Nr. 170/September 2021 € 5,00 ISSN 1022-1611

QCOS

CLUBCOMPUTER · DIGITAL SOCIETY

Österreichische Post MZ 16Z040679 M ClubComputer, Siccardsburggasse 4/1/22 1100 Wien

CLUBSYSTEM

WINDOWS 10 TEIL 4

14 Datenträger, Start, Notfall
15 Sicherheitseinstellungen
17 Bedienung der Tastatur

Inhalt

LiesMich

1 **Cover**
Franz Fiala

Windows begleitet uns nun schon seit fast 30 Jahren. Christian Zahler ermöglicht uns eine sehr ausführliche Beschreibung in mehreren Teilen

2 **Liebe Leser, Inhalt**
Franz Fiala

2 **Impressum, Autoren, Inserenten, Services**

ClubSystem

2 **Windows-10 Inhalt**
Christian Zahler

3 **14 Datenträger, Start, Notfall**
Christian Zahler

28 **15 Sicherheitseinstellungen**
Christian Zahler

37 **17 Bedienung der Tastatur**
Christian Zahler

41 **Inhaltsverzeichnis (nur online in PDF-Datei)**
Christian Zahler

Windows-10 Inhalt

Christian Zahler

Kapitel	PCNEWS-Seite	
01	167-07	Das Betriebssystem Microsoft Windows 10
02	167-11	Informationsquellen und Hilfe
03	167-12	Windows 10-Installation
04	167-20	An- und Abmeldung, Benutzerkonten und Kennwörter
05	167-23	Desktop, Startmenü, Taskleiste, Dateimanagement
06	168-07	Softwareinstallation und -deinstallation
07	168-09	Windows 10-Verwaltung
08	168-20	Windows 10 im Netzwerk
09	169-04	Benutzerverwaltung und Anmeldung
10	169-14	Rechte und Berechtigungen
11	169-23	Fernwartung und Fernzugriff
12	169-26	Windows 10-Features mit Windows Server 2016/2019
13	169-27	Drucker
14	170-03	Datenträgerverwaltung, Startvorgang und Notfallwiederherstellung
15	170-28	Windows 10-Sicherheitseinstellungen
16	168-25	Virtualisierung - Client Hyper-V
17	170-37	Bedienung der Tastatur

Autoren

***Fiala** Franz Dipl.-Ing. 1948* **1,2**

Präsident von ClubComputer, Leitung der Redaktion und des Verlags der PCNEWS, Lehrer für Nachrichtentechnik und Elektronik i.R.
Werdegang Arsenal-Research, TGM Elektronik
Absolvent TU-Wien, Nachrichtentechnik
franz.fiala@clubcomputer.at
http://fiala.cc/

***Zahler** Christian Ing. Mag. 1968* **3-39**

Erwachsenenbildung, MCSE, Lehrer für Elektro– und Automatisierungstechnik, Technische Mechanik und Informatik am Francisco-Josephinum Wieselburg
Firma HBLFA Francisco-Josephinum; WIFI
Absolvent TU-Wien
office@zahler.at
http://www.zahler.at/

Inserenten

techbold **40**

Impressum

Impressum, Offenlegung

Richtung Auf Anwendungen im Unterricht bezogene Informationen über Personal Computer Systeme. Berichte über Veranstaltungen des Herausgebers.
Erscheint 4 mal pro Jahr: Mär, Jun, Sep, Nov
ISSN 1022-1611
Herausgeber und Verleger **ClubComputer**
Siccardsburggasse 4/1/22 1100 Wien
01-6009933-11 FAX:-12
buero@clubcomputer.at
https://clubcomputer.at/
ZVR: 085514499
IBAN: AT74 1400 0177 1081 2896
Mitgliedsbeitrag 2019: 46,-Euro
Konto: AT74 1400 0177 1081 2896
oder
PayPal *office@clubcomputer.at*

Digital Society
Graben 17/10 1010 Wien
01-314 22 33
info@DigiSociety.at
https://digisociety.at/
ZVR: 547238411
IBAN: AT45 3266 7000 0001 9315

Druck **Ultra Print**
Pluhová 49, SK-82103 Bratislava
http://www.ultraprint.eu/

Versand 16Z040679 M
PDF-Version *http://d.pcnews.at/_pdf/n170.pdf*

Liebe Leser!

Franz Fiala

Windows 10 Teil 4

Wir schließen unseren Lehrgang über Windows 10 von **Christian Zahler** mit den Kapiteln **14 Datenträger, Start, Notfall, 15 Sicherheitseinstellungen** und **17 Bedienung der Tastatur** ab (Seite 3 bis 39).

Clubabende

Dienstag, 7. September, 18:00
Mittwoch, 22. September, 18:00
Dienstag, 5. Oktober, 18:00
Dienstag, 19. Oktober, 18:00
Dienstag, 9. November, 18:00
Mittwoch, 24. November, 18:00

Franz Fiala

Services

http://buero.clubcomputer.at?svc=xx|yyy

Diese Adresse zeigt alle Aspekte einer Mitgliedschaft bei ClubComputer. Online sind alle Inhalte menügeführt. Das Kürzel ist wichtig für den Verweis auf eine konkrete Seite.

Wer lieber ein gedrucktes Dokument liest, kann ein solches über den Druck-Button rechts oben herstellen. Über den Menü-Button kann man das Menü ausblenden, über den Link-Button kann man über einen QR-Code die Seite am Handy anzeigen lassen. Über ◂▸ kann man im Verlauf der bereits besuchten Seiten blättern.

In der PDF-Version dieser Ausgabe führen die Links direkt zu der betreffenden Seite.

Verein
cc|clubcomputer · cc|finanzen · cc|history · cc|hotline · cc|konto · cc|mitglieder · cc|support · cc|vorstand ·

Öffentlich
at|wissen · cc|allapps · cc|exweb · cc|inhalte · cc|newsletter · cc|wapps · pc|123 · pc|pdf ·

Persönlich
at|asp · at|domain · at|drive · at|ftp · at|mail · at|panel · at|php · at|press · at|server ·

Extern
at|facebook · at|status · cc|facebook · cc|medien · cc|youtube · ds|facebook · ds|medien · ds|youtube ·

Druck
cc|folder · cc|pp · cc|visit · ds|folder · pc|news ·

Partner
at|cccat · at|htl3r · cc|adim · cc|jix · cc|kultur · cc|mcca · cc|metro · cc|techbold · cc|tgm · ds|digisociety · pc|mtm · pc|pcnews · pc|ultraprint ·

Wir
cc|calendar · cc|heuriger · cc|meating · cc|weihnacht · ds|digitalk ·

Du
cc|card · cc|clubid · cc|mitmachen · cc|webfree · cc|welcome ·

Hilfe
cc|statuten · xx|hilfe · xx|links · xx|pages · xx|sitemap · xx|standorte ·

14 Datenträger, Start, Notfall

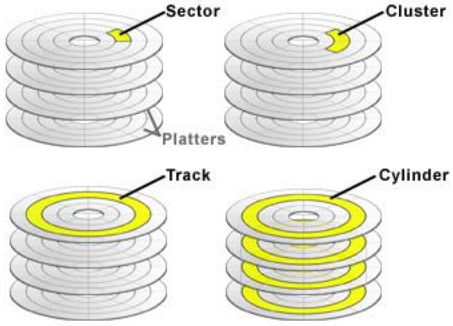
Christian Zahler

14.1 Datenspeicherung auf Datenträgern

Um Daten auf Datenträgern wie Festplatten, USB-Laufwerken etc. speichern zu können, müssen zwei Aktionen durchgeführt werden:

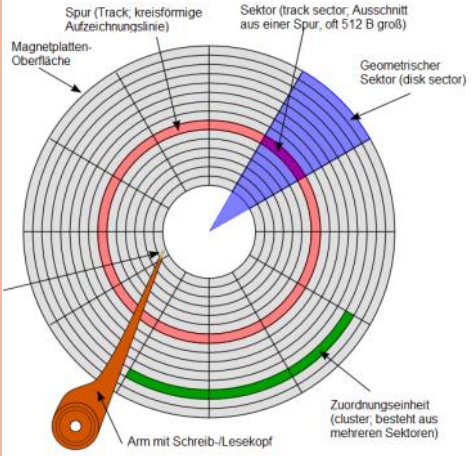
- **Partitionierung:** Bei der Partitionierung wird die Festplatte in Volumes (logische Laufwerke) unterteilt, auf die von Betriebssystemen aus zugegriffen werden kann.
- **Formatierung:** Die Formatierung bewirkt, dass auf einem Volume ein Dateisystem installiert wird. Dateisysteme sind notwendig, damit gespeicherte Daten physisch lokalisiert werden können.

Grundlegender Aufbau von Festplattensystemen: Die meisten Festplatten benutzen die Ober- und Unterseite der Scheiben und verfügen über mehrere Magnetscheiben. Die Schreib-/Leseköpfe für alle Oberflächen sind als Einheit montiert, sie können sich nicht unabhängig bewegen. Deshalb liegen die Spuren auf den Plattenoberflächen exakt übereinander. Ein Satz von übereinander liegenden Spuren trägt den Namen Zylinder (engl. cylinder).



Grafik: https://stackoverflow.com/questions/32642016/chs-to-lba-mapping-disk-storage

Spuren und Sektoren
(Quelle: http://lnx.cx/docs/vdg-2/html/apb.html, adaptiert)



Die drei Begriffe Zylinder (oder Spur), Kopf und Sektor spielen bei der Verwaltung von Festplatten eine zentrale Rolle. Denn über die Angabe dieser drei Werte lässt sich jede Stelle auf der Festplatte eindeutig adressieren. Diese **CHS-Notation** war bis etwa 1997 Standard und wurde auch danach noch für Festplatten kleiner 8 GByte verwendet. Die Zählweise beginnt bei Spuren und Köpfen bei 0, Sektoren starten bei 1. Statt des Begriffs Head ist oft auch Seite im Gebrauch, denn jeder Schreib-/Lesekopf korrespondiert ja mit einer Seite einer Magnetscheibe der Festplatte.

Heute wird statt der CHS-Notation meist die **Logische Blockadressierung (LBA,** englisch *„Logical Block Addressing“)* verwendet. Die Blöcke der Festplatte werden im Gegensatz zur dreidimensionalen Zylinder-Kopf-Sektor-Adressierung (CHS) unabhängig von der Geometrie adressiert. Dabei werden die Blöcke beim LBA einfach gezählt, beginnend mit Null.

Bei LBA wird zwischen 28 und 48 bit unterschieden. Das 28-bit-LBA ermöglicht lediglich 137 GB große Festplatten. Als Erweiterung wird mit ATA-6 eine 48-bit-Adressierung (48-bit-LBA) eingeführt, mit der 281 474 976 710 656 Blöcke oder 144 PB adressiert werden können (512 Byte pro Block zugrunde gelegt). 48-bit LBA kommt bei den Festplatten mit Kapazitäten von mehr als 137 GB zum Zuge.

Die kleinste ansprechbare Einheit auf einer Festplattenpartition wird als **Zuordnungseinheit** (engl. *allocation unit*; auch als *Cluster* bezeichnet) bezeichnet. Die Unterteilung in Zuordnungseinheiten wird bei der Formatierung vorgenommen; die Clustergröße hängt vom verwendeten Dateisystem und der Gesamtpartitionsgröße ab. Dateien können immer nur **Vielfache von Clustern** belegen; beträgt die Clustergröße also 32 KB, so benötigt eine 33 KB große Datei 2 Cluster (31 KB bleiben ungenutzt).

Die tatsächlich belegte Größe auf einem Datenträger lässt sich in den Dateieigenschaften feststellen:

Größe:	5 Bytes (5 Bytes)
Größe auf Datenträger:	32,0 KB (32.768 Bytes)

Man unterscheidet die Partitionsformate MBR und GPT:

- **MBR-Datenträger** *(Master Boot Record)* können das Volumes mit einer Größe von bis zu 2 Terabyte und bis zu 4 Primärpartitionen pro Datenträger (oder 3 Primärpartitionen, eine erweiterte Partition und eine unbegrenzte Anzahl logischer Laufwerke) verwalten.
- **GPT-Datenträger** sind Datenträger des GPT-Partitionstyps (auch GUID-Partitionstabelle) mit einer Größe von maximal 18 Exabyte und bis zu 128 Partitionen. GUID Partition Table (GPT) ist ein Standard für das Format von Partitionstabellen auf Festplatten. Die Spezifikation ist Teil des EFI-Standards (EFI = Extensible Firmware Interface), der das BIOS in PCs ersetzen sollte. GPT ist somit der Nachfolger der MBR-Partitionstabellen.

  Im Gegensatz zu MBR-Datenträgern werden alle Daten in Partitionen abgelegt – auch die für den Betrieb der Plattform zwingend notwendigen (MBR-Datenträger sichern diese in unpartitionierten oder versteckten Sektoren). GPT -Datenträger besitzen redundante Primär- und Sicherungspartitionstabellen; dies erhöht die Integrität der Daten.

  Während im MBR ursprünglich mit dem *Cylinder Head Sector*-Verfahren adressiert wurde, verwendet die GPT *Logical Block Addressing* mit 64 Bit, so dass Festplatten bei 512 Byte Sektorgröße bis zu einer Gesamtgröße von 18 Exabyte adressiert werden und diese in bis zu 128 Partitionen aufgeteilt werden können.

14.1.1 MBR-Datenträger

Der Master Boot Record (MBR): Damit überhaupt mehrere Betriebssysteme auf einer Festplatte Platz finden, muss sich diese in Bereiche aufteilen lassen. Und die exakte Position dieser Bereiche muss an einer allgemein bekannten Stelle der Festplatte gespeichert sein: in Spur 0, Seite 0, Sektor 1. Dort ist bei jeder Festplatte im PC der *Master Boot Record*, kurz MBR, gespeichert.

Adresse		Funktion / Inhalt	Größe (Bytes)
hex	dez		
0x0000	0	Boot-Loader	max. 440
0x01B8	440	Disk-Signatur (seit Windows 2000)	4
0x01BC	444	Null (0x0000)	2
0x01BE	446	**Partitionstabelle (4 Einträge à 16 Byte)**	64
0x01FE	510	55_{hex} MBR-Signatur (0xAA55)	2
0x01FF	511	AA_{hex}	
Gesamt			**512**

Partitionstabelle: Ein einzelner Eintrag in einer Partitionstabelle hat ebenfalls einen festen Aufbau und ist 16 Byte lang.

Ein solcher Eintrag ist wie folgt gegliedert:

Adresse (Hex)	Größe (Bytes)	Inhalt
0x00	1	Bestimmt, ob Partition gestartet werden kann oder nicht (80hex=bootfähig, 00hex=nicht bootfähig)
0x01	3	CHS-Eintrag des ersten Sektors
0x04	1	Typ der Partition (Dateisystem / Partitionstyp)
0x05	3	CHS-Eintrag des letzten Sektors
0x08	4	Startsektor (relativ zum Anfang der Festplatte, oder zur erweiterten Partitionstabelle)
0x0C	4	Anzahl der Sektoren in der Partition

Unbenutzte Einträge sind mit Nullen gefüllt.

In Byte 0 zeigt der Wert 80h (das oberste Bit ist gesetzt) an, dass diese Partition die Bootpartition mit einem Betriebssystem ist. Die Master-Boot-Routine wertet dieses Byte aus, um das Betriebssystem zu finden.

Die Bytes 1 bis 3 enthalten die Startposition der Partition: Kopf, Spur und Sektor. Das gilt für Festplatten bis zu einer Größe von 8 GByte. Größere Festplatten verwenden stattdessen die Bytes ab Position 7. Hier ist jeweils als 32-Bit-Zahl die Position des erstens Sektors der Partition (bezogen auf den Plattenanfang) und die Länge der Partition gespeichert. Mit den 32-Bit-Adressen sind Festplattengrößen bis 2048 GByte möglich.

Das Byte 4 spielt eine wichtige Rolle: Es enthält die Typkennung der Partition. Jedes Betriebssystem benutzt ein Dateisystem, um seine Verzeichnisse und Dateien auf der Festplatte zu organisieren. Der Typ gibt an, um welche Art Dateisystem es sich handelt. Die gebräuchlichsten Systeme sind: (Tabelle oben mitte)

Betriebssysteme der Windows NT-Reihe kümmern sich nicht um die Typkennung. Sie analysieren den Inhalt der Partition (genau gesagt: deren Partitionssektor/Bootsektor) und binden eine erkannte Partition, auf die sie zugreifen können, automatisch ein. Es ist nicht notwendig, dass die Reihenfolge in der Partitionstabelle der physikalischen Reihenfolge auf der Festplatte entspricht. Die erste Partition im MBR kann durchaus in der Mitte der Festplatte bei Spur 600 beginnen.

Typbyte (hex)	Dateisystem
0x00	leer/unbenutzt
0x01	FAT12 (Floppy Disks)
0x04	FAT16 < 32 MiB
0x05	erweiterte Partition
0x06	FAT16 > 32 MiB
0x07	HPFS (OS/2) oder NTFS (Windows NT)
0x0B	FAT32
0x0C	FAT32 mit BIOS-Extensions
0x0E	FAT16 > 32 MiB mit BIOS-Extensions
0x0F	erweiterte Partition mit BIOS-Extensions
0x12	OEM Partition für Konfiguration, Diagnose, BIOS-Erweiterung (für Microsoft-Betriebssysteme unsichtbar)
0x42	Dynamischer Datenträger
0x82	Linux Swap / Solaris 2.6 X86 bis Solaris 9 X86
0x83	Linux Native
0x8E	Linux LVM
0xA5	FreeBSD
0xA6	OpenBSD
0xA9	NetBSD

Primäre und erweiterte Partitionen

Insgesamt bietet die Partitionstabelle des MBR Platz für vier Partitionen. Grundsätzlich gibt es zwei verschiedene Arten von Partitionen: primäre und erweiterte.

- Eine **primäre Partition** verweist direkt auf einen Bereich der Festplatte, der Dateien enthält. Meistens sind Betriebssysteme in primären Partitionen installiert, vor allem Microsoft-Systeme setzen dies sogar zwingend voraus. Die Definition ist etwas umständlich: Eine primäre Partition ist immer in der Partitionstabelle des MBR eingetragen und nicht durch die Typkennung als erweiterte Partition ausgewiesen.
- Eine **erweiterte Partition** enthält im Gegensatz dazu keine Dateien, sondern ist quasi ein Container für weitere Partitionen. Die Typkennungen 05h oder 0Fh weisen eine solche erweiterte Partition aus. Eine Partition innerhalb einer erweiterten Partition ist ein logisches Laufwerk. Durch diesen Kniff ist es möglich, mehr als vier Partitionen pro Festplatte zu realisieren. Für Microsoft-Betriebssysteme sind insgesamt bis zu 23 logische Laufwerke erlaubt, denn mehr Laufwerksbuchstaben ab C gibt es nicht.

Anmerkung: Über Laufwerkspfade, die eine Zuordnung einer Partition ohne eigenen Laufwerksbuchstaben zu einem Unterverzeichnis ermöglichen, ist es möglich, mehr als 23 logische Laufwerke anzusprechen. Außerdem können A und B auch für Festplattenpartitionen verwendet werden, falls keine Diskettenlaufwerke vorhanden sind.

Jede erweiterte Partition enthält einen Partitionssektor, der in seinem Aufbau exakt dem MBR entspricht. Allerdings fehlt hier die Master-Boot-Routine, es wird nur die Partitionstabelle genutzt. In diesem Partitionssektor haben wiederum vier Partitionen Platz. Wie erreicht man dann aber 23 logische Laufwerke? Eine erweiterte Partition nutzt immer nur zwei Einträge ihrer Partitionstabelle: Der Erste beschreibt die Position des logischen Laufwerks, der Zweite die Position einer zusätzlichen erweiterten Partition. Diese wiederum bietet Platz für ein logisches Laufwerk und so fort. So entsteht quasi eine Kette von erweiterten Partitionen, die jeweils ein logisches Laufwerk enthalten. Dabei ist die erste erweiterte Partition (die im MBR definiert ist) so groß, dass die anderen Partitionen darin Platz finden.

Bootsektor: Innerhalb jeder primären Partition gibt es einen weiteren Sektor, dessen Position immer gleich ist: der Bootsektor. Er liegt im ersten Sektor der Partition und ist damit leicht über die Einträge in der Partitionstabelle zu ermitteln. Jedes Betriebssystem verwendet hier seinen eigenen Aufbau, lediglich einige Daten sind immer identisch. Bei Microsoft-Betriebssystemen ist der Bootsektor weit gehend gleich, im Folgenden deshalb eine Beschreibung der Variante von Windows 98 (Nächste Seite links oben).

14.1.2 GPT-Datenträger

Vergleich der Partitionstabelle eines dynamischen MBR-Datenträgers mit einem GPT-Datenträgers (Nächste Seite rechts oben)

1. MBR-Schutzpartition (Protective MBR; 512 Byte groß)

Im ersten Block des Datenträgers befindet sich ein *Master Boot Record*, in dem der gesamte Platz als eine einzige MBR-Partition hinterlegt ist. Findet ein Betriebssystem, das nur MBR- aber keine GPT-Partitionstabellen lesen kann, den Daten-

Bootsektor bei Windows 98 (512 Byte)

Adresse	Inhalt	Größe
+00h	Sprung zur Bootroutine	3 Byte
+03h	Herstellername und Versionsnummer	8 Byte
+0Bh	Byte pro Sektor	1 Word
+0Dh	Sektoren pro Cluster	1 Byte
+0Eh	Anzahl reservierter Sektoren von der ersten FAT	1 Word
+10h	Anzahl FATs	1 Byte
+11h	Anzahl Einträge im Hauptverzeichnis	1 Word
+13h	Anzahl Sektoren in der Partition. 0000, wenn das Laufwerk über 32 MByte Speicherkapazität hat.	1 Word
+15h	Media Descriptor	1 Byte
+16h	Anzahl Sektoren pro FAT	1 Word
+18h	Sektoren pro Spur	1 Word
+1Ah	Anzahl der Schreib-/Leseköpfe	1 Word
+1Ch	Entfernung des ersten Sektors in der Partition vom ersten Sektor der Festplatte (siehe +0Eh)	1 DWord
+20h	Anzahl der Sektoren, wenn das Laufwerk mehr als 32 MByte Kapazität hat.	1 DWord
+24h	Partitionstyp (80h für primäre Partition)	1 Byte
+25h	reserviert	1 Byte
+26h	Erweiterte Boot-Signatur (immer 29h)	1 Byte
+27h	Datenträger-ID	4 Byte
+28h	Datenträgerbezeichnung	11 Byte
+33h	Dateisystemtyp (12-Bit-FAT oder 16 Bit-FAT)	8 Byte
-1FFh	Boot Routine	Rest

© tecChannel.de

träger, erscheint für dieses der gesamte Platz als belegt.

2. Header der GUID Partitionstabelle:

Erst im zweiten Block beginnt die eigentliche GPT-Information mit der primären Partitionstabelle, die nochmals redundant in den letzten Block der Festplatte geschrieben wird (sekundäre Partitionstabelle). Da im Header der Partitionstabelle auch eine CRC32-Prüfsumme hinterlegt ist, kann im Fehlerfall schnell festgestellt werden, welcher der beiden Header der konsistente ist.

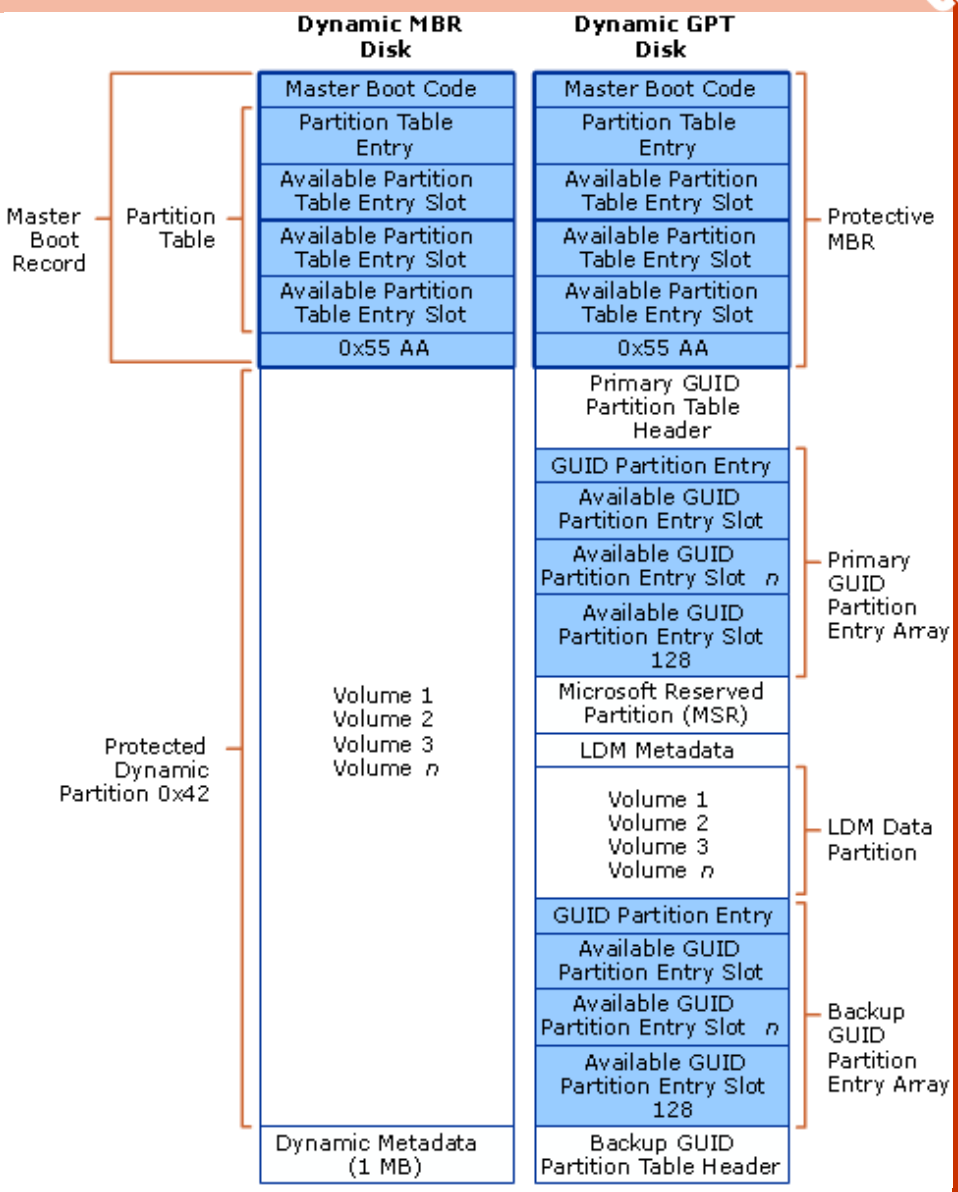
Im Header der GPT sind folgende Informationen abgelegt:

- Signatur (8 Bytes) - „EFI PART“
- Revision (4 Bytes) - 0x00010000
- Header-Größe (4 Bytes)
- Header-Prüfsumme (4 Bytes)
- Reservierter Platz (4 Bytes) - darf nicht belegt sein
- Position der primären Partitionstabelle (8 Bytes)
- Position der sekundären Partitionstabelle (8 Bytes)
- Position des ersten benutzbaren Blocks (8 Bytes)
- Position des letzten benutzbaren Blocks (8 Bytes)
- GUID (16 Bytes)
- Position der Partitionstabelle (8 Bytes)
- Anzahl der Partitionen (4 Bytes)
- Größe des Partitionseintrags (4 Bytes)
- Partitionstabellen-Prüfsumme (4 Bytes)

GUID Partitionseintrag (128 Byte pro Eintrag)

Im Partitionseintrag selbst sind folgende Daten hinterlegt:

- Partitionstyp (ID) (16 Bytes)
- GUID der Partition (16 Bytes)



Dateisystem	Maximale Partition	Berechtigungen	Clustergröße
FAT12 (File Allocation Table): Wurde für Disketten entwickelt und ist bis heute auf 3,5“-Disketten in Verwendung	16 MiB	–	512 B – 4 KiB
FAT16 (File Allocation Table)	2 GiB (unter Windows NT 4 GiB)	–	4 KiB –
FAT32 (verbesserte Variante von FAT, Microsoft unterstützt maximal 32 GiB-FAT32-Partitionen, um NTFS zu fördern); maximale Dateigröße 4 GiB.	32 GiB (theoretisch 16 TiB)	–	512 B – 128 KiB
exFAT (Extended FAT): speziell für Flash-Laufwerke entwickelt	512 TiB (theoretisch 64 ZiB)	–	4 KiB – 32 MiB
NTFS (NT File System): Standard-Dateisystem für Festplatten	256 TiB (theoretisch 16 EiB)	ACL	4 KiB – 2 MiB
ReFS (Resilient File System, „robustes Dateisystem”): maximale Dateigröße 262144 EiB, bessere Fehlerkorrektur, nicht für Windows 10 Home; Einträge basieren auf einem B-Tree-System.	1 YiB (2^{80} Byte)	ACL	4 KiB oder 64 KiB
UDF (Universal Disk Format): vor allem für DVDs verwendetes, plattformunabhängiges Dateisystem			

- Beginn der Partition (8 Bytes)
- Ende der Partition (8 Bytes)
- Attribute (8 Bytes)
- Partitionsname (72 Bytes)

Im Gegensatz zu MBR-Datenträgern werden alle Daten in Partitionen abgelegt - auch die für den Betrieb der Plattform zwingend notwendigen (MBR-Datenträger sichern diese in unpartitionierten oder versteckten Sektoren).

14.2 Formatierung und Dateisysteme

Beim Formatieren wird ein sogenanntes **Dateisystem** (File System) auf die Partition geschrieben. Dateisysteme sind dafür verantwortlich, einem logischen Dateinamen (einschließlich einer hierarchischen „Ordnerstruktur“) den physischen Speicherplatz der Datei auf einem Laufwerk zuzuordnen. Es besteht daher aus einer Datenbank (auch: Tabelle), in der diese Zuordnungen gespeichert sind.

In Microsoft-Windows-Betriebssystemen werden folgende Dateisysteme unterstützt: (Tabelle vorige Seite)

14.2.1 Theorie zu Dateisystemen

FAT-Dateisysteme (File Allocation Table)

Das FAT-Dateisystem verwaltet eine Dateizuordnungstabelle, in der Informationen über die Position aller Dateien gespeichert sind. Aufgrund ihrer grundlegenden Bedeutung für das Dateisystem existieren in der Regel zwei Kopien, um bei Datenverlust noch immer eine funktionsfähige andere FAT zu haben. Mit diversen Programmen ist eine Datenwiederherstellung in vielen Fällen möglich.

FAT-Versionen:

- **FAT12** (wurde für Disketten aller Art verwendet)
- **FAT16** (wird heute meist auf allen Arten von mobilen Datenträgern verwendet, die kleiner als 2 GiB sind)
- **FAT32** (wird z. B. in allen Arten von mobilen Speichern von mehr als 2 GB Kapazität genutzt. Von neueren DOS-Systemen, Windows 9x/ME und Windows NT-Versionen ab 2000 unterstützt. FAT32 verwendet 32 bit-Clusterkennungen, reserviert allerdings die oberen 4 bit, somit sind 28 bit-Clusteradressen im Einsatz. Die Maximalgröße eines FAT32-Clusters beträgt 32 KB. FAT32 hätte theoretisch also die Fähigkeit, 8 TB große Partitionen zu adressieren; die Implementierung ab Windows 2000 begrenzt die Maximalgröße für FAT32-Partitionen allerdings auf 32 GB. (Sollte eine FAT32-Partition größer als 32 GB unter Windows 9x/ME angelegt worden sein, dann wird sie natürlich auch von neueren Betriebssystemen unterstützt.) Ein Volume muss mindestens 65 527 Cluster enthalten, damit das FAT32-Dateisystem verwendet werden kann.

Genauere Informationen über die Beschränkungen des FAT32-Dateisystems findet man im Microsoft-Knowledge Base-Artikel 184006.

Größe der Zuordnungseinheiten für FAT16:

Partitionsgröße	FAT16
(0 ... 32) MB	512 Byte
(33 ... 64) MB	1 KB
(65 ... 128) MB	2 KB
(129 ... 256) MB	4 KB
(257 ... 512) MB	8 KB
(512 ... 1023) MB	16 KB
(1 ... 2) GB	32 KB
(2 ... 4) GB	64 KB (nur unter Windows NT 4.0 unterstützt)
> 4 GB	nicht unterstützt

Größe der Zuordnungseinheiten für FAT32:

Partitionsgröße	FAT32
(0 ... 512) MB	nicht unterstützt
(513 ... 8192) MB	4 KB
(8 ... 16) GB	8 KB
(16 ... 32) GB	16 KB
32 GB	32 KB

NTFS-Dateisystem (New Technology File System)

Aus Sicht des Dateisystems ist alles Teil einer Datei, auch die Informationen des Systems. Die Hauptdatei ist die MFT *(Master File Table)*. In dieser Datei befinden sich die Einträge, welche Blöcke zu welcher Datei gehören, die Zugriffsberechtigungen und die Attribute. Jede Eigenschaft einer Datei ist unter NTFS ein Attribut, auch der eigentliche Dateiinhalt.

Sehr kleine Dateien und Verzeichnisse werden in der MFT direkt abgespeichert. Größere Dateien werden dann als Attribut in einem Datenlauf gespeichert.

Beim Formatieren der Festplatte wird für die MFT ein fester Platz reserviert, der nicht von anderen Dateien belegt werden kann. Wenn dieser voll ist, beginnt das Dateisystem freien Speicher vom Datenträger zu benutzen, wodurch es zu einer Fragmentierung der MFT kommen kann. Standardmäßig wird ein reservierter Bereich von 12,5 % der Partitionsgröße angenommen. Es sind jedoch auch Werte von 25 %, 37,5 % und 50 % konfigurierbar.

Beim Speichern von Meta-Daten wird ein Journal geführt. Das bedeutet, dass eine geplante Aktion zuerst in das Journal geschrieben wird. Dann wird der eigentliche Schreibzugriff auf die Daten ausgeführt und abschließend wird das Journal aktualisiert. Wenn ein Schreibzugriff nicht vollständig beendet wird, zum Beispiel wegen eines Stromausfalls, muss das Dateisystem nur die Änderungen im Journal zurücknehmen und befindet sich anschließend wieder in einem konsistenten Zustand.

Bis Windows 8 wurde das Journal **`$LogFile`** in der Version 1.1 geführt, Windows 8.1/Windows 10 verwenden eine neue Version 2.0, die mit der älteren Version inkompatibel ist.

NTFS verwendet 64 bit-Clusterkennungen. Das würde eine Maximal-Partitionsgröße von 16 EB (= 6,7 Mrd. GB) möglich machen; allerdings begrenzt Windows die Größe eines NTFS-Volumes auf einen Umfang, der mit 32 bit-Clusteradressen adressierbar ist, also auf ca. 256 TB. In diesem Fall beträgt die Clustergröße 64 KB.

NTFS-Versionen

- NTFS 1.X - Windows NT 3.1, 3.5 und 3.51
- NTFS 2.X - Windows NT 4.0
- NTFS 3.0 - Windows 2000
- NTFS 3.1 - Windows XP, Windows 2003, Windows Vista, Windows Server 2008 (R2), Windows 7, Windows 8, Windows 8.1, Windows 10. Diese Version wird manchmal auch als Version 5 bezeichnet.

Größe der Zuordnungseinheiten für NTFS:

Partitionsgröße	Voreingestellte NTFS-Clustergröße
(0 ... 512) MB	512 Byte
(513 ... 1024) MB	1 KB
(1025 ... 2048) MB	2 KB
> 2 GB	4 KB

Größere Zuordnungseinheiten sind beim Formatieren manuell konfigurierbar. So ist etwa für Volumes, die SQL Server-Datenbanken aufnehmen sollen, eine Größe von 64 KB empfehlenswert, da SQL Server immer in 64 KB-Einheiten liest bzw. schreibt.

ReFS (Resilient File System)

Das ReFS (Resilient File System, deutsch etwa „robustes Dateisystem“) ist in der Lage, defekte Dateien automatisch zu reparieren. Außerdem gilt ReFS im Vergleich zu NTFS als wesentlich unempfindlicher gegenüber Abstürzen des Betriebssystems oder dem Ausschalten des Servers ohne vorheriges Herunterfahren. Das neue Dateisystem arbeitet optimal mit den neuen

Beschreibung	FAT16	FAT32	NTFS
Maximale Dateigröße	2^{32} – 1 Byte	2^{32} – 1 Byte	2^{44} – 64K bytes (geplant bis 2^{64} – 1 Byte)
Anzahl Dateien pro Volume	2^{16}	2^{28}	2^{32} – 1
Minimale Volume-Größe	4085 Zuordnungseinheiten	65535 Zuordnungseinheiten	1 MB
Maximale Volume-Größe	65536 – 12 Zuordnungseinheiten; maximale Partitionsgröße: 2 GB	Theoretisch: 2^{28} Zuordnungseinheiten. **Ab Windows 2000:** Formatierung bis 32 GB, Zugriff auf größere Einheiten **Windows ME:** Bis zu 2^{28} – 12 Zuordnungseinheiten **Windows 95/98:** 4,177,918 Zuordnungs-	Theoretisch: 2^{64} Zuordnungseinheiten Aktuell: 2^{32} Zuordnungseinheiten
Größe einer Zuordnungseinheit	Für alle Dateisysteme: **Windows NT-Linie:** zwischen 2^{9} (512) und 2^{16} (65536) Byte **Windows 95/98/ME:** zwischen 2^{9} (512) und 2^{15}		
Verzeichnisgröße	2^{16} – 2 physikalische Verzeichniseinträge, allerdings spezielle Einschränkungen für das Stammverzeichnis	2^{16} – 2 physikalische Verzeichniseinträge	Keine Begrenzung

Speicherpools zusammen. Speicherpools erlauben das Zusammenfassen mehrerer physischer Datenträger zu einem logischen Pool.

Das neue Dateisystem ReFS ist auf Windows 10 und Windows Server 2016/2019 verfügbar, wobei das Erstellen von ReFS-Volumes nur für Windows 10 Pro/Enterprise-Versionen möglich ist. Neben der automatischen Korrektur benötigt das neue Dateisystem keine langen Ausfallzeiten mehr durch Reparaturmaßnahmen und kann zur Reparatur heruntergefahren werden.

In ReFS lassen sich Metadaten und Prüfsummen von Dateien wesentlich effizienter integrieren als in Vorgängerversionen. Das Dateisystem protokolliert Änderungen in Dateien und kann ursprüngliche Änderungen speichern. NTFS überschreibt ältere Versionen von Metadaten und Prüfsummen unwiederbringlich. Das heißt, Daten gehen nicht verloren, sondern können im Dateisystem wieder hergestellt werden, auch wenn Anwender Dateien geändert haben. Das funktioniert ähnlich wie bei den Schattenkopien in NTFS, ist aber nicht vom Erstellen solcher Schattenkopien abhängig, sondern läuft ständig im Hintergrund. Die Technik entspricht in etwa den transaktionalen Datenbanken. Der Vorteil dabei ist, dass auch bei Stromausfällen keinerlei Daten auf ReFS-Datenträgern verloren gehen können.

Allerdings handelt es sich bei ReFS um kein Dateisystem, das Daten in Datenbanken speichern kann. Microsoft hat nur einige Vorteile des transaktionalen Systems integriert. ReFS unterstützt keine Wechseldatenträger.

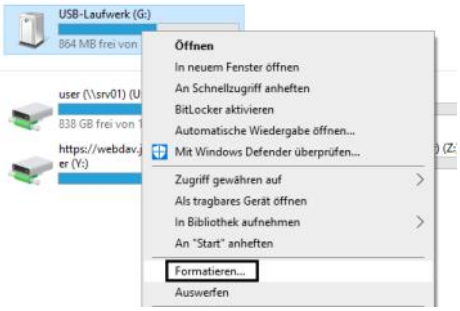
ReFS trägt auch den immer größeren Dateien und Festplatten Rechnung. Das System unterstützt eine in nächster Zeit unerreichbare Größe von Dateien und Festplatten, die weit über die Möglichkeiten von NTFS hinausgehen. Laut Angaben von Microsoft beherrschen ReFS-Datenträger eine Größe von 16 Exabyte. Ordner auf ReFS-Dateiträgern können nahezu eine unbegrenzte Anzahl Dateien speichern, und auch die Anzahl der Ordner kann mehrere Trillionen betragen. Dateinamenkönnen eine Länge von 32.000 Zeichen erreichen. Die Leistung soll durch große Dateien aber nicht einbrechen, dafür sorgt die neue Technologie im Hintergrund, die Daten effizienter speichert.

Wie NTFS lassen sich auch in ReFS Berechtigungen auf Basis der Zugriffssteuerungslisten (ACL) vergeben. Daten können Anwender weiterhin mit BitLocker verschlüsseln. ReFS unterstützt aber keine Komprimierung von Dateien über das Dateisystem mehr, und auch keine Verschlüsselung einzelner Dateien. Auch Quotas auf dem Datenträger unterstützt ReFS nicht. Microsoft will konsequent wenig verwendete Features aus dem Dateisystem entfernen.

Anwender bemerken bei der Verwendung des neuen Dateisystems keinen Unterschied zu NTFS, die Bedienung ist vollkommen transparent. Auch Entwickler können die standardmäßige API von NTFS für den Zugriff auf ReFS nutzen. Laut Microsoft sollen auch keine Inkompatibilitäten mit aktuellen Anwendungen bestehen. Programme, die mit NTFS funktionieren, sollen auch mit ReFS laufen. Das liegt nicht zuletzt daran, dass die Zugriffsschnittstelle (API), mit der das Dateisystem kommuniziert, dem von NTFS entspricht. Nur die zugrunde liegende Technik ist unterschiedlich. Die Master File Table (MFT) auf ReFS-Datenträgern unterscheidet sich ebenfalls von NTFS.

14.2.2 „Old School"-Formatierung

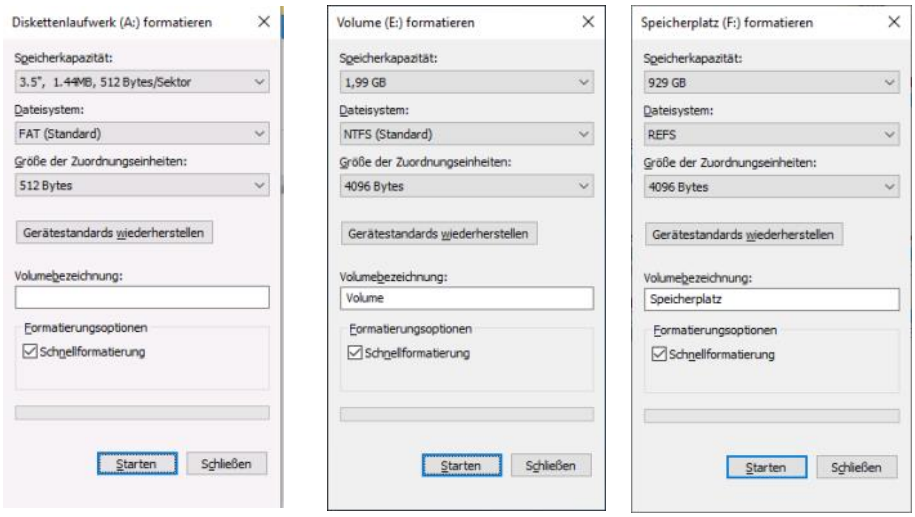
Die älteste Methode, einen Datenträger zu formatieren, steht tatsächlich noch immer zur Verfügung: Klicken Sie im Windows Explorer mit der rechten Maustaste auf ein Datenträgersymbol und wählen Sie den Kontextmenüeintrag **Formatieren**.



Wählen Sie im nun erscheinenden Dialogfeld das gewünschte Dateisystem aus.

Klicken Sie auf Starten, um mit der Formatierung zu beginnen.

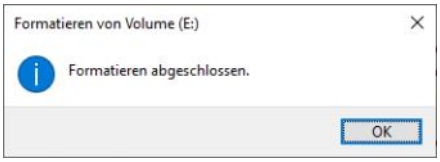
Die Option Schnellformatierung bewirkt, dass die Daten auf dem Datenträger nicht gelöscht werden, sondern nur die Dateizuordnungstabelle neu geschrieben wird. Damit sind die Daten „nicht mehr auffind-



bar“; allerdings können diese mit Datenrettungssoftware wiederhergestellt werden, solange sie nicht durch andere Daten überschrieben wurden.

Es wird ein Hinweis angezeigt, dass die Daten auf dem Datenträger gelöscht werden. Der Formatierungsprozess beginnt, wenn Sie auf Ok klicken.

Nach einiger Zeit erhalten Sie die Erfolgsmeldung:



14.2.3 Datenträgerverwaltung

Datenträger und Dateisysteme werden vom **Dienst für virtuelle Datenträger** verwaltet.

Die Datenträgerverwaltung ist grafisch über die MMC-Konsole **Computerverwaltung – Datenträgerverwaltung** erreichbar (Bild links unten).

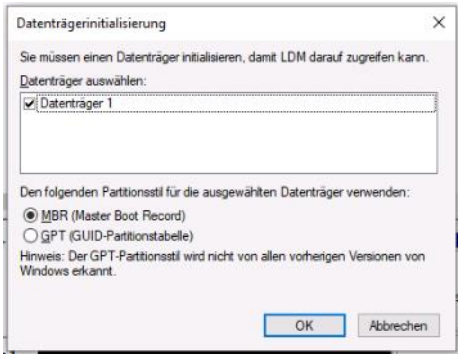
Windows unterscheidet zwei Arten von Datenträgern:

- **Basisdatenträger:** Hier wird ein zu anderen Systemen kompatibler Master Boot Record erstellt und verwaltet. Daher gibt es für Basisdatenträger die Beschränkung auf max. 4 Partitionseinträge in den MBR. Auf Basisdatenträgern können bootfähige primäre und nicht bootfähige erweiterte Partitionen angelegt werden. Um erweiterte Partitionen für die Datenspeicherung nützen zu können, müssen innerhalb dieser Partitionen noch „logische Laufwerke“ definiert werden.
- **Dynamische Datenträger:** Proprietäres Microsoft-System, nicht kompatibel mit anderen Betriebssystemen. Nur auf dynamischen Datenträgern können RAID- oder übergreifende Laufwerke angelegt werden.

Basisdatenträger können ohne Datenverlust in dynamische Datenträger konvertiert werden; der umgekehrte Vorgang ist aber nicht möglich (es würde eine Neupartitionierung erfolgen, die alle bestehenden Daten unzugänglich macht).

Beim Konvertieren von Basis- zu dynamischen Datenträgern wird der Partitionierungsstil geändert. Partitionen auf dynamischen Datenträgern werden vom **LDM (Logical Disk Manager)** verwaltet.

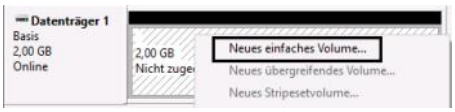
Werden zusätzliche Datenträger (Festplatten) eingebaut, so müssen sie zunächst initialisiert werden. Beim Initialisieren muss der Partitionsstil ausgewählt werden (**MBR** oder **GPT**).



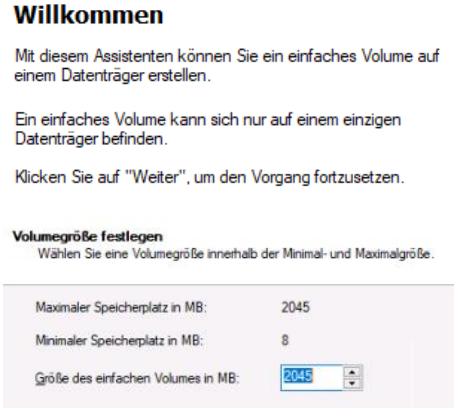
Nach dem Fertigstellen wird der Status des Datenträgers auf **Online** geändert.

14.2.4 Erstellen von einfachen Volumes

Klicken Sie mit der rechten Maustaste in einen als **Nicht zugeordnet** gekennzeichneten Bereich eines Datenträgers, um ein Volume (eine Partition) in diesem Bereich zu erstellen. Für Basisdatenträger wählen Sie **Neues einfaches Volume**.

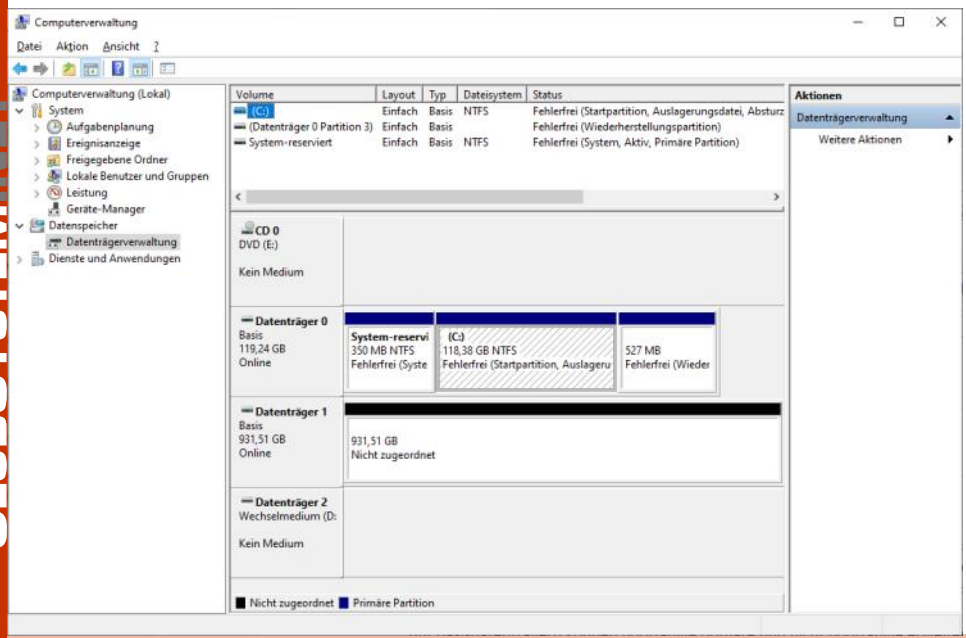


Es startet ein Assistent, der Sie durch den Partitionierungsvorgang führt.

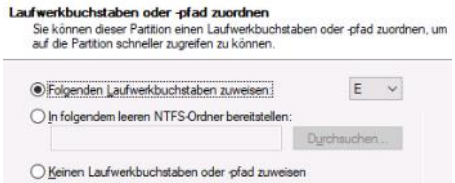


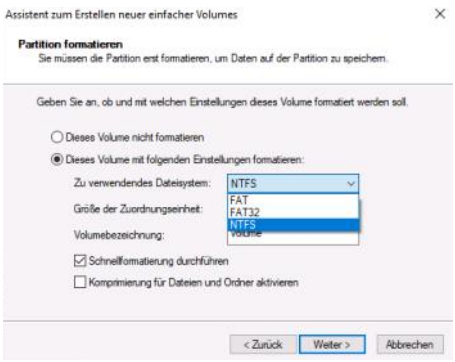
Im nächsten Schritt geht es um die Laufwerkskennung („Laufwerksbuchstaben“):

- Es kann – wie üblich – ein noch nicht verwendeter Laufwerksbuchstabe vergeben werden.
- Es ist auch möglich, die Partition wie einen Ordner auf einer anderen NTFS-Partition erscheinen zu lassen.
- Schließlich kann man auf die Zuordnung



eines Laufwerksbuchstabens verzichten, dies bedeutet aber, dass über den Windows-Explorer **kein Zugriff** auf dieses Volume möglich ist.

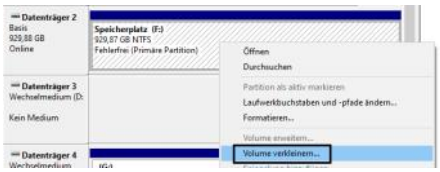


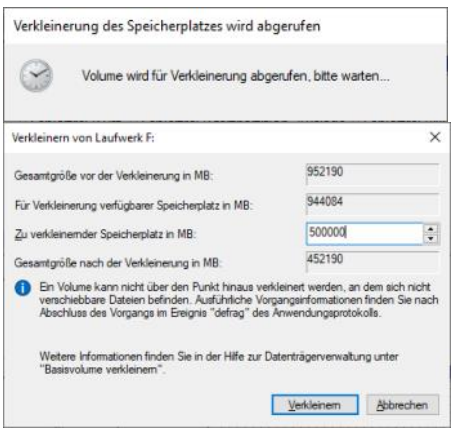


Primäre Partitionen auf Basis-Datenträgern werden in **dunkelblauer Farbe** dargestellt.

14.2.5 Verkleinern von Volumes

Unter bestimmtern Voraussetzungen ist es möglich, bestehende Partitionen zu verkleinern, etwa um Platz für zusätzliche Volumes zu schaffen.





14.3 Dynamische Datenträger und RAID

14.3.1 RAID-Grundlagen

Bereits seit Jahrzehnten war **Datensicherheit** sowie **Zugriffsgeschwindigkeit** im Zusammenhang mit der Verwendung von Festplatten die beiden wichtigsten Themen.

Um nun den Datenzugriff auf Massenspeicher zu beschleunigen und die Datensicherheit zu erhöhen, entwickelten 1987 die Professoren Gibson, Katz und Patterson der Berkeley University den RAID-Standard Die Abkürzung bedeutet **Redundant Array of Inexpensive/Independent Disks**.

Der Begriff **Redundanz** kommt aus dem Lateinischen (redundantia = Überfluss, Überfülle) und bezieht sich in der Informationstechnologie auf mehrfach gespeicherte (also eigentlich überflüssige) Daten, die aber verwendet werden können, um im Fehlerfall Datenverlust zu vermeiden.

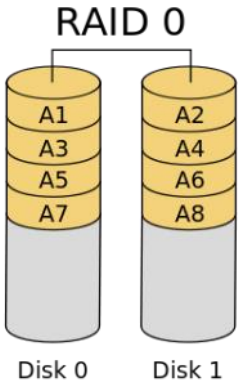
Man unterscheidet **verschiedene „RAID-Levels“,** die entweder Leistung oder Datensicherheit oder beides ermöglichen.

RAID Level 0 (Striping)

Streng genommen keine echte RAID-Implementierung. Bei der Datenspeicherung werden die Daten in „Streifen“ zerteilt, diese Datenstücke werden auf mindestens zwei Platten aufgeteilt.

Zweck: schnellerer Datendurchsatz

Verfügbare Speicherkapazität: 100 %

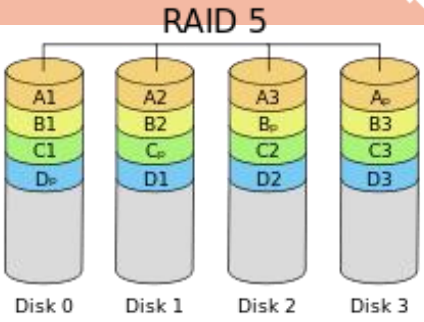


RAID Level 5 (Block Striping with Parity)

Möglich sind RAID 5-Arrays mit mindestens drei, Platten. Die beste Leistung bieten Systeme mit 3, 5 oder 9 Platten.

Die Daten werden (so wie bei RAID 0) in Blöcke zerteilt, zusätzlich werden aber Paritätsinformationen auf alle Platten verteilt geschrieben.

RAID 5 bietet Performancesteigerung bei gleichzeitiger Erhöhung der Betriebssicherheit (eine Platte des RAID 5-Arrays darf ausfallen).



Verfügbare Speicherkapazität:

Laufwerke	Belegt	Verfügbar	Redundanz
3	6 GB	4 GB = 67 %	33 %
4	8 GB	6 GB = 75 %	25 %
5	10 GB	8 GB = 80 %	20 %

Hintergrund – Funktionsweise der Paritätsprüfung

Das Paritätsprüfungsverfahren ist bereits seit vielen Jahren bekannt und ermöglicht die Erkennung und Behebung von Fehlern. Technisch betrachtet, werden die Daten der Nutzlaufwerke über eine logische Exklusiv-Oder-Operation (XOR) verknüpft, das Ergebnis dieser Verknüpfung wird als Paritätsinformation bezeichnet und auf einem eigenen Parity-Laufwerk gespeichert.

Das Ergebnis der Verknüpfung ist dann 1, wenn eine ungerade Anzahl von Bitstellen eine 1 aufweist. Bei einer geraden Anzahl dagegen ist das Ergebnis 0.

Beispiel:

Disk 0	Disk 1	Disk 2	Parität (Disk 3)
0	1	1	0
1	0	0	1

In der ersten Zeile sieht man, dass zwei Bitstellen 1 sind, also eine gerade Anzahl – daher wird als Paritätsinformation eine 0 gespeichert. In der zweiten Zeile sieht man, dass nur eine Bitstelle 1 ist, eine ungerade Anzahl – daher wird als Parität der Wert 1 gespeichert.

Hinweis: Nur in diesem Beispiel wird die Parität auf Disk 3 gespeichert – wie auf der Grafik ersichtlich ist, werden die Paritätsinformationen auf allen Platten verteilt.

Die Rekonstruktion kann durch eine weitere XOR-Verknüpfung erfolgen.

Beispiel

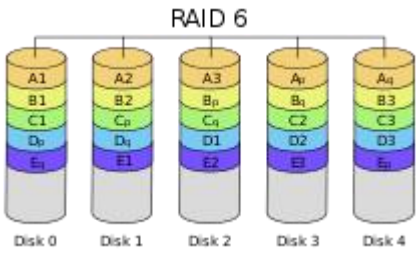
Disk 0	Disk 1	Disk 2	Parität (Disk 3)
0	defekt	1	0
1	defekt	0	1

Nehmen wir an, dass Disk 1 defekt ist – die fehlenden Informationen müssen also wiederhergestellt werden.

Auf Disk 0 ist eine binäre 0 gespeichert, auf Disk 2 eine binäre 1 – also eine ungerade Anzahl von 1-Werten. Wenn also auf Disk 1 eine 0 gespeichert wäre, so müsste die Parität 1 sein; da die Parität aber 0 ist, ergibt sich somit für den fehlenden Wert auf Disk 1 der Wert 1. Analog lässt sich für die zweite Zeile ableiten, dass eine binäre 0 fehlt.

RAID Level 6 (Striping with double Parity)

Ähnliches Konzept wie RAID 5, allerdings werden doppelte Paritätsinformationen verteilt gespeichert, sodass der Ausfall von zwei Platten toleriert wird. Die minimale Anzahl von Platten beträgt 4.



Unter **RAID 10** (genauer: RAID 1+0) versteht man die Kombination von RAID 0 und RAID 1, also ein RAID 0-Array aus zwei Platten, das mit RAID 1-Technologie gespiegelt wird. Dafür sind mindestens 4 Festplatten notwendig.

14.3.2 Hardware- und Software-RAID

RAID-Systeme können hardwaretechnisch oder softwaretechnisch realisiert werden.

- **Hardware-RAID:** Hier wird das Zusammenarbeiten mehrerer Festplatten durch einen **RAID-Controller** organisiert. Solche Controller befinden sich meist in physischer Nähe der verwalteten Festplatten, entweder im Computergehäuse selbst oder als Teil eines Storage-Systems. Hardware-RAID-Systeme sind im Server-Bereich üblich. Moderne RAID-Systeme verfügen über zusätzliche Sicherheits- und Überwachungsmechanismen, wie etwa die Möglichkeit des „Hot Mounting“ (Austausch im laufenden Betrieb) und der laufenden Überprüfung des Zustandes der Festplatten. Ein weiteres Merkmal von modernen RAID-Systemen ist die Integration von eigenem Cache-Speicher, der die Leistungsfähigkeit stark erhöhen kann.
- **Software-RAID**: Die Organisation der Festplatten wird in diesem Fall vom Betriebssystem übernommen. Windows Server-Betriebssysteme bieten seit der Version Windows Server 2000 eine Software-RAID-Implementierung an. Die Festplatten werden zunächst ohne RAID-Controller als sogenannte JBODs *(„just a bunch of disks“)* ins System integriert, dann wird per Software-RAID die RAID-Funktionalität realisiert.

Für welche Variante man sich entscheidet, wird von Kosten-Nutzen-Überlegungen abhängen. Folgende Fragen sollten gestellt werden:

- Wie wichtig – d.h. sicherheitsrelevant – sind Daten?
- Wie oft muss auf die Daten zugegriffen werden?
- Handelt es sich um wenige große oder viele kleine Dateien?

Beachten Sie: In keinem Fall stellen RAID-Systeme einen Ersatz für ein regelmäßiges Backup dar!

14.3.3 Software-RAID mit dynamischen Datenträgern

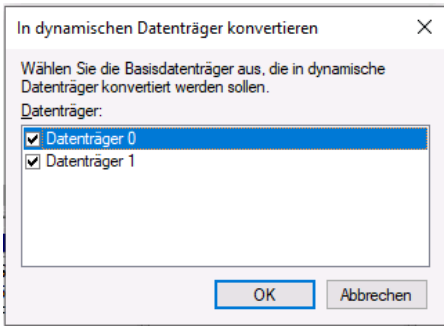
Hinweis: Die Verwendung dynamischer Datenträger wird nicht mehr empfohlen, unter anderem deshalb, weil sich dynamische Datenträger mit „Windows-Bordmitteln“ nicht mehr ohne Datenverlust in Basis-Datenträger zurückkonvertieren lassen. Verwenden Sie stattdessen Storage Pools (siehe 14.4).

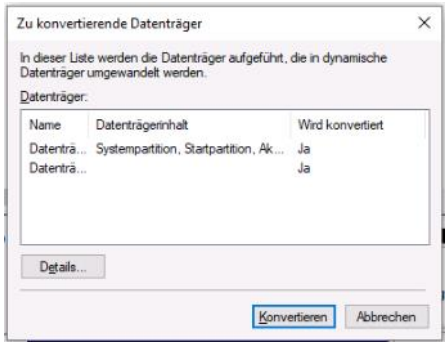
Bei Verwendung dynamischer Datenträger wird von Windows 10 und Windows Server 2016/2019 die Erstellung folgender Volume-Typen unterstützt:

- **Übergreifendes Volume:** Diese Option wird verwendet, wenn der benötigte Platz auf einem Datenträger alleine nicht aufgebracht werden kann. Die Leistung wird nicht erhöht, es wird auch keine Redundanz angeboten. Fällt einer der Datenträger aus, so steht das gesamte Volume nicht zur Verfügung. Ein übergreifendes Volume entspricht dem ***JBOD (Just a Bunch of Disks)-Ansatz***, es wird weder eine Leistungssteigerug noch eine erhöhte Datensicherheit erreicht.
- **Stripeset-Volume** (auch: RAID 0-Datenträger): Diese Technologie arbeitet so, dass die zu schreibenden Daten abwechselnd auf zwei Datenträger verteilt werden. Damit wird – die entsprechende Hardwarekonfiguration – die Schreibleistung erhöht. Auch hier ist keine Redundanz verfügbar - fällt einer der Datenträger aus, so steht das gesamte Volume nicht zur Verfügung.

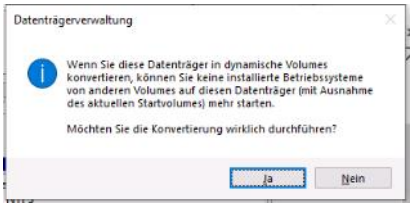
Konvertieren von Basis-Datenträgern in dynamische Datenträger

Klicken Sie dazu den entsprechenden Datenträger mit der rechten Maustaste an und wählen Sie den Kontext-Menüeintrag **In dynamischen Datenträger konvertieren...**:





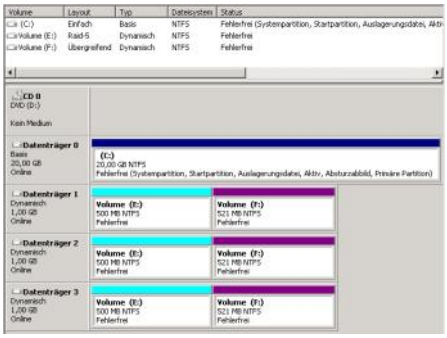
Einfache Volumes auf dynamischen Datenträgern werden in **olivgrüner Farbe** dargestellt.



① Übergreifendes Volume

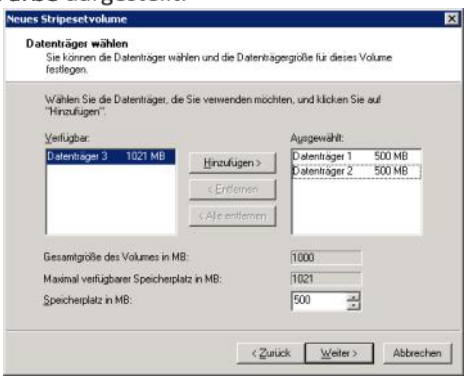
Übergreifendes Volume = Partition, die auf zwei oder mehrere physische Festplatten verteilt ist (untere Abb: Laufwerk F:)

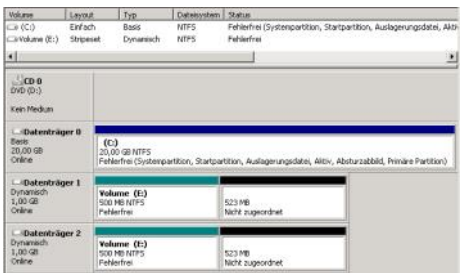
Übergreifende Volumes auf dynamischen Datenträgern werden in **violetter Farbe** dargestellt.



② RAID 0 = Stripeset-Volume (Volume E:)

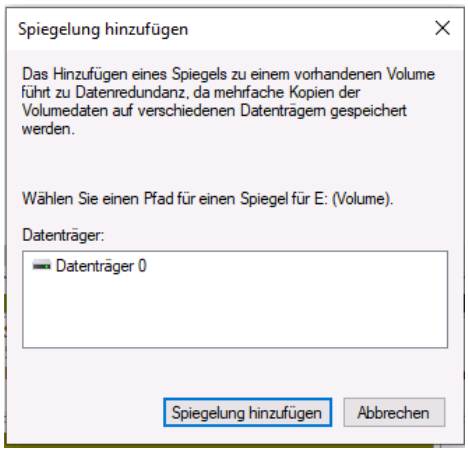
Stripeset-Volumes werden in **blaugrüner Farbe** dargestellt.

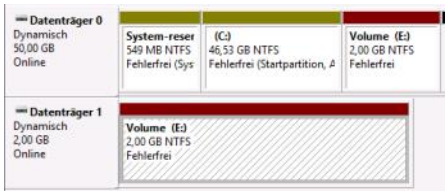




③ RAID 1 = Gespiegeltes Volume (Laufwerk E:)

Gespiegelte Volumes werden in **dunkelroter Farbe** dargestellt.

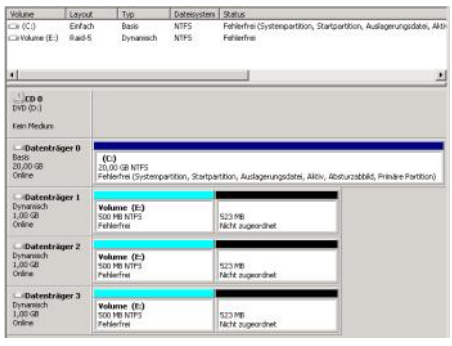




④ RAID 5-Volume (Laufwerk E:)

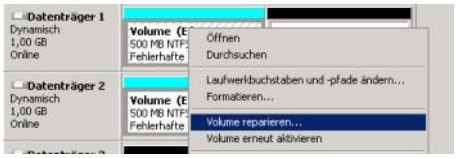
RAID 5-Volumes werden in **hellblauer Farbe** dargestellt.

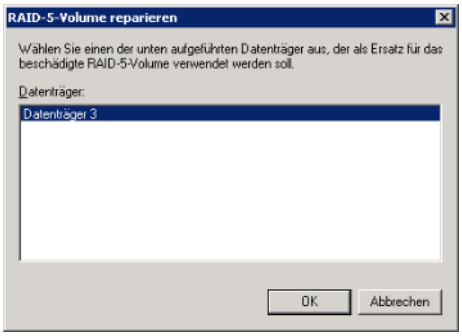
Sie benötigen mindestens 3 Datenträger, um ein RAID 5-Volume zu erstellen.



Fällt eine der mindestens 3 RAID-5-Platten aus, so ist der Zugriff auf das Volume zwar weiterhin möglich, es wird aber die Meldung „Fehlende Redundanz“ angezeigt:

Steht ein Ersatz-Datenträger (in der Abbildung: Datenträger 3) zur Verfügung, so kann das RAID-5-Volume repariert werden:





Strategieüberlegungen: RAID 1 oder RAID 5?

Gespiegelte und RAID 5-Datenträger bieten einen unterschiedlichen Grad an Fehlertoleranz. Die Auswahl der zu implementierenden Lösung hängt vom Grad des benötigten Schutzes und den Hardwarekosten ab. Die Hauptunterschiede zwischen gespiegelten Datenträgern (RAID 1) und RAID 5-Datenträgern liegen bei Leistung und Kosten. Die folgende Tabelle erklärt Unterschiede zwischen den Softwareimplementierungen von RAID 1 und RAID 5.

Gespiegelte Datenträger bieten in der Regel eine vergleichbare Lese- und Schreibleistung wie Einzelfestplatten. RAID 5-Datenträger bieten jedoch eine bessere Leseleistung als gespiegelte Datenträger, insbesondere mit mehreren Controllern, da die Daten auf mehrere Laufwerke verteilt sind. Dadurch, dass die Paritätsinformationen berechnet werden müssen, wird jedoch mehr Arbeitsspeicher benötigt, wodurch sich die Schreibleistung verlangsamen kann.

Gespiegelte Datenträger benötigen den doppelten Speicherplatz, weshalb die Kosten pro Gigabyte (GB) höher sind als bei Laufwerken ohne Spiegelung. Bei Verwendung der Mindestanzahl an Festplatten (drei) belegen RAID 5-Datenträger 33% des verfügbaren Speicherplatzes mit Paritätsinformationen. Werden weitere Festplatten hinzugefügt, wird die Speicherplatzbelegung durch Paritätsinformationen entsprechend gesenkt.

Gespiegeltes Volume (RAID 1)	RAID 5-Volume
Unterstützen FAT und NTFS	Unterstützten FAT und NTFS
Können System- oder Startpartition schützen	Können System- oder Startpartition nicht schützen
Benötigen zwei Festplatten	Benötigen mindestens drei Festplatten und maximal 32 Festplatten
Höhere Kosten pro Megabyte	Niedrigere Kosten pro Megabyte
50 %-ige Speicherbelegung	Mindestens 33 %-ige Speicherbelegung
Gute Schreibleistung	Mittelmäßige Schreibleistung
Gute Leseleistung	Hervorragende Leseleistung
Benötigen weniger Systemspeicher	Benötigen mehr Systemspeicher

14.4 Speicherpools und Speicherplätze (Storage Pools, Storage Spaces)

Ganz neu in Windows 10 ist die Möglichkeit, Speichervirtualisierung zu verwenden. Dies wird mit sogenannten **Speicherpools** bewerkstelligt. Ein Speicherpool ist eine Zusammenfassung mehrerer Festplatten. In einem solchen Speicherpool können Sie mehrere Speicherplätze erstellen. Diese verhalten sich in Windows wie normale Datenträger, lassen sich freigeben, sichern oder mit BitLocker verschlüsseln. Die Daten im Speicherplatz verteilt Windows auf den Festplatten, die im Speicherpool integriert sind.

Damit entsprechen Speicherpools dem **RAID**-Konzept (Redundant Array of Independent Disks).

In der Systemsteuerung finden Sie unter **System und Sicherheit – Speicherplätze** die Anwendung zum Erstellen und Verwalten von Speicherpools (Storage Pools) und Speicherplätzen (Storage Spaces).

Stellen Sie sicher, dass Sie über nicht benützte Datenträger verfügen, die Sie zu einem Speicherpool zusammenfassen können, und klicken Sie dann auf **Neuen Pool und Speicherplatz erstellen**.

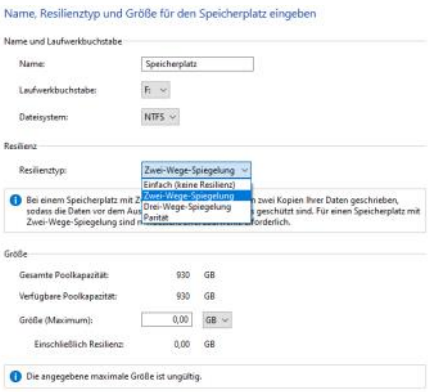
Es werden folgende Arten von Laufwerken unterstützt:

- USB-Laufwerke
- SATA-Festplatten
- SAS-Festplatten

Es wird empfohlen, dass Sie ausschließlich Laufwerke ohne Dateisystem (also weder partitioniert noch formatiert) verwenden.

Wählen Sie alle passenden Laufwerke durch Anklicken des Kontrollkästchens aus und klicken Sie auf **Pool erstellen**.

Es startet ein Assistent, der einige Konfigurationseinstellungen verlangt.



Zunächst legen Sie den **Namen** und den **Laufwerksbuchstaben** fest, mit dem der Speicherplatz in Windows zur Verfügung stehen soll.

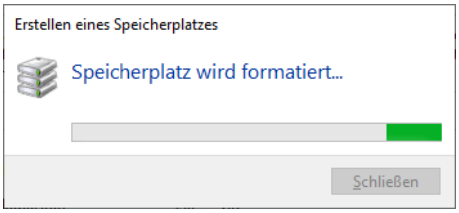
Bei **Resilienz** legen Sie die Ausfallsicherheit des Speicherplatzes innerhalb des Pools fest. Dabei haben Sie folgende Möglichkeiten:

- **Einfach (keine Resilienz; RAID 0):** Diese Einstellung dient vor allem dazu, Speicherplatz auf mehreren Festplatten zu einem einzigen großen Volume zusammenzufassen. Bei dieser Auswahl sind die Daten nicht vor dem Ausfall eines Datenträgers geschützt. Fällt die Festplatte im Pool aus, auf der die Daten gespeichert sind, lassen sich diese nicht mehr verwenden. Sie können sie aber wiederherstellen, wenn Sie den Dateiversionsverlauf konfiguriert haben. Bei dieser Auswahl ist der verwendete Speicherplatz der Daten so groß wie die Daten selbst, da es keine Ausfallsicherheit gibt.
- **Zwei-Wege-Spiegelung (Spiegelung, RAID 1):** Bei dieser Auswahl kopiert Windows 10 automatisch alle Daten auf mindestens zwei Datenträger im Pool, um den Ausfall einer Festplatte zu vermeiden. Dazu muss im Pool natürlich mindestens eine zweite Festplatte enthalten sein. Auf diesem Weg belegen die Daten den doppelten Speicherplatz.
- **Drei-Wege-Spiegelung (doppelte Spiegelung):** Bei dieser Auswahl sichert Windows 10 alle Daten auf bis zu drei physikalische Laufwerke im Pool. Diese Auswahl schützt Sie vor dem Ausfall von zwei Festplatten im Pool. Damit Sie diese Option verwenden können, müssen auch mindestens fünf physikalische Festplatten im Pool integriert sein. Wenn Sie diesen Typ verwenden, belegen die Daten den dreifachen Speicherplatz.
- **Parität (RAID 5):** Diese Auswahl sichert die Daten so, dass im Pool ein Laufwerk verloren gehen kann. Sie brauchen dazu aber mindestens drei Laufwerke im Pool. Die Daten benötigen den doppelten Speicherplatz.

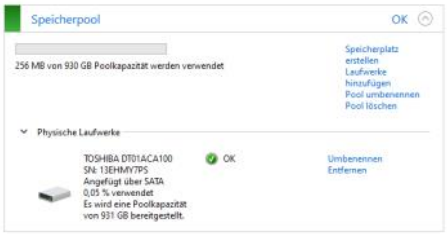
Sie können die Resilienz nachträglich nicht ändern, aber die Größe eines Speicherplatzes den Laufwerksbuchstaben und den Namen. Auch dazu verwenden Sie die Systemsteuerung.

Im unteren Bereich legen Sie fest, wie groß der Speicherplatz im Pool sein darf. Sie können auch mehr Speicherplatz zuweisen, als der Pool zur Verfügung hat. Sobald der Platz ausgeht, erscheint eine Meldung, und Sie können im Pool eine weitere Platte integrieren.

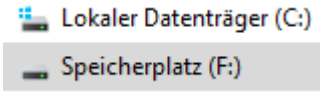
Haben Sie die Auswahl getroffen, lassen Sie mit **Speicherplatz erstellen** den Speicherplatz um den Pool anlegen. Wie bei Speicherpools auch, haben Sie bei Speicherplätzen die Möglichkeit, Einstellungen jederzeit zu ändern.



Speicherplätze sehen Sie in der Steuerung der Speicherpools innerhalb des einzelnen Pools. Haben Sie Pools und Speicherplätze angelegt, erscheinen diese im Explorer.



Der erstellte Speicherplatz wird als normales lokales Laufwerk im Windows-Explorer angezeigt:



14.5 Befehlszeilentools zur Datenträgerverwaltung

14.5.1 Befehlszeilentool diskpart

Dieses sehr umfangreiche Tool bietet interaktive Eingabemöglichkeiten und eine Reihe von Kontexten, die aufgerufen werden können: (Befehlsliste rechts oben)

14.5.2 Befehlszeilentool fsutil

Mit dem **Befehlszeilentool fsutil** können Detailinformationen zu Partitionen (Volumes) abgefragt werden.

Beispiel für die Abfrage von Informationen mit `fsutil`:

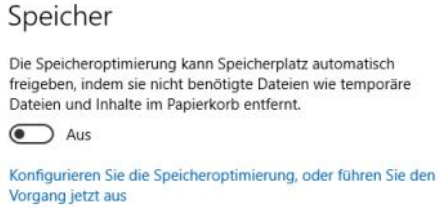
```
C:\>fsutil fsinfo ntfsinfo C:

NTFS-Volumeseriennummer :          0x94708419708403e8
Version :                          3.1
Anzahl der Sektoren :              0x000000000445c7ae
Gesamtzahl Cluster :               0x000000000088b8f5
Freie Cluster :                    0x00000000007a1800
Insgesamt reserviert :             0x0000000000007f10
Bytes pro Sektor :                 512
Bytes pro Cluster :                4096
Bytes pro Dateidatensatzsegment :  1024
Cluster pro Dateidatensatzsegment : 0
MFT-gültige Datenlänge :           0x0000000000d0fc00
MFT-Start-LCN :                    0x0000000000c0000
MFT2-Start-LCN :                   0x0000000000445c7a
MFT-Zonenstart :                   0x00000000000c0ae0
MFT-Zoneende :                     0x0000000001d1720
```

14.6 Speicheroptimierung

Wenn der Speicherplatz auf einer Festplatte knapp wird, so müssen Sie aktiv werden. Besonders wichtig ist es, auf dem Systemdatenträger ausreichend Speicherplatz zur Verfügung zu haben, da sonst das System langsam bzw. instabil wird.

Einstellungen (⊞ + I) – System – Speicher

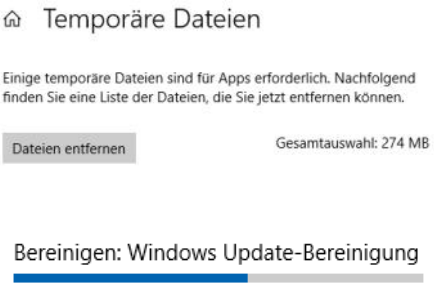
Hier sehen Sie eine Übersicht über Software-Elemente, welche Festplattenspeicherplatz verbrauchen; es kann entschieden werden, nicht benötigte Elemente zu entfernen, um wieder Platz zu schaffen.



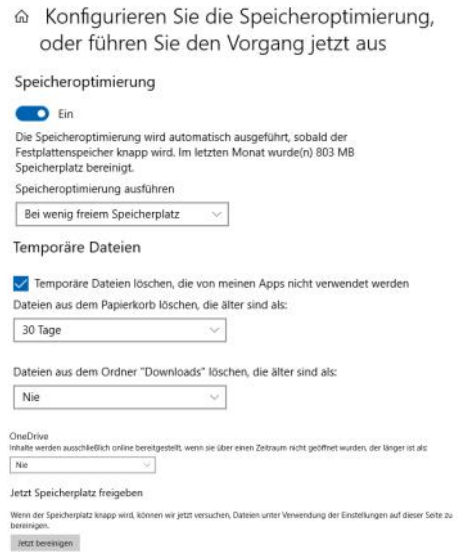
ACTIVE	Markiert die ausgewählte Basispartition als aktiv.
ADD	Fügt eine Spiegelung einem einfachen Volume hinzu.
ASSIGN	Weist dem gewählten Volume einen Laufwerkbuchstaben oder einen Bereitstellungspunkt zu.
ATTRIBUTES	Ändert Volumeattribute.
AUTOMOUNT	Aktiviert oder deaktiviert die automatische Bereitstellung von Basisvolumes.
BREAK	Teilt eine Spiegelung auf.
CLEAN	Löscht die Konfigurations oder alle Informationen vom Datenträger.
CONVERT	Führt Konvertierungen zwischen Datenträgerformaten durch.
CREATE	Erstellt ein Volume oder eine Partition.
DELETE	Löscht ein Objekt.
DETAIL	Zeigt Details über ein Objekt an.
EXIT	Beendet die Datenträgerpartitionierung.
EXTEND	Erweitert ein Volume.
FILESYSTEMS	Zeigt das aktuelle Dateisystem und die unterstützten Dateisysteme auf dem Volume an.
FORMAT	Formatiert das Volume oder die Partition.
GPT	Weist der ausgewählten GPT-Partition Attribute zu.
HELP	Zeigt eine Liste der Befehle an.
IMPORT	Importiert eine Datenträgergruppe.
INACTIVE	Markiert die ausgewählte Basispartition als inaktiv.
LIST	Zeigt eine Liste aller Objekte an.
ONLINE	Schaltet einen als offline markierten Datenträger online.
REM	Keine Aktion. Wird für Skriptkommentare verwendet.
REMOVE	Entfernt einen Laufwerkbuchstaben oder eine Bereitstellungspunktzuordnung.
REPAIR	Repariert ein RAID-5-Volume mit einem fehlerhaftem Mitglied.
RESCAN	Überprüft den Computer erneut auf Datenträger und Volumes.
RETAIN	Setzt eine beibehaltene Partition unter ein einfaches Volume.
SELECT	Verschiebt den Fokus auf ein Objekt.
SETID	Ändert den Partitionstyp.
SHRINK	Verkleinert die Größe des ausgewählten Volumes.

Klicken Sie auf einen Bereich, um Details anzuzeigen und Dateien zu entfernen.

Achten Sie bei den temporären Dateien beispielsweise darauf, dass Sie nicht irrtümlich Ihre persönlichen Downloads löschen.



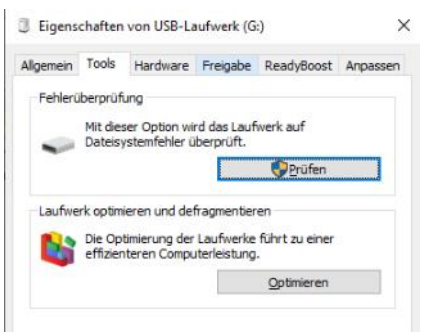
Sie können auch die Speicheroptimierung automatisieren. Klicken Sie dazu auf den Link **Konfigurieren Sie die Speicheroptimierung**:



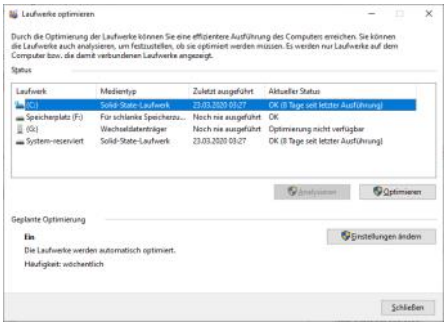
14.7 Defragmentierung

14.7.1 Defragmentierung über Datenträgereigenschaften

Auf grafischem Weg lässt sich die Optimierung und Defragmentierung über die Eigenschaften des entsprechenden Laufwerks erreichen.



Klicken Sie auf **Prüfen**, um das Laufwerk (etwa den USB-Stick) auf Dateisystemfehler zu prüfen.
Klicken Sie auf **Optimieren**, um das Laufwerk zu defragmentieren.



14.8 ReadyBoost

ReadyBoost ist der Name einer Cache-Technik, mit der durch die Einbindung von Flash-Speicher auf einem USB-Stick, SD-Card, CompactFlash oder einer anderen Art Flash-Speicher geringere Reaktionszeiten ermöglicht werden und dadurch die Systemleistung erhöht werden kann.

Hinweis: Moderne Geräte sind meist so schnell, dass ReadyBoost nicht mehr sinnvoll angewendet werden kann.

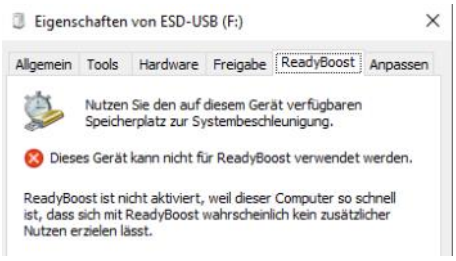
Bei Anwendung eines ReadyBoost-fähigen Speichergerätes zur Zwischenspeicherung ermöglicht das Betriebssystem wahlfreie Lesevorgänge mit einer Geschwindigkeit, die üblicherweise acht bis zehn Mal größer ist als die herkömmlichen Lesevorgänge von einer Festplatte.

Dieses Zwischenspeichern wird auf den gesamten Datenspeicher angewendet, nicht nur etwa auf die Auslagerungsdatei oder Systemdateien. Flash-Speicher sind im sequentiellen Lesen und Schreiben normalerweise langsamer als Festplatten, deshalb wurde in ReadyBoost eine Logik implementiert, die große, sequentielle Lesevorgänge erkennt und diese Anfragen direkt über die Festplatte ausführt. Die Schreibzugriffe werden auf dem Datenträger möglichst gleichmäßig verteilt, um Verschleiß an besonders häufig beschriebenen Stellen vorzubeugen.

Benchmarks zeigen, dass ReadyBoost in der aktuellen Fassung unterschiedliche Ergebnisse hervorbringen kann. Gerade auf älteren Rechnern mit wenig physikalischem RAM kann ReadyBoost einen deutlich messbaren Performance-Vorteil bringen. Wenn ein kompatibles Gerät angeschlossen wird, bietet das Windows-AutoPlay-Dialogfenster eine zusätzliche Option zur Beschleunigung des Systems an. Ein zusätzlicher ReadyBoost-Reiter wird im Eigenschaften-Dialog des jeweiligen Laufwerks hinzugefügt, wo die Menge des dafür vorgesehenen Speicherplatzes angepasst werden kann.

Ein Gerät muss die folgenden Voraussetzungen für die Kompatibilität erfüllen:

- Das USB-Gerät muss über mindestens 256 MB Kapazität verfügen. Maximal 4 GB sind für ReadyBoost nutzbar.
- Das USB-Gerät muss USB 2.0 unterstützen.
- Das Gerät muss eine Lese-Geschwindigkeit von mindestens 2,5 MB/s für 4-kB-Blöcke und 1,75 MB/s für 512-kB-Blöcke – jeweils zufällige, gleichmäßig über das komplette Gerät verteilte Lesevorgänge – aufweisen (Sticks mit dem enhanced for ReadyBoost-Label mindestens 5 MB/s für 4-kB-Blöcke und 3 MB/s für 512-kB-Blöcke).
- Das Gerät muss über mindestens 230 MB freien Speicher verfügen.
- Weiterhin wird empfohlen, zwischen ein - und dreimal soviel Speicherplatz für ReadyBoost zu reservieren, wie RAM installiert ist.



14.9 Startvorgang von Windows 10

Wird der Computer eingeschaltet, wird zuerst das BIOS oder das EFI geladen. Im Fall eines BIOS-basierenden Systems liest das BIOS den MBR der Festplatte oder eines anderen Speichermediums ein und führt ihn aus. Durch den dort befindlichen Code wird dann der Bootsektor der als aktiv markierten Partition geladen und ausgeführt. Der Code aus dem Bootsektor einer Partition, auf der eine entsprechende Windows-Installation installiert wurde, ist nun fähig, die Datei **bootmgr** im Wurzelverzeichnis eines NTFS-Dateisystems zu finden und auszuführen. Das Programm **bootmgr** liest die Datei **\Boot\BCD** ein und zeigt ein Bootmenü zur Auswahl des zu startenden Betriebssystems an. Zudem überprüft **bootmgr** die Disk-Signatur (Bytes 440-443 im MBR) mit seinen gespeicherten Booteinträgen aus der BCD. Wurde die Disk-Signatur verändert, verweigert Windows den Start mit einem „winload error".

Die wichtigsten Komponenten während des Startvorgangs von Windows 10 findet man im Stammverzeichnis der Startpartition:

- **bootmgr:** Diese Applikation kontrolliert den Windows 10 Startvorgang. In einer Multiboot-Umgebung stellt bootmgr das Betriebssystem-Auswahlmenü dar. Bis Windows XP/Server 2003 war das Programm ntldr für diese Aufgaben verantwortlich.
- **Boot Configuration Data (BCD):** Windows 10 speichert Startkonfigurationen in BCD. Das Programm bootmgr liest BCD, um das Betriebssystem-Auswahlmenü darstellen zu können. BCD ist der Nachfolger der Datei boot.ini, die in früheren Windows-Versionen verwendet wurde. Die Datenstruktur im BCD ist ähnlich wie ein Registry-Hauptschlüssel gespeichert und kann nicht direkt mit einem Texteditor bearbeitet werden.

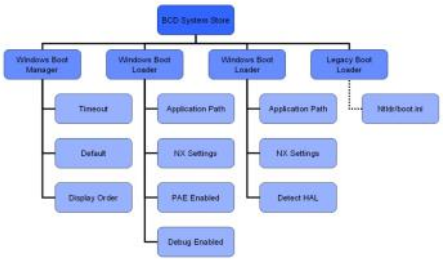
Beispiel (Quelle: www.tecchannel.de**):** Der BCD-Store enthält ein Objekt für den Bootmanager, zwei für Windows 7 und höher und einen für Windows XP/2000/2003.

14.7.2 Befehlszeilentool defrag

Hinweis: Seit Windows Vista sind erhöhte Administratorprivilegien für dieses Programm nötig.

Beschreibung: Sucht und konsolidiert fragmentierte Dateien auf lokalen Datenträgern, um die Systemleistung zu verbessern.

```
Syntax:  defrag <Volume> -a [-v]
         defrag <Volume> [{-r | -w}] [-f] [-v]
         defrag       -c [{-r | -w}] [-f] [-v]
Parameter:
Wert           Beschreibung
<Volume>       Legt das zu defragmentierende bzw. zu analysierende Laufwerk
               bzw. den Bereitstellungspunkt des Volumes fest.
-c             Defragmentiert alle Volumes auf diesem Computer.
-a             Führt nur eine Fragmentierungsanalyse durch.
-r             Führt eine teilweise Defragmentierung durch (Standard). Versucht
               nur Fragmente zu konsolidieren, die kleiner als 64 MB sind.
-w             Führt eine vollständige Defragmentierung durch. Versucht alle
               Dateifragmente ohne Berücksichtigung der Größe zu konsolidieren.
-f             Erzwingt die Defragmentierung des Volumes, wenn wenig
               Speicherplatz zur Verfügung steht.
-v             Legt den ausführlichen Modus fest. Die Defragmentierungs- und
               Analyseausgabe ist detaillierter.
-?             Zeigt diese Hilfeinformation an.
Beispiele:
defrag d:
defrag d:\volume\Bereitstellungspunkt -w -f
defrag d: -a -v
defrag -c –v
```

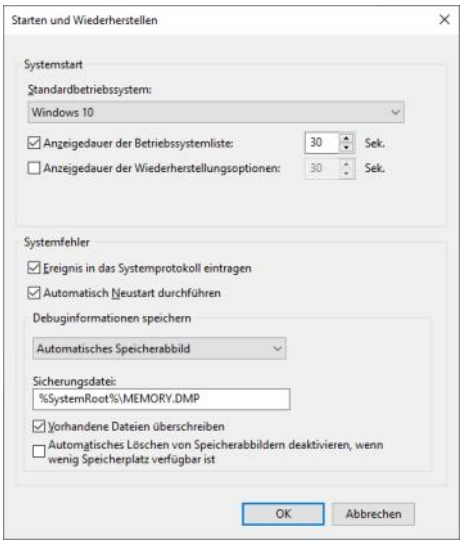


- **Winload.exe**: Dieses Programm lädt das Betriebssystem selbst. Falls aus dem Betriebssystem-Auswahlmenü Windows 10 ausgewählt wird, so wird die Kontrolle an Winload.exe übergeben. Es lädt den Kernel, den Hardware Abstraction Layer (HAL) und diverse Treiber in den Arbeitsspeicher. In einer Multiboot-Umgebung hat jede Windows 10-Instanz ihren eigenen winload.exe.
- **Winresume.exe**: Das ist das „WiederaufnahmeStartprogramm" für Windows 10, falls das Betriebssystem aus dem Energiesparmodus (engl. „hibernation mode") wieder in Betrieb genommen wird.

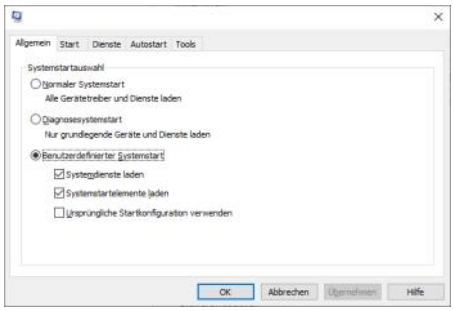
14.9.1 Tools zum Beeinflussen des Startvorgangs

In früheren Windows-Versionen konnte die Datei boot.ini manuell mit jedem beliebigen Text-Editor verändert werden. Dies ist heute nicht mehr möglich; der Startvorgang kann mit folgenden Methoden verändert werden:

Systemeigenschaften (⊞ + PAUSE), Karteikarte **Erweitert**, Rubrik **Start und Wiederherstellung**:



- Systemkonfiguration (msconfig.exe)



- **BCDEdit:** Dieses Tool ermöglicht die umfangreichsten Konfigurationsmöglichkeiten („fast alle") für den Startvorgang. Damit ist auch ein Export und Import von Konfigurationsdaten möglich.

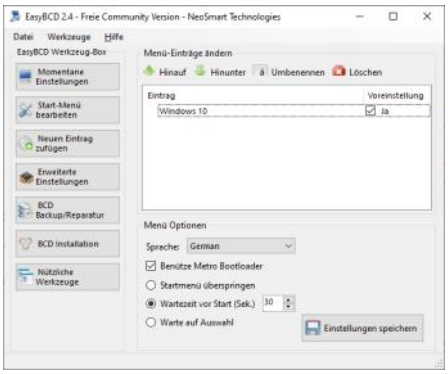
Beispiel: Anzeige aktueller Konfigurationsdaten:

```
C:\>bcdedit /enum
Windows-Start-Manager
---------------------
Bezeichner              {bootmgr}
device                  partition=C:
description             Windows Boot Manager
locale                  de-DE
inherit                 {globalsettings}
default                 {current}
resumeobject            {a7cf2159-9ce5-11db-9b34-
824fb58ca61f}
displayorder            {current}
toolsdisplayorder       {memdiag}
timeout                 30
Windows-Startladeprogramm
-------------------------
Bezeichner              {current}
device                  partition=C:
path                    \Windows\system32\winload.exe
description             Microsoft Windows Vista
locale                  de-DE
inherit                 {bootloadersettings}
osdevice                partition=C:
systemroot              \Windows
resumeobject            {a7cf2159-9ce5-11db-9b34-
824fb58ca61f}
nx                      OptIn
```

- **Windows Management Interface (WMI):** Diese Programmierschnittstelle ist die einzige Möglichkeit, kompletten Zugriff auf den BCD-Speicherbereich zu bekommen.

Ein Drittanbietertool, **EasyBCD**, ermöglicht die grafische Darstellung und Änderung des BCD-Stores.

Hersteller: https://neosmart.net/EasyBCD/ (nichtkommerzielle Testversion gratis, Vollversion ca. USD 30).



14.10 Boot-Optionen, Aktivieren von Windows RE

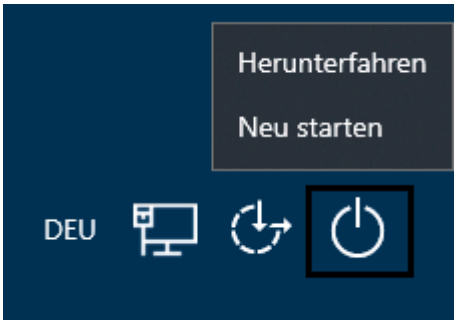
Früher gab es die Möglichkeit, beim Fehlschlagen eines Systemstarts mit der Funktionstaste F8 erweiterte Startoptionen aufzurufen. Da bei einem modernen PC die Zeit viel zu kurz wäre, um diese Taste drücken zu können, hat sich Microsoft entschieden, diese Möglichkeit nicht mehr anzubieten.

Bei einer herkömmlichen Neuinstallation ist in der (versteckten) Startpartition neben den nötigen Startdateien (BCD, winload.exe usw.) auch das Windows Recovery Environment (kurz: Windows RE) installiert, eine Minimalversion von Windows, über die diverse Möglichkeiten zur Systemwiederherstellung aktiviert werden können.

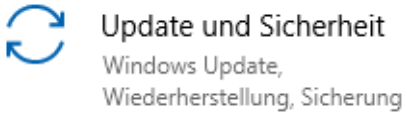
14.10.1 Neustart in das Windows Recovery Environment

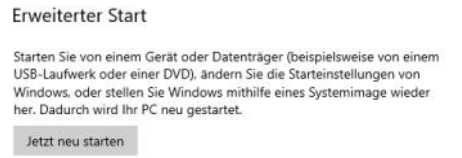
Hinweis: Alle diese Methoden funktionieren nur mit lokalen Benutzerkonten und Domänenbenutzerkonten, welche administrative Rechte besitzen; Microsoft-Konten können diese Möglichkeiten nicht verwenden.

Variante 1: Vom Anmeldebildschirm aus auf das I/O-Symbol klicken und mit gedrückter **SHIFT**-Taste **Neu Starten** klicken.



Variante 2: Systemeinstellungen – Bereich **Update und Sicherheit** – **Erweiterter Start** – **Jetzt neu starten**





Variante 3: ⊞ + R, Befehl **`shutdown /o /r`** eintragen.

Variante 4: `msconfig.exe`, Karteikarte **Start**, **Startoptionen**

Variante 5: Vom Windows 10 USB-Stick bzw. von der Windows 10-DVD starten (gegebenenfalls Boot-Reihenfolge des Systems ändern).

Klicken Sie den links unten befindlichen Link **Computerreparaturoptionen** statt **Windows installieren** an.

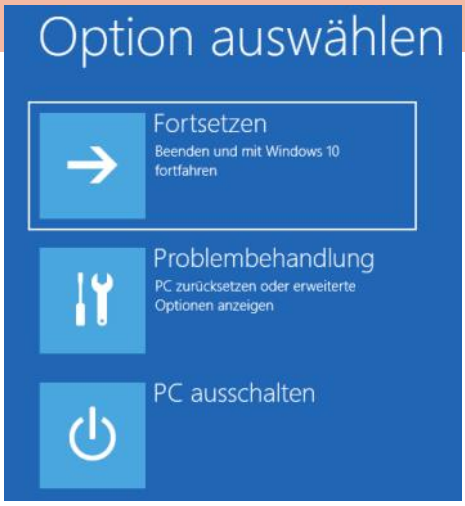
Variante 6: Windows RE übers Netzwerk (PXE-fähige Netzwerkkarte) starten (professionelle Variante; Verwendung von WDS = Windows-Bereitstellungsdienste, Windows Deployment Services, siehe Unterlage „Windows 10 – Deployment“).

Variante 7 („Holzhammermethode“): Wenn der PC nicht in die erweiterten Startoptionen kommt, hilft es, ihn ca. 3 Mal während des Bootvorgangs einfach auszuschalten (bzw. sogar den Stecker zu ziehen). Bei Notebooks/Tablets muss der Akku entfernt werden und dann 3 Mal der Bootvorgang durch Abschalten bzw. durch Entfernen der Netzspannung „abgewürgt“ werden.

Hintergrund: Wenn Windows startet, dann setzt das Programm `winload.exe` ein Statusflag, welches kennzeichnet, dass der Startvorgang begonnen hat. Bevor der Logon-Bildschirm erscheint, wird dieses Statusflag üblicherweise gelöscht. Falls allerdings der Startvorgang fehlschlägt, wird dieses Flag nicht gelöscht, und winload.exe findet beim nächsten Systemstart das Flag noch immer vor, weiß damit, dass es einen fehlgeschlagenen Startvorgang gegeben hat, und startet beim dritten Versuch WinRE statt Windows.

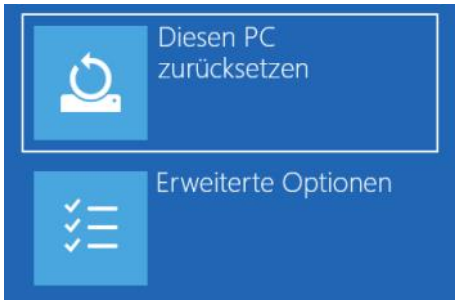
14.10.2 Oberfläche von Windows RE

Windows RE bietet eine Kacheloberfläche, die sich auch auf Notebooks und Tablets bedienen lässt. Direkt nach dem Start kommt man zur obersten Auswahlebene:



Fortsetzen führt einen ganz normalen Windows-Systemstart durch, **PC ausschalten** ist selbsterklärend. Die nächste Menüebene erreicht man mit **Problembehandlung**.

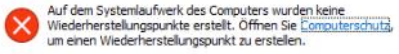
Hier haben Sie zwei Auswahlmöglichkeiten zur Problembehandlung:



Die Option **Diesen PC zurücksetzen** wird im nächsten Abschnitt behandelt. Klick auf **Erweiterte Optionen** führt in die dritte Menüebene.

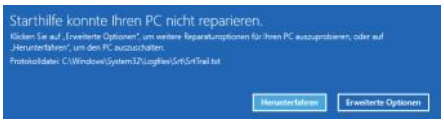
Hier können Sie verschiedene Möglichkeiten zur Reparatur eines defekten Systems auswählen:

- **System wiederherstellen:** Herstellen von Windows über vorhandene Wiederherstellungspunkte (Konfiguration von Wiederherstellungspunkten siehe nächstes Kapitel). Wenn keine Wiederherstellungspunkte verfügbar sind, wird folgende Fehlermeldung angezeigt:



- **Updates deinstallieren:** Es kann vorkommen, dass die Instabilität durch ein Sicherheits- oder Funktionsupdate entstanden ist. Diese Updates können wieder deinstalliert werden.
- **Systemimage-Wiederherstellung:** Stellt das System mit Hilfe eines zuvor mit Windows Backup erstellten Systemabbilds wieder her.
- **Starthilfe:** Automatisches Reparieren von Windows Startproblemen (Bootsektor usw.) mit Hilfe von Windows RE (Recovery Environment); die Installation von Windows RE auf Datenträger wird auf Seite 279 beschrieben.

Windows wird beendet, nach dem Neustart wird Windows RE angezeigt. Sie müssen sich mit einem lokalen Administrator-Konto anmelden.



- **Eingabeaufforderung**: Kommandozeile/Eingabeaufforderung

  Hier kann man diverse Systemüberprüfungstools aufrufen, etwa:

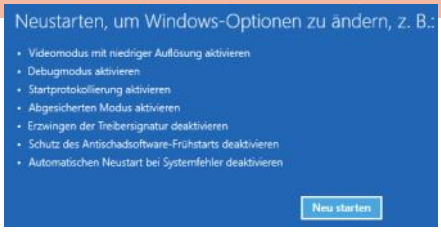
  ```
  DISM.exe /Online /Cleanup-image /Restorehealth
  ```

  Überprüft Systemdateien und stellt aus Windows-Update (Internet) jene Dateien bereit, die zur Reparatur erforderlich sind.

  ```
  sfc /scannow
  ```

  Überprüft alle geschützten Systemdateien und ersetzt die beschädigten Dateien durch eine zwischengespeicherte Kopie, die sich in einem komprimierten Ordner unter `%WinDir%\System32\dllcache` befindet.

- **UEFI Firmware-Einstellungen**: Dieser Menüpunkt ist nur sichtbar, wenn Sie einen Computer mit UEFI-Firmware (statt des veralteten BIOS) besitzen. BIOS-Einstellungen müssen nach wie vor durch Unterbrechen des Startvorgangs (etwa durch Drücken der Taste F2) geändert werden.
- **Starteinstellungen:** Dieses Menü ersetzt die Möglichkeiten, die unter früheren Windows-Versionen durch Drücken der Taste F8 während des Startvorgangs erreichbar waren:



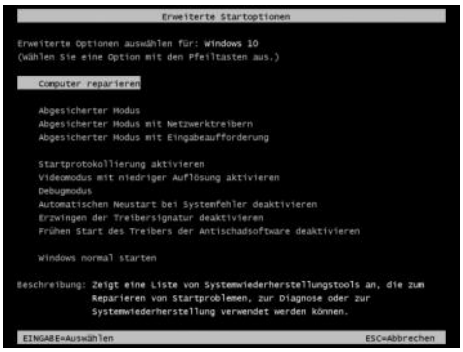
- **Zum vorherigen Build zurückkehren:** Dieser Menüpunkt wird 28 Tage nach einer Update-Installation von einer vorigen Betriebssystemversion angezeigt. Diese wird in einem Ordner **`Windows.old`** gespeichert – löscht man diesen Ordner, verschwindet auch die Option aus Windows RE.

14.10.3 Textorientiertes Startmenü mit F8 aktivieren/deaktivieren

Es ist mit Hilfe des Command Shell-Tools bcdedit möglich, das alte, textorientierte erweiterte Startmenü, welches in älteren Windows-Versionen mit der Taste F8 während des Startvorgangs erreichbar war, zu reaktivieren:

```
bcdedit /set {default} bootmenupolicy legacy
```

Damit erreichen Sie folgendes Startmenü:



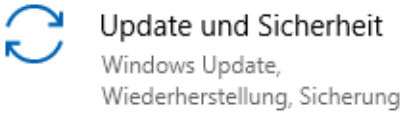
Hinweis: Da die Zeit für das Drücken der F8-Taste sehr kurz ist, sind mit hoher Wahrscheinlichkeit mehrere Versuche nötig, bis das System in das textorientierte erweiterte Startmenü bootet.

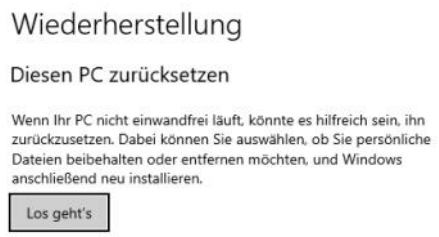
Dieses Startmenü kann auch wieder deaktiviert werden, sodass die Kachel-Darstellung von Windows RE erscheint:

```
bcdedit /set {default} bootmenupolicy
standard
```

14.101.4 PC rücksetzen

Variante 1: **Systemeinstellungen** – Bereich **Update und Sicherheit – Wiederherstellung – Diesen PC rücksetzen – Los geht's**





Variante 2: In **Windows RE** booten (siehe vorher) – **Problembehandlung – Diesen PC rücksetzen**

Hier hat man die Auswahl, die Apps und Einstellungen zu entfernen, aber die persönliche Daten zu erhalten.

Die Option **Alles löschen** entspricht im Prinzip einer Neuinstallation von Windows 10; alle Daten gehen verloren.

14.11 Backup und Restore, Notfallwiederherstellung

14.11.1 Dateiversionsverlauf

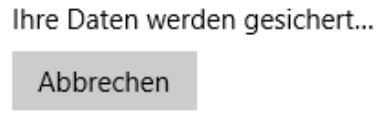
Es ist möglich, mehrere Versionen von Dateien regelmäßig auf einem anderen Datenträger zu sichern. Damit können versehentlich gelöschte Dateien, aber auch ältere Versionen von versehentlich überschriebenen Dateien wiederhergestellt werden. Der Dateiversionsverlauf muss aktiviert werden.

Variante 1: Öffnen Sie die App **Einstellungen** (⊞ + I) – **Update und Sicherheit – Sicherung.**

Fügen Sie zunächst ein anderes Laufwerk hinzu, auf dem Sie die Sicherungsdaten ablegen möchten. Das kann ein Wechseldatenträger oder eine andere Festplatte sein.

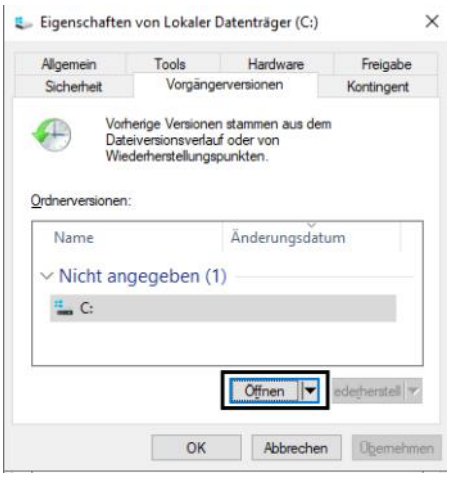
Klicken Sie auf **Ein**, um den Dateiversionsverlauf zu aktivieren.

Durch Klicken auf **Weitere Optionen** können Sie die Sicherung sofort starten. Weiters ist es möglich, das Sicherungsintervall zu konfigurieren.
Wenn Sie auf **Jetzt sichern** klicken, wird die Sicherung gestartet.

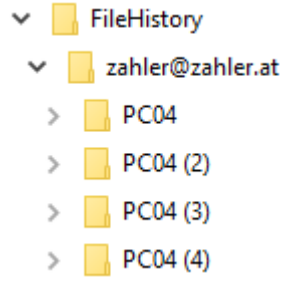


Variante 2 („Old School"): Sie können auch das Systemsteuerungselement **Dateiversionsverlauf** benützen, um dieses Feature zu aktivieren.

In den Eigenschaften von Laufwerken, Ordnern und Dateien kann man vorhergehende Versionen in der Registerkarte **Vorgängerversionen** ansehen und – bei Bedarf – wiederherstellen.



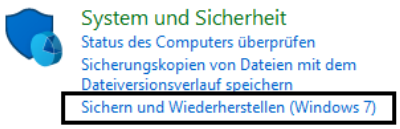
Auf dem angegebenen Datenträger entsteht folgende Orderstruktur:

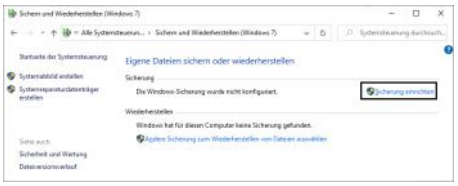


14.11.2 Altes Backup-Tool (Windows 7)

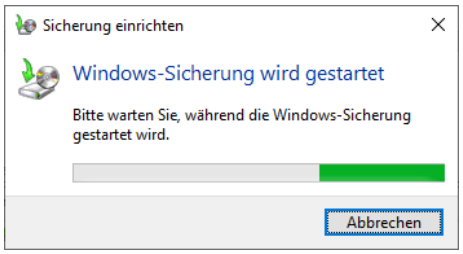
Das alte Tool ist über die **Systemsteuerung – Sichern und Wiederherstellen (Windows 7)** erreichbar; alternativ gibt es einen Link im App **Einstellungen – Update und Sicherheit – Sicherung**.

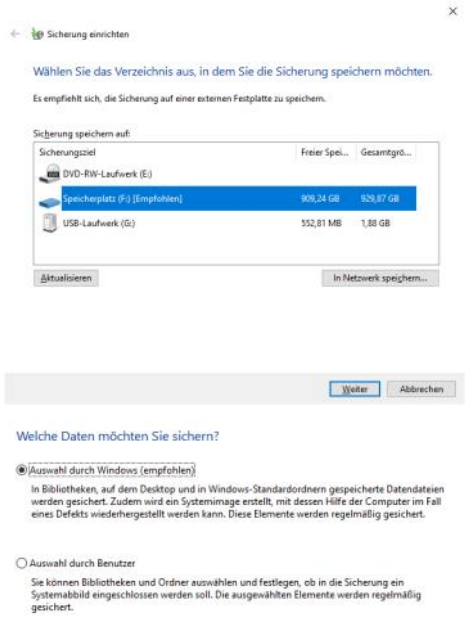
In der Systemsteuerung findet man das Windows 7-Backup unter **System und Sicherheit**:





Klickt man auf **Sicherung einrichten**, so wird nach der Initialisierung des Backup-Features nach dem Sicherungs-Datenträger gefragt. Neben lokalen Datenträgern (Wechselplatte, zweite Festplatte) ist auch ein Sicherungsvorgang ins Netzwerk möglich. Dafür muss der UNC-Pfad auf einen freigegebenen Ordner eingegeben werden, etwa `\\srv09\backup`.

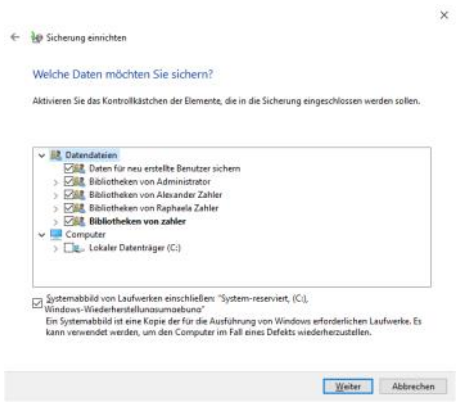


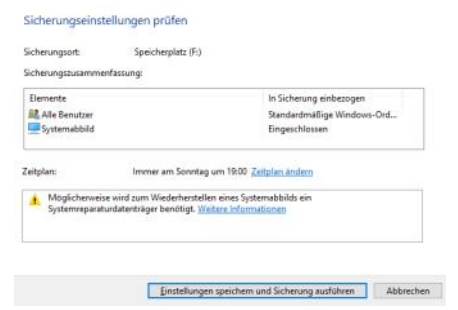


Klickt man auf **Auswahl durch Windows**, so werden folgende Elemente gesichert:

- **Bibliotheken**: Alle Dateien, die sich in Bibliotheken befinden, vorausgesetzt, sie sind lokal gespeichert und das Laufwerk ist mit NTFS formatiert.
- **Desktop**: Alle Dateien, die sich auf dem Desktop befinden.
- **System-Image**: Falls genug Platz auf dem Sicherungsmedium vorhanden ist, wird ein System-Image mit dem gesamten Betriebssystem, allen Treibern, Registry-Einstellungen und installierten Softwareprodukten erstellt.

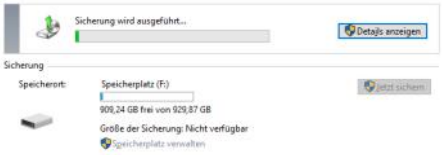
Wählt man **Auswahl durch Benutzer**, dann kann aus allen Ordnern selbst eine Auswahl getroffen werden:





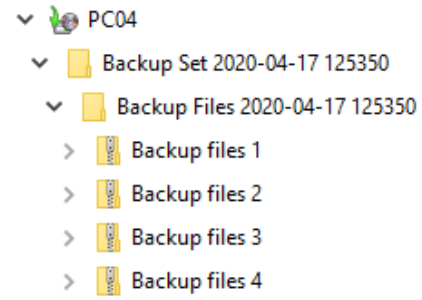
Für eine wiederkehrende Sicherung kann ein Zeitplan erstellt werden.

Während die Sicherung ausgeführt wird, ist ein Weiterarbeiten möglich, der Sicherungsfortschritt wird aber angezeigt:



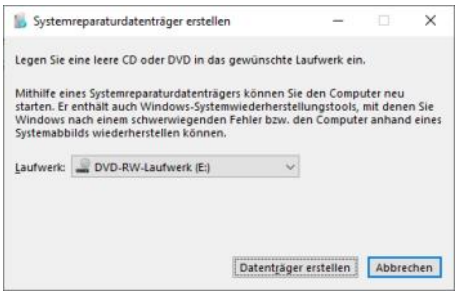
Nach Fertigstellung der Sicherung wird ein Status angezeigt, außerdem wird die Größe der Sicherungsdatei angezeigt.

Aufbau des Backup-Verzeichnisses:



14.11.3 Systemreparatur-Datenträger

Außerdem ist es möglich, einen **Systemreparatur-Datenträger** zu erstellen:



14.11.4 Wiederherstellung mit dem alten Backup/Restore-Tool (Windows 7)

Es ist möglich, einzelne Dateien aus einem Backup herzustellen, das mit dem Windows 7-kompatiblen Backup/Restore-Tool erstellt wurde.

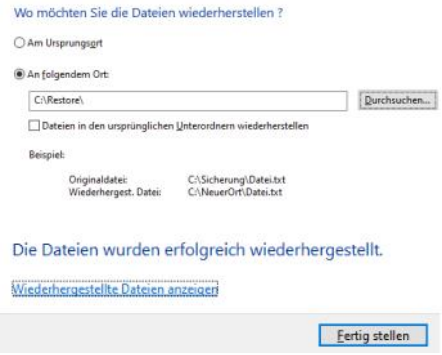
Im Systemsteuerungs-Element **Sichern und wiederherstellen (Windows 7)** klicken Sie im Abschnitt **Wiederherstellen**

auf die Schaltfläche **Eigene Dateien wiederherstellen**.

Klickt man doppelt auf den PC-Namen, so erscheint folgendes Menü:

Auf diese Art ist es möglich, einige oder alle Dateien aus der durchgeführten Sicherung wiederherzustellen. Wählen Sie eine passende Sicherung aus (standardmäßig wird immer die neueste Sicherung ausgewählt) und klicken Sie auf **Nach Dateien suchen.** In der Sicherung können Sie durch die Ordnerhierarchie klicken, um bestimmte Dateien aufzufinden.

Es wird empfohlen, die ausgewählten Dateien an einem anderen Speicherort wiederherzustellen, damit nicht irrtümlich neue, noch nicht gesicherte Dateiversionen durch alte überschrieben werden.

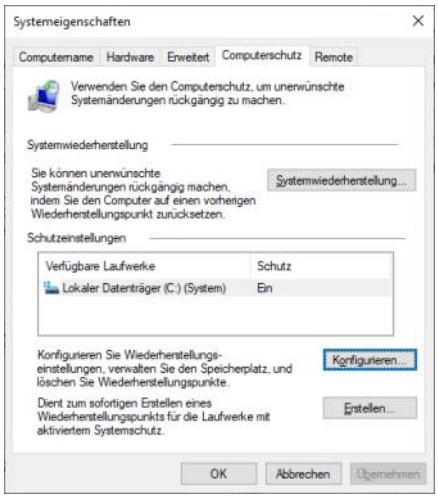


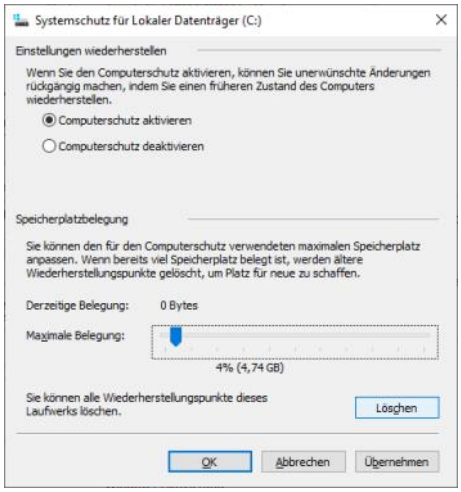
14.11.5 Systemwiederherstellung und Volumenschattenkopien („Volume Shadow Copies“)

Die Systemwiederherstellung wurde unter Windows XP eingeführt, damit Benutzer ihre Computer in einen vorherigen Zustand zurückversetzen können, ohne persönliche Datendateien zu verlieren (wie z. B. Microsoft Office Word-Dokumente, Grafikdateien und E-Mail-Nachrichten). Für die Systemwiederherstellung müssen keine Systemsnapshots erstellt werden, da das System einfach erkennbare Wiederherstellungspunkte automatisch anlegt, mit deren Hilfe Sie Ihr System auf einen früheren Zeitpunkt zurücksetzen können. Wiederherstellungspunkte werden sowohl zum Zeitpunkt wichtiger Systemereignisse (z. B. bei der Installation von Anwendungen oder Treibern) als auch in regelmäßigen Abständen (täglich) erstellt. Sie können Wiederherstellungspunkte jederzeit erstellen und benennen.

Unter Windows 10 ermöglicht die Systemwiederherstellung eine Wiederherstellung nach einer größeren Vielfalt von Änderungen als unter Windows XP. Wenn nun ein Wiederherstellungspunkt erforderlich ist, wird eine **Schattenkopie** einer Datei oder eines Ordners erstellt. Eine Schattenkopie ist im Wesentlichen eine frühere Version der Datei oder des Ordners zu einem bestimmten Zeitpunkt. Windows 10 kann Wiederherstellungspunkte automatisch oder nach Aufforderung erstellen. Wenn das System wiederhergestellt werden muss, werden Dateien und Einstellungen aus der Schattenkopie auf das aktive von Windows 7 verwendete Volume kopiert. Dadurch wird die Integration mit anderen Aspekten der Sicherung und Wiederherstellung verbessert und die Systemwiederherstellungsfunktion noch nützlicher.

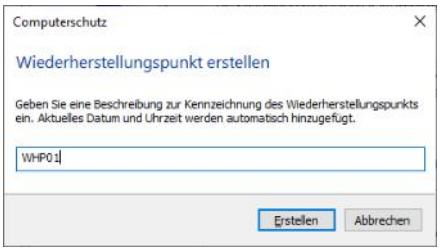
Aktivieren des Computerschutzes: Unter Systemeigenschaften – Computerschutz:

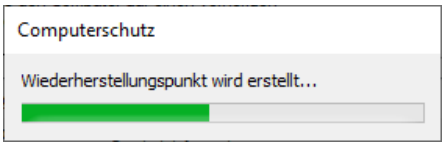


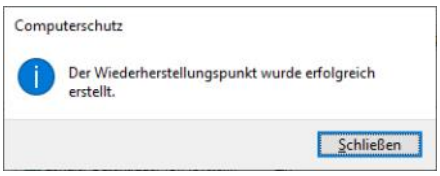


Schattenkopien werden automatisch als **Teil eines Wiederherstellungspunkts** in den Systemeigenschaften gespeichert. Wenn der Computerschutz aktiviert ist, erstellt Windows automatisch Schattenkopien von Dateien, die seit dem letzten Wiederherstellungspunkt, also in der Regel seit einem Tag, geändert wurden. Wenn die Festplatte partitioniert ist oder wenn mehrere Festplatten im Computer installiert sind, müssen Sie den Computerschutz auch auf den anderen Partitionen oder Festplatten aktivieren.

Sie können jederzeit selbst einen Wiederherstellungspunkt erstellen, indem Sie in **Systemeigenschaften** – Registerkarte **Computerschutz** auf die Schaltfläche **Erstellen** klicken.

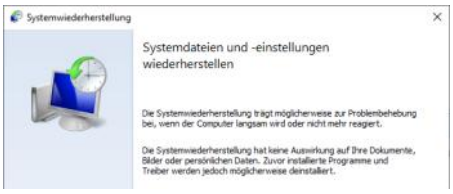


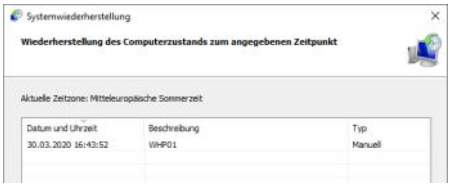


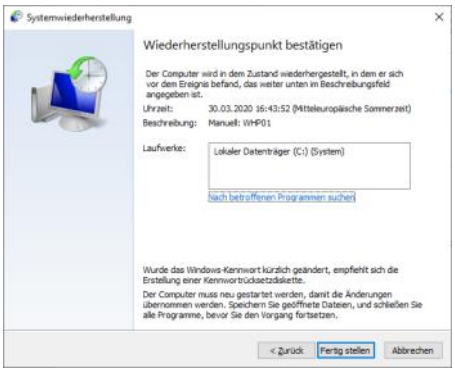


Wenn Sie in **Systemeigenschaften** – Registerkarte **Computerschutz** auf die Schaltfläche **Systemwiederherstellung...** klicken, so ist es möglich, das System auf den Stand eines anzugebenden Wiederherstellungspunktes zurückzusetzen.

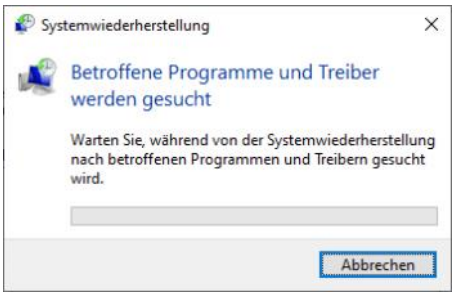
Das kann notwendig sein, wenn die Installation einer Software oder eines Treibers das System instabil gemacht hat.





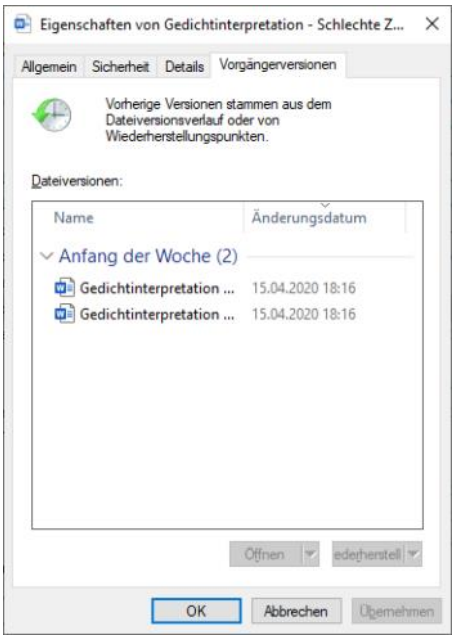


Sie können auf den Link **Nach betroffenen Programmen** suchen, um Änderungen einzelner Programme bzw. Treiber herauszufinden.



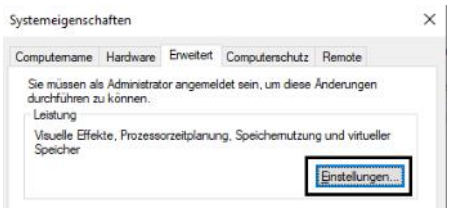
Klicken Sie mit der rechten Maustaste auf die Datei bzw. den Ordner, und klicken Sie dann auf **Vorherige Versionen wiederherstellen**.

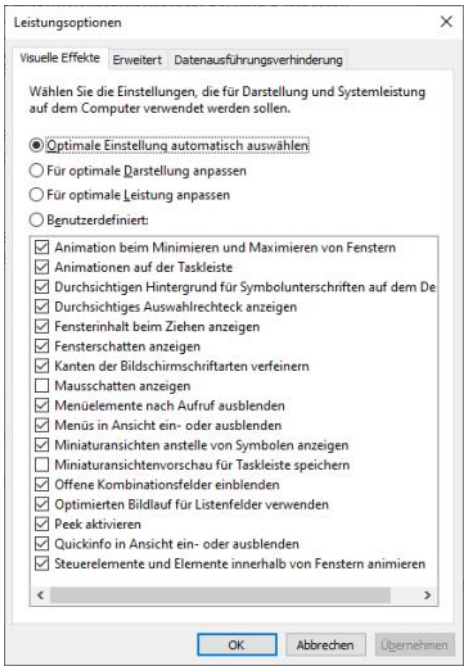
Es wird eine Liste der verfügbaren vorherigen Datei- oder Ordnerversionen angezeigt. Die Liste enthält sowohl Sicherungs- als auch Schattenkopien, sofern beide Typen vorhanden sind.

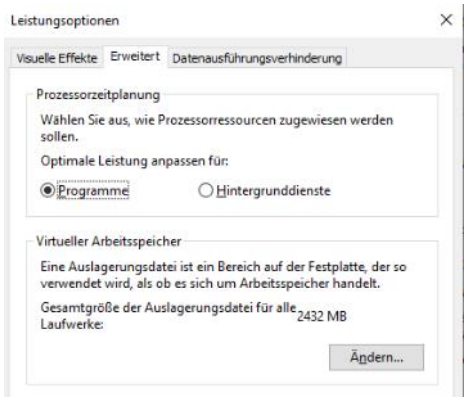


14.12 Systemleistungsoptionen und Auslagerungsdatei

Systemeigenschaften – Erweiterte Systemeinstellungen, Registerkarte **Erweitert**.

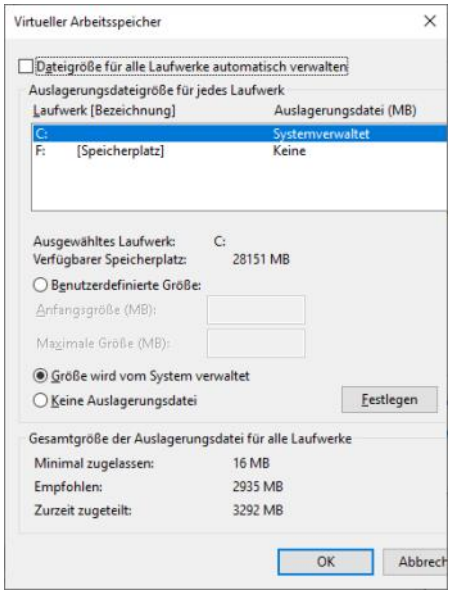






Durch Klick auf "Ändern" kann der virtuelle Arbeitsspeicher (d.h. Größe der Auslagerungs-datei, engl. Swap-Datei) geändert werden.

Empfohlene Größe der Auslagerungsdatei: etwa 1,5 x des installierten Hauptspeichers (mehr hat keinen Sinn, da sonst Performance-Verluste auftreten!). Braucht man mehr, so ist es sinnvoller, physischen Speicherplatz zu ergänzen.



Windows NT-Betriebssysteme unterstützen einen 32 bit Adressraum, das bedeutet einen virtuellen Adressbereich von 4 GB. Jedem Programm wird ein solcher virtueller 4 GB-Adressraum zugeordnet. (Hätte man diesen Speicher auch physikalisch, so könnte das Programm diesen Speicher auch nutzen!)

Die Zuordnung zwischen tatsächlich vorhandenem Speicher und virtuellem Speicher wird vom VMM = *Virtual Memory Manager* durchgeführt.

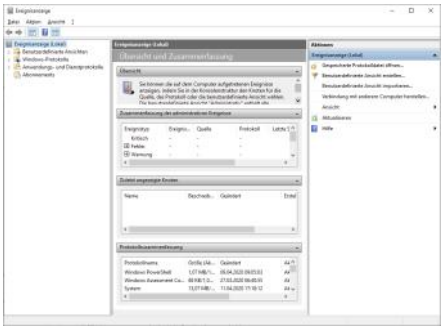
Ist für mehrere Programme eine Zuweisung von tatsächlichem RAM nicht mehr möglich (*Page Fault* = Seitenzuordnungsfehler), so muss ein Teilbereich aus dem RAM auf die Festplatte ausgelagert werden. Damit werden diese Daten auf die "Swap-Datei" (Auslagerungsdatei) auf die Festplatte ausgelagert.

Die Auslagerung erfolgt generell in 4 KB-Blöcken.

14.13 Ereignisanzeige (Event Viewer)

Alle Vorgänge, die auf einem Windows-PC ablaufen, werden in Form von Ereignissen protokolliert. Diese Ereignisse sind in der Ereignisanzeige sichtbar. Es kann sich dabei um bloße Informationen handeln (etwa ob ein Dienst gestartet wurde), aber auch Warn- und Fehlermeldungen gehören zu den Ereignissen. Das macht die Ereignisanzeige zu einem mächtigen Fehleranalyse-Werkzeug, das Sie bei der Lösung von Hard- und Softwareproblemen unterstützt.

Die Ereignisanzeige ist ein MMC-Snap-In, welches über die vordefinierte Konsole **`eventvwr.msc`** erreichbar ist.

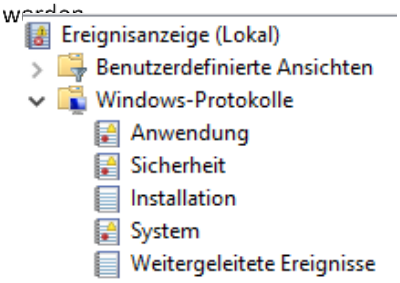


Die Aufzeichnung von Informationen erfolgt in der Ereignisanzeige anhand verschiedener Protokolle, auf die Sie über die linke Spalte zugreifen können.

- **Anwendung:** Hier werden sämtliche Informationen zu Programmen und Anwendungen aufgezeichnet.
- **Sicherheit:** Hier landen alle Einträge, die die Sicherheit betreffen, etwa An- und Abmeldevorgänge, Zugriffe auf Ordner und Dateien usw. Beachten Sie, dass Sie dafür unter Umständen vorher die Sicherheitsprotokollierung aktivieren müssen.
- **Installation:** Hier finden Sie Informationen zu installierten Sicherheitsupdates, Features usw.
- **System:** Hier sind Fehlermeldungen,

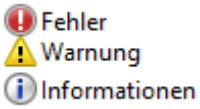
Warnungen und Informationen des Betriebssystems und der Systemdienste protokolliert.

- **Weitergeleitete Ereignisse:** Hier finden Sie Ereignisse, die von anderen Computern an dieses Protokoll weitergeleitet werden.



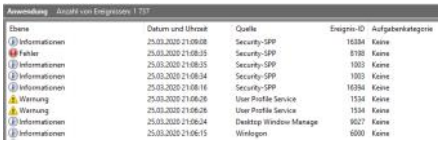
Die Ereignisse in der Ereignisanzeige werden in drei Kategorien eingeteilt:

- **Fehler** (roter Kreis mit Rufzeichen): Solche Ereignisse beschreiben größere Probleme, die auch zu Datenverlust oder eingeschränkter Funktionsfähigkeit des Systems führen können.
- **Warnung** (gelbes Dreieck): Warnungen beschreiben Ereignisse, das nicht unmittelbar ein Problem darstellen, sich aber zukünftig zu einem entwickeln könnte.
- **Informationen** (blaues Rufzeichen): signalisieren die erfolgreiche Ausführung eines Dienstes, Treibers oder Programms, Konfigurationsänderungen oder ähnliche Vorgänge.



14.13.1 Aufbau von Ereignissen, Beheben von Systemfehlern mit Hilfe der Ereignisanzeige

Jedem Ereignis ist eine Nummer, die sogenannte **Event-ID**, zugeordnet. Jede Nummer hat eine spezifische Bedeutung. Die **Quelle** gibt an, woher das Ereignis stammt; die Quelle „EventLog" bedeutet, dass die Ereignisprotokollieren selbst das Ereignis erzeugt hat, die Quelle „Kernel-General" gibt an, dass der Betriebssystem-Kernel das Ereignis generiert hat.



Die Ereignis-Details können durch Doppelklick auf das Ereignis eingesehen werden.

Mit Hilfe dieser Detailinformationen können Fehlersituationen schneller erkannt, analysiert und damit auch behoben werden (Tabelle unten links).

Wichtige Website: Auf der Website **eventid.net** können Sie die Bedeutung einzelner Ereignisse an Hand der Event-ID nachlesen. In dieser umfangreichen Datenbank finden Sie wertvolle Erklärungen, die bei der Fehlersuche und Fehlerbehebung interessant sind.

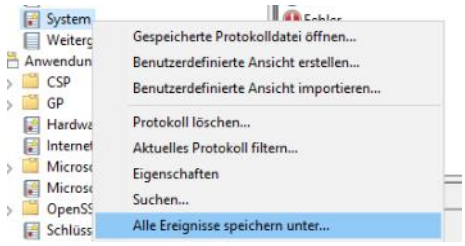
14.13.2 Speichern von Protokollinhalten

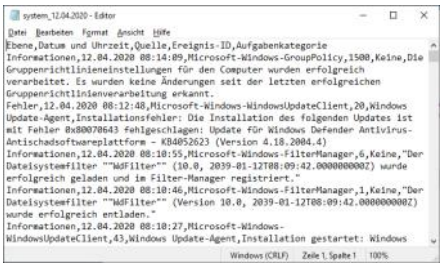
Im Kontextmenü eines Protokolls wählen Sie den Eintrag **Alles Ereignisse speichern unter.**

Protokolldateien können in verschiedenen Formaten gespeichert werden:

*.EVTX - internes Format
*.XML – XML-Datei
*.TXT - Textdatei
*.CSV (comma separated value) - in Excel weiterverarbeitbar

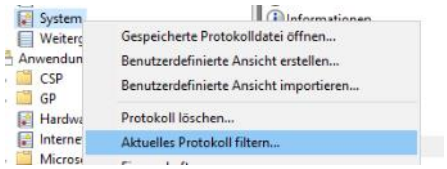
Beispiel für CSV-Datei:



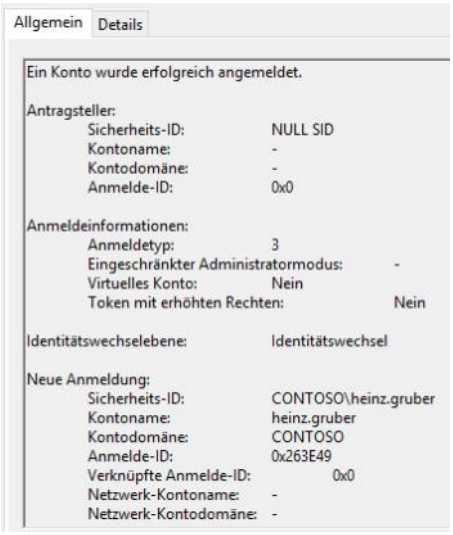


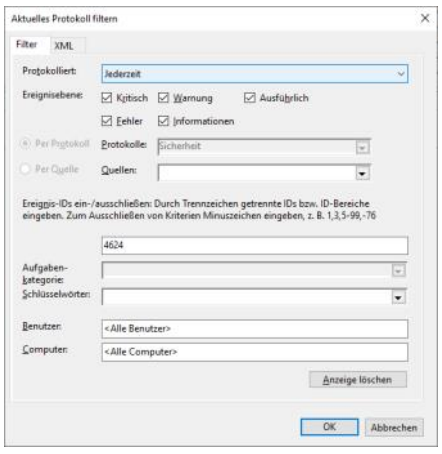
14.13.3 Filtern von Ereignissen

Die Vielzahl der möglichen Ereignisse macht die Ereignisanzeige unübersichtlich. Es ist daher in vielen Fällen hilfreich, nur eine Teilmenge anzuzeigen.



Beispiel: Wenn man sich einen Überblick verschaffen möchte, wer sich an einem PC angemeldet hat, so filtert man das Sicherheitsprotokoll und sucht nach Ereignissen mit der Ereignis-ID **4624**.





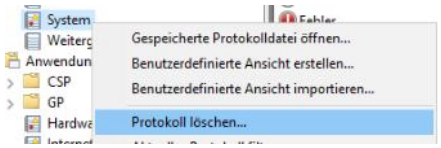
Links sieht man das Detail eines Logon-Ereignisses: Der Domänenbenutzer heinz.gruber hat sich erfolgreich angemeldet.

Aus dem Anmeldetyp lässt sich ablesen, welche Art der Anmeldung erfolgt ist: (Tabelle nächste Seite rechts oben)

Event-ID	Kategorie	Beschreibung
1100	Event Log	Das Ereignisprotokoll wurde gestoppt.
4624	Logon/Logoff	Ein Account wurde erfolgreich angemeldet.
4634	Logon/Logoff	Ein Account wurde abgemeldet.
5025	System	Der Windows-Firewall-Dienst wurde gestoppt.
6008	System	Enthält den Absturzzeitpunkt nach einem unerwarteten Systemneustart.
6009	System	Erscheint beim Start und enthält unter anderem Informationen über das Betriebssystem.

14.13.4 Protokoll löschen

Es ist möglich, durch Anklicken eines Protokolls mit der rechten Maustaste und Auswahl des Kontextmenüeintrags Protokoll löschen… alle momentan gespeicherten Ereignisse in einem Protokoll zu entfernen.



Vor dem Entleerungsvorgang besteht aber noch die Möglichkeit, den Inhalt in einer Protokolldatei zu speichern.

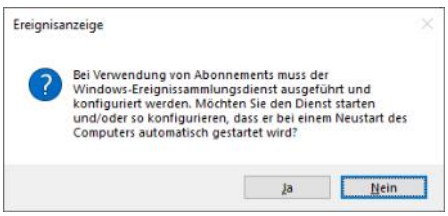
14.13.5 Weiterleiten und Sammeln von Ereignissen (Pull-Abonnements)

Ereignisse, die auf verschiedenen Computern entstanden sind, können auch auf einem Sammlungscomputer zusammengefasst werden.

Es gibt dazu zwei Möglichkeiten:

- **Sammlungsinitiiert:** Der Sammlungscomputer stellt periodisch eine Verbindung zu den Quellcomputern her und sammelt die gewünschten Ereignisse ein. Diese Variante wird in diesem Abschnitt beschrieben, sie eignet sich allerdings nur für kleine Infrastrukturen mit wenigen PCs.
  Auf den Quellcomputern muss dafür *Windows Remote Management* (WinRm) aktiviert werden.
- **Quellcomputerinitiiert:** In diesem Fall übertragen die Quellcomputer aktiv die entsprechenden Ereignisse auf den Sammlungscomputer. Hier muss über eine Gruppenrichtlinie festgelegt werden, welche Computer Ereignisse senden sollen.

Für die Konfiguration des Sammlungscomputers ist es notwendig, auf dem Sammlungscomputer den **Windows-Ereignissammlung** (**wecsvc**) zu starten. Beim ersten Klicken auf **Abonnements** kommt folgende Meldung, die mit **Ja** bestätigt werden muss.



Dieser Dienst kann mit dem Command Shell-Tool **wecutil** konfiguriert werden.

```
C:\>wecutil qc

Der Startmodus für den Dienst wird in den
Modus für verzögerten Start geändert.

Möchten Sie mit dem Vorgang fortfahren ( J-
Ja oder N- Nein)?j

Der Windows-Ereignissammlungsdienst wurde
erfolgreich konfiguriert.
```

2	Interaktive Anmeldung (meist durch Benutzername/Kennwort), verarbeitet durch die LSA
3	Netzwerkanmeldung, meist verursacht durch den Zugriff auf einen freigegebenen Ordner oder Drucker
5	Dienst hat sich angemeldet, Anmeldung wurde durch die LSA verarbeitet
7	Computer wurde entsperrt
8	Klartext-Authentifizierung (**Sicherheitsrisiko!**), früher von IIS verwendet (Standardauthentifzierung)
10	Remotedesktop-Anmeldung, verarbeitet durch die LSA
11	Anmeldung mit zwischengespeicherten Anmeldeinformationen („cached credentials“)

Auf allen Computern, die Ereignisse liefern sollen, muss **Windows Remote Management (WinRm)** aktiviert werden. WinRM verwendet standardmäßig TCP-Port 5985 bzw. 5986 (früher TCP-Port 80 bzw. 443).

```
C:>winrm quickconfig

WinRM wurde nicht für Verwaltungsremotezu-
griff auf diesen Computer konfiguriert.

Folgende Änderungen müssen durchgeführt
werden:

Erstellen Sie einen WinRM-Listener auf
HTTP://*, um die WS-
Verwaltungsanforderungen an eine beliebige
IP-Adresse auf diesem Computer zu akzeptie-
ren.

Aktivieren Sie die WinRM-Firewallausnahme.

Diese Änderungen durchführen [y/n]? y

WinRM wurde für die Remoteverwaltung aktua-
lisiert.

Auf HTTP://* wurde ein WinRM-Listener er-
stellt, um die WS-Verwaltungsanforderungen
an eine beliebige IP-Adresse auf diesem
Computer zu akzeptieren.

Die WinRM-Firewallausnahme ist aktiviert.
```

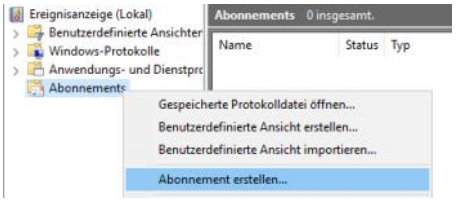
Falls WinRM bereits ausgeführt wird, erscheint folgende Meldung:

```
Der WinRM-Dienst wird auf diesem Computer
bereits ausgeführt.

WinRM ist bereits für die Remoteverwaltung
auf diesem Computer eingerichtet.
```

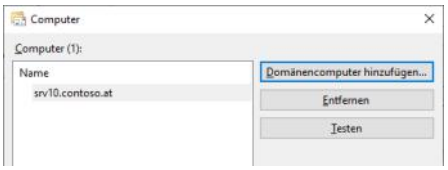
Beispiel: Wir wollen alle Dienststeuerungsereignisse sammeln, das heißt, wir möchten zum Beispiel wissen, wenn ein Dienst am Quellcomputer gestartet oder beendet wird.

Dienststeuerungsereignisse haben die ID 7036.

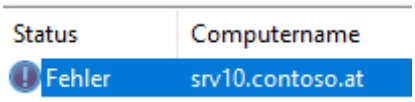
Erstellen Sie nun am Sammlungscomputer ein Abonnement, indem Sie mit der rechten Maustaste auf Abonnements klicken und den Kontextmenü **Abonnement erstellen…** wählen.

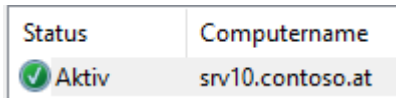


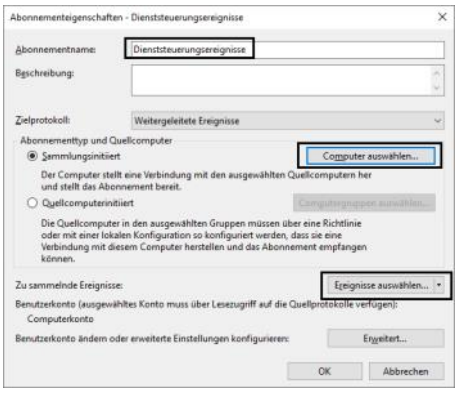
Es erscheint ein Dialog **Abonnementeigenschaften**. Vergeben Sie einen Abonnementnamen und klicken Sie auf **Computer auswählen**. Fügen Sie all jene Domänencomputer ein, von denen die Ereignisse gesammelt werden sollen.



Mit der Schaltfläche Testen können Sie einen Konnektivitätstest ausführen, der eine Information darüber gibt, ob der Computer Ereignisse liefern kann.

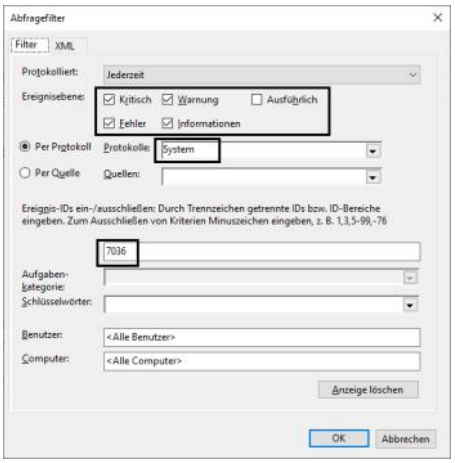




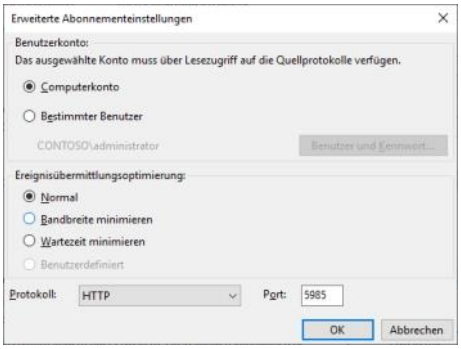


Klicken Sie anschließend auf die Schaltfläche **Ereignisse auswählen**.

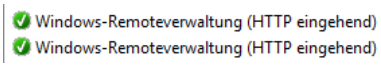
Konfigurieren Sie im Dialog **Abfragefilter** die Option **Per Protokoll** und wählen Sie als Protokolltyp **System** aus. Wählen Sie alle zutreffenden Ereignisebenen aus. Fügen Sie Ereignis-ID 7036 für das Systemprotokoll hinzu und klicken Sie auf **Ok**.



Sie benötigen nun ein Benutzer- oder Computerkonto, das die Berechtigung hat, die Quellprotokolle der überwachten Computer auszulesen.



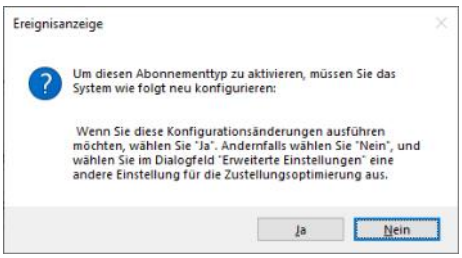
Hinweis: Falls der TCP-Port 5985 verwendet wird, so ist in der Firewall-Konfiguration zu überprüfen, ob dieser Port geöffnet ist. Gegebenenfalls muss die vordefinierte eingehende Regel **Windows-Remoteverwaltung** aktiviert werden.



Alternativ ist natürlich auch eine Kommunikation mit TCP-Port 80 möglich, hier muss aber auf Wechselwirkungen mit einem eventuell vorhandenen Webserverdienst geachtet werden.

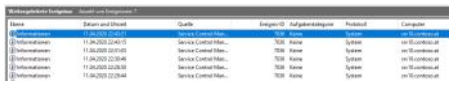
Hinweis: Wenn Sie mit dem Computerkonto des Sammlungscomputers auf die Ereignisprotokolle der überwachten Computer zugreifen wollen, so ist es notwendig, das Computerkonto des Sammlungscomputers zur lokalen Gruppe **Ereignisprotokollleser** der überwachten Computer hinzuzufügen.

Klicken Sie auf **Ok**, um das Abonnement zu erstellen. Falls noch Konfigurationsänderungen nötig sind, kann folgende Meldung erscheinen, die Sie mit **Ja** bestätigen müssen.



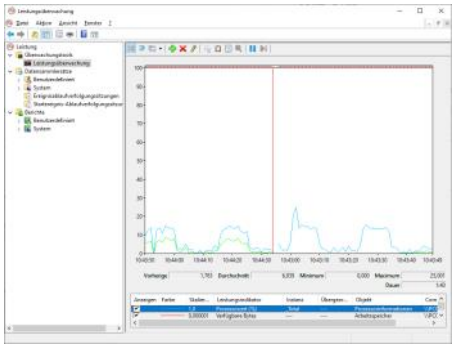
Ab diesem Zeitpunkt erscheint das konfigurierte Abonnement in der Abonnement-Liste:

Wird nun auf dem Quellcomputer beispielsweise der DNS-Serverdienst gestoppt und wieder gestartet, so findet man diese Ereignisse unter „Weitergeleitete Ereignisse“ am Zielcomputer:



14.14 Leistungsüberwachung

Die MMC-Konsole Leistungsüberwachung bietet eine Vielzahl von Berichten.



Berichte, z.B. System Diagnostics

14.15 Problembehandlung

14.15.1 Windows Troubleshooting Platform (WTP)

Die neue Windows Troubleshooting Platform verwendet Powershell-Scripts zur Analyse und Behebung computerbezogener Probleme.

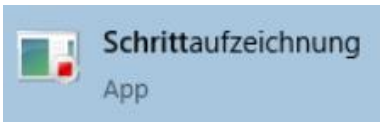
Die WTP beinhaltet drei Komponenten:

- Troubleshooting Packs: Ein solches Paket besteht aus einer XML-Manifest-Datei, die die ursprünglichen Ursachen eines Zustands beschreiben, sowie aus Powershell-Scripts, die das Problem analysieren und gegebenenfalls lösen. Windows 10 enthält etwa 24 integrierte Pakete.
- Troubleshooting Engine
- Troubleshooting Wizard: Mit diesem Assistenten kann der Benutzer durch die einzelnen Schritte geführt werden, die ein Troubleshooting Pack benötigt.

14.15.2 Schrittaufzeichnung (Problem Steps Recorder)

Windows 10 enthält ein Tool mit dem Namen **Problem Steps Recorder** (Dateiname psr.exe), mit dem Benutzer ihre Aktionen als Folge von Screenshots aufzeichnen können.

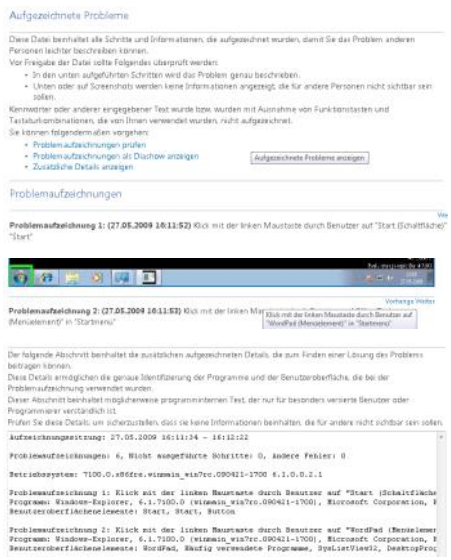
Sie finden das Tool im Startmenü in der Programmgruppe **Windows-Zubehör**, oder Sie suchen nach **psr** (oder nach Schrittaufzeichnung):



Der Recorder startet, mit „Aufzeichnung starten“ wird die Aufzeichnung begonnen.

Nun wiederholt der Anwender genau die Schritte, die zu seinem Problem geführt haben, und beendet dann die Aufzeichnung.

Nach Beendigung der Aufzeichnung wird ein gezipptes MHT-Dokument erstellt (die folgende Abbildung stellt nur einen Ausschnitt aus einem derartigen Dokument dar):



14.16 Treiber und Hardware-Installation

14.16.1 Installation von Plug & Play-Geräten

Beim Anstecken von USB-Geräten oder anderen Plug-and-Play-Geräten wird eine automatische Hardwareerkennung durchgeführt.

Die Installation und der erfolgreiche Abschluss wird als Info Center-Meldung angezeigt (als Beispiel: eine USB-Webcam):

Da die mit Windows 10 mitgelieferte Treiberbibliothek sehr umfangreich ist, werden die einzelnen Teilkomponenten von heute üblichen Geräten automatisch erkannt.

Sie können die installierten Geräte in den Einstellungen  überprüfen; wenn das

Gerät nicht erkannt wurde, so wählen Sie **Bluetooth- oder** anderes **Gerät hinzufügen**.

14.16.2 Geräte-Manager

Ein Eingreifen ist allerdings dann möglich, wenn in der Windows-Treiberbibliothek kein passender Treiber für eine Hardwarekomponente gefunden wird.

Öffnen Sie dazu den **Geräte-Manager**. Dieser ist über das Systemsteuerungselement System (Tastenkombination ⊞+ Pause) erreichbar:

Solche Komponenten werden unter der Rubrik **Andere Geräte** mit einem gelben Warnsymbol angezeigt, wie in der folgenden Abbildung ersichtlich:

Hier wurde eine neue Netzwerkkarte eingebaut, deren Treiber aber nicht in der mitgelieferten Treiberbibliothek von Windows enthalten ist.

In diesem Fall gibt es mehrere Möglichkeiten:

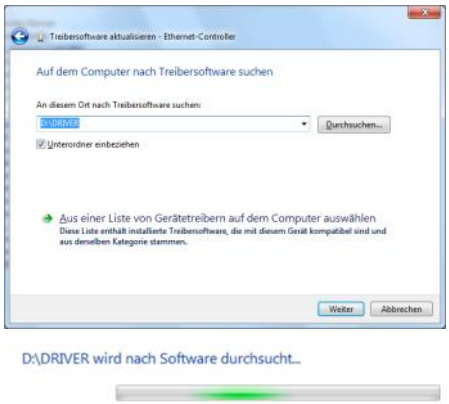
- Sie verfügen über einen vom Hersteller mitgelieferten Datenträger (CD) mit dem passenden Treiber.
- Sie laden vom Internet (Herstellerseite) den passenden Treiber herunter und speichern ihn auf einem Datenträger.

Legen Sie den Datenträger mit der Treibersoftware ins passende Laufwerk ein und klicken Sie mit der rechten Maustaste auf das Gerät, für das kein passender Treiber vorhanden war. Wählen Sie den Menüpunkt **Treibersoftware aktualisieren…**:

Es erscheint nun ein Dialog, in welchem Sie auswählen können, ob automatisch nach Treibern gesucht werden soll, oder ob Sie einen Pfad eingeben wollen.

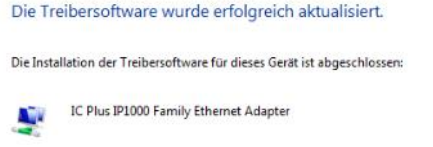
Die automatische Suche bezieht immer auch das Internet mit ein. In unserem Beispiel ist diese Variante nicht möglich, weil die Anbindung ans Internet über die soeben eingebaute Netzwerkkarte erfolgen sollte. (Das muss natürlich nicht so sein; es gibt auch USB-Geräte und WLAN-Karten, die für die Herstellung der Internetkonnektivität verwendet werden können.)

Wenn Sie einen Datenträger mit Treibern haben, so wählen Sie **Auf dem Computer nach Treibersoftware suchen** und legen im nächsten Schritt den Pfad zum Ordner fest, in welchem sich die Treiber befinden.

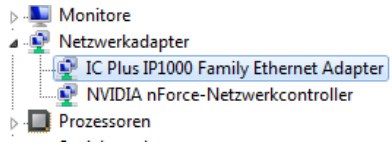


Wird am angegebenen Speicherort passende Software gefunden, so wird diese sofort installiert:

Der Abschluss des Vorgangs wird gemeldet:



Prüfen Sie im Geräte-Manager nach, ob die Komponente nun unter der korrekten Kategorie (Netzwerkadapter) erscheint und auch ohne Warnsymbol angezeigt wird:



Nun können Sie davon ausgehen, dass die neu installierte Komponente auch funktioniert.

Ressourcenverwaltung

Jede Hardwarekomponente benötigt eine Reihe von Ressourcen, um ihre Arbeit fehlerfrei durchführen zu können.

Zu diesen Ressourcen gehören:

- IRQ
- E/A-Speicherbereich
- RAM-Speicherbereich
- bei manchen Geräten: DMA-Kanal (zum Beispiel Diskettenlaufwerkscontroller)

IRQ (Interrupt Requests)

Das BIOS enthält Funktionen, die während des Betriebs von großer Bedeutung sind, die so genannte **Hardware-Interrupt-Verwaltung**. Hardware-Interrupts sind Signale, die von externen Geräten (Tastatur, Bildschirm, Drucker) ausgelöst werden und die CPU bei ihrer laufenden Arbeit unterbrechen. An dieser Stelle wird zunächst in der so genannten Interrupt-Tabelle (die sich im RAM befindet und auch geändert werden kann) nachgesehen. Dort befindet sich die Adresse des entsprechenden BIOS-Programms, welches dann aufgerufen wird.

Es gibt auch Interrupts, die nicht von den Geräten stammen, sondern von gerade laufenden Programmen. Diese heißen sinngemäß **Software-Interrupts.** Auch diese Interrupts rufen spezielle BIOS-Programme auf. Hardware- und Software-Interrupts arbeiten unabhängig voneinander, dienen aber demselben Zweck – sie regeln die Ein- und Ausgabe von Daten.

Die Interruptsignale müssen über eigene Interrupt-Leitungen übertragen werden. Hier unterscheidet man 16 IRQ-Leitungen (*IRQ = interrupt request*).

Die möglichen Belegungen können je nach Typ der Hardware folgendermaßen eingestellt werden:

- Jumper (Steckbrücken)
- Konfigurationsprogramm (dabei muss die E/A-Adresse bekannt sein)
- BIOS: über das CMOS-Setup-Programm
- Plug-and-Play-Erweiterungen

IRQ-Leitung	mögliche Belegung
IRQ 0	Zeitgeber
IRQ 1	Tastatur
IRQ 2	2. Interrupt-Controller
IRQ 3	COM2/4
IRQ 4	COM1/3 (meist für Maus oder Modem)
IRQ 5	LPT2
IRQ 6	Controller für das Diskettenlaufwerk
IRQ 7	LPT1 (meist für Drucker)
IRQ 8	Uhr, Kalender
IRQ 9	Rückführung von IRQ 2
IRQ 10	frei
IRQ 11	frei
IRQ 12	frei (oder PS/2-Maus)
IRQ 13	Coprozessor
IRQ 14	IDE-Controller (Kanal 1)
IRQ 15	IDE-Controller (Kanal 2)

Der Interrupt-Controller arbeitet nahezu gleichzeitig auftretende Interrupts nach Prioritäten ab. Dabei gilt: Je niedriger die Nummer des IRQs, desto höher ist dessen Priorität.

Seit vielen Jahren (80286-Prozessor) werden zwei Interrupt-Controller verwendet. Diese beiden Controller sind so verschaltet, dass der Ausgabe des zweiten Interrupt-Controllers mit dem IRQ 2 des ersten Controllers verbunden ist. Man spricht von „Kaskadierung“ der Interrupt-Controller.

Auf Grund dieser Kaskadierung ergibt sich folgende Reihenfolge an IRQ-Prioritäten:

0, 1, [8, 9, 10, 11, 12, 13, 14, 15], 3, 4, 5, 6, 7

Die in eckigen Klammern dargestellten IRQs werden vom zweiten Interrupt-Controller zur Verfügung gestellt und an Stelle des IRQ 2 „eingefügt“.

Heute kommt bei vielen PCs statt der beiden normalen Interrupt-Controller ein **APIC (Advanced Programmable Interrupt Controller)** zum Einsatz, der Peripheriegeräten insgesamt **24 IRQs** zur Verfügung stellen kann und darüber hinaus über erweiterte Funktionen wie etwa dynamische Prioritätenvergabe verfügt.

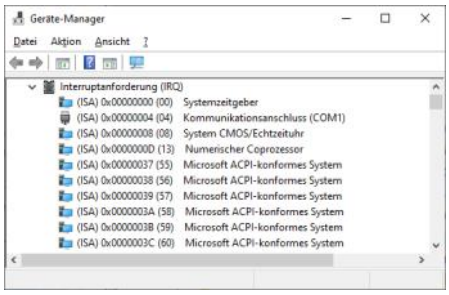


Abbildung: Auszug aus dem Windows 10-Gerätemanager: Ressourcen nach Typ

Jeder Interrupt hat eine eigene hexadezimale Kenn-Nummer (INT 01h, INT 02h, ...).

Übersicht über Interrupt-Belegungen: http://www.ctyme.com/intr/int.htm

Man unterscheidet beim PC:

- prozessorinterne Interrupts = „Traps“ (INT 00h – 07h, z.B. bei Division durch 0 wird INT 00h ausgelöst)
- durch Peripheriegeräte ausgelöste Interrupts (INT 08h – 0Fh)
- BIOS-Interrupts (Nummer INT 10h – 1Ah)
- Anwender-Interrupts (INT 1Bh – 1Fh, z. B.. INT 1Bh = Drücken von CRTL-Break)

Betriebssystem-Interrupts (INT 20h – FFh, z. B. INT 3Dh = Vorhandene Datei öffnen)

Funktionsweise von BIOS-Interrupts anhand der Tastatursteuerung:

Hier ist der BIOS-Interrupt mit der Nummer 16h zuständig. Drückt man eine Taste auf der Tastatur, so entsteht ein elektrischer Impuls, der an eine spezielle Schaltung, die **Tastatursteuerlogik**, weitergeleitet wird. Diese Schaltung erzeugt einen so genannten Scancode, der genau der gedrückten Taste entspricht. Danach wird ein Interrupt an die CPU gesendet; die CPU löst dann ein BIOS-Programm (eine so genannte **Interrupt-Service-Routine, ISR**) aus, die dem Tastatursignal den entsprechenden ASCII-Code zu-ordnet. ASCII-Code und Scancode werden im Tastaturpuffer abgelegt, von wo sie zur Darstellung des Zeichens auf dem Bildschirm oder Drucker verwendet werden können. **Treiber-programme** wirken genau hier: Sie „stehlen“ den Interrupt und statt des BIOS-Programms wird das Treiberprogramm ausgeführt. Das heißt, über Tastaturtreiber kann man eine geänderte Tastaturbelegung erreichen (z. B. englisch/deutsch). Übrigens: manche **Viren** wirken genauso!

- Bildschirmsteuerung: INT 10h.
- *Drucker:* INT 17h.
- Floppy Disk: INT 13h.

Ports (I/O-Adressen)

Neben dem Arbeitsspeicher kann der Prozessor auf einen speziellen Speicherbereich zugreifen, den man als "Ein-/Ausgabebereich" bezeichnet.

Das **Isolated I/O-Verfahren** (isolierte Adressierung) ein Verfahren zur Adressierung von Speicherzellen angeschlossener Peripheriegeräte in einem Mikrocomputer. Beim Memory Mapped I/O werden die Register des Peripheriegerätes auf Speicherzellen innerhalb des gewöhnlichen Adressraumes abgebildet und vom Prozessor auch als solche angesteuert. Beim Isolated I/O verwendet man hingegen einen isolierten Adressraum, der wesentlich kleiner ist und separat vom Hauptspeicher-Adressraum angesteuert wird. Dieser Adressraum wird auch als I/O -Adressraum bezeichnet. Zur Auswahl des jeweiligen Adressraumes wird bei der Adressierung durch den Mikroprozessor ein zusätzliches Signal wie z. B. MREQ (Memory Request) verwendet. Die ansteuernde Software muss über spezielle I/O-Befehle verfügen, die diese Signale aktivieren und so den eigenen Adressraum ansprechen.

Ein typisches Beispiel ist der Framebuffer des Monitors, der in einem geschützten Speicherbereich oder auf der Grafikkarte liegt, und vom Grafiktreiber unabhängig von der Ausleserate des Anzeigegeräts befüllt werden kann.

Hier befinden sich die externen Bausteine, die besondere Funktionen wie etwa Zeiterfassung, Bildschirmsteuerung usw. realisieren. Diese Bausteine werden vom Prozessor gesteuert und müssen daher Informationen an die CPU liefern (Eingabe) oder Informationen von der CPU erhalten (Ausgabe).

Der I/O-Bereich ist wesentlich kleiner als der Hauptspeicher. Es stehen genau 64 KByte (= 65536) Adressen zur Verfügung.

Um diesen Bereich zu adressieren, benötigt man 16 bit-Adressen (int-Variablen).

Eingeblendete RAM-Bereiche (Memory Mapped I/O)

Wenn Peripheriegeräte dem System größere Speichermengen zur Verfügung stellen müssen (etwa Grafikkarten), wird der auf den Geräten befindliche Speicher in den RAM „eingeblendet". Das hat zur Folge, dass das System den Speicher auf dem Gerät genauso ansprechen kann wie „normale" Informationen im RAM. Damit kann sowohl die CPU als auch das Gerät (die Karte) auf den Speicherbereich zugreifen.

DMA (Direct Memory Access)-Kanäle

Damit Daten weiter verarbeitet werden können, müssen sich diese im RAM befinden. Wird von einem externen Datenträger – etwa einer Festplatte – gelesen, so hat die CPU zwei Möglichkeiten, die Daten vom Festplattencontroller in den RAM zu verschieben:

- Sie liest so lange von einer Portadresse, bis keine Daten mehr vorhanden sind (Programmed I/O, kurz PIO). Der Nachteil dieses Verfahrens ist, dass die CPU durch relativ simple Vorgänge stark belastet wird. So verursachen IDE-Systeme im PIO-Modus bei Schreib-/Lese-Operationen CPU-Lasten von bis zu 70 %!
- Die CPU beauftragt den DMA-Controller, Daten so lange vom Gerät in den RAM zu verschieben, bis keine Daten mehr vorhanden sind. Durch diese Vorgangsweise wird die CPU entlastet, da ein eigener Controller den Datentransfer vornimmt. Ist der DMA-Controller fertig, so meldet er dies an die CPU, die sich dann um die weitere Verarbeitung der Daten kümmern kann.

DMA-Kanäle können je nach Alter und Typ des Geräts (der Karte) folgendermaßen konfiguriert werden:

- Jumper (Steckbrücken)
- Konfigurationsprogramme (I/O-Adresse muss bekannt sein)
- BIOS: über das CMOS-Setup-Programm

14.17 Debugging Blue Screens

Fehlerhafte Treiber, systemnahe fehlerhafte Software oder physisch schadhafte Hardwarekomponenten können bewirken, dass Windows-NT-basierte Betriebssysteme (zu denen auch Windows 10 gehört) instabil werden und nicht mehr ausführbar sind. In diesem Fall wird ein „Blue Screen of Death" angezeigt (siehe Abbildung).

Windows erzeugt in diesem Fall einen Mini-Speicherdump im Verzeichnis C:\ mit *.tmp-Dateien wie diese: (rechts unten)

I/O-Adressen		
Adressbereich	**Anzahl Bytes**	**Funktion (ab AT)**
000 - 00F	16	1. DMA-Controller (8237) für 8 bit-Transfers
010 - 01F	16	reserviert
020 - 021	2	1. Interrupt-Controller 8259 (IRQ 0 - IRQ 7, INT 08 - 0F in Interrupttabelle)
040 - 043	4	Zeitgeber (8253)
060	1	Tastaturport (Scan-Code)
061	1	Systemstatusbyte (zB NMI-Kontrolle)
064	1	Tastaturkommando-Port
066 - 067	2	PC-Konfiguration (herstellerabhängig!)
070 - 071	2	CMOS-RAM (Setup)
080 - 087	8	DMA Page Register und RAM Refresh
0A0 - 0A1	2	2. Interrupt-Controller für IRQ8 - IRQ15
0C0 - 0CF	16	2. DMA-Controller für 16 bit-Transfers
0F0 - 0FF	16	Coprozessor (8087, 80287)
1F0 - 1F8	4/8	Festplatten-Controller
200 - 20F	16	Game-Adapter
278 - 27F	8	LPT2
2E8 - 2EF	8	COM4
2F8 - 2FF	8	COM2
378 - 37F	8	LPT1
3C0 - 3CF	8	EGA/VGA-Karte
3E8 - 3EF	8	COM3
3F0 - 3F7	8	Floppy Disk Drive Controller
3F8 - 3FF	8	COM1

Notieren Sie den sogenannte **Stopcode**, also die Fehlermeldung, die im unteren Bereich angezeigt wird (in diesem Fall: PAGE FAULT IN NONPAGED AREA).

Mit den Debugging Tools von Windows wird eine Fehleranalyse erleichtert:

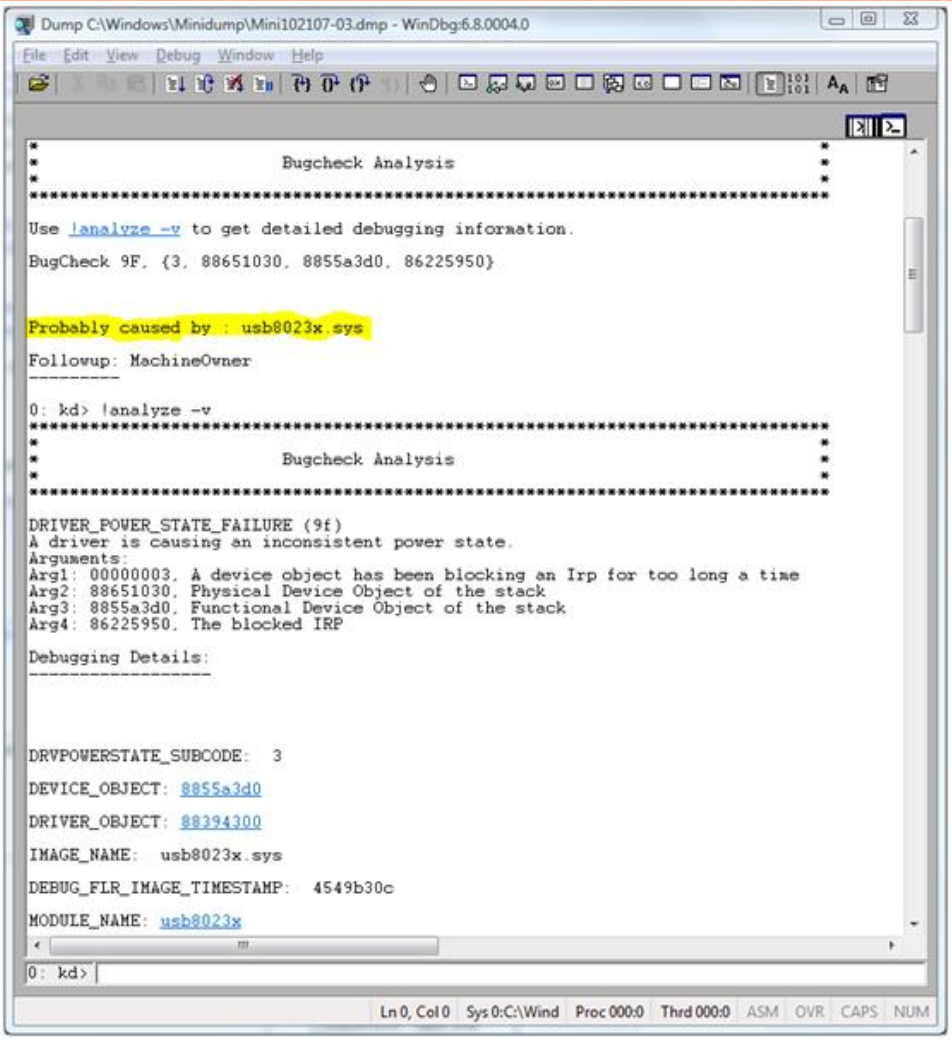
- Zunächst besorgen wir uns die Debugging Tools für unsere Plattform: https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/debugger-download-tools
  Es gibt sowohl die „klassischen" Tools als Bestandteil des Windows 10 SDK (Software Development Kit) als auch eine Neuentwicklung, die als Microsoft Store-App vertrieben wird.
- Dann starten wir **windbg** - Wichtig: Als Administrator ausführen!
- Im File Menü, klicken wir auf Symbol File Path.
- Im Symbol Path Fenster geben wir folgendes ein:
- `"srv*c:\cache*http://msdl.microsoft.com/download/symbols;"`
  und bestätigen mit 'ok'
- Im File Menü wählen wir "open crash dump..." und wählen unter c:\Windows\Minidump das File aus, das wir analysieren wollen - in der Regel das neueste.
  Für jeden Crash liegt ein Crash Dump File mit einem Namen wie Mini102107-03.dmp in dem Verzeichnis.
- Jetzt ein paar Sekunden auf das Ergebnis warten - Falls die Firewall sich meldet - es wird versucht auf die Symbol Files unter msdl.microsoft.com/download/symbols zuzugreifen - muss man die Firewall Warnung bestätigen, windbg schließen und noch einmal bei Punkt 2 bestätigen.

Im Ergebnisfenster sucht man die Zeile „Probably caused by:" - Danach steht der Übeltäter fest: (Bild rechts)

Mit einer guten Suchmaschine findet man schnell Näheres heraus, dann einfach eine neue Treiberversion vom Hersteller herunterladen und das Problem sollte behoben sein.

Möchte man mehr wissen, kann man noch !analyze -v ausführen und bekommt dann noch genauere Hinweise: (Text unter dem Bild rechts)

In diesem Fall war also der Übeltäter usb8023x.sys - der Remote NDIS USB driver.



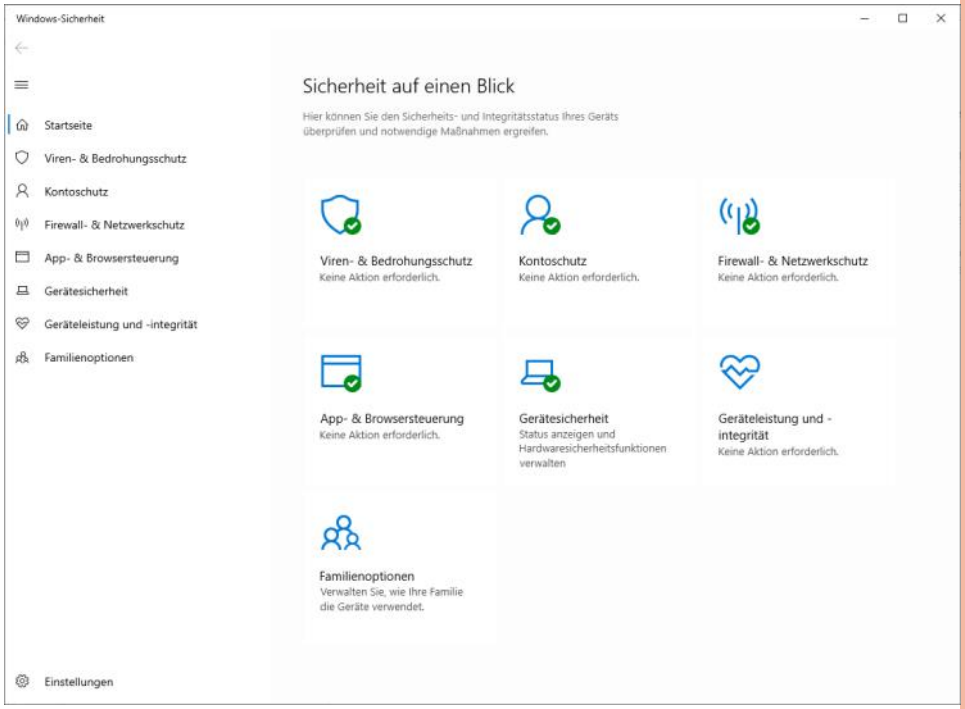

```
*******************************************************************************
*                                                                             *
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************
DRIVER_POWER_STATE_FAILURE (9f)
A driver is causing an inconsistent power state.
Arguments:
Arg1: 00000003, A device object has been blocking an Irp for too long a time
Arg2: 88651030, Physical Device Object of the stack
Arg3: 8855a3d0, Functional Device Object of the stack
Arg4: 86225950, The blocked IRP
```

15 Sicherheitseinstellungen

Christian Zahler

15.1 Windows-Sicherheit

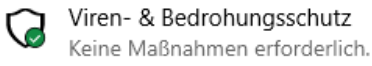
In Windows 10 gibt es das App **Windows-Sicherheit**, das eine zentrale Stelle für die Konfiguration von Sicherheitsmaßnahmen aller Art ist. Hauptsächlich geht es dabei um den Schutz vor Bedrohungen von außen, also um Anti-Malware-Funktionalität und Firewallkonfiguration. (Bild rechts)



Einige wenige Einstellungen sind noch über die **Systemsteuerung – Sicherheit und Wartung** erreichbar.

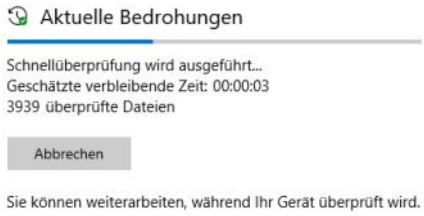
15.1.1 Windows Defender Antivirus (Viren- und Bedrohungsschutz)

Über die Einstellungen können Sie im Bereich **Windows-Sicherheit** unter anderem den Viren- und Bedrohungsschutz konfigurieren.

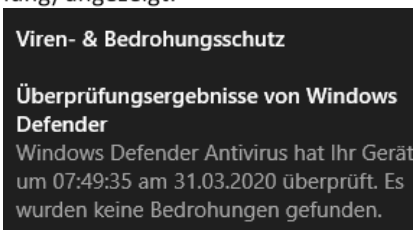


Windows Defender Antivirus ist Ihr Echtzeitschutz gegen Bedrohungen wie Viren und Schadsoftware in E-Mails, Apps und im Web.

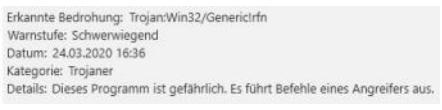
Sie können eine Schnellüberprüfung durchführen und Einstellungen verwalten.



Im Infocenter wird nach Abschluss des Scans eine Erfolgsmeldung (oder Warnung) angezeigt:

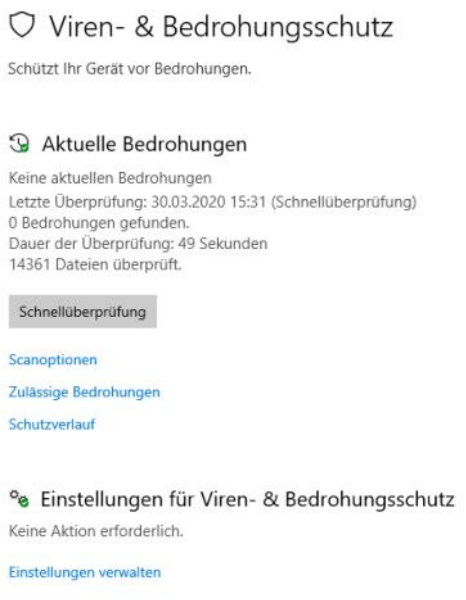


Wird eine Bedrohung gefunden, so wird sofort eine Warnmeldung angezeigt:



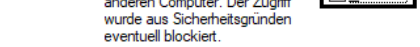
Umgehen von Microsoft Defender

Es kann vorkommen, dass eine Softwareinstallation fehlschlägt, weil die aus dem Internet heruntergeladenen Dateien von Microsoft Defender als potentielle Bedrohung angesehen werden.



Dies zeigt sich in Form einer Meldung wie der folgenden:

Umgehen dieser Meldung: Dateieigenschaften – Sicherheit: **Zulassen** anklicken



Online Scan

Manchmal ist es interessant, ohne zusätzliche Installation einer Anti-Malware-Software ein System oder unbekannte Dateien zu überprüfen; es ist durchaus empfehlenswert, fallweise auch Produkte anderer Anbieter einzusetzen.

Beispiele für Anbieter von Online-Scan-Tools:

- ESET
  https://www.eset.com
  Vollversion kostenpflichtig
- VirusTotal
  https://www.virustotal.com/gui/home
  nur einzelne Dateien

Hinweis: Die Installation mehrerer Antivirenprodukte auf einem System wird nicht empfohlen, da dies üblicherweise zu Leistungseinbußen führt.

15.1.2 Windows Defender Firewall

Die Windows Defender-Firewall sorgt für einen Schutz vor Hackern, Viren und Würmern, die versuchen, aus dem Internet auf Ihren Computer zu gelangen.

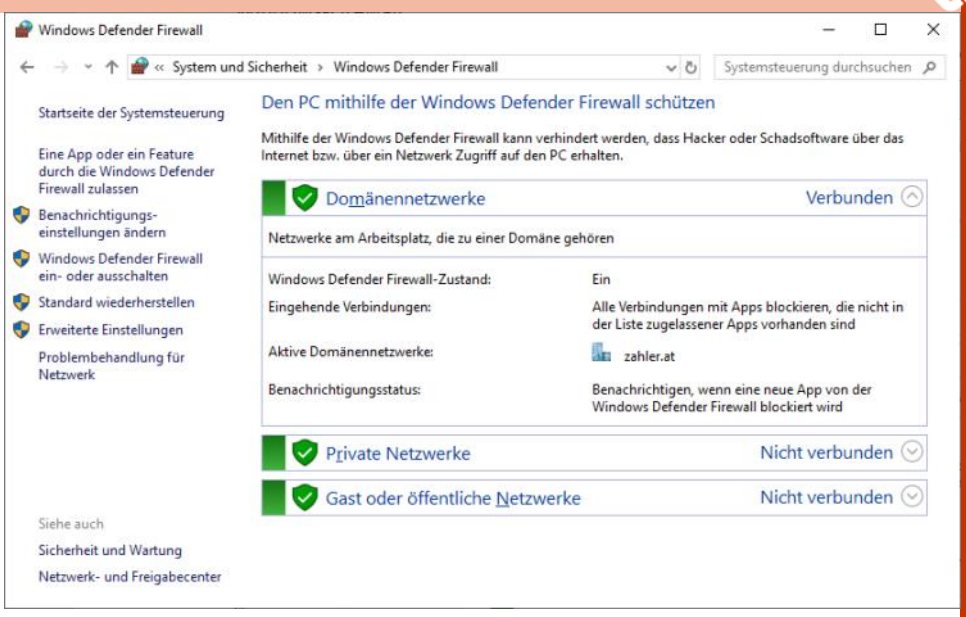
Eine Firewall trägt zur Sicherheit des Computers bei. Sie schränkt die Übertragung von Informationen, die von anderen Computern bei Ihrem Computer eingehen, ein, so dass Sie eine bessere Kontrolle über die Daten auf Ihrem Computer haben und besser vor Personen oder Programmen (einschließlich Viren und Würmer) geschützt sind, die unaufgefordert versuchen, eine Verbindung mit Ihrem Computer herzustellen.

Sie können sich eine Firewall wie eine Absperrung vorstellen, die die Daten (häufig auch Verkehr genannt), die aus dem Internet oder einem Netzwerk eingehen, überprüft und diese Daten dann in Abhängigkeit von den Firewalleinstellungen entweder zurückweist oder zum Computer passieren lässt.

In Microsoft Windows 10 ist die Windows-Firewall standardmäßig aktiviert. (Möglicherweise wird sie jedoch von einigen Computerherstellern und Netzwerkadministratoren deaktiviert.) Es ist nicht nötig, die Windows-Firewall zu verwenden; Sie können jeden gewünschten Firewall installieren und ausführen. Informieren Sie sich über die Features anderer Firewalls, und entscheiden Sie dann, welcher Firewall Ihre Anforderungen am besten erfüllt. Wenn Sie sich für die Installation und Ausführung einer anderen Firewall entscheiden, sollten Sie die Windows-Firewall deaktivieren.

Funktionsweise: Wenn ein Benutzer im Internet oder in einem Netzwerk versucht, eine Verbindung mit Ihrem Computer herzustellen, sprechen wir bei diesem Versuch von einer "unverlangten Anforderung". Wenn eine unverlangte Anforderungen bei Ihrem Computer eingeht, wird die Verbindung von der Windows-Firewall gesperrt. Wenn Sie ein Programm ausführen, z. B. ein Instant Messaging-Programm oder ein Multiplayer-Netzwerkspiel, das auf den Empfang von Daten aus dem Internet oder einem Netzwerk angewiesen ist, werden Sie von der Firewall gefragt, ob die Verbindung gesperrt bleiben oder die Sperrung aufgehoben (d. h. die Verbindung zugelassen) werden soll. Wenn Sie die Sperrung der Verbindung aufheben, erstellt der Windows-Firewall eine Ausnahme, so dass sich der Firewall in Zukunft nicht mehr daran stört, wenn dieses Programm Daten empfangen muss.

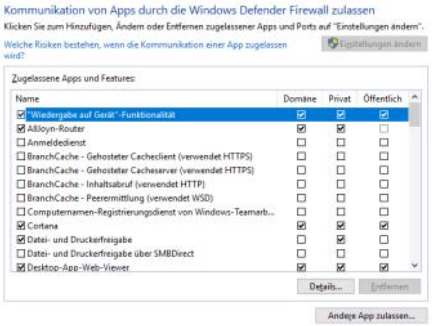
Wenn Sie beispielsweise Sofortnachrichten mit einer anderen Person austauschen, die Ihnen eine Datei (z. B. ein Foto) senden möchte, werden Sie vom Windows-Firewall gefragt, ob Sie die Sperrung für die Verbindung aufheben und den Empfang des Fotos auf Ihrem Computer zulassen möchten. Wenn Sie zusammen mit Freunden ein Multiplayerspiel über das Internet spielen möchten, können Sie das Spiel ebenfalls als Ausnahme hinzufügen, so dass der Firewall den Empfang der Spieledaten auf Ihrem Computer zulässt.



Konfiguration der Windows Firewall: Systemsteuerung – Windows Defender Firewall

Hier kann man verschiedene Basiseinstellungen setzen, etwa die Firewall komplett ausschalten (**nicht empfohlen!**) oder Benachrichtigungseinstellungen ändern.

Klickt man auf **Eine App oder ein Featzure durch die Windows Defender Firewall zulassen**, so kommt man zu einem Dialog, in welchem man die Firewall für bestimmte Apps durchlässig machen kann.



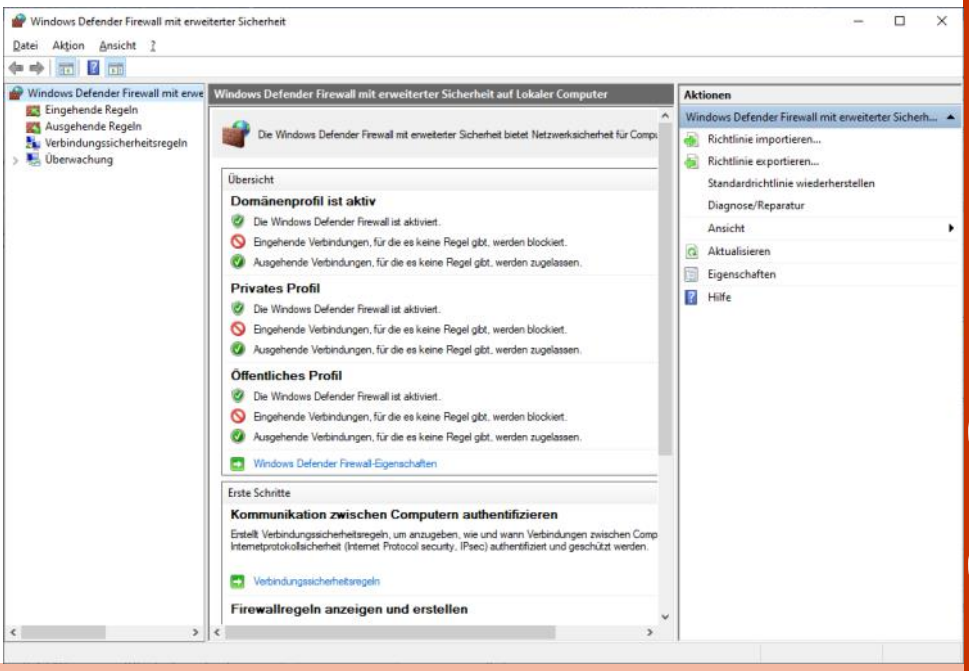
Erweiterte Firewall-Konfiguration

Klickt man auf Erweiterte Einstellungen, so kommt man zum Systemsteuerungselement **Windows-Firewall mit erweiterter Sicherheit**. Hier lassen sich Firewallregeln detailliert konfigurieren (Bild rechts unten).

Beispiele für benötigte Ports:

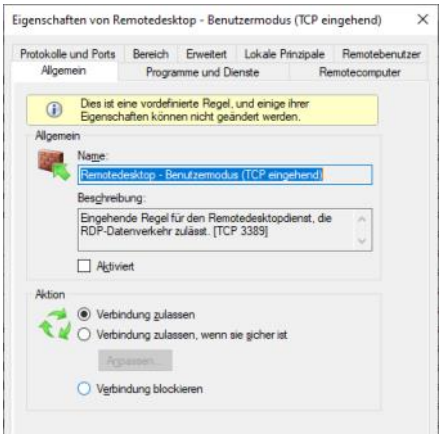
Datei- und Druckerfreigabe: TCP 139, 445, UDP 137, 138

Remote-Desktop: 3389



VPN: 1723

Beispiel: Eingehende Firewall-Regel für RDP (Remote Desktop Protocol)



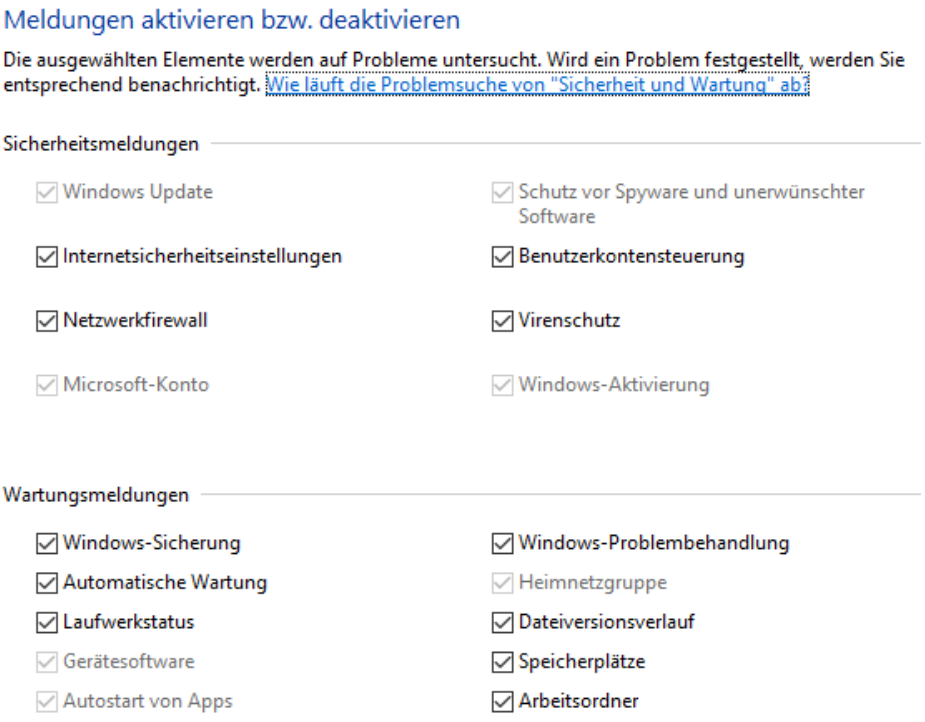
15.2 Konfigurieren von Benachrichtigungen und Meldungen

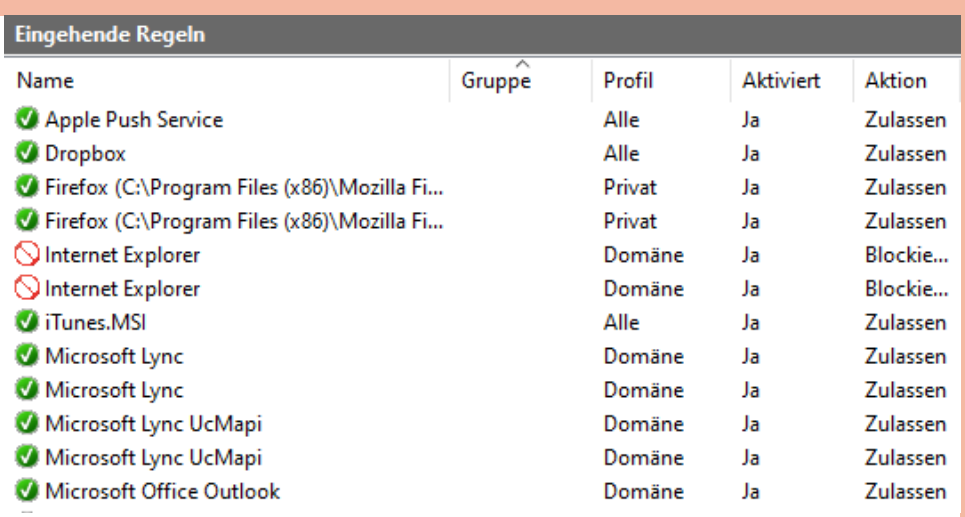
Im Infocenter werden periodisch Systemmeldungen angezeigt. Diese Meldungen lassen sich in der **Systemsteuerung – Sicherheit und Wartung** konfigurieren. Klicken Sie dazu auf den Link **Einstellungen für „Sicherheit und Wartung“** ändern.

Wenn Sie auf den Link Sicherheit und Wartung klicken, so erhalten Sie einen Überblick über Wartungsmeldungen. (Bild links unten)

5.3 Windows Update

Windows Update sorgt durch die Bereitstellung von Microsoft Windows 10-Softwareupdates dafür, dass Ihr Computer sicherheitstechnisch auf dem neuesten





Eingehende Regeln

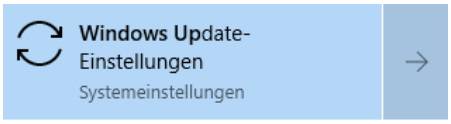
Name	Gruppe	Profil	Aktiviert	Aktion
Apple Push Service		Alle	Ja	Zulassen
Dropbox		Alle	Ja	Zulassen
Firefox (C:\Program Files (x86)\Mozilla Fi...		Privat	Ja	Zulassen
Firefox (C:\Program Files (x86)\Mozilla Fi...		Privat	Ja	Zulassen
Internet Explorer		Domäne	Ja	Blockie...
Internet Explorer		Domäne	Ja	Blockie...
iTunes.MSI		Alle	Ja	Zulassen
Microsoft Lync		Domäne	Ja	Zulassen
Microsoft Lync		Domäne	Ja	Zulassen
Microsoft Lync UcMapi		Domäne	Ja	Zulassen
Microsoft Lync UcMapi		Domäne	Ja	Zulassen
Microsoft Office Outlook		Domäne	Ja	Zulassen

Stand bleibt. Sie können Windows Update so konfigurieren, dass Updates automatisch heruntergeladen und installiert werden. Sie müssen dieses Feature lediglich aktivieren und brauchen sich anschließend nicht mehr darum zu kümmern.

Updates beinhalten Fehlerkorrekturen, Sicherheitspatches und Verbesserungen und sollten daher regelmäßig eingespielt werden.

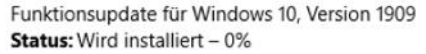
15.3.1 Updates verwalten und einspielen

Die Verwaltung des Update-Dienstes erfolgt in den **Systemeinstellungen**. Geben Sie in der Windows-Suche das Wort „Update“ ein; dann werden Ihnen die beiden Systemeinstellungs-Menübereiche **Windows Update-Einstellungen** und **Nach Updates suchen** automatisch vorgeschlagen.



Klickt man auf die Schaltfläche **Nach Updates suchen**, so wird auch außerhalb der regelmäßigen Update-Intervalle nach Updates gesucht. Das kann einige Zeit in Anspruch nehmen.

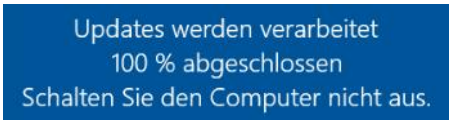
Sind Updates verfügbar, so werden diese angezeigt, außerdem wird ein Link **Herunterladen und installieren** angezeigt. Während der Installation kann das Fenster geschlossen werden; bleibt es offen, so wird der Installationsstatus angezeigt.



Bei großen Funktionsupdates oder sicherheitskritischen Updates muss nach dem Einspielen der Computer neu gestartet werden.

In diesem Fall wird folgende Meldung angezeigt:

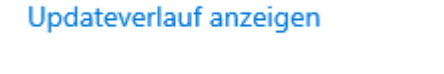
Achtung: Die Verarbeitung der Updates beim Neustart kann wirklich lange dauern (unter Umständen auch Stunden). Es wird üblicherweise folgende Meldung angezeigt:



Die Anweisung, den Computer nicht auszuschalten (oder gar den Netzstecker zu ziehen), ist ernst gemeint – es könnte nämlich sonst sein, dass die Systemstabilität derart in Mitleidenschaft gezogen wird, dass ein Neustart gar nicht möglich ist.

15.3.2 Updates anzeigen und deinstallieren

Über den Link **Updateverlauf anzeigen** kommt man zu einer Übersicht, welche Updates wann eingespielt wurden.



Hier ist es möglich, Updates zu deinstallieren.

15.3.3 Windows-Update im Domänenbetrieb

In Windows-Domänen werden die Update-Einstellungen teilweise zentral vom Domänenadministrator verwaltet. Sie können das erkennen, wenn folgende Meldung dargestellt wird:

Die vom Administrator eingestellten Gruppenrichtlinien können angezeigt werden:

15.3.4 Updates von anderen Clientcomputern beziehen

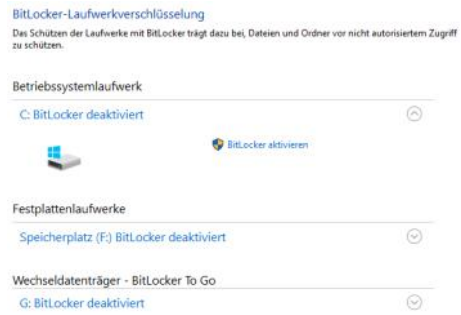
Neu in Windows 10 ist die Möglichkeit, heruntergeladene Updates im internen Netzwerk zu verteilen, ohne dass ein zentraler Update-Server (WSUS-Server) vorhanden ist (Bild unten, mitte).

15.4 BitLocker Drive Encryption

Eine der größten Neuerungen im Business-Bereich ist die Verschlüsselungstechnik rund um BitLocker. Enthalten ist die neue Technologie in den Ultimate- und der Enterprise-Edition sowie der kommenden Server-Version. Bitlocker verschlüsselt die Windows-Partition; dabei ist der Schutz bereits während des Bootvorgangs aktiv.

Sie können die Konfiguration Laufwerksverschlüsselung über **Systemsteuerung – System und Sicherheit** erreichen:

Sie sehen zunächst den aktuellen Status der lokalen Laufwerke sowie der angeschlossenen Wechseldatenträger bzw. USB-Sticks.



Hinweis: Für die Verschlüsselung weiterer Partitionen steht **EFS (Encrypting File System)** zur Verfügung.

BitLocker Drive Encryption wurde entworfen, um Endbenutzern einen bestmöglichen Umgang mit Systemen zu ermöglichen, die über einen kompatiblen TPM-Mikrochip und ein entsprechendes BIOS verfügen. Ein TPM gilt als kompatibel, wenn es ein TPM der Version 1.2 mit allen entsprechenden BIOS-Änderungen ist, die erforderlich sind, um die von der Trusted Computing Group definierte BIOS-Erweiterung Static Root of Trust Measurement zu unterstützen. Das TPM interagiert mit BitLocker Drive Encryption, um beim Systemstart nahtlosen Schutz zu bieten.

BitLocker Drive Encryption kann auch auf Computern ohne ein kompatibles TPM verwendet werden. In diesem Fall können Sie mit BitLocker Drive Encryption zwar die Funktionen zur Volumeverschlüsselung verwenden, Sie erhalten jedoch nicht die zusätzliche Sicherheit durch die frühe Integritätsüberprüfung der Startdatei. Stattdessen wird die Identität des Benutzers beim Starten mithilfe eines USB-Flashlaufwerks überprüft.

BitLocker verfügt über zwei TPM-Modi:

- **TPM-only (Nur TPM):** Dieser Modus ist für den Benutzer transparent, und die Benutzeranmeldung erfolgt unverändert. Wenn das TPM jedoch fehlt oder geändert wird, startet BitLocker den Wiederherstellungsmodus, und Sie benötigen einen Wiederherstellungsschlüssel oder ein Wiederherstellungskennwort, um wieder auf die Daten zugreifen zu können.
- **Startup key (Systemstartschlüssel):** Der Benutzer benötigt einen Systemstartschlüssel, um sich am Computer anzumelden. Ein Systemstartschlüssel kann ein physischer (ein USB-Flashlaufwerk, auf das ein computerlesbarer Schlüssel geschrieben wurde) oder ein persönlicher (eine vom Benutzer festgelegte PIN) Schlüssel sein.

Außerdem unterstützt BitLocker einen Modus für Systeme ohne TPM:

- **USB Flash Drive key** (Schlüssel auf einem USB-Flashlaufwerk): Der Benutzer schließt vor dem Einschalten ein USB-Flashlaufwerk an den Computer an. Der Computer wird mit dem auf dem Flashlaufwerk gespeicherten Schlüssel entsperrt.

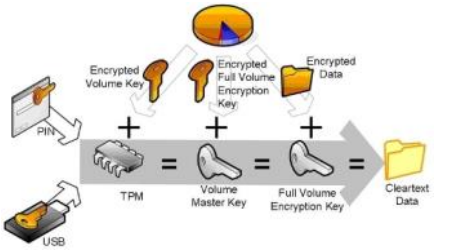
Bild nächste Seite, rechts oben

Gesicherte Daten: BitLocker arbeitet mit dem TPM zusammen und schützt so die Daten zuverlässig. (Quelle: Microsoft)

BitLocker verwendet bevorzugt Systeme, die ein **Trusted Platform Module Version 1.2** (TPM 1.2) oder höher aufweisen. Der notwendige Chip ist aktuell nur in einzelnen Business-Systemen verbaut, soll aber Bestandteil der kommenden Sicherheitsarchitekturen Presidio (AMD) und LaGrande (Intel) sein.

BitLocker schützt Festplatten sogar nach ihrem aktiven Einsatz. Wenn der Lebenszyklus einer Platte beendet ist, musste sie bisher entweder mechanisch verschrottet oder aufwendig gelöscht werden, um wirklich alle darauf enthaltenen Daten zu beseitigen. Nun reicht es, die entsprechenden Schlüssel zu löschen. Selbst wenn jemand die Festplatten in einen anderen PC einbaut, bleiben die Daten ohne die passenden Zugangsdaten unlesbar.

Die BitLocker-Technologie setzt an zwei Punkten an. Zum einen führt sie bei jedem Bootvorgang eine Integritätsprüfung durch, zum anderen verschlüsselt sie die ausgewählten Festplattenpartitionen.



Zutritt verweigert: Nur wenn alle digitalen Schlüssel passen, werden die Daten entschlüsselt. (Quelle: Microsoft)

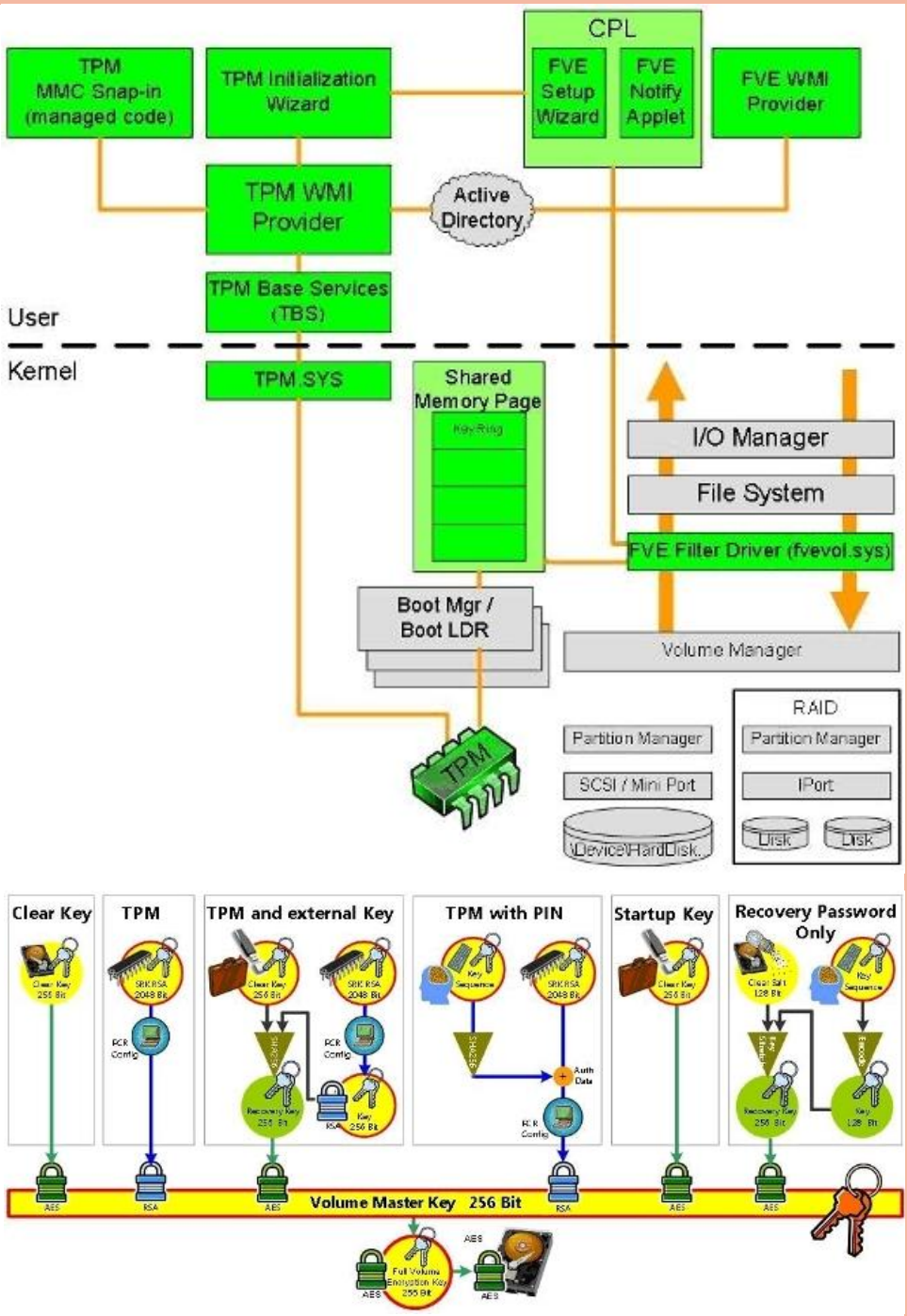
BitLocker greift dabei auf TPM zurück, um von dem System eine Art Fingerabdruck zu erzeugen. Solange an der eigentlichen Hardware nichts manipuliert wird, bleibt der digitale Fingerabdruck derselbe. Während des Bootvorgangs gleicht BitLocker die Daten ab, erst wenn die beiden Schlüssel übereinstimmen, werden die Daten auf der Festplatte entschlüsselt.

Wahlweise kann der Administrator auch einen PIN oder einen Hash-Key auf einem USB-Stick anfordern lassen, mit dem sich der Nutzer zusätzlich verifizieren muss. Erst wenn alle Schlüssel als gültig anerkannt sind, werden die Daten entschlüsselt, und der Startvorgang wird fortgesetzt.

Die Verschlüsselung der Partitionen macht sich ebenfalls TPM zu Nutze. Zunächst wird die angegebene Partition mit dem Full Volume Encryption Key (FVEK) verschlüsselt; dieser nutzt einen 256-Bit-AES-Algorithmus. Anschließend wird der FVEK erneut verschlüsselt, diesmal mit dem Volume Master Key (VMK), ebenfalls in 256 Bit AES.

Der Volume Master Key wird also als zusätzliche Schicht zwischen dem Anwender und den verschlüsselten Daten eingeführt. Das hat mehrere Vorteile. Der Anwender kommuniziert nie direkt mit dem Basisschlüssel, kann diesen also nicht mitloggen oder auslesen. Wenn die Sicherheit kompromittiert wurde, muss zudem nur der VMK neu erzeugt werden. Ein Ent- und anschließendes Neuverschlüsseln sämtlicher Partitionen mit geändertem Key ist daher nicht notwendig.

Aus dem VMK schließlich werden alle Schlüsselwerte für den Nutzer und die Recovery-Optionen erstellt. Löscht man also einen kompromittierten VMK, haben alle damit erstellten Schlüssel keinen Zugriff mehr.



Schlüsselbrett: Der Volume Master Key dient als zentraler Zugangsschlüssel. (Quelle: Microsoft)

15.4.1 Vorbereiten der Laufwerkskonfiguration für den Einsatz von BitLocker

Windows BitLocker-Laufwerkverschlüsselung ist ein Feature, das ein oder mehrere an den Computer angeschlossene Volumes (Laufwerke) verschlüsselt und die Integrität früher Startkomponenten mit einem TPM (Trusted Platform Module) verifizieren kann. Da BitLocker das gesamte Datenvolume verschlüsselt, muss der Computer mit einer aktiven, vom Betriebssystemvolume getrennten Partition konfiguriert sein, die für den Start verwendet wird. Dies wird als Konfiguration mit aufgeteilter Last (**Split-Load-Konfiguration**) bezeichnet. Benutzerdaten werden entweder auf dem Betriebssystemvolume oder zusätzlichen Datenvolumes gespeichert, die ebenfalls mit BitLocker verschlüsselt werden können.

Wichtig: **BitLocker funktioniert nur mit Basis-Datenträgern**! Dynamische Datenträger werden nicht unterstützt!

Voraussetzungen für die Aktivierung der BitLocker-Laufwerkverschlüsselung:

- **Mindestens zwei Partitionen** (auch Volumes genannt). Eine Partition ist für das Betriebssystem vorbehalten (in der Regel Laufwerk C) und wird von BitLocker verschlüsselt, während die andere Partition die aktive Partition ist, die unverschlüsselt bleiben muss, damit der Computer gestartet werden kann. Die Größe der aktiven Partition muss mindestens 1,5 GB betragen.
- Beide Partitionen müssen mit dem **NTFS-Dateisystem** formatiert sein.

Ein standardmäßiges Windows 10-Setup richtet die Partitionen bereits passend ein.

Sollten Sie von Windows Vista auf Windows 10 migrieren, so können Sie die Änderungen der Konfiguration mit dem **BitLocker Drive Preparation Tool** (KB933246) durchführen, welches die nötigen Laufwerksänderungen automatisch durchführt. Konkret werden folgende Prozesse automatisiert:

1. Ein zweites Volume wird erstellt, wenn noch keines vorhanden ist.

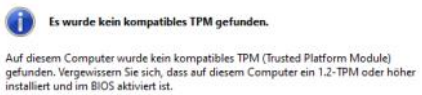
2. Die Startdateien werden auf das richtige Volume verschoben, und es wird sichergestellt, dass das Betriebssystem ordnungsgemäß konfiguriert ist, damit die Dateien beim Start gefunden werden.

3. Das richtige Volume wird als aktive Partition auf dem Laufwerk für den Start konfiguriert.

Starten Sie den Computer neu, wenn das Tool fertig ist. Das Festplattenlaufwerk des Computers wird dann ordnungsgemäß für BitLocker konfiguriert.

Unter **TPM-Verwaltung** (MMC-Konsole **tpm.msc**) sieht man einen Überblick über den Status des TPM-Moduls.

Beispiel 1: Computer ohne TPM-Chip



Würde man auf den Link **BitLocker aktivieren** klicken, so erscheint folgende Meldung:

Beispiel 2: Computer mit deaktiviertem TPM-Chip

In diesem Beispiel muss der TPM-Chip im CMOS-Setup aktiviert werden.

Beispiel 3: Computer mit vorhandenem, aktiviertem TPM-Chip

Die folgende Konfiguration zeigt einen PC mit aktiviertem, für BitLocker verwendbaren TPM-Chip.

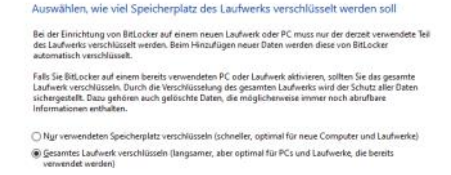
15.4.2 Aktivieren von BitLocker bei vorhandenem TPM-Modul

Nach diesen vorbereitenden Schritten kann BitLocker aktiviert werden. Durch Anklicken der Systemsteuerungsoption „BitLocker-Laufwerksverschlüsselung“ erscheint folgende Darstellung:

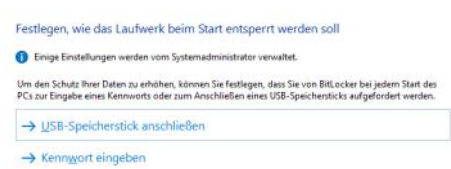
Klicken Sie auf „BitLocker aktivieren“ und folgen Sie den Anweisungen des Installations-Assistenten für BitLocker:

Anschließend wird das Laufwerk initialisiert.

Sie müssen sich nun entscheiden, ob das gesamte Laufwerk verschlüsselt werden soll oder nur die darauf gespeicherten Dateien.



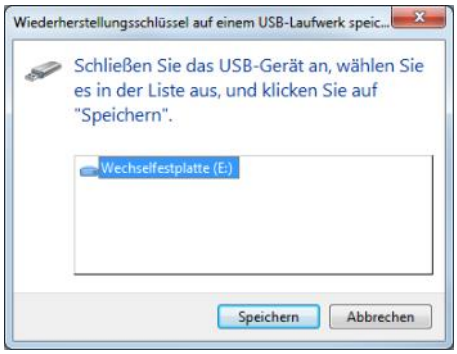
Klicken Sie auf **Weiter**.



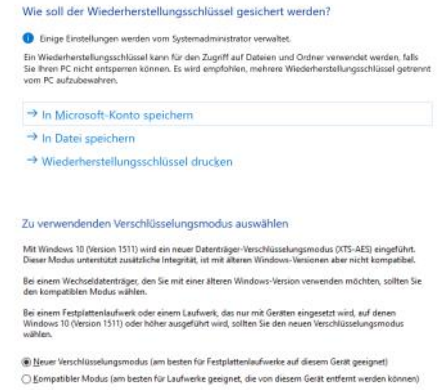
Üblicherweise wird man einen USB-Stick verwenden, um den Schlüssel darauf zu speichern, aber auch USB-Festplatten oder Speicherkarten können hier ausgewählt werden.

Diese Lösung hat den zusätzlichen Charme, dass der USB-Stick damit quasi zum „Generalschlüssel“ für den Computer wird. Ist der Stick nicht eingesteckt, fährt der Rechner nicht hoch.

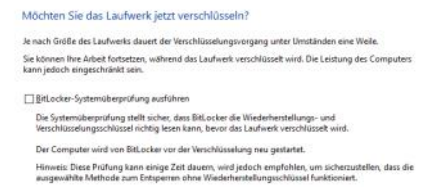
Ebenso fatal sind natürlich die Folgen, wenn der Stick versehentlich gelöscht wird oder einen Defekt erleidet. Man sollte die Schlüsseldaten daher doppelt und dreifach sichern, sonst kommt man im Fall des Falles nicht mehr an seine eigenen Daten.



Wählt man **Kennwort eingeben**, so muss das entsprechende Kennwort festgelegt werden.



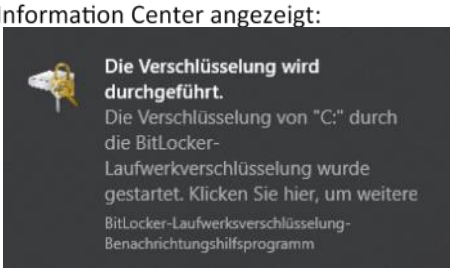
Klicken Sie auf **Weiter**.



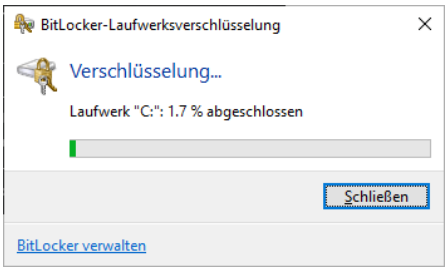
Klicken Sie auf **Verschlüsselung starten**, um mit der Laufwerksverschlüsselung zu beginnen. Der Computer wird neu gestartet.

Nach dem Neustart erfolgt der Verschlüsselungsvorgang, der ziemlich lange dau-

ern kann. Es wird folgende Meldung vom Information Center angezeigt:



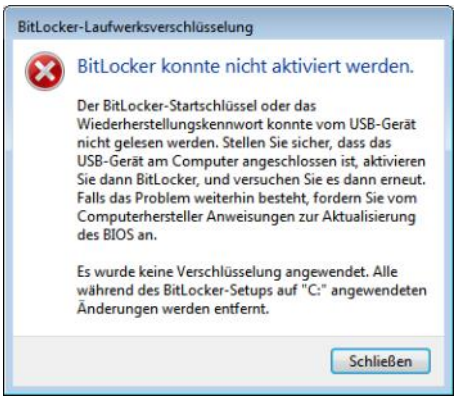
Während der Verschlüsselung kann weitergearbeitet werden; der Computer reagiert aber langsamer.



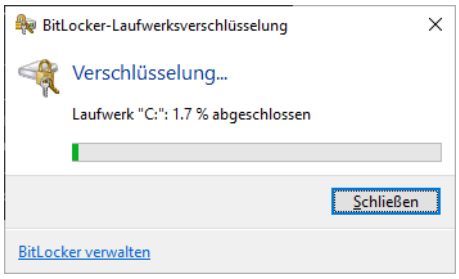
Speichert man das Wiederherstellungskennwort, so entstehen Dateien wie folgende:

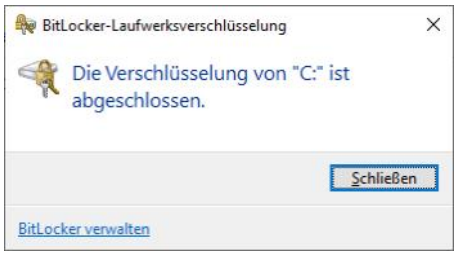
Der Dateiname ist gleichzeitig die Kennwort-ID.

Aktiviert man die **Bitlocker-Systemüberprüfung**, so wird vor der eigentlichen Verschlüsselung ein Neustart durchgeführt und gleichzeitig versucht, vom USB-Stick das Wiederherstellungskennwort zu lesen. Gibt es dabei Probleme, so wird nicht verschlüsselt und folgende Meldung angezeigt:



Wenn alles in Ordnung war, so wird online mit der Verschlüsselung begonnen. Ein paralleles Weiterarbeiten ist möglich, der PC reagiert aber langsamer.





Nach dem Verschlüsselungsvorgang wird das Betriebssystemlaufwerk wie folgt dargestellt:

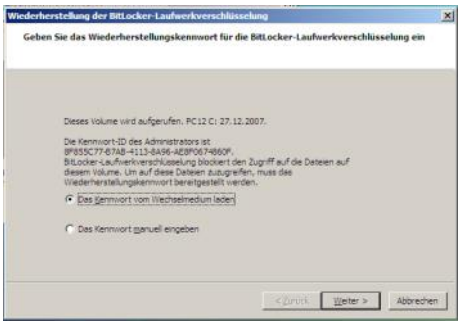
Startet man nun den PC ohne dem USB-Stick, so kann Windows nicht gestartet werden. Stattdessen erscheint folgende Meldung:

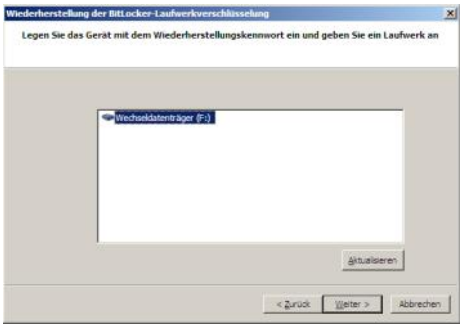
Es bestehen nun zwei Möglichkeiten:

- Anschließen des USB-Sticks, auf dem der Schlüssel gespeichert wurde und ESC für nochmaligen Startvorgang
- ENTER für Recovery-Modus: Hierfür wird das ausgedruckte bzw. in einer Textdatei gespeicherte Kennwort benötigt.

Dieses Kennwort mit Hilfe der Funktionstasten F1 – F10 eingegeben, wie am folgenden Bildschirm erläutert wird:

Versucht man, den Datenzugriff durch eine Reparaturinstallation (von Windows 10-DVD starten, Reparaturoptionen wählen), so wird ebenfalls der USB-Stick verlangt:





Nachdem der Schlüssel vom USB-Stick geladen wurde, kommt die abschließende Meldung:

15.4.3 Aktivieren von BitLocker ohne TPM-Chip

Normalerweise ist für einen sinnvollen Einsatz der BitLocker-Laufwerksverschlüsselung ein TPM-Chip notwendig.

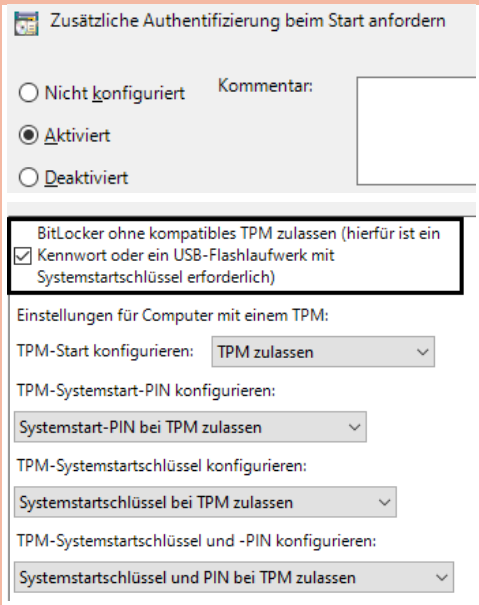
Es gibt jedoch eine Möglichkeit, BitLocker auch ohne TPM-Chip zu nutzen.

Öffnen Sie den **Gruppenrichtlinien-Editor** (gpedit.msc im Startmenü eingeben)

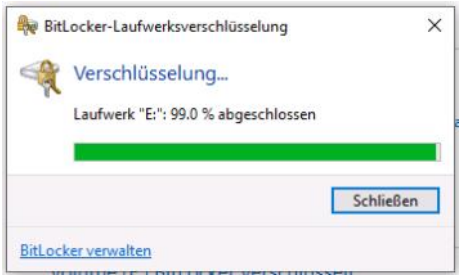
Bearbeiten Sie auf Computerkonfiguration – Administrative Vorlagen – Windows-Komponenten – BitLocker-Laufwerkverschlüsselung – Betriebssystemlaufwerke die Richtlinie „Zusätzliche Authentifizierung beim Start anfordern“.

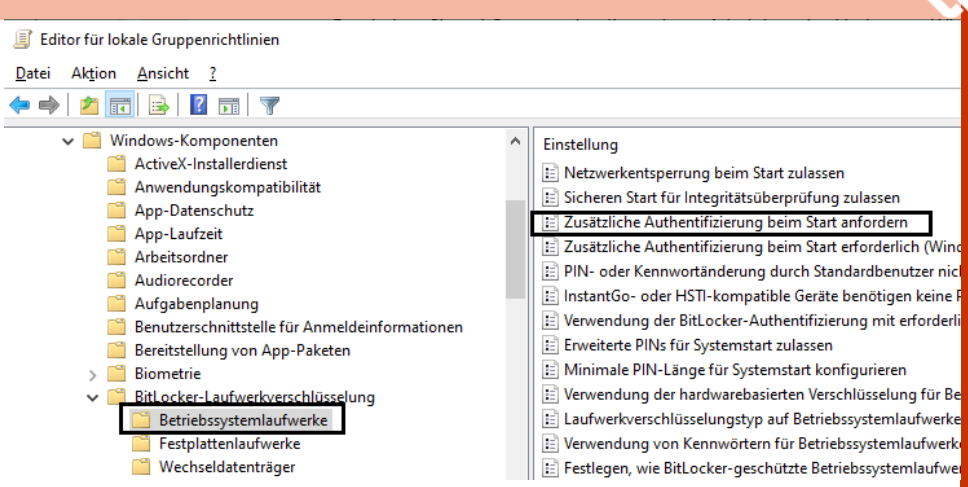
Bild nächste Seite rechts oben.

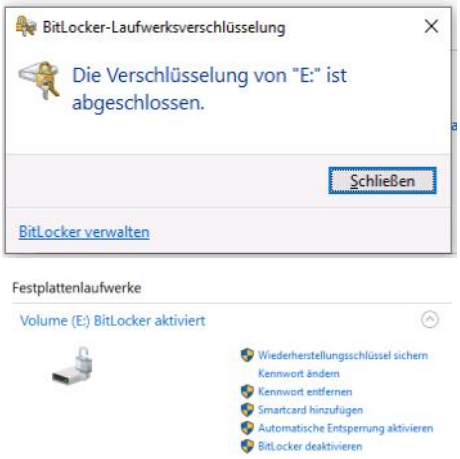
Wählen Sie nun im oberen Fensterteil „aktiviert“ und setzen Sie darunter das Häkchen in „BitLocker ohne kompatibles TPM zulassen“ - schließen Sie alle Fenster mit ok.



Starten Sie nun die BitLocker-Konfiguration erneut.







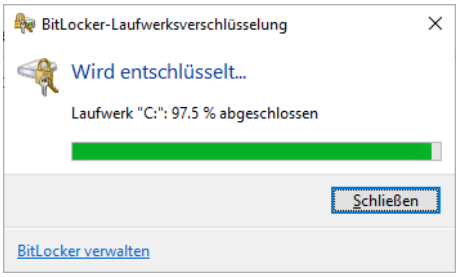
15.4.4 Deaktivieren von BitLocker

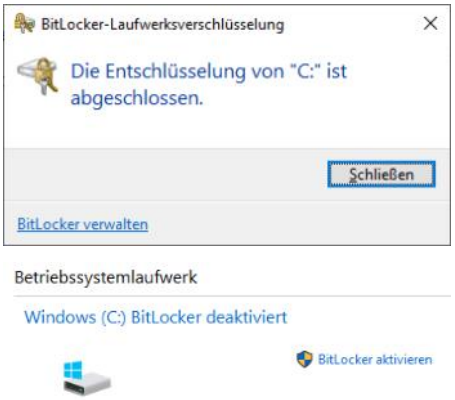
BitLocker kann auf zwei Arten deaktiviert werden: durch **Anhalten** von BitLocker oder durch **Entschlüsseln** des Laufwerks. Wenn Sie BitLocker anhalten, ist das Laufwerk immer noch verschlüsselt, aber der Computer verwendet zum Lesen der Informationen einen Nur-Text-Entschlüsselungsschlüssel, der auf dem Laufwerk gespeichert ist. Wenn Sie das Laufwerk entschlüsseln, wird der gesamte Inhalt des Laufwerks entschlüsselt.

Durch Anhalten der BitLocker-Laufwerkverschlüsselung wird der BitLocker-Schutz vorübergehend entfernt, wobei das Laufwerk, auf dem Windows installiert ist (das Betriebssystemlaufwerk), nicht entschlüsselt wird. Halten Sie BitLocker an, wenn Sie das BIOS (Basic Input/Output System) oder die Startdateien des Computers aktualisieren müssen. Diese Maßnahme hilft zu verhindern, dass BitLocker das Laufwerk sperrt, und kann einen zeitaufwändigen Entschlüsselungsprozess vermeiden. Wenn die Aktualisierung abgeschlossen ist und der Computer neu gestartet wurde, können Sie auf Schutz fortsetzen klicken.

BitLocker kann nur auf Betriebssystemlaufwerken angehalten werden. Wenn Sie Bitlocker auf einem eingebauten Datenlaufwerk (z. B. einer internen Festplatte) oder einem Wechseldatenträger (z. B. einer externen Festplatte oder einem USB-Flashlaufwerk) deaktivieren möchten, müssen Sie das Laufwerk entschlüsseln.

Beim **Entschlüsseln** eines Betriebssystemlaufwerks wird der BitLocker-Schutz vom Computer entfernt. Dieser Vorgang kann sehr zeitaufwändig sein. Klicken Sie dazu auf **Systemsteuerung – System und Sicherheit – BitLocker Laufwerksverschlüsselung,** anschließend klicken Sie auf den Link **Bitlocker deaktivieren**.





15.4.5 BitLocker To Go

BitLocker To Go ermöglicht die Verschlüsselung externer Medien, wie etwa USB-Sticks oder Wechselplatten.

Mit BitLocker To Go kann man auch wunderbar lokale Partitionen und / oder externe Festplatten schützen, aber dazu an anderer Stelle mehr. Der BitLocker unterstützt exFat, FAT 16, FAT 32 und NTFS. Die **Stärke der Verschlüsselung ist mit 128 Bit** und einer **AES-Verschlüsselung** als recht sicher zu bezeichnen. Über den **Local Group Policy Editor** kann man die Stärke der Verschlüsselung noch auf 256 Bit erhöhen sowie eine andere Art der Verschlüsselung wählen.

Ein durch BitLocker To Go verschlüsselter USB-Stick kann auf jedem Windows-Rechner, an den man ihn anschließt, be-

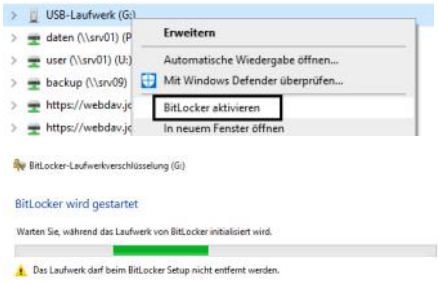
nutzt werden. Nur unter Windows 7/8/8.1/10 hat man Lese- **und** Schreibrechte, d.h. **unter älteren Betriebssystemen wie Windows XP und Windows Vista** kann man die **verschlüsselten Daten nur lesen, aber nicht speichern**!

Der Zugriff auf die **verschlüsselten Dateien wird durch ein Passwort** oder eine **Smartcard** geschützt. Ein unter Windows 10 verschlüsselter USB-Stick funktioniert wie ein verschlüsselter Container, d.h. Dateien, die man hinein verschiebt sind geschützt und Dateien, die man hinaus kopiert sind nicht mehr geschützt.

Aktivieren von BitLocker-to-Go:

Standardmäßig beginnt man in der Systemsteuerungs-Kategolie **System und Sicherheit – BitLocker-Laufwerksverschlüsselung**.

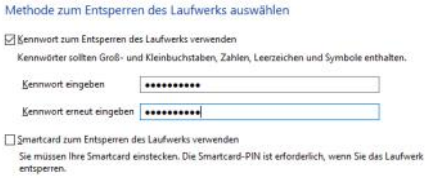
Die Aktivierung kann auch über das Kontextmenü des Wechseldatenträgers (USB-Sticks) erfolgen:



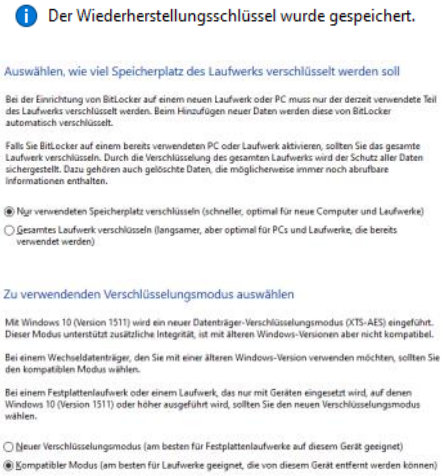
Im nächsten Schritt wählt man, wie der Wiederherstellungsschlüssel gespeichert werden soll.

Die Datei bietet keine Sicherheit vor Hackern und der analoge Weg bietet Einbrechern die Chance Deine wertvollen verschlüsselten Daten zu entschlüsseln. Ich habe mich für digitalen Schlüssel entschieden, weil ich noch weite Schlüssel dieser Art habe.

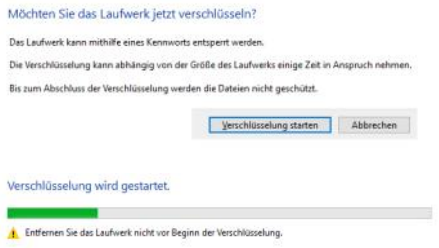
Wichtig! Der Wiederherstellungsschlüssel ist zur Wiederherstellung der Daten, wenn man das Kennwort vergessen hat. Die BitLocker-Verschlüsselung knacken dürfte nicht leicht werden, so dass ich empfehle den Wiederherstellungsschlüssel gut aufzubewahren!



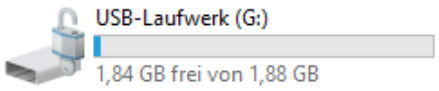
Wir wählen eine Datei aus, in welcher der Wiederherstellungsschlüssel gespeichert wird.



Im nächsten Schritt wird der Stick verschlüsselt. Das Verschlüsseln USB-Sticks kann – je nach Größe – einige Zeit in Anspruch nehmen.



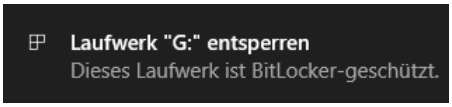
Im Explorer erscheint der verschlüsselte USB-Stick mit einem Schloss-Symbol:



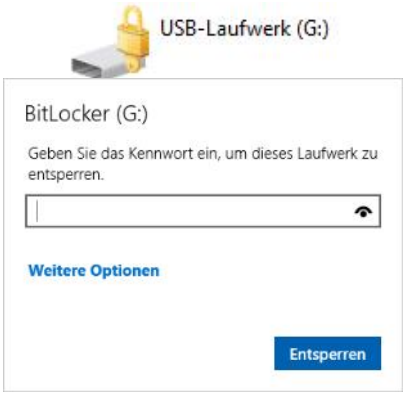
Über das Kontextmenü kann man den BitLocker USB-Stick verwalten:

Die Option **Automatische Entsperrung aktivieren** ist kritisch zu betrachten, da dann der Schutz durch die Verschlüsselung nicht gegeben ist.

Ein verschlüsselter USB-Stick, der an einen Windows-Rechner gesteckt wird, meldet sich per Autostart mit dieser Meldung:



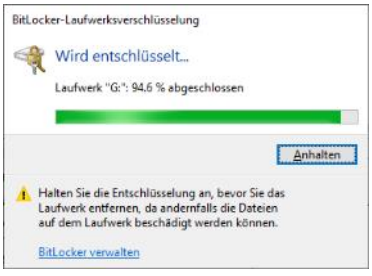
Solange das Passwort nicht eingegeben wurde, wird im Explorer der USB-Stick mit versperrtem goldfarbenen Schloss-Symbol dargestellt; ein Anklicken des Laufwerks führt zur Abfrage des Kennwortes.

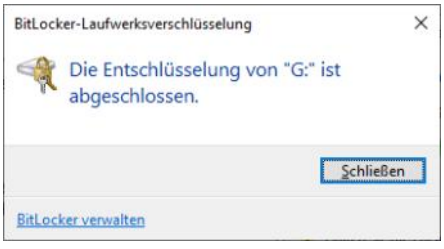


Verschlüsselung entfernen (Deaktivieren von Bitlocker)

Die einfachste Möglichkeit, die BitLocker-Verschlüsselung zu entfernen ist die Neuformatierung des USB-Sticks – dadurch gehen aber alle Daten verloren.

Der bessere Weg ist über **Systemsteuerung – System und Sicherheit – BitLocker Laufwerksverschlüsselung,** anschließend klicken Sie auf den Link **Bitlocker deaktivieren**.





17 Bedienung der Tastatur

Quelle: Microsoft Knowledge Base, http://support.microsoft.com -> Suche Tastaturkürzel

Christian Zahler

17.1 Wichtige Tasten

 [STRG]	**Steuerung**, englisch **Control** Diese Taste wird meist für Tastenkombinationen verwendet. Hinweis: Diese Taste heißt nicht "String", auch nicht "Strong" und schon gar nicht "Strange"!
 [ALT]	engl. **alternate** (=wechseln) Diese Taste wird meist für Tastenkombinationen verwendet.
 [ALTGR]	engl. **Alternate Graph(ic)**, auch: **Alternate Green/Gray** Diese Taste aktiviert Drittbelegungen auf der Tastatur. Die Herkunft ist nicht völlig geklärt, da selbst IBM in seinen Keyboard-Beschreibungen die Bedeutung dieser Abkürzung nicht letztgültig klärt. Es gibt mehrere Deutungen: IBM selbst beschreibt diese Taste
 [WINDOWS]	**Windows-Logo-Taste** Diese Taste wird meist für Tastenkombinationen verwendet.
	**Kontextmenü-Taste** Diese Taste ruft das Kontextmenü auf und ersetzt den Klick mit der rechten Maustaste.

17.2 Allgemeine Tastenkombinationen

17.2.1 Wichtige Windows-Tastenkombinationen

[WINDOWS] oder [STRG] + ESC	Anzeigen oder Schließen des Startmenüs
[WINDOWS] + A	Anzeigen des Info-Centers
[WINDOWS] + B	Aktiviert das Symbol „Ausgeblendete Symbole“ in der Taskleiste
[WINDOWS] + D	Anzeigen des Desktops
[WINDOWS] + E	Windows-Explorer starten
[WINDOWS] + F	Feedback-Hub
[WINDOWS] + [STRG] + F	Nach Computern suchen
[WINDOWS] + I	App Windows-Einstellungen
[WINDOWS] + L	PC sperren, Sperrbildschirm anzeigen
[WINDOWS] + M	Aktuelles Programmfenster minimieren
[WINDOWS] + [UMSCHALT] + M	Minimiertes Programmfenster wiederherstellen
[WINDOWS] + O	Auf Tablets: Anzeigerichtung zwischen Hochformat und Querformat umstellen
[WINDOWS] + P	Öffnen der Projektor-Einstellungen; diese benötigen Sie, wenn Sie beispielsweise eine Präsentation auf einem Notebook über einen Videobeamer einem Publikum zeigen wollen – in diesem Fall ist es nötig, die Anzeige auf einen zweiten Bildschirm zu duplizieren.
[WINDOWS] + Q	App suchen
[WINDOWS] + R	Ausführen
[WINDOWS]+ T	Vorschau auf das erste geöffnete Programmfenster (engl. „task“) in der Taskleiste; wiederholten Drücker führt zu den weiteren aktiven Tasks.
[WINDOWS] + [UMSCHALT]+T	Vorschau auf das letzte geöffnete Programmfenster (engl. „task“) in der Taskleiste; wiederholtes Drücken führt zu den vorangegangenen Tasks.
[WINDOWS] + U	Ruft das Center für erleichterte Bedienung (Systemsteuerung) auf. Hier können Sie Bedienungshilfen wie Bildschirmlupe, Bildschirmtastatur, Sprachausgabe oder höheren Kontrast einrichten.
[WINDOWS] + X	Links unten wird eine Art "Übersichtsmenü" angezeigt
[WINDOWS] + F1	Windows-Hilfe und Support
[WINDOWS] + 1, + 2 usw.	Startet die in der Taskleiste erste, zweite usw. als Symbol angeheftete App
[WINDOWS] + [PAUSE]	Dialogfeld Systemeigenschaften anzeigen
[WINDOWS] + [LEERTASTE]	Tastaturlayout anzeigen bzw. wechseln
[WINDOWS] + nicht unterstützter Buchstabe	Öffnet die Suche ([WINDOWS]+A würde also nach Apps suchen, die mit dem Buchstaben A beginnen, selber Effekt, wie wenn man nur A allein drücken würde, wenn der Desktop dargestellt wird)

17.2.2 Allgemeine Tastenkombinationen

[WINDOWS] + [PLUS]	Zeigt den aktiven Bildschirm vergrößert an
[WINDOWS] + [MINUS]	Macht die Bildschirmvergrößerung wieder rückgängig

17.2.3 Tastenkombinationen für Programmfenster

[WINDOWS] + [NACH-OBEN-TASTE]	Fenster als Vollbild darstellen
[WINDOWS] + [NACH-UNTEN-TASTE]	Fenster minimieren bzw. mittelgroß darstellen
[WINDOWS] + [NACH-LINKS-TASTE]	Fenster in die linke Bildschirmhälfte positionieren
[WINDOWS] + [NACH-RECHTS-TASTE]	Fenster in die rechte Bildschirmhälfte positionieren
[WINDOWS] + [UMSCHALT] + [NACH-LINKS-TASTE]	Bei mehreren Bildschirmen: Fenster im linken Bildschirm darstellen
[WINDOWS] + [UMSCHALT] + [NACH-RECHTS-TASTE]	Bei mehreren Bildschirmen: Fenster im rechten Bildschirm darstellen

17.3 Tastenkombinationen für Anwendungsprogramme (Apps)

[STRG] + [C]	Kopieren
[STRG] + [X]	Ausschneiden
[STRG] + [V]	Einfügen
[STRG] + [Z]	Rückgängig
[ENTF]	Löschen
[UMSCHALT] + [ENTF]	Markiertes Element dauerhaft entfernen, ohne es in den Papierkorb zu verschieben
[STRG] beim Ziehen eines Elements	Markiertes Element kopieren
[STRG] + [UMSCHALT] beim Ziehen eines Elements	Verknüpfung zum markierten Element erstellen
[F2]	Markiertes Element umbenennen
[STRG] + [NACH-RECHTS-TASTE]	Einfügemarke an den Anfang des nächsten Wortes stellen
[STRG] + [NACH-LINKS-TASTE]	Einfügemarke an den Anfang des vorigen Wortes stellen
[STRG] + [NACH-UNTEN-TASTE]	Einfügemarke an den Anfang des nächsten Absatzes stellen
[STRG] + [NACH-OBEN-TASTE]	Einfügemarke an den Anfang des vorigen Absatzes stellen
[STRG] + [UMSCHALT] mit einer beliebigen Pfeiltaste	Textblock markieren
[UMSCHALT] mit einer beliebigen Pfeiltaste	Mehrere Elemente in einem Fenster oder auf dem Desktop markieren oder Text in einem Dokument markieren
[STRG] + [A]	Alles markieren
[F3]	Datei oder Ordner suchen
[ALT] + [EINGABE]	Eigenschaften des markierten Elements anzeigen
[ALT] + [F4]	Aktives Element schließen oder aktives Programm beenden
[ALT] + [EINGABE]	Eigenschaften des markierten Objekts anzeigen
[ALT]+[LEERTASTE]	Kontextmenü für aktives Fenster öffnen
[STRG] + [F4]	In Programmen, die das gleichzeitige Öffnen mehrerer Dokumente zulassen: Aktives Dokument schließen
[ALT] + [TAB]	Zwischen geöffneten Elementen wechseln
[ALT]+[ESC]	Elemente in der Reihenfolge durchlaufen, in der sie geöffnet wurden
[F6]	Bildschirmelemente in einem Fenster oder auf dem Desktop durchlaufen
[F4]	Adressleistenliste in "Arbeitsplatz" oder im Windows Explorer anzeigen
[UMSCHALT] + [F10]	Kontextmenü für markiertes Element anzeigen
[ALT] + [LEERTASTE]	Systemmenü für aktives Fenster anzeigen
[ALT] + Unterstrichener Buchstabe in einem Menünamen	Entsprechendes Menü anzeigen
Unterstrichener Buchstabe in einem Befehlsnamen oder in einem geöffneten Menü	Entsprechenden Befehl ausführen
[F10]	Menüleiste im aktiven Programm aktivieren
[NACH-RECHTS-TASTE]	Nächstes Menü nach rechts oder Untermenü öffnen
[NACH-LINKS-TASTE]	Nächstes Menü nach links öffnen oder Untermenü schließen
[F5]	Aktives Fenster aktualisieren
[RÜCKTASTE]	Übergeordneten Ordner in "Arbeitsplatz" oder im Windows Explorer anzeigen
[ESC]	Aktuellen Vorgang abbrechen
[UMSCHALT] beim Einlegen einer CD-ROM	Automatisches Abspielen der CD-ROM verhindern
[STRG]+[UMSCHALT]+[ESC]	Task-Manager öffnen

17.4 Kombinationen aus Tastatur- und Maustasten bei Desktop -Elementen

[UMSCHALT] + Rechte Maustaste	Kontextmenü anzeigen, das alternative Verben enthält.
[UMSCHALT] + Doppelklick	Alternativen Standardbefehl (zweites Element im Menü) ausführen.
[ALT] + Doppelklick	Eigenschaften anzeigen

17.5 Tastenkombinationen für Dialogfelder

Falls Sie in den Listenfeldern mit erweiterter Auswahl die Tastenkombination [UMSCHALT]+[F8] drücken, aktivieren Sie den Modus zur erweiterten Auswahl. In diesem Modus können Sie die Navigationstasten verwenden, um den Cursor zu bewegen, ohne dass sich die Auswahl verändert. Sie können [STRG]+[LEERTASTE] oder [UMSCHALT]+[LEERTASTE] drücken, um die Auswahl zu verändern. Den Modus zur erweiterten Auswahl können Sie wieder mit [UMSCHALT]+[F8] beenden. Die erweiterte Auswahl wird automatisch beendet, wenn Sie ein anderes Steuerelement fokussieren.

[STRG] + [TAB]	Vorwärts durch die Registerkarten navigieren
[STRG] + [UMSCHALT]+ [TAB]	Rückwärts durch die Registerkarten navigieren
[TAB]	Vorwärts durch die Optionen navigieren
[UMSCHALT] + [TAB]	Rückwärts durch die Optionen navigieren
[ALT] + Unterstrichener Buchstabe	Entsprechenden Befehl ausführen oder entsprechende Option auswählen
[EINGABE]	Befehl für aktive Option oder Schaltfläche ausführen
[LEERTASTE]	Kontrollkästchen aktivieren oder deaktivieren, wenn die aktive Option ein Kontrollkästchen ist
Pfeiltasten	Schaltfläche auswählen, wenn die aktive Option eine Gruppe von Optionsschaltflächen ist
[F1]	Hilfe anzeigen
[F4]	Elemente in der aktiven Liste anzeigen
[RÜCKTASTE]	Übergeordneten Ordner anzeigen, wenn ein Ordner im Dialogfeld Speichern unter oder Öffnen markiert ist

17.6 Navigation im Microsoft Internet Explorer

[STRG] + [B]	Dialogfeld Favoriten verwalten öffnen
[STRG] + [E]	Suchleiste öffnen
[STRG] + [F]	Dienstprogramm "Suchen" starten
[STRG] + [H]	Leiste "Verlauf" öffnen
[STRG] + [I]	Leiste "Favoriten" öffnen
[STRG] + [L]	Dialogfenster Öffnen öffnen
[STRG] + [N]	Weitere Browserinstanz mit derselben Webadresse öffnen
[STRG] + [O]	Dialogfenster Öffnen öffnen, wie bei [STRG]+[L]
[STRG] + [P]	Dialogfenster Drucken öffnen
[STRG] + [R]	Aktuelle Webseite aktualisieren
[STRG] + [W]	Aktuelles Fenster schließen

17.7 Tastenkombinationen für Eingabehilfen

Acht Sekunden lang [UMSCHALT RECHTS]	Anschlagverzögerung ein- oder ausschalten
[ALT LINKS] + [UMSCHALT LINKS] + [DRUCK]	Kontrast ein- oder ausschalten
[ALT LINKS] + [UMSCHALT LINKS] + [NUM]	Tastaturmaus ein- oder ausschalten
Fünfmal [UMSCHALT]	Einrastfunktion ein- oder ausschalten
Fünf Sekunden lang [NUM]	Statusanzeige ein- oder ausschalten
[WINDOWS] + [U]	Hilfsprogramm-Manager öffnen

17.8 Tastenkombinationen für den Windows Explorer

[ENDE]	Ende des aktiven Fensters anzeigen
[POS1]	Anfangs des aktiven Fensters anzeigen
[NUM]+Stern *	Alle Unterordner zum markierten Ordner anzeigen
[NUM]+Pluszeichen +	Inhalt des markierten Ordners anzeigen
[NUM]+Minuszeichen -	Markierten Ordner reduzieren
[NACH-LINKS-TASTE]	Aktuelle Auswahl reduzieren, sofern sie erweitert ist, oder übergeordneten Ordner markieren
[NACH-RECHTS-TASTE]	Aktuelle Auswahl erweitern, sofern sie reduziert ist, oder ersten Unterordner markieren

17.9 Tastenkombinationen für die Zeichentabelle

Nach dem Doppelklicken auf ein Zeichen in der Zeichentabelle können Sie sich mithilfe der folgenden Tastenkombinationen durch die Tabelle bewegen:

[NACH-RECHTS-TASTE]	Nach rechts oder an den Anfang der nächsten Zeile
[NACH-LINKS-TASTE]	Nach links oder an das Ende der vorigen Zeile
[NACH-OBEN-TASTE]	Eine Zeile nach oben
[NACH-UNTEN-TASTE]	Eine Zeile nach unten
[BILD-AUF]	Zum vorherigen Bildschirm
[BILD-AB]	Zum nächsten Bildschirm
[POS1]	Zum Zeilenanfang
ENDE	Zum Zeilenende
[STRG] + [POS1]	Zum ersten Zeichen
[STRG] + [ENDE]	Zum letzten Zeichen
[LEERTASTE]	Bei markiertem Zeichen zwischen Vergrößerungs- und Normalmodus wechseln

17.10 Microsoft Management Console: Hauptfenster

[STRG] + [O]	Gespeicherte Konsole öffnen
[STRG] + [N]	Neue Konsole öffnen
[STRG] + [S]	Geöffnete Konsole speichern
[STRG] + [M]	Konsolenelement hinzufügen oder entfernen
[STRG] + [W]	Neues Fenster öffnen
[F5]	Inhalt aller Konsolenfenster aktualisieren
[ALT] + [LEERTASTE]	MMC-Fenstermenü anzeigen
[ALT] + [F4]	Konsole schließen
[ALT] + [A]	Menü "Aktion" anzeigen
[ALT] + [V]	Menü "Ansicht" anzeigen
[ALT] + [F]	Menü "Datei" anzeigen
[ALT] + [O]	Menü "Favoriten" anzeigen

17.11 Microsoft Management Console: Konsolenfenster

[STRG] + [P]	Aktuelle Seite oder aktives Fenster drucken
[ALT] + [-]	Fenstermenü für aktives Konsolenfenster anzeigen
[UMSCHALT] + [F10]	Aktionskontextmenü für markiertes Element anzeigen
[F1]	Hilfethema zu markiertem Element anzeigen, sofern vorhanden
[F5]	Inhalt aller Konsolenfenster aktualisieren
[STRG] + [F10]	Aktives Konsolenfenster maximieren
[STRG] + [F5]	Aktives Konsolenfenster wiederherstellen
[ALT] + [EINGABE]	Dialogfenster Eigenschaften für markiertes Element anzeigen, sofern vorhanden
[F2]	Markiertes Element umbenennen
[STRG] + [F4]	Aktives Konsolenfenster schließen. Wenn eine Konsole nur ein Konsolenfenster hat, schließt diese Tastenkombination die Konsole.

17.12 Navigation bei Remotedesktop-Verbindungen

[STRG] + [ALT]+ [ENDE]	Microsoft Windows NT-Dialogfenster Sicherheit öffnen
[ALT] + [BILD-AUF]	Wechseln zwischen Programmen, von links nach rechts
[ALT] + [BILD-AB]	Wechseln zwischen Programmen, von rechts nach links
[ALT] + [EINFÜGEN]	Programme in Reihenfolge der letzten Verwendung durchlaufen
[ALT] + [POS1]	Startmenü anzeigen
[STRG] + [ALT]+ [PAUSE]	Umschalten zwischen Fenster und Vollbild auf Clientcomputer
[ALT]+[ENTF]	Windows-Menü anzeigen
[STRG] + [ALT] + [-]	Snapshot des gesamten Fensterbereichs auf dem Client in die Terminalserver-Zwischenablage stellen und Funktionalität wie bei Betätigung von [ALT]+ [DRUCK] auf einem lokalen Computer bereitstellen
[STRG] + [ALT] + [+]	Snapshot des aktiven Fensters auf dem Client in die Terminalserver-Zwischenablage stellen und Funktionalität wie bei Betätigung von [DRUCK] auf einem lokalen Computer bereitstellen

techbold

WIR BAUEN DEINEN PC

Nutze die langjährige Erfahrung der techbold Computer Experten für die perfekte Konfiguration deines PC-Systems. Egal ob Gaming Maschine, Office-PC oder Workstations für professionelle Anwendungen wie CAD, 3D Grafik und Videoschnitt – wir erstellen dir ein Angebot mit dem perfekten Preis-Leistungs-Verhältnis.

www.techbold.at/pc-zusammenstellen

BERATUNG
Umfangreicher Support von zertifizierten Experten

QUALITÄT
Ausschließlich geprüfte Markenkomponenten

TESTS
Jede Konfiguration wird umfangreich getestet

GARANTIE
3 Jahre Garantie auf alle individuellen PC-Systeme

Windows 10 *Inhaltsverzeichnis*

Christian Zahler

Teil 1 *PCNEWS-167*

1 Das Betriebssystem Microsoft Windows 10 (Seite 7)
1.1 Editionen (SKUs, Stock Keeping Units) von Windows 10
1.2 Übersicht: Neue Features in Windows 10
1.3 Prozessorarchitektur: 32 bit/64 bit-Versionen
1.4 Hardwarevoraussetzungen
1.5 Architektur von Windows
2 Informationsquellen und Hilfe (Seite 11)
2.1 Knowledge Base
2.2 Whitepapers
2.3 Hilfefunktionen
3 Windows 10-Installation (Seite 12)
3.1 Grundsätzlicher Installationsablauf
3.2 Ablauf einer beaufsichtigten Neuinstallation
3.3 Startfähiges USB-Installationsmedium mit dem Media Creation Tool
3.4 Upgrade von Windows 7, Windows 8 oder 8.1 auf Windows 10
3.5 Windows 10-Lizenzierung und Produktaktivierung
3.6 Windows 10-Funktionsupgrades
3.7 Hinzufügen von optionalen Features
4 An- und Abmeldung, Benutzerkonten und Kennwörter (Seite 20)
4.1 Anmeldung und Abmeldung
4.2 Computer sperren und entsperren
4.3 Benutzer wechseln
4.4 Windows herunterfahren
4.5 Kennwörter (Passwords)
4.6 Kennwörter ändern
5 Desktop, Startmenü, Taskleiste, Dateimanagement (Seite 23)
5.1 Startmenü
5.2 Finden und Aufrufen von Apps
5.3 App-Symbole an die Taskleiste anheften
5.4 Sprunglisten
5.5 Info-Center
5.6 Arbeiten mit Desktop-Apps
5.7 Virtuelle Desktops
5.8 Screenshots
5.9 Videos und Screencasts mit Windows 10-Bordmitteln
5.10 Tabletmodus
5.11 Der Windows-Explorer
5.12 OneDrive
5.13 Präsentieren mit Laptop und Videobeamer
5.14 Webbrowser

Teil 2 *PCNEWS-168*

6 Softwareinstallation und -deinstallation (Seite 7)
6.1 Beziehen von Apps aus dem Microsoft Store
6.2 Apps installieren und deinstallieren
6.3 Installation von Office 2019 Enterprise Edition
7 Windows 10-Verwaltung (Seite 9)
7.1 Grafische Verwaltungstools
7.2 Textorientierte Oberflächen
7.3 Hintergrundbild ändern
7.4 Sperrbildschirm konfigurieren, Windows-Blickpunkt
7.5 Schriftgröße einstellen
7.6 Anpassen der Bildschirmeinstellungen
7.7 Energieverwaltung
7.8 Task- und Prozessverwaltung
7.9 Registry (Registrierungsdatenbank)
8 Windows 10 im Netzwerk (Seite 20)
8.1 Netzwerk-Grundlagen, wichtige Begriffe
8.2 Netzwerkeinstellungen
8.3 Konfiguration der Netzwerkkarte: IP-Adressen
8.4 Verbindung mit einem WLAN herstellen
8.5 Netzwerkprofile
16 Virtualisierung - Client Hyper-V (Seite 25)
16.1 Client Hyper-V
16.2 Booten von VHD – Dual- bzw. Multi-Boot-Konfigurationen
16.2.1 Erstellen einer VHD auf grafischem Weg
16.2.2 Erstellen einer virtuellen Festplatte mit diskpart
16.2.3 Windows im virtuellen Datenträger bereitstellen und Startmenüeintrag erstellen

Teil 3 *PCNEWS-169*

9 Benutzerverwaltung und Anmeldung (Seite 4)
9.1 Ablauf des Anmeldevorgangs in Windows
9.2 Arten von Benutzerkonten
9.3 Anmeldeoptionen und Windows Hello
9.4 Security Principals
9.5 Kontotyp: Lokale Benutzer zu lokalen Administratoren machen
9.6 Kennwörter an Webseiten und eigene Anmeldeinformationen verwalten
9.7 Benutzerverwaltung lokaler Benutzer in der Computerverwaltung
9.8 UAC (Benutzerkontosteuerung, User Account Control)
9.9 Programmausführung mit geändertem Benutzerkontext
9.10 Benutzerprofile
9.11 Öffentliche Ordner
10 Rechte und Berechtigungen (Seite 14)
10.1 Lokale Gruppen
10.2 NTFS-Berechtigungen
10.3 Zugriffstoken und Sicherheitsdeskriptoren
10.4 Netzwerkerkennung und Freigaben
11 Fernwartung und Fernzugriff (Seite 23)
11.1 Remotedesktop
11.2 Remotehilfe
11.3 Remoteunterstützung
11.4 TeamViewer
12 Windows 10-Features mit Windows Server 2016/2019 (Seite 26)
12.1 Always On VPN
12.2 Neue Remote Desktop-Dienste
12.3 BranchCache
13 Drucker (Seite 27)
13.1 Ablauf des Druckvorgangs
13.2 Einrichten eines lokalen Druckerobjekts
13.3 Drucker entfernen
13.4 Erzeugen eines TCP/IP-Druckeranschlusses
13.5 Druckserver konfigurieren
13.6 Druckerverwaltung
13.7 Einrichten eines Druckerpools
13.8 Berechtigungen für logische Druckerobjekte

Teil 4 *PCNEWS-170*

14 Datenträgerverwaltung, Startvorgang und Notfallwiederherstellung (Seite 3)
14.1 Datenspeicherung auf Datenträgern
14.2 Formatierung und Dateisysteme
14.3 Dynamische Datenträger und RAID
14.4 Speicherpools und Speicherplätze (Storage Pools, Storage Spaces)
14.5 Befehlszeilentools zur Datenträgerverwaltung
14.6 Speicheroptimierung
14.7 Defragmentierung
14.8 ReadyBoost
14.9 Startvorgang von Windows 10
14.10 Boot-Optionen, Aktivieren von Windows RE
14.11 Backup und Restore, Notfallwiederherstellung
14.12 Systemleistungsoptionen und Auslagerungsdatei
14.13 Ereignisanzeige (Event Viewer)
14.14 Leistungsüberwachung
14.15 Problembehandlung
14.16 Treiber und Hardware-Installation
14.17 Debugging Blue Screens
15 Windows 10-Sicherheitseinstellungen (Seite 28)
15.1 Windows-Sicherheit
15.2 Konfigurieren von Benachrichtigungen und Meldungen
15.3 Windows Update
15.4 BitLocker Drive Encryption
15.5 AppLocker
17 Bedienung der Tastatur (Seite 37)
17.1 Wichtige Tasten
17.2 Allgemeine Tastenkombinationen
17.3 Anwendungsprogramme (Apps)
17.4 Tastatur- und Maustasten bei Desktop-Elementen
17.5 Dialogfelder
17.6 Microsoft Internet Explorer
17.7 Eingabehilfen
17.8 Windows Explorer
17.9 Zeichentabelle
17.10 Microsoft Management Console: Hauptfenster
17.11 Microsoft Management Console: Konsolenfenster
17.12 Remotedesktop-Verbindungen