateien gelöscht oder manipuliert werden, kann dies zu einem instabilen Windows führen. Praktischerweise hat Windows aber das entsprechende Gegenmittel eingebaut: Der »System File Check« oder kurz SFC kann die Systemdateien überprüfen und bei Bedarf wiederherstellen.

**sfc** ... Ohne Parameter, wird eine Kurzhilfe aufgerufen.

1. Windows-Kommandozeile mit Administratorrechten öffnen.
2. Befehlseingabe: **sfc /scannow**

3. Windows überprüft nun die Dateisystemstruktur. Sollten dabei Fehler festgestellt werden, versucht Windows, diese automatisch zu beheben.

4. Damit es nicht zu Fehlern kommt, sollte man sich während des Reparaturvorgangs durch Windows in Geduld üben.

5. Nach Abschluss des Vorgangs, ist der Rechner neu zu starten und anschließend zu prüfen, ob die Reparaturen erfolgreich waren.

**Hinweis:** Bei einigen älteren Windows-Versionen, muss zusätzlich noch die Windows-CD ins Laufwerk eingelegt werden. Sollte SFC nicht zum gewünschten Erfolg führen, so kann man es mit DISM probieren. Mit dem Befehl `sfc /scannow` werden alle geschützten Systemdateien überprüft und die beschädigten Dateien durch eine zwischengespeicherte Kopie ersetzt, die sich in einem komprimierten Ordner unter »%WinDir%\System32\dlcache« befindet. Der Platzhalter %WinDir% steht für den Windows-Betriebssystemordner.

## Windows 10 Systemdateien reparieren mit DISM

Neben dem System File Checker gibt es in Form von DISM (Deployment Image Servicing and Management) ein zweites Kommandozeilentool, das bei der Reparatur von Windows helfen kann. Mit DISM kann man auf der Kommandozeile ebenfalls dafür sorgen, dass defekte Windows-Dateien wiederhergestellt werden.

**dism** ... Ohne Parameter, wird eine Kurzhilfe von DISM (Deployment Image Servicing and Management tool) aufgerufen.

**dism /Get-WimInfo /WimFile:d:\sources\boot.wim** ... Informationen über die Datei boot.wim anzeigen.

1. Windows-Kommandozeile mit Administratorrechten öffnen.
2. Befehlseingabe: **dism /Online /Cleanup-Image /ScanHealth**  
Windows 10 überprüft nun den Zustand der Installation, was einige Minuten dauert.

## Windows 10 reparieren 2/4

3. Falls bei der Überprüfung Fehler auftreten, meldet DISM dies nach Abschluss des Scans. In diesem Fall ist folgender Befehl einzugeben: **dism /Online /Cleanup-Image /RestoreHealth**
4. Windows 10 repariert nun die gefundenen Fehler und ersetzt defekte Dateien durch die Originale. Damit es nicht zu Fehlern kommt, sollte man sich während des Reparaturvorgangs durch Windows in Geduld üben.
5. Nach Abschluss des Vorgangs, ist der Rechner neu zu starten und anschließend zu prüfen, ob die Reparaturen erfolgreich waren.

### Reparatur durch ein Windows-Update

Oft ist die Windows-Reparatur vergleichsweise simpel zu realisieren: Man führt einfach eine Suche nach Windows-Updates durch und installiert diese Updates. Werden die Probleme beispielsweise durch veraltete oder auch fehlerhafte Treiber ausgelöst, besteht eine Chance, dass diese per Windows-Update aktualisiert werden. Auch können Sicherheits- und Funktionsupdates für Windows dafür sorgen, dass zuvor fehlerhafte Dateien erneuert werden.

Update durchführen: Einstellungen von Windows 10 aufrufen und unter »Update und Sicherheit - Windows Update« nach verfügbaren Aktualisierungen suchen lassen. Anschließend sind diese Updates zu installieren und anschließend ein Rechner-Neustart durchzuführen. Mit etwas Glück funktioniert danach alles wieder.

**Hinweis:** Durch die Installation von aktuellen Windows-Updates kann man in vielen Fällen dafür sorgen, dass Windows wieder funktioniert.

### Windows 10 per Upgrade-Installation reparieren

Eine weitere Möglichkeit zur Reparatur einer defekten Windows-10-Umgebung ist die Upgrade-Installation.

Dabei startet man einfach die Installation von Windows 10 von einem entsprechenden Datenträger oder über das ISO-Image direkt vom Desktop aus.

Der Clou: führen Sie die Windows-10-Installation auf einem Windows-10-PC aus, erkennt das System dies und lässt die installierten Programme sowie Ihre persönlichen Dokumente und Dateien in Ruhe. Stattdessen installiert das Windows-Setup die neueste Version von Windows 10.

Angenehmer Nebeneffekt: Auf diese Weise repariert das System auch alle fehlerhaften Systemdateien und sorgt dafür, dass Windows wieder starten kann.

Dazu benötigt man lediglich ein aktuelles Installationsmedium von Windows 10, das man direkt bei Microsoft herunterladen kann. Die nötigen Informationen dazu findet man auf den offiziellen Microsoft-Webseiten. Sobald die ISO-Datei auf der Festplatte sich befindet, kann man sie per Doppelklick einbinden und über den Explorer das Programm setup.exe starten. Mit Hilfe des Setup-Assistenten sollte die Option »Persönliche Dateien und Apps behalten« aktiviert sein. Anschließend kann man die Reparaturinstallation von Windows 10 durchführen. Sobald diese abgeschlossen ist, sollte das System wieder funktionieren.

**Hinweis:** Durch das »Drüberinstallieren« von Windows 10 kann man eine defekte Installation in den meisten Fällen retten.

# Windows 10 reparieren 3/4

## Windows-Assistenten zur Problembehandlung nutzen

Windows bietet seit vielen Jahren eingebaute Assistenten, die bei der Reparatur bestimmter Fehler helfen können. In neueren Versionen von Windows 10 sammelt Microsoft diese in den Systemeinstellungen. Vor allem, wenn man mit bestimmten Systemfunktionen (z.B. den Netzwerkverbindungen) Probleme hat, können die Assistenten bei der Reparatur von Windows helfen.

Öffnen der Einstellungen von Windows 10 über das Startmenü und Navigation zum Punkt »Problembehandlung«.

Hier listet Windows 10 eine Reihe von Assistenten zur Behebung diverser Systemprobleme auf. Die Assistenten sind nach Kategorien sortiert, sodass Sie einfach nach einer möglichen Lösung fahnden können.

Man klickt einen Punkt an, der auf die aktuelle Windows-Installation zutrifft. Anschließend wählt man den Punkt »Problembehandlung ausführen«.

Windows öffnet nun den zugehörigen Assistenten. Hier kann man - je nach Problem - weitere Optionen auswählen. Man muss sich jetzt durch die einzelnen Schritte durchklicken.

Windows 10 führt nun eine Reihe von Überprüfungen durch. Findet das System dabei Probleme, kann man die entsprechenden Reparaturen jetzt durchführen lassen.

## Windows-10-Installation auffrischen oder zurücksetzen

Wenn alle Stricke reißen, kann man Windows 10 zurücksetzen.

Das System bietet dazu gleich zwei praktische Funktionen, die eine Neuinstallation deutlich einfacher machen als bei den Vorgängern.

Man hat dabei sogar die Wahl, ob die persönlichen Dateien sowie die aus dem Windows Store heruntergeladenen Anwendungen erhalten bleiben oder ob man komplett wieder bei Null anfängt.

Die entsprechenden Optionen finden Sie in den Windows-Einstellungen unter »Update und Sicherheit« im Unterpunkt »Wiederherstellung«.

Dort ist der Punkt »Diesen PC zurücksetzen« anzuklicken. Nach einen weiteren Klick auf »Los geht's« wird der Vorgang gestartet (Anweisungen folgen). Sobald der Vorgang abgeschlossen ist, kann man wieder auf eine funktionierende Installation von Windows 10 zurückgreifen.

**Hinweis:** Die Zurücksetzung des Rechners ist nur durchzuführen, wenn Windows gar nicht mehr funktionieren will.

# Windows 10 reparieren 4/4

## Windows 10 per USB-Stick reparieren

Für die Reparatur, ist zunächst ein bootfähiger USB-Stick mit dem »Media Creation Tool« zu erstellen.

1. »Media Creation Tool« herunterladen und das »Media Creation Tool« anschließend starten. Nach der Akzeptierung der Rechtshinweise und Lizenzbedingungen steht das Tool zur Verfügung.
2. Auswahl des Installationsmediums und auf »Weiter« klicken.
3. Entfernung der Markierung bei den empfohlenen Optionen.  
Anschließend Auswahl der Sprache, der Windows-Version und die Rechner-Architektur (32 oder 64 Bit). Bei aktuellen Rechner ist es meistens 64-Bit.
4. Auswahl der Option USB-Speicherstick. Alternativ kann man auch eine ISO-Datei erstellen.
5. Angeschlossener USB-Stick aus der Liste auswählen. Eventuell ist die Laufwerkliste zu aktualisieren.
6. Der USB-Stick wird nun erstellt (Windows 10 wird heruntergeladen). Der Vorgang kann je nach Internetgeschwindigkeit mehrere Stunden dauern.

## Windows 10 Reparatur mit dem erstellten USB-Stick

1. mit dem USB-Stick booten
2. Unter Umständen musst die Bootreihenfolge im BIOS geändert werden, damit der Bootvorgang starten kann.
3. Bedienungssprache bestätigen und die Computerreparaturoptionen auswählen
4. auf Problembehandlung klicken → Erweiterte Optionen → Starthilfe
5. den Eintrag Windows 10 auswählen

Windows startet nun die Reparatur. Das kann einige Zeit in Anspruch nehmen. Alternativ kann man im Dialog »Problembehandlung → Erweiterte Optionen« auch eine Systemwiederherstellung durchführen.

## Windows 10 im Reparatur-Modus öffnen

- Windows 10 starten und anmelden
- Windows 10 Startmenü öffnen und den Beenden-Button anklicken
- [Shift]-Taste drücken und halten und auf »Neu starten« klicken
- Reparaturmodus auswählen und anschließend steht die Windows-Konsole (CMD) zur Verfügung (Administratorrechte erforderlich)

## Windows 10 im abgesicherten Modus starten

- Tastenkombination [Strg] + [F8] während des Bootvorganges mehrfach betätigen
- **Hinweis:** Das Zeitfenster um in den abgesicherten Modus zu gelangen ist recht klein. Dies gilt insbesondere für schnelle Festplatten (SSD).
- **Alternative Methode 1:** 4 x booten und den Rechner über den Button »Power« (etwa 4 Sekunden drücken) wieder ausschalten.
- **Alternative Methode 2:** Windows 10 starten und anmelden
- Windows 10 Startmenü öffnen und den Beenden-Button anklicken
- [Shift]-Taste drücken und halten und auf »Neu starten« klicken
- Abgesicherten Modus auswählen (Administratorrechte erforderlich)

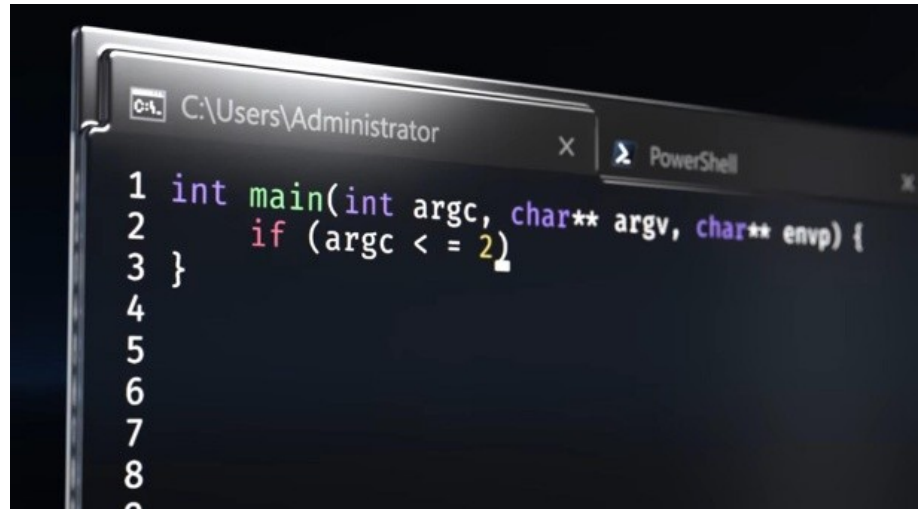
# Hinweise und Ankündigungen für Windows 10

## Update-Zyklus:

Im Frühjahr und Herbst werden für Windows 10 gesammelte Änderungen (Großupdate) installiert. Die angekündigten Termine können sich mitunter um einige Wochen verschieben.

## Windows Terminal:

Zum Ende des Jahres 2019 wird ein neues Terminal angekündigt. Dies Terminal soll in Zukunft **CMD** (cmd.exe), **Powershell** (pwsh.exe) und **WSL** bzw. **WSL2** (Windows Subsystem für Linux, Linux-Kompatibilitätsschicht) vereinigen.



Eine Besonderheit des »Windows Terminal« ist beispielsweise, dass Nutzer mehrere Registrierkarten in einem Fenster öffnen können, so wie in einem Internet-Browser.

Das »Windows Terminal« ist Open Source, das heißt, der Code kann von allen Nutzern eingesehen werden. Microsoft hat den Quellcode auf der Entwicklerplattform Github veröffentlicht.

Windows 10 benötigt für das »Windows Terminal« zwingend das Update auf Version 1903.

# Mobilfunk-Standard 5G 1/3

## Die technischen Grundlagen von 5G

Die Architektur des Netzes der 5. Mobilfunkgeneration richtet sich nach den Anforderungen der Anwender vor Ort: Ob in einem Gewerbegebiet ein sehr breitbandiges Netz mit hohen Datenraten, an einem Verkehrsweg ein schnelles Netz mit Fokus auf kurze Antwortzeiten und hoher Zuverlässigkeit oder in einer Werkshalle ein Netz errichtet wird, das eine extreme hohe Anzahl von Geräten und Menschen gleichzeitig miteinander arbeiten lässt - das entscheiden die Nutzer mit ihren Wünschen vor Ort.

Die Techniker unterscheiden beim 5G-Netz drei unterschiedliche Anwendungsbereiche: das ultra-schnelle mobile Breitband (Enhanced Mobile Broadband), die Kommunikation zwischen Maschinen und Anwendungen (Massive Machine Type Communications, M2M) oder das Internet der Dinge (Internet of Things - IoT), sowie ein Hoch-Zuverlässigkeitsnetz mit kurzen Antwortzeiten (Ultra-Reliable and Low Latency Communications, Antwortzeiten: 4G-Netz - 30 Millisekunden, 5G-Netz - 1 Millisekunde).

## Einsatz von Kleinzellen - Small Cells

Kleinzellen (Small Cells) kommen insbesondere an Orten mit hoher Nutzerdichte zum Einsatz (Beispiel: Fußgängerzonen, Hotspots).

Mehr Zellen in einem kleinen Gebiet bedeutet auch, dass die Kapazität, also die Anzahl möglicher gleichzeitiger Nutzer mit gleichzeitig hohem Datendurchsatz, signifikant erhöht wird.

Eine Small Cell ist eine Mobilfunkzelle mit geringer Sendeleistung (< 10 Watt). Der Versorgungsradius liegt bei etwa 150 Metern.

Die Kleinzellen können an Litfaßsäulen, Hauswänden, in Straßenbeleuchtungen oder öffentlichen Telefonanlagen montiert werden.

## Mehrantennen- Systeme - Massive Multiple Input Multiple Output (MIMO)

Für die weitere Steigerung der Kapazität kommen größere Mehrantennen-Systeme zum Einsatz.

Die Mehrantennen-Systeme ermöglichen die Nutzung mehrerer Sende- und Empfangsantennen zur drahtlosen Kommunikation.

Ein spezielles Codierungsverfahren nutzt sowohl die zeitliche als auch die räumliche Dimension zur Informationsübertragung (Space-Time-Coding). So lassen sich die Qualität und die Datenrate deutlich verbessern, obwohl nicht mehr Frequenzen herangezogen werden.

Derzeit werden Mehrfachantennensysteme mit bis zu 200 Antennen-Elemente entwickelt.

## Ausrichtung auf die Endgeräte - Beamforming

Eine weitere technische Möglichkeit im Rahmen der Mehrfachantennen (MIMO) liegt in der gezielten Versorgung einzelner Teilnehmergeräte durch ein sogenanntes Beamforming.

Dabei wird die Antennen-Senderichtung so verändert, dass ein maximales Signal am gewünschten Ort (Endgerät) ankommt. Mit der Bündelung der Funkwellen kann, statt der sonst üblichen kreisförmigen Ausbreitung der Funksignale, eine präzise Ausrichtung des Signals in Richtung des Kunden bzw. des Gerätes erreicht werden.

Die Hauptsenderichtung wird beim Beamforming räumlich so ausgerichtet, dass einzelne Endgeräte mit dem ihm zugewiesenen Signal angesprochen werden - sei es direkt bei Sichtverbindung oder indirekt über Reflexionsflächen in der Umgebung.



## Mobilfunk-Standard 5G 2/3

### Frequenz entscheidend für die Reichweite

Ausschlaggebend für die Reichweite ist vor allem die verwendete Frequenz der Basisstation auf der gefunkt wird.

Hier gibt also die Physik den Ton an und weniger die Technik. Allgemein gilt, dass mit zunehmender Wellenlänge bei elektromagnetischen Wellen auch die Reichweite steigt.

Darüber hinaus gilt – je niedriger die Frequenz, desto höher die Wellenlänge. Der Zusammenhang zwischen Wellenlänge und Frequenz lautet im Detail:

$$\text{Wellenlänge } l = \frac{\text{Lichtgeschwindigkeit } c}{\text{Frequenz } f}$$

$$l = \frac{c}{f} \frac{300.000.000 \text{ m/s}}{800 \text{ MHz}} = 0,375 \text{ m}$$

$$l = \frac{c}{f} \frac{300.000.000 \frac{\text{m}}{\text{s}}}{3600 \text{ MHz}} = 0,083 \text{ m}$$

Man sieht also, dass die höhere Frequenz eine deutlich geringere Wellenlänge und damit auch eine geringere Reichweite aufweist, sofern die Sendeleistung gleich bleibt.

### Ultrakurze Reichweite bei mmWave

Die Reichweite im Bereich über 2 GHz ist äußerst gering. Für 5G sind aber noch höhere Frequenzen im mm-Bereich geplant – bei 6 bis 30 GHz.

Derartige Funkzellen haben eine Reichweite von nur wenigen hundert oder gar unter 50 Metern, ähnlich wie heimische WLAN-Netze. Man spricht daher auch von Small- oder Micro-Cells.

Durch den Einsatz diverser Verfahren, können 5G-Stationen dennoch eine etwas höhere Reichweite erzielen. Möglich macht das der Einsatz spezieller Mehrantennentechniken (MIMO) und vor allem Beamforming.

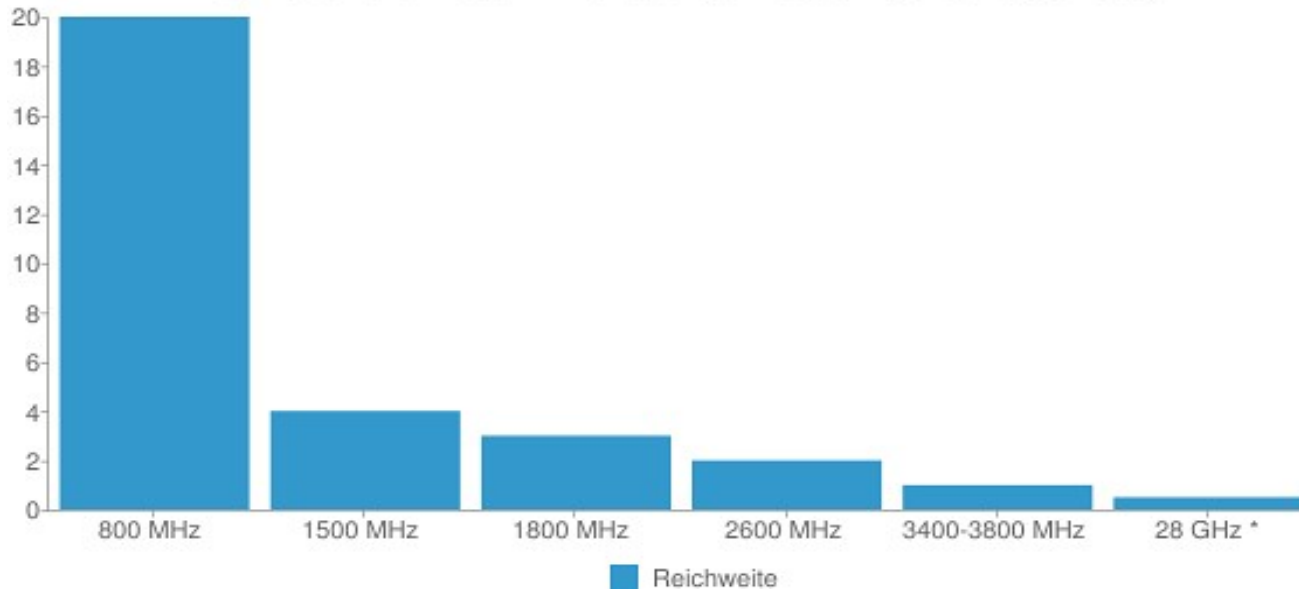
Während herkömmliche 4G-Masten die Funkstrahlen praktisch in alle Richtungen feuern, wird bei 5G jedes Endgerät direkt angepeilt. Vereinfacht ausgedrückt, sendet der Mast einen gebündelten Funkkegel zum Nutzer, als ob man mit einer Taschenlampe im Dunkeln eine Person anstrahlt.

In der Summe ergeben sich geringere Reichweitenverluste und die Kapazität der Station erhöht sich enorm. Der Mast kann so ein Vielfaches mehr an Nutzern versorgen - etwa um den Faktor 1000.

Tatsächlich ist es fast unmöglich eine genaue Angabe zur Reichweite bei einer bestimmten Mobilfunkfrequenz zu machen. Schuld daran sind extrem viel beeinflussende Faktoren. Zusätzlich spielen aber noch Wetter, umgebende Bebauung/Topologie und die Geschwindigkeit der Nutzer und Geräte eine Rolle.

# Mobilfunk-Standard 5G 3/3

Maximale Reichweite in Kilometern je Frequenz (Erfahrungswerte)



- 5G-Netz: Frequenzbereich reicht von 2,1 bis 3,6 GHz; Frequenzbereiche für 6 bis 30 GHz sind in Planung
- 5G-Netz: Versorgungsradius - maximal 1km
- 5G-Netz: Datenraten bis zu 20 Gbit/s
- Small Cells: Versorgungsradius liegt bei etwa 25 Metern bis 150 Metern, je nach Bebauungsdichte.
- Antwortzeiten: 3G-Netz - 100 Millisekunden, 4G-Netz - 30 Millisekunden, 5G-Netz - 1 Millisekunde
- Kritik am 5G-Standard: Durch die hohe Anzahl der Geräte (IoT - Internet der Dinge) kann die Sicherheit niemals garantiert werden.

## Fazit

Sofern für 5G-Mobilfunk künftig keine Frequenzbereiche unter 3 GHz eingesetzt werden, ist mit einer sehr geringen Reichweite zu rechnen. Respektive benötigt man für den Ausbau eine extrem hohe Dichte an Funkstationen (Smart Cells).

Nur im Zusammenspiel (3G, 4G und 5G) mit den Bändern die heute für UMTS (3G) oder LTE (4G) eingesetzt werden, im Bereich von 0,7-2 GHz (3G, 4G), ließen sich größere Flächen kostengünstig erschließen.

# Tipps

## Video-Bearbeitung mit Bordmittel

Video-Ausschnitt aus einem Video herausschneiden:

- Video über das Kontextmenü mit dem Programm Fotos oder Video öffnen
- Video bearbeiten – Symbol »Bleistift« anklicken
- die beiden weißen Punkte mittels der Maus verschieben, um den entsprechenden Filmausschnitt zu markieren
- über das Menü den markierten Filmausschnitt einen Namen vergeben und speichern

## Powerpoint-Präsentation in ein Video umwandeln

Mit Powerpoint 2016 können Präsentationen in ein MP4-Video umgewandelt werden (Speichern unter → Dateiformat: mp4). Sind in der Powerpoint-Präsentation bereits Videos eingebettet, so kann die Qualität der Audioausgabe der eingebetteten Videos sich in der Gesamtdatei (MP4-Video) stark verringern. Dies Qualitätseinbuße der Audioausgabe macht sich immer dann bemerkbar, wenn das MP4-Video auf andere Systeme (TV-Geräte, Linux, ...) abgespielt wird.

## Einheiten mit Calc umrechnen

- [W] + [R] → calc
- erweiterte Ansicht des Taschenrechners aufrufen

## PC-Name, Rechnername ändern

- [W] + [I] → System → Info und »Diesen PC umbenennen«
- erlaubte und zu bevorzugende Zeichen: Buchstaben (ohne deutsche Umlaute), Zahlen, Bindestrich, Unterstrich
- verbotene Zeichen: [ \ ] ^ ' : ; < = > ? @ ! " # \$ % ` ( ) + / . , \* & , und Leerzeichen

## Langen Dateipfad in die CMD eintragen

- Datei vom Desktop oder aus dem Datei-Explorer einfach in das CMD-Fenster ziehen.

## Schutzsoftware von TrendMicro

- Die Schutzsoftware (Anti-Virussoftware) der amerikanischen Firma »TrendMicro« war im Jahr 2019 inkompatibel mit dem Windows 10 Update 1903.

## Batch-Datei: Windows-Dienst starten oder beenden

```
@echo off
set DIENSTNAME1="Nachrichtendienst"
net stop %DIENSTNAME1% 2>nul
if errorlevel 2 (
 echo Dienst ist bereits gestoppt . . . Starte %DIENSTNAME1%
 net start %DIENSTNAME1%
)
pause
```

Sollte der Dienst bereits gestoppt sein, so verhindert "2>nul" eine Fehlermeldung. Das "pause" ermöglicht, das man einen Blick auf die letzte Ausführung erhält und mit einem beliebigen Tastendruck das Skript beenden kann.

**Hinweis:** Bei der Eingabe an der Befehlszeile müssen Dienstnamen, die aus zwei oder mehr Zeichengruppen bestehen, in Anführungszeichen (") eingeschlossen werden, z. B. startet NET START "Plug & Play" den Plug & Play-Dienst.

# Internet-Links 1/2

## **Bandbreitenmessung:**

<https://breitbandmessung.de/>  
<https://speedtest.computerbild.de/run.php>  
<https://speedtest.chip.de/>

## **Wiederherstellung von Dateisysteme: TestDisk**

[https://www.cgsecurity.org/wiki/TestDisk\\_Download](https://www.cgsecurity.org/wiki/TestDisk_Download)  
[https://www.cgsecurity.org/wiki/Schritt\\_f%C3%BCr\\_Schritt\\_Wiederherstellungsbeispiel](https://www.cgsecurity.org/wiki/Schritt_f%C3%BCr_Schritt_Wiederherstellungsbeispiel)

## **Panopticklick - im Internet ist jeder einzigartig und auch erkennbar:**

Betreiber der Webseite: EFF  
<https://panopticklick.eff.org/>

## **GEO-Targeting:**

[www.utrace.de](http://www.utrace.de)  
[www.netip.de](http://www.netip.de)  
[www.hostip.info](http://www.hostip.info)

## **Eigene IP-Adresse ermitteln:**

[myip.is](http://myip.is)

## **Windows 10 – Telemetrie:**

<https://www.windowspro.de/wolfgang-sommergut/windows-10-sendet-daten-microsoft-telemetrie-einschraenken-ueber-gpos>  
<https://winfuture.de/special/windows10/faq/Windows-10-Diese-neun-Einstellungen-sollte-man-als-erstes-aendern-226.html>  
[https://de.wikipedia.org/wiki/Microsoft\\_Windows\\_10](https://de.wikipedia.org/wiki/Microsoft_Windows_10)  
 Batchfile: <https://gist.github.com/vip3rc0de/a0d2d90f52f9e7c90de0>  
[www.kuketz-blog.de/windows-10-dem-kontrollverlust-entgegenwirken/](http://www.kuketz-blog.de/windows-10-dem-kontrollverlust-entgegenwirken/)

## **Lichtwellenleiter und andere:**

[https://www.glasfaserkabel.de/Der-Unterschied-zwischen-Singlemode-und-Multimode-LWL-Kabeln:\\_:13.html](https://www.glasfaserkabel.de/Der-Unterschied-zwischen-Singlemode-und-Multimode-LWL-Kabeln:_:13.html)  
<https://www.opternus.de/wissen/kleine-lwl-stecker-lehre>  
<https://de.wikipedia.org/wiki/LWL-Steckverbinder>  
<https://www.metz-connect.com/de/cables-wires/configuration-key>

## **SFP-Ports:**

[https://de.wikipedia.org/wiki/Small\\_Form-factor\\_Pluggable](https://de.wikipedia.org/wiki/Small_Form-factor_Pluggable)

## **Administrierung, News, Tipps, etc.:**

<https://www.it-administrator.de/>

## **Festplattenbearbeitung:**

<https://www.com-magazin.de/praxis/windows/festplattenverwaltung-diskpart-52963.html>

## **Netzwerkausrüster:**

<https://www.juniper.net/de/de/>  
 Juniper Networks bietet Service Providern, privaten und öffentlichen Unternehmen leistungsstarke Netzwerk- und Cybersicherheitslösungen.  
<https://www.triotronik.com/download>  
 LWL, Schränke und anderes

## **RAID:**

<http://www.thomas-krenn.com/de/wiki/RAID>  
[www.attingo.at](http://www.attingo.at) ... RAID Datenrettung

## Internet-Links 2/2

### **Domaininhaber ermitteln:**

[www.internic.at](http://www.internic.at)

### **Anmeldenamen für Internetdienste überprüfen:**

[www.namecheckr.com](http://www.namecheckr.com)

[www.namecheck.com](http://www.namecheck.com)

**Hinweis:** Über einige Webseiten, können vorhandene oder neue Anmeldenamen auf deren Verfügbarkeit überprüft werden. Die Webseiten verändern reale vollständige Namen automatisch mit den üblichen Sonderzeichen und Zahlen (**Beispiel:** Beate Meier → beatemeier28). Aus diesem Grund, sollten Anmeldenamen nur mit sicheren Passwörtern benutzt werden.

### **Geolocation:**

[www.utrace.de](http://www.utrace.de)

[www.maxmind.com/en/locate-my-ip-address](http://www.maxmind.com/en/locate-my-ip-address)

[www.infosniper.net](http://www.infosniper.net)

### **Online-Übersetzer:**

[deepl.com](http://deepl.com) → Hinweis: Nach einer mehrmaligen Benutzung des Übersetzers, wird DEEPL für einige Zeit gesperrt.

[google.de](http://google.de) → Optionsmenü der Startseite → Übersetzer

### **AfB - gebrauchte gut erhaltene IT-Technik (Rechner, ...)**

[www.afb-group.de](http://www.afb-group.de)

### **Suchmaschine und Anonymizer**

[www.startpage.com](http://www.startpage.com)

StartPage benutzt Google ohne Google über die Suchgewohnheiten der Benutzer zu informieren. Zu jedem Suchergebnis, wird auch ein Link angeboten mit dem man die Webseite anonym aufrufen kann.

## Literatur-Tipps

**PC-Netzwerke** von Axel Schemberg, Martin Linten – Verlag: Galileo  
Computing



# Index 1/2

## A

ABAP ... 154  
 Abgesicherter Modus ... 168, 169, 186  
 Access-Points ... 84  
 Admin-Rechte für einzelne Programme ... 42  
 Aktivierung von Windows anzeigen ... 08  
 Alleinstellungsmerkmale ... 133  
 Anmeldung ... 11, 20, 61  
 Anschlussbelegung – Netzwirkkabel ... 71

## B

Backup ... 126  
 Backup-Alternative ... 134  
 Backup-Programme ... 63  
 Batch-Datei ... 13  
 Batch-Datei: Windows-Dienst starten oder beenden ... 191  
 Batch-Dateien, Telemetrie ... 192  
 Beacon ... 47  
 Benutzerverwaltung ... 11  
 BIOS ... 08, 18, 19, 85, 86, 112-115, 117, 118-119  
 BIOS-Batterie: CR 2032 ... 85  
 BitLocker ... 182  
 Boot-Menü aufrufen ... 117, 118

## C

calc ... 191  
 chkdsk ... 10  
 cleanmgr ... 174

cmd mit Administratorrechten öffnen ... 08, 162  
 convert ... 10  
 Copy ... 13  
 Cygwin ... 134

## D

Datenträgerverwaltung ... 10, 12, 161, 162  
 Datenschutzerklärung von Microsoft ... 41, 43  
 Datum und Uhrzeit ... 09  
 dir, Textfragment ... 10  
 Dienste neu starten ... 13  
 Dienstverwaltung ... 09, 16  
 Diskpart ... 12, 95, 162, 163  
 DISM ... 156, 183  
 DLP - Data Loss Prevention ... 181  
 DoS ... 25, 26, 27-29  
 Drucker ermitteln ... 20

## E

Einheiten mit calc umrechnen ... 191  
 ETW ... 57-60  
 Excel ... 155

## F

Fehlerbeseitigung ... 160-175  
 Ferrule ... 77  
 FIDO ... 24, 148-152  
 FireEye ... 144, 175  
 Firefox-Referer ... 158  
 Firefox Add-on ... 158  
 Format ... 12, 95  
 Format vfat mit Linux ... 113

## G

Gateway ... 16  
 Gastkonto aktivieren ... 160  
 GetWmiObject ... 19, 20  
 Geolocation ... 193  
 Geo-Targeting ... 192  
 Gruppenrichtlinie (Group Policy) ... 13

## H

Hardware-Info ... 07  
 hiberfil.sys ... 166, 167  
 Hotfixes, Updates anzeigen ... 11, 19  
 Hwinfo32 ... 07

## I

Interrupt ... 47

## J

## K

## L

Laufwerksbuchstabe, Windows PE ... 161, 163  
 Lexware ... 66  
 Login, Anmeldung ... 11, 19, 20

## M

mkfs.vfat ... 113

## N

net user ... 11, 120

## Index 2/2

- O
  - Optionalfeatures ... 12
  - OpenSQL ... 154
- P
  - Paketfilter ... 16
  - Pairing-Modus ... 62
  - Pigtail ... 76
  - Power over Ethernet ... 84
  - Power over Ethernet (PoE) ... 84
  - ProductKey ... 18
  - Prozess anzeigen, stoppen ... 09, 13, 18
  - Produkt-Key ändern ... 08
  - Pulsweitenmodulation, Lüfter ... 160
- Q
- R
  - Recovery-Partition – Status anzeigen ... 13
  - Recuva ... 70
  - Rembo ... 147
  - Robocopy ... 13
  - Rsync ... 134
- S
  - Sandbox ... 12
  - Schutzsoftware ... 181
  - Secure Boot ... 117
  - sfc /scannow ... 173, 183
  - SFP ... 79
  - Shutdown ... 11
  - SiSyPHuS Win10 ... 44
  - Spare-Festplatten , Hot-Spare... 107
  - Scrubbing ... 29
- SORM ... 29
- Storage ... 128-132
- Swapping-Festplatten, Hot-Swapping ... 107
- Systeminformationen ... 07, 09
- T
  - Tasklist ... 09, 13
  - Taskkill ... 09, 13
  - Tastatur-Kurzbefehle ... 08
  - Taskmanager ... 09, 15
  - Telemetrie ... 42, 44, 45,, 192
- U
  - Überwachungskameras ... 84
  - UEFI ... 117
  - USB-Steckverbinder ... 81, 82, 84
  - Updates anzeigen ... 11, 19
- V
  - VEEAM-Backup ... 132-135
  - Video- und Geräteverbinder ... 82
  - VDSL-Vectoring ... 97
  - Videobearbeitung ... 191
- W
  - Windows-Dienste starten oder beenden ... 11, 191
  - Windows PE, Laufwerksbuchstabe ... 161, 163
  - Windows-Product-Key-Viewer ... 18
  - Windows Update Delivery Optimization (WUDO) ... 15
  - WMIC ... 17
- wuauserv ... 173
- X
  - Xcopy ... 13
- Y
- Z
  - Zeitzone anzeigen ... 13
  - Zwei-Faktor-Authentiisierung ... 24
- 0..9
  - 3G ... 190
  - 4G ... 190
  - 5G ... 188-190