Netzwerkadministrator
Clientbetriebssystem Windows 10

Was Sie in den nächsten **24 LE** erwartet:

- Installation von Windows 10
- Windows 10 Benutzeroberfläche
- Benutzer und Gruppen
- Datenträgerverwaltung
- Dateisysteme
- NTFS-Berechtigungen
- Freigaben
- Startvorgang
- Ereignisanzeige
- Dienste
- Taskmanager
- Systemwiederherstellung
- Registry

INSTALLATION

Editionen

- Windows 10 Home
  - enthält alle Funktionen, die auf den Markt für Heimanwender abzielen
  - Windows Defender Antivirus

- Windows 10 Pro
  - Nachfolger von Windows 7 Professional/Ultimate bzw. Windows 8 Pro
  - alle Features von Windows 10
  - Domänenmitgliedschaft möglich
  - Hyper-V
  - Bitlocker

Editionen

- Windows 10 Pro for Workstations
  - Hardwareunterstützung für Hochleistungs-PCs
    - bis zu 4 CPUs (statt 2 CPUs)
    - 6 TB RAM (statt 2 TB)
  - ReFS
  - Persistent Memory (NVDIMM-N)
  - SMB Direct

Editionen

- Windows 10 Enterprise
  - alle Features von Windows 10 Pro und Windows 10 Pro for Workstations
  - erweiterte Verwaltungsmöglichkeiten (Analysen, Reports und Deployment)
  - Windows To Go
  - Direct Access
  - BranchCache
  - AppLocker
  - Windows Defender Advanced Threat Protection
  - Windows 10-LTSC-Zugriff

Editionen

- Windows IoT (Internet of Things)
  - "kompakteste" Windows 10 Betriebssystem-Variante
  - standardmäßig ohne Desktop und Anwendungen installiert
    - Windows IoT Core
    - Windows IoT Enterprise

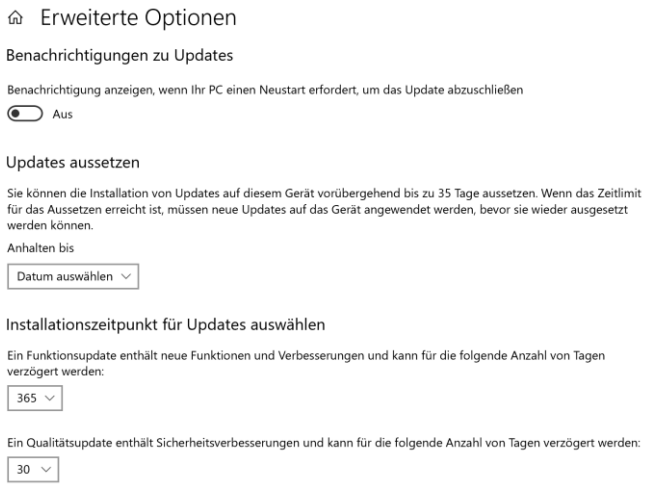
- Windows 10 S
  - Nur Windows Store Apps, Edge und Bing
  - kann auf Windows 10 Pro upgegradet werden

Windows as a Service

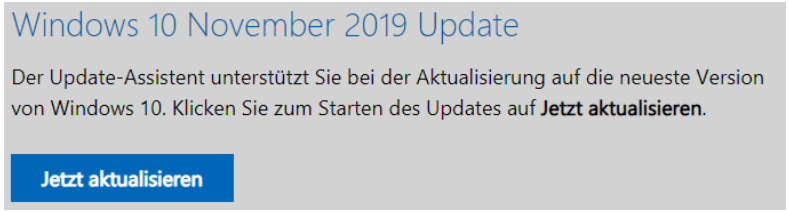
- Keine neuen Windows Versionen (wie Windows 7→ Windows 8→ Windows 8.1)
- Feature-Upgrades:
  - Semi-Annual Channel (SAC): 2 mal im Jahr (Planmäßig März und September)
  - Long Term Servicing Channel (LTSC): neue Features wahlweise nur alle 2-3 Jahre
- Quality Updates: monatlich (v.a. Securityupdates)

Windows Update Varianten und -tools

- **Windows Update (stand-alone)**
  - geringfügige Kontrolle über Feature-Updates über *Einstellungen | Updates | Erweiterte Optionen*
  - Installation verzögern möglich:
    - Funktionsupdates bis max. 365 Tage
    - Qualitätsupdates bis max. 30 Tage



- **Windows 10-Update-Assistant**
  - kostenloses Tool von Microsoft um Windows Update manuell zu starten
  - wenn Sie nicht auf ein automatisches Update warten möchten



Windows Update Varianten und -tools

- **Windows Update for Business**
  - Kontrolle über Gruppenrichtlinien
  - Installation verzögern möglich:
    - Funktionsupdates bis max. 365 Tage
    - Qualitätsupdates bis max. 30 Tage
- **Windows Server Update Services (WSUS)**
  - Intensive Kontrollmöglichkeiten
  - Möglichkeit Updates zu genehmigen oder nicht zu genehmigen
- **System Center Configuration Manager**
  - Größtmögliche Kontrolle über den Updateprozess

Hardware Voraussetzungen

- Prozessor: 1-GHz- oder schneller
- RAM:
  - 1 GB (32 Bit)
  - 2 GB (64 Bit)
- Festplatte (frei)
  - 16 GB (32 Bit)
  - 20 GB (64 Bit)
- DirectX9-fähige Grafikkarte mit WDDM 1.0 oder höherem Treiber

Zusätzliche Anforderungen für bestimmte Features

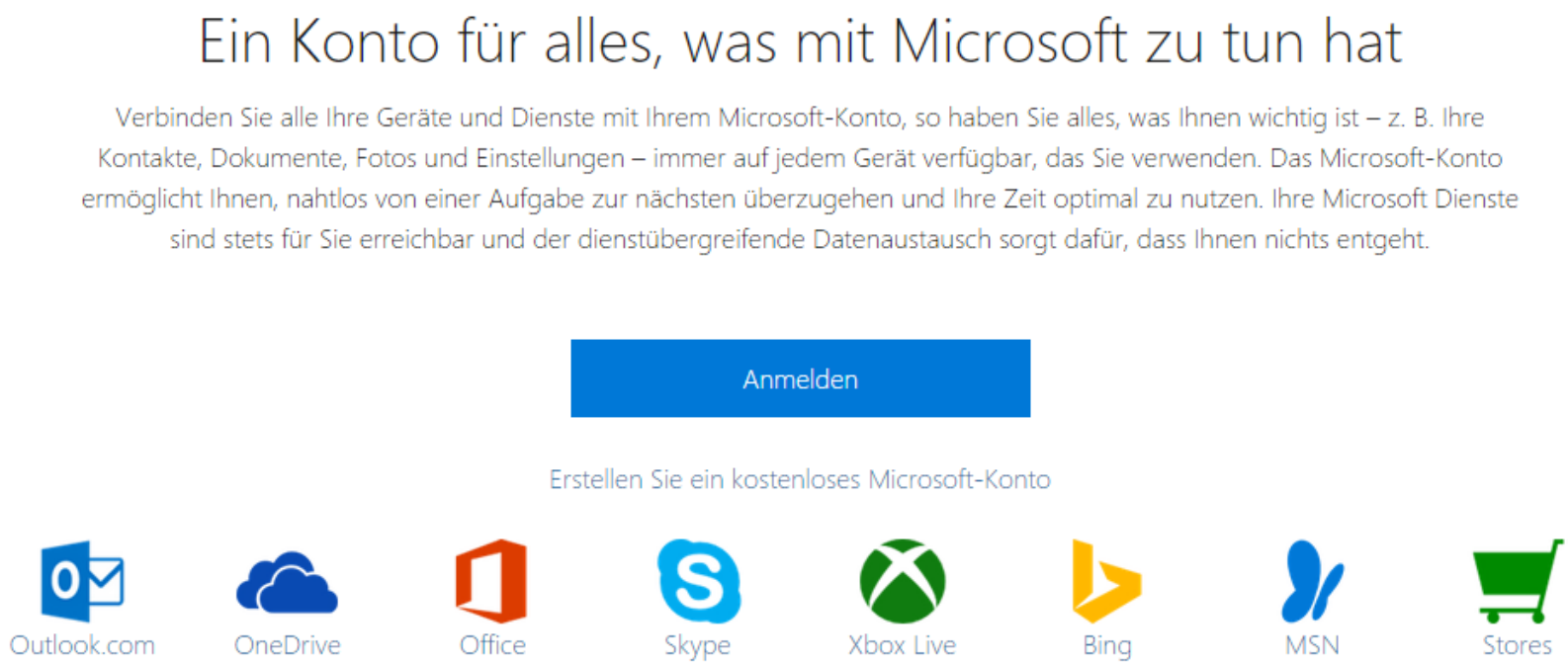
- Verfügbarkeit der Spracherkennung
  - Gerätemikrofon
- Windows Hello
  - Infrarotkamera für Gesichts- und Iris-Erkennnung
  - Fingerabdruckleser (mit Windows Biometrie-Framework-Unterstützung)
- Zwei-Schritt-Anmeldung:
  - PIN, Biometrie (Fingerabdruck oder Infrarotkamera) oder Smartphone mit W-LAN oder Bluetooth

Zusätzliche Anforderungen für bestimmte Features

- Bitlocker
  - Trusted Platform Module (TPM)
  - Intel® Platform Trust Technology (Intel® PTT)
  - (oder USB-Stick)
- Client-Hyper-V
  - 64-Bit-System mit Second Level Address Translation (SLAT)
    [bestimmte Intel-Prozessoren Core i7,i5,i3 und AMD seit Opteron]

Zusätzliche Anforderungen für bestimmte Features

- Für einige Funktionalitäten Microsoft-Konto erforderlich



Installationstypen

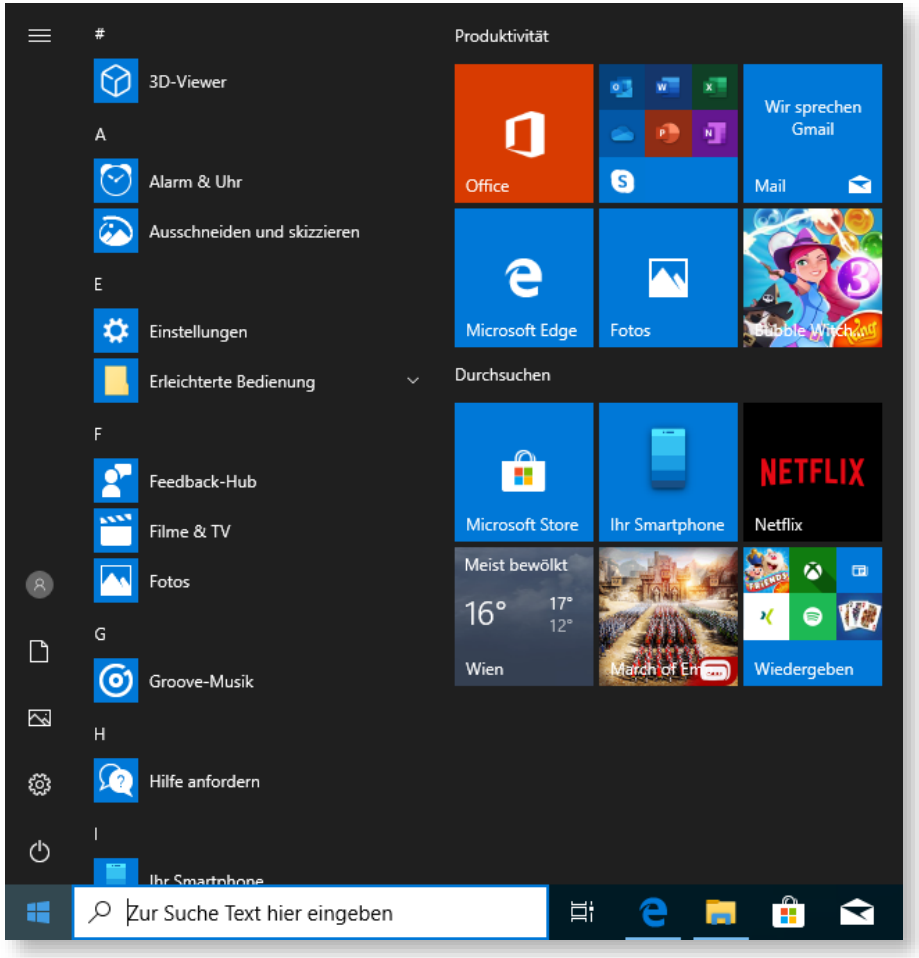
- Clean Install
  - DVD, USB
  - Netzwerk
  - Bereitstellungsdienste
- Upgrade (Inplace-Upgrade)
- Wipe & Load (z.B. Neuer PC)
  - Backup der Benutzerdaten und –Einstellungen
  - Clean install
  - Wiedereinspielen der Benutzerdaten und –Einstellungen
  - Reinstallation der Applikationen
- Provisionierung
  - Konfiguration ohne Reimaging

Ablauf der Windows 10-Installation

1. Boot von Windows PE
2. Start der Installation
3. Partitionierung
4. Aufspielen des Installationsimages
5. Neustart / Fertigstellen der Installation

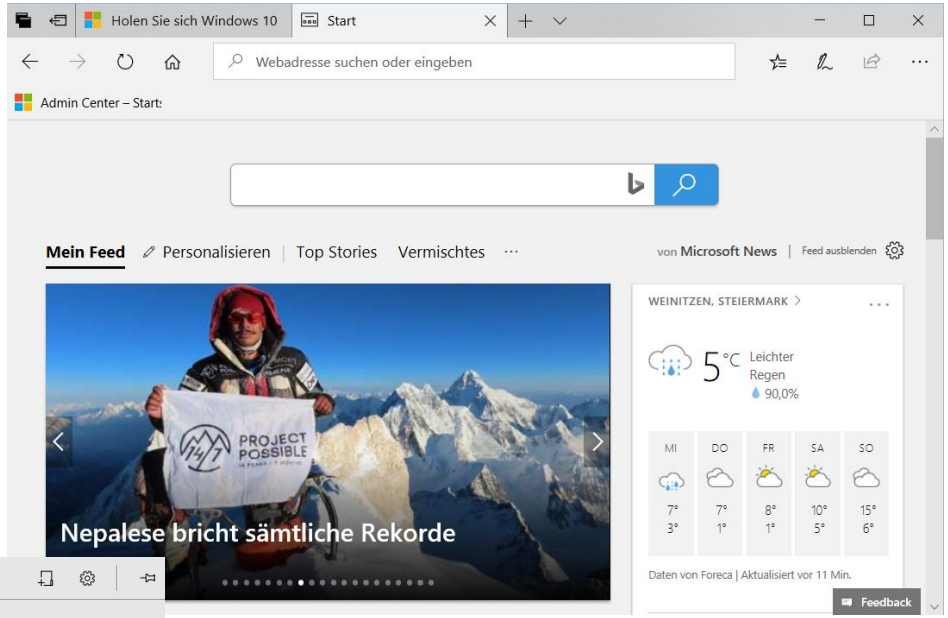
WINDOWS 10 OBERFLÄCHE

Das Startmenü



Microsoft Edge

- Inhalte im Web
  - Finden
  - Lesen
  - Kommentieren
- Hub
  - Favoriten
  - Leseliste
  - Verlauf
  - Downloads



Virtuelle Desktops

- Je nach Bedarf kann man beliebig viele virtuelle Desktops anlegen
- In der Taskleiste:
  Aktive Anwendungen → Neuer Desktop
- Tastenkombinationen zum Bedienen von virtuellen Desktops beginnen mit
  Windows + STRG

Wichtige Tastenkombinationen

Windows-Taste +	Aktion
Keine andere Taste	Startmenü
Tab	Task-Ansicht
D	Zeigt den Desktop
E	Öffnet den Windows Explorer
S oder Q	Suche
I	Einstellungen
H	Diktat beginnen
L	Benutzer sperren
O	Lageabhängiges Drehen des Bildschirms deaktivieren
Pfeil links/rechts	Schiebt das aktuelle Fenster an den linken/rechten Bildrand
Pfeil hoch	Fenster maximieren oder in obere Bildschirmhälfte verschieben
Pfeil runter	Fenster auf halbe Displaygröße oder minimieren
Pause	Systemeigenschaften
Umschalt + S	Einen Screenshot eines Teils des Bildschirms aufnehmen.

Wichtige Tastenkombinationen

Windows-Taste +	Aktion
STRG + D	Neuen virtueller Desktop erstellen
STRG + Pfeil links/rechts	Wechsel zwischen den virtuellen Desktops
STRG + F4	Schließen des aktuellen, virtuellen Desktops
A	Info-Center
P	Projektionsoptionen
R	Ausführen
X	Power User Kommandos
C	Cortana im Spracherkennungsmodus öffnen (ist standardmäßig deaktiviert)

BENUTZERMANAGEMENT

Benutzer und Gruppen

- Bei der Installation wird ein Administratorenkonto eingerichtet
- "Administrator" selbst ist deaktiviert, hat kein Kennwort
- Bei den Benutzerkonten werden folgende Kategorien unterschieden:
  - Administrator (Administratorengruppe)
  - Standardbenutzer (Benutzergruppe)

Administratoren

- Sind mit erweiterten Rechten ausgestattet:
  - können Programme, Hardwaretreiber installieren/deinstallieren
  - können auf Dateien aller Benutzer der lokalen Maschine zugreifen
  - können Benutzer verwalten

Standardbenutzer

- Normale Benutzerrechte
  - Verwaltung des eigenen Kontos
  - können mit eigenen Dateien und Apps arbeiten
  - können Teile der Ereignisanzeige (Anwendungs- und Systemprotokoll) auslesen

2 besondere Benutzerkonten:

- Gast
  - lässt sich aktivieren/deaktivieren
  - lässt sich nicht löschen
  - besitzt niedrigste Benutzerrechte
- Administrator
  - Wird automatisch beim Setup angelegt
  - standardmäßig deaktiviert
  - standardmäßig kein Kennwort
  - standardmäßig keine Einschränkung durch UAC

Benutzerverwaltung:

- Anlegen und Verwalten von Benutzern
  - Einstellungen | Konten
  - Computerverwaltung | Benutzer und Gruppen
    - lusrmgr.msc
  - Systemsteuerung
  - Command Line: Net user <Benutzername> /add
  - PowerShell: New-LocalUser

Vordefinierte lokale Gruppen

- Mitgliedschaft kann von einem Administrator festgelegt werden
  - Administratoren
  - Benutzer
  - Gäste
  - Hauptbenutzer
  - Remotedesktopbenutzer
  - Netzwerkkonfigurations-Operatoren

Systemgruppen (Sondergruppen, besondere Identitäten)

- Mitgliedschaft wird dynamisch vom Betriebssystem bestimmt – z.B.:
  - Anonymous-Anmeldung
    - Diese Gruppe stellt Benutzer und Dienste dar, die über das Netzwerk auf einen Computer und seine Ressourcen zugreifen, ohne Kennwort oder Domänennamen zu verwenden
  - Authentifizierter Benutzer
    - Die Gruppe "Authentifizierter Benutzer" schließt alle Benutzer und Computer ein, deren Identitäten authentifiziert wurden. "Authentifizierter Benutzer" schließt "Gast" nicht mit ein, auch wenn das Konto "Gast" über ein Kennwort verfügt. Die Mitgliedschaften in den Gruppen "Authentifizierter Benutzer" und "Anonymous-Anmeldung" sind gegenseitig ausschließend.
  - Jeder
    - Diese Gruppe stellt alle aktuellen Netzwerkbenutzer dar, einschließlich Gäste und Benutzer aus anderen Domänen

Systemgruppen (Sondergruppen, besondere Identitäten)

- Netzwerk
  - Die Gruppe "Netzwerk" repräsentiert Benutzer, die derzeit über das Netzwerk auf bestimmte Ressourcen zugreifen
- Interaktiv
  - Diese Gruppe stellt alle Benutzer dar, die aktuell an einem bestimmten Computer angemeldet sind und die auf eine bestimmte Ressource zugreifen, die sich auf diesem Computer befindet
- System
  - Die Gruppe "System" wird vom Betriebssystem und von Diensten verwendet, die unter Windows ausgeführt werden. Sie verfügt über Rechte ähnlich denen der Gruppe "Administratoren". Das Konto "System" ist ein internes Konto, welches im Benutzer-Manager nicht aufgeführt wird und anderen Gruppen nicht hinzugefügt werden kann. Auch lassen sich ihm keine Benutzerrechte zuweisen.
- Ersteller-Besitzer
  - Die Gruppe "Ersteller-Besitzer" ist ein Platzhalter in einem vererbbaren ACE

BENUTZERRECHTE UND BENUTZERKONTENSTEUERUNG

Benutzerrechte:

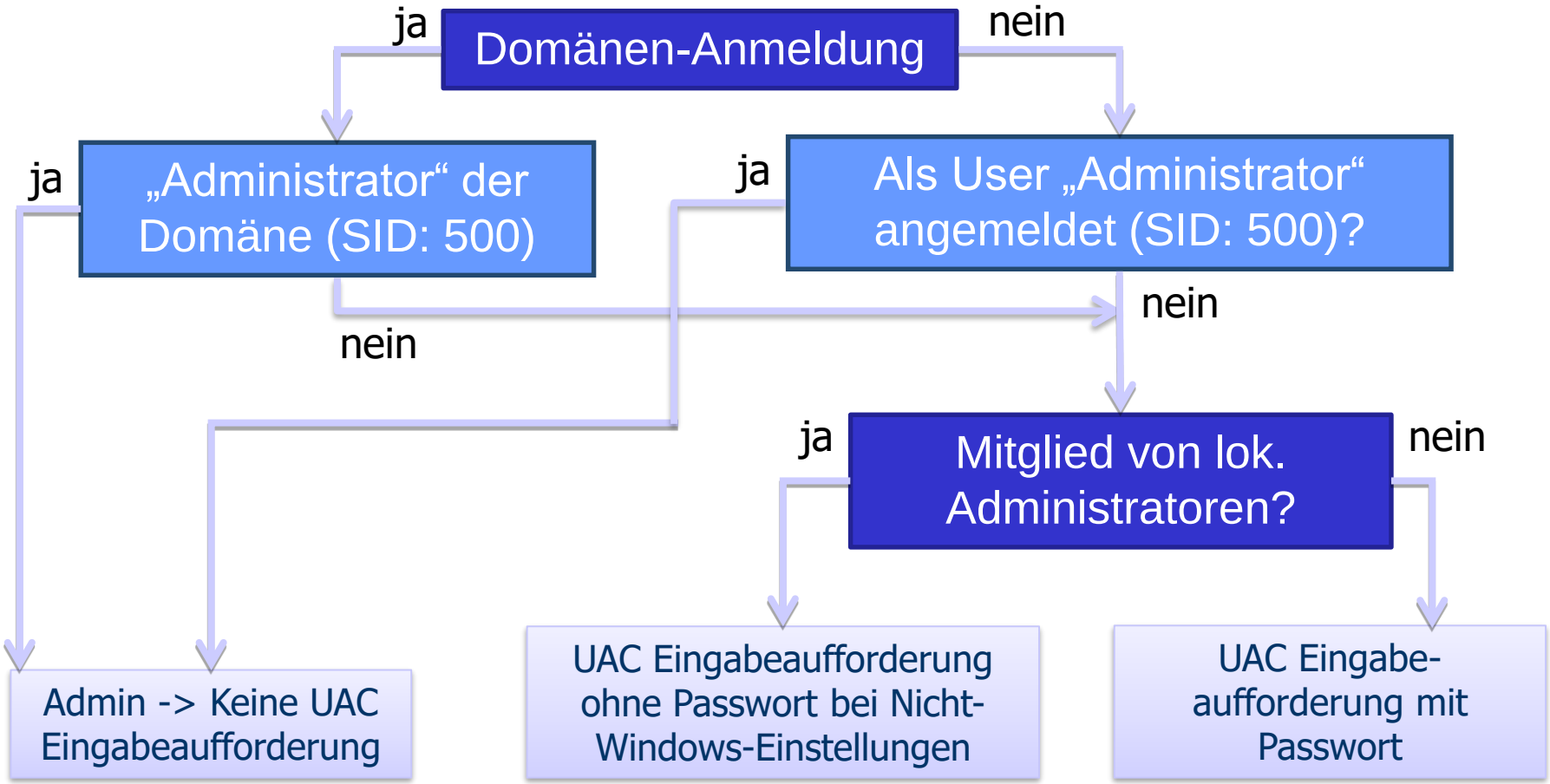
- Aufgaben, die ein Benutzer auf einem Computer durchführen darf
  - z.B. Ändern der Systemzeit (SeSystemTime)
- Benutzerrechte werden durch Sicherheitseinstellungen auf dem Computer gesteuert
- Diese werden in der Regel vom Systemadministrator festgelegt

Benutzerkontensteuerung (UAC)

- Soll nicht autorisierte Änderungen am Computer verhindern
  (z.B. Schutz gegen unbeabsichtigte Spyware-Installation)

- Zustimmung / Kennworteingabe eines Administrators bzw. Verweigerung für jede Tätigkeit, die administrative Rechte benötigt

UAC Standardverhalten



Benutzerkontensteuerung (UAC)

- Anpassen der UAC:
  - Systemsteuerung | Benutzerkonten und Jugendschutz
  - Benutzerkonten | Einstellungen der Benutzerkontensteuerung

- Benutzerkontensteuerung über Richtlinien anpassen:
  - Gruppenrichtlinieneditor | Computerkonfiguration | Windows Einstellungen | Sicherheitseinstellungen | Lokale Richtlinien | Sicherheitsoptionen

BENUTZERPROFILE

Benutzerprofile

- Sammlung von Einstellungen, die Darstellung und Funktion des Computers anpassen
- Einstellungen für Desktophintergründe, Bildschirmschoner, Netzwerkdruckerverbindungen, …
- Jedem Benutzerkonto ist ein Benutzerprofil zugeordnet

Benutzerprofile

- Aufbau
  - Dokumente (aka Eigene Dateien)
  - Desktop
  - Startbildschirm
  - Ntuser.dat (Registry)
  - Individuelles Benutzerprofil
    - `C:\Users\%Username%`
- All Users
  - `C:\Users\All Users` → `C:\programdata`
  - `C:\Users\All Users\Desktop` → `C:\Users\Public\Desktop`
  - `C:\Users\All Users\Start Menu` → `C:\programdata\Microsoft\Windows\Start Menu`
- Default User
  - `C:\Users\Default User` → `C:\Users\Default`

DATENTRÄGERVERWALTUNG

Datenträgerverwaltung

- Partitionierungsstile
  - MBR (max. 4 Partitionen, max. 2 TB)
  - GPT (nur durch OS-Implementierung begrenzt)
  - Bei Boot von GPT-Datenträger UEFI notwendig
- MBR-Partitionen
  - Primär
  - Erweitert
- Systempartition
- Startpartition

Dateisysteme

- FAT32
  - 512 MB – 2 TB
  - Unter Windows 10 formatiert: max. 32 GB
  - Dateigröße: max. 4 GB
  - Keine Zugriffsberechtigungen

- exFAT
  - V.a. für Datenaustausch Windows, Mac OS X, tw. Linux und Android)
  - max. Partitionsgröße 64 ZB
  - Dateigröße > 4 GB (bis 64 ZB)
  - Für Flashspeicher optimiert
  - Manchmal bei externen Festplatten und USB-Sticks eingesetzt

Dateisysteme

- NTFS
  - Zugriffsberechtigungen auf Dateisystemebene
  - Verschlüsselung (EFS)
  - Komprimierung
  - Kontingente
  - Indizierung

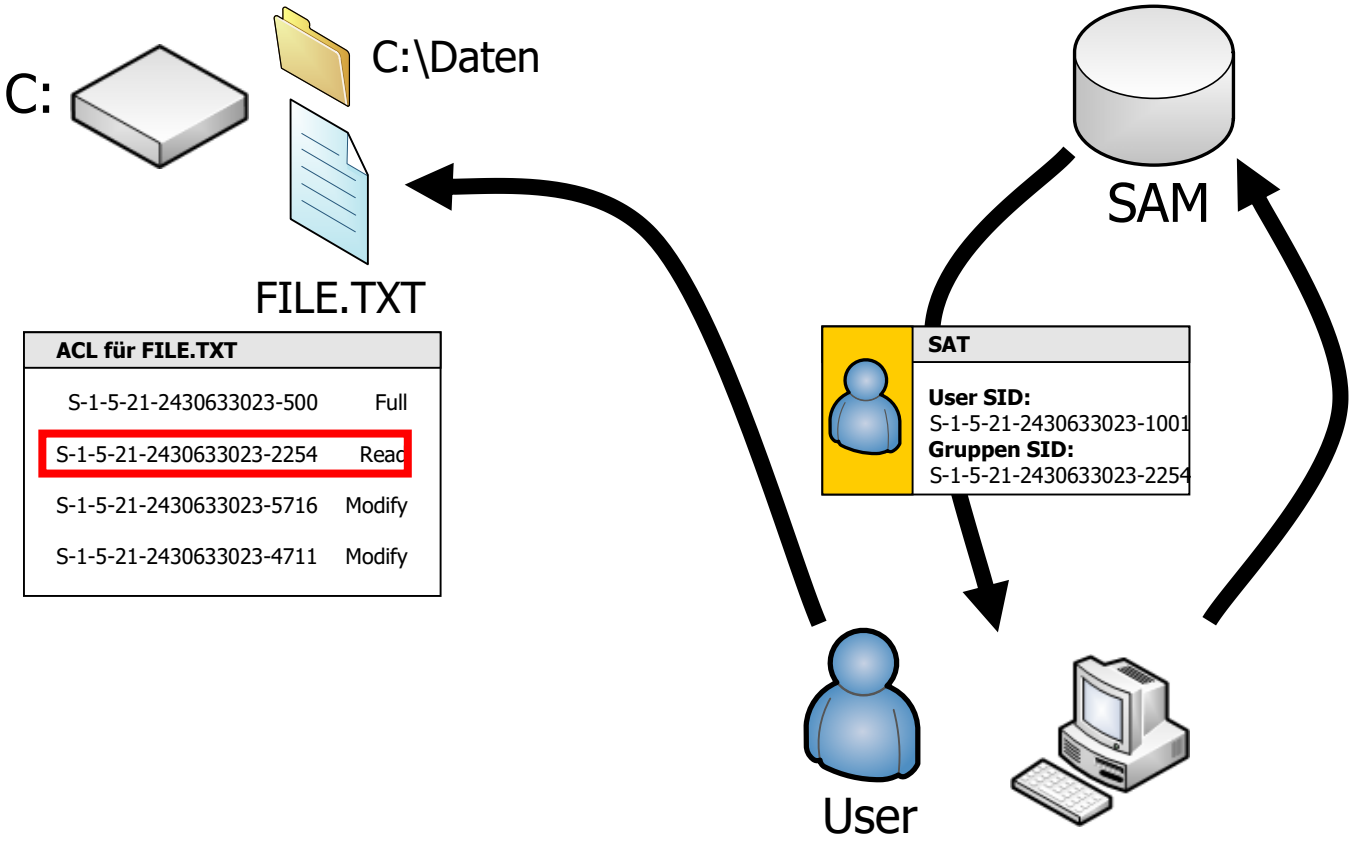
- Konvertierung FAT/FAT32 ➔ NTFS:
  - `convert [volume]: /FS:NTFS`
  - One-Way Operation!

NTFS-BERECHTIGUNGEN

Berechtigungen auf Dateisystemebene

- Berechtigungen sind Regeln, die Objekten auf einem Computer zugeordnet sind, z. B. Dateien und Ordnern
- Durch Berechtigungen wird bestimmt, ob Sie auf ein Objekt zugreifen können und welche Aktionen Sie damit ausführen können

Zugriff auf Dateien



Berechtigungen auf Dateisystemebene - Dateien

Berechtigung	Beschreibung
Lesen	Datei lesen; Dateiattribute, Besitz und Berechtigungen auslesen.
Schreiben*	Datei überschreiben, Dateiattribute ändern, Besitz und Berechtigungen auslesen.
Lesen & Ausführen	Programm ausführen und alle Berechtigungen von „Lesen“.
Ändern	Ändern und Löschen der Datei und alle Berechtigungen von „Schreiben“ und „Lesen & Ausführen“.
Vollzugriff	Berechtigungen verändern, Besitz übernehmen, und alle Berechtigungen von „Ändern“.

*Die Berechtigung „Schreiben“ bedingt nicht das Vorhandensein der Berechtigung „Lesen“

Berechtigungen auf Dateisystemebene - Ordner

Berechtigung	Beschreibung
Lesen	Dateien und Unterordner sehen; Attribute, Besitz und Berechtigungen dieses Ordners auslesen.
Schreiben	Neue Dateien und Unterordner anlegen, Attribute ändern, Besitz und Berechtigungen auslesen.
Ordnerinhalt anzeigen	Dateien und Unterordner anzeigen
Lesen & Ausführen	In den Ordner hineinwechseln, um andere Dateien oder Ordner zu erreichen und alle Ordnerberechtigungen von „Lesen“ und „Ordnerinhalt auflisten“.
Ändern	Löschen des Ordners und alle Berechtigungen von „Schreiben“ und „Lesen & Ausführen“
Vollzugriff	Berechtigungen verändern, Besitz übernehmen, Löschen von Unterordner und Dateien, und alle Berechtigungen von „Ändern“

Berechtigungen auf Dateisystemebene

- Zusammenwirken von Berechtigungen
- Besitz
- Kopieren und Verschieben von Dateien

Verschieben von Dateien mit aktivierter Vererbung

Buchhaltung: Lesen/Ausführen
Geschäftsführung: Lesen/Ausführen

C:\Bilanzen

Verschieben

Archivleser: Lesen/Ausführen
Archivadmins: Vollzugriff

C:\Archiv

ACL
Vererbung: **Aktiviert**
Gerhard: Vollzugriff

ACL
Vererbung: **Aktiviert**
Gerhard: Vollzugriff

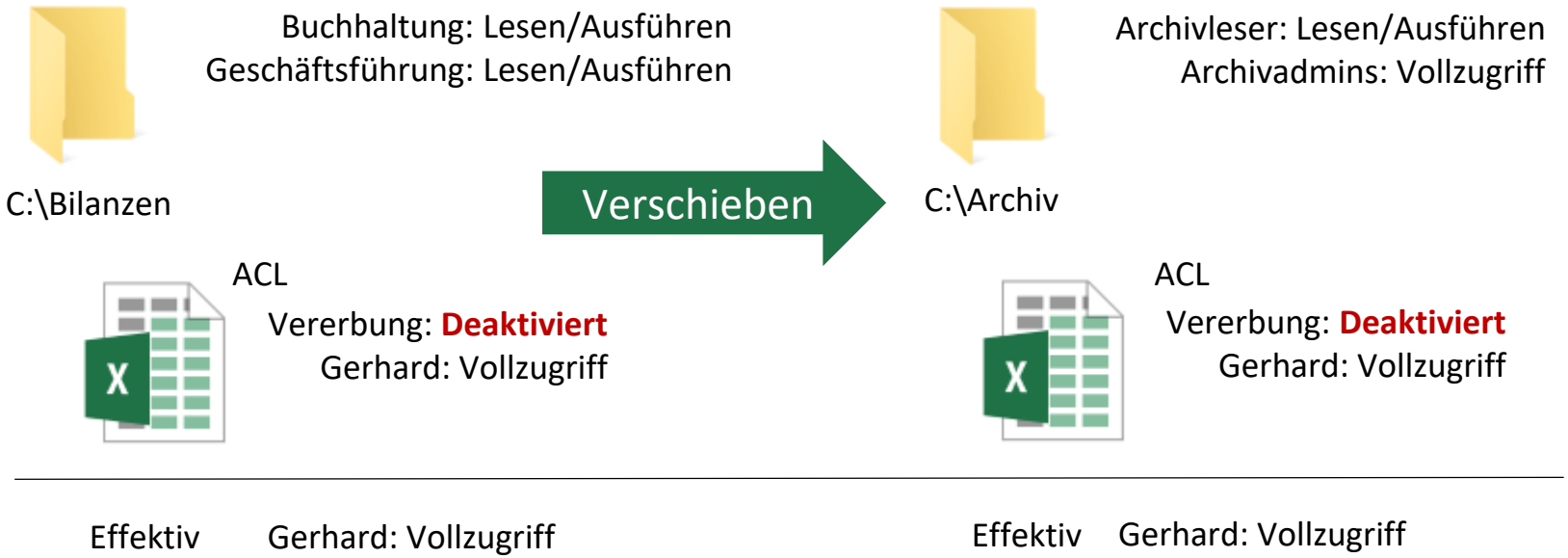
Effektiv

Buchhaltung: Lesen/Ausführen
Geschäftsführung: Lesen/Ausführen
Gerhard: Vollzugriff

Effektiv

Archivleser: Lesen/Ausführen
Archivadmins: Vollzugriff
Gerhard: Vollzugriff

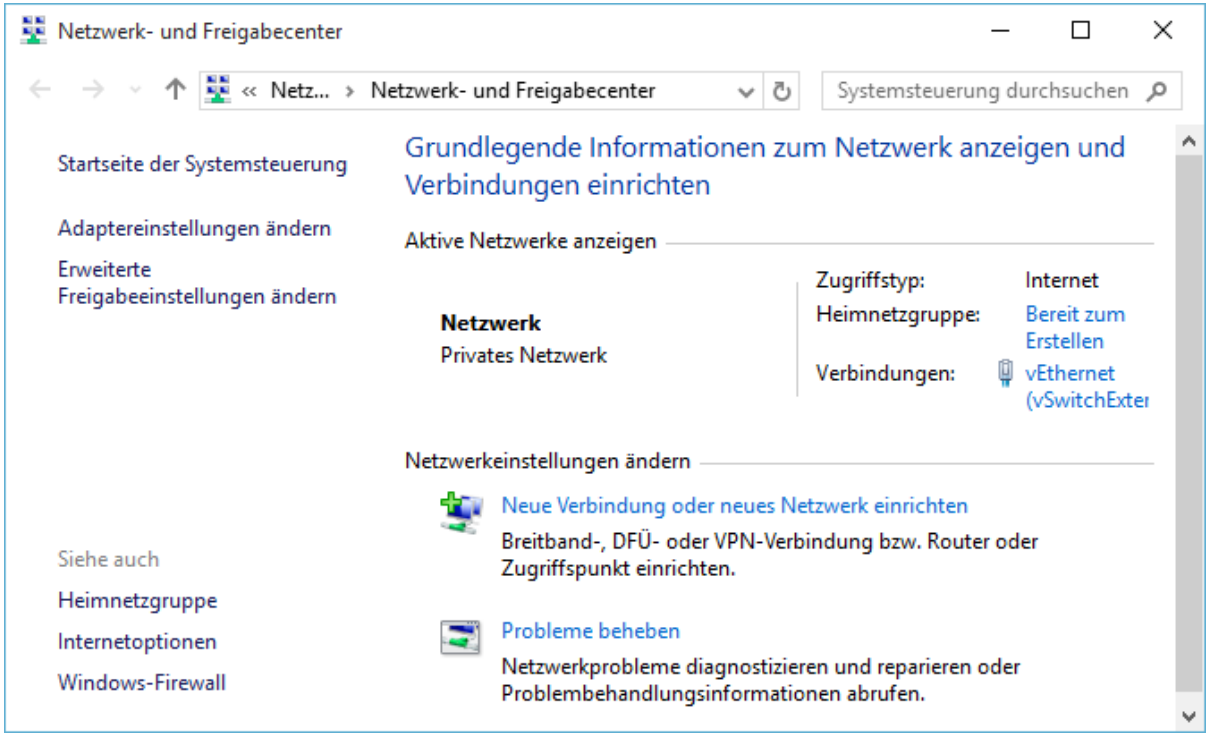
Verschieben von Dateien mit deaktivierter Vererbung



FREIGABE VON ORDNERN

Netzwerkkonfiguration

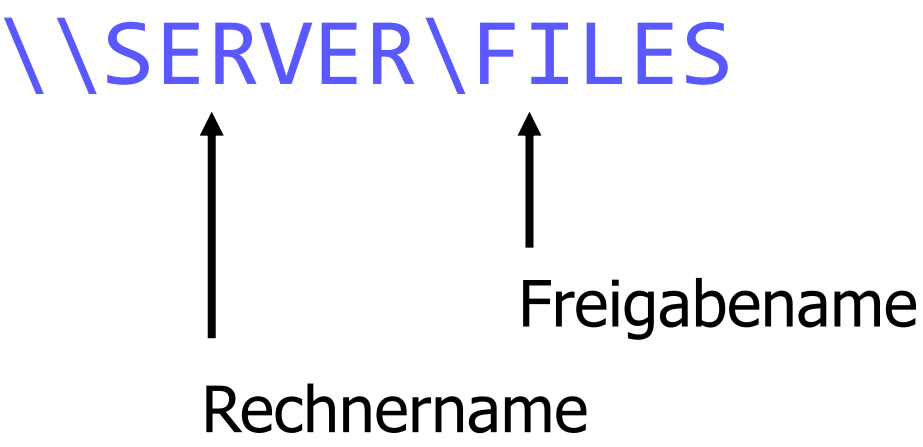
- Netzwerkkonfigurationscenter
  - Netzwerktyp
    - Öffentlich
    - Privat
- Arbeitsstationsdienst
- Serverdienst



Freigaben und –berechtigungen

- 3 Möglichkeiten:
  - Erweiterte Freigabe
    - Vollzugriff
    - Ändern
    - Lesen
  - Freigabe-Assistent
    - Automatische Konfiguration von NTFS und Freigabeberechtigungen
    - Integration der Heimnetzgruppe
  - `net share`

UNC-Pfad



Administrative Freigaben

- Werden automatisch erstellt
  - Für eingebaute HD-Laufwerke/Partitionen: C$,D$,E$
  - Für das SYSTEMROOT:
    ADMIN$
  - Für interne Funktionen (Netzwerkdruck, Fernverwaltung über MMC): IPC$
  - Für Druckertreiber:
    PRINT$

Verbinden von Netzlaufwerken

- An verschiedenen Stellen in der GUI
  - Netzlaufwerk zuordnen

- Command Line
  - `net use <Buchstabe>: \\SERVER\SHARE [/persistent:no]`

Zusammenwirken von Berechtigungen

- Mit Hilfe der Freigabeberechtigungen, können die NTFS-Berechtigungen für den Zugriff aus dem Netzwerk

  beschränkt,

  jedoch **nie erweitert** werden.

- Stellen Sie sich Freigabeberechtigungen als Filter vor den NTFS-Berechtigungen vor!

Übungen: Zusammenwirken von Berechtigungen

- Legen Sie als Admin einen Ordner D:\Permissions an und legen Sie im Ordner einige Dateien namens ADMIN1.TXT, ADMIN2.TXT, etc an.
- Geben Sie den Ordner frei
- Entfernen Sie alle Standardberechtigungen
- Berechtigungen:

Berechtigungen	PG1	PG2	PG3
NTFS	Ändern	Lesen/Ausführen	Vollzugriff
Freigabe	Vollzugriff	Ändern	Lesen
Effektiv			

Übungen: Zusammenwirken von Berechtigungen

Berechtigungen	PG1	PG2	PG3
NTFS	Ändern	Lesen/Ausführen	Vollzugriff
Freigabe	Vollzugriff	Ändern	Lesen
Effektiv	**Ändern**	**Lesen/Ausführen**	**Lesen**

System Essentials – Überblick

- Der Startprozess
- Ereignisanzeige
- Dienste
- Gerätemanager und Hardwaretreiber
- Taskmanager
- Systemwiederherstellung
- Systemreparatur
- Registrierung

STARTPROZESS

BIOS vs. UEFI

- Zum Starten eines PCs wird eine Firmware benötigt, die in einem nicht-flüchtigen Speicher auf dem Mainboard liegt
  (=Mini-Betriebssystem für das Mainboard)

- BIOS (Basic Input/Output System)
  - Regelt Einstellungen für Hardwarekomponenten, um diese für den Bootvorgang ansprechbar zu machen
  - Nachteile:
    - Technische Limitierungen wie max. Größe der Boot-Festplatte
    - nur 1 MB RAM adressierbar
    - kennt keine Dateisystemtreiber

BIOS vs. UEFI

- UEFI (Unified Extensible Firmware Interface)
  - „BIOS-Nachfolger“
  - GPT-Unterstützung
  - Beinhaltet Treiber für verschiedene Dateisysteme und Hardware (Grafikkarte, Netzwerkkarte, USB, etc)
  - Bei Installation eines Betriebssystems wird das Ladeprogramm als Binary (*.efi) auf einer EFI-Systempartition hinterlegt

Der Startprozess (BIOS)

- Start des Computers
  - BIOS
  - POST
  - Laden des MBR
  - PBS
- Windows Start-Manager
  - Bootmgr
  - Startkonfigurationsdatenbank (BCD)
  - winload.exe

Der Startprozess (UEFI)

- Start des Computers
  - Pre-EFI Initialisierung
  - Start des EFI-Bootloaders
  - Mounten der EFI-Systempartition
  - Suche und Anzeige der Bootloader
  - Ausführen des Betriebssystem-Bootloaders (EFI-Binary)
- Windows Start-Manager bootmgfw.efi
  - Bootmgr.efi
  - BCD
  - winload.efi

Der Startprozess

- Laden von Geräten und Diensten
  - Statusleiste am Bildschirm
  - Treiber für die erkannten HW-komponenten werden geladen und initialisiert
  - Startinformationen für Dienste werden aus der Registry gelesen

Der Startprozess

- Anmeldesequenz
  - Authentifizierung (Lokaler SAM oder Verbindung mit Domäne)
  - Laden des Benutzerprofils und der Betriebssystemshell
  - Abschließen der Initialisierung der verzögerten Startdienste

Boot Configuration Data (BCD)

- Datenbank für Bootkonfiguration
- ersetzt boot.ini (Windows XP/2003)
- Speicherort:
  - EFI System Partition
  - \Boot\BCD auf der Systempartition
- editieren mittels bcdedit oder WMI

EREIGNISANZEIGE

Ereignisanzeige

- Tool zur Überwachung des Systemzustands
- Anzeigen von Ereignissen aus verschiedenen Ereignisprotokollen
- Speichern nützlicher Ereignisfilter
- Planen eines Tasks als Reaktion auf ein Ereignis

Ereignisanzeige

- Windows Protokolle
  - Anwendung
  - System
  - Installation
  - Sicherheit
- Benutzerdefinierte Ansichten
  - z.B. Administrative Ereignisse
    (nur Kritisch, Fehler und Warnungen)

Ereignisanzeige - Aktionen

- Sortieren
- Suchen
- Filtern
- Exportieren/Importieren

DIENSTE

Dienste

- Überblick über verfügbare Dienste (Services)
- Starten und Stoppen von Diensten
- Starttyp
- Wiederherstellung von Diensten
- Abhängigkeiten

Dienste - Überblick

- Dienst: Programm, das im Hintergrund läuft
- Viele Dienste werden erst gestartet, wenn sie benötigt werden.
- Auflisten von Diensten
  - Dienste-Snapin (services.msc)
  - Computerverwaltung
  - Systemkonfigurationsprogramm (msconfig.exe)
  - Taskmanager (taskmgr.exe)

Dienste

- Starttyp
  - Automatisch
  - Automatisch (Verzögerter Start)
  - Automatisch/Manuell (Start durch Auslöser)
  - Manuell
  - Deaktiviert
- Status
  - Beendet
  - Gestartet
  - Angehalten

Dienste - Eigenschaften

- Kontext
  - Mit welchem Benutzerkonto wird der Dienst gestartet?
- Abhängigkeiten
  - Welche Dienste müssen vor dem Dienst gestartet sein?
  - Welche Dienste benötigen diesen Dienst
- Pfad zum Binary, Startparameter
- Wiederherstellung
  - Z.B. automatischer Neustart, wenn Dienst unerwartet beendet wird

HARDWARE UND TREIBER

Hardware und Treiber

- Gerätemanager
- Zustand eines Geräts
  - Funktionierendes Gerät
  - Unbekanntes Gerät
    (Treiber nicht installiert)
  - Nicht gestartetes Gerät
    (falscher Treiber oder fehlerhafte Hardware)
  - Nicht verbundenes Gerät
    (Treiber „schlummert“ – Gerät nicht sichtbar)

Hardware und Treiber

- Geräte
  - Deinstallieren
    (Plug&Play Hardware beim nächsten Neustart wieder erkannt)
  - Deaktivieren
    (Gerät ist abgeschaltet, wird auch beim Neustart nicht erneut erkannt)

Treibereigenschaften

- Treiberdetails – Version
  - Wichtige Daten, wie Hersteller, Datei(en)
- Treiber aktualisieren
  - Neue Versionen einspielen
- Vorheriger Treiber
  - Alten Treiber wiederherstellen, falls Aktualisierung nicht erfolgreich war

Treiber-Troubleshooting

- Treibersuche bei unbekannten Geräten
  - Anzeige der Hardware-IDs
  - Suche auf www.pcilookup.com
- Anzeigen nicht verbundener Geräte

TASKMANAGER UND VIRTUELLER SPEICHER

Taskmanager

- Werkzeug zur Überwachung des laufenden Systems und aller verwendeter Applikationen und deren Prozesse

- Unter Windows 10 gibt es zwei Ansichten
  - Einfach (zum Anzeigen und „killen“ von Anwendungen)
  - Detailliert (zur genauen Analyse des Systems)

- Analyse von Speicher- , Prozessor-, Datenträger und Netzwerkauslastung

Taskmanager

Wichtige Informationen beim Troubleshooting

- Suche nach sog. „Flaschenhälsen“ durch Anzeige von
  - Prozessor-Leistung
  - Arbeitsspeicherverlauf
  - Festplattenverwendung
  - Netzwerkverbindungen
- PID – Prozess-ID zum „Aufspüren“ von ev. unerwünschten Prozessen
  - netstat -ano
- Beenden von Tasks bzw. von Prozessen

Auslagerungsdatei

- Virtueller Arbeitsspeicher
  - Speicher von Programmen, der während deren Ausführung gerade nicht benötigt wird, wird bei Bedarf in die Auslagerungsdatei geschrieben
  - Das Programm hat dennoch den Eindruck vollständig im Speicher zu sein
  - Erfolgt ein Zugriff auf den ausgelagerten Speicher durch das Programm, lädt das Betriebssystem die benötigten, ausgelagerten Teile nach.

Auslagerungsdatei

- Seitenfehler
  - Ist eine Speicherseite (4KB großer Speicherabschnitt) ausgelagert, und versucht ein Programm auf diesen Bereich zuzugreifen, lädt das Betriebssystem die Seite von der Auslagerungsdatei nach
  - Dies bezeichnet man als Seitenfehler

Auslagerungsdatei – Best Practice

- Auf eigenen, schnellen Datenträger
- Richtwert: RAM x 1.5
- Dateiname: pagefile.sys

TROUBLESHOOTING SYSTEMWIEDERHERSTELLUNG

Troubleshooting - Übersicht

- Systemwiederherstellung
  - Systemwiederherstellungspunkte
  - PC zurücksetzen
    1. Apps und Einstellungen entfernen, eigene Daten behalten („Auffrischen“)
    2. Alles Löschen (auf Originalzustand „Zurücksetzen“
  - Systemimage-Wiederherstellung (erfordert selbst erstelltes Recovery-Image)

- Windows RE (Repair Environment)
  - Automatischer Start
  - Manueller Start

Troubleshooting - Übersicht

- Startoptionen
  - Computer reparieren bzw. Wiederherstellungsumgebung starten
  - Abgesicherter Modus
  - Abgesicherter Modus mit Netzwerk
  - Abgesicherter Modus mit Eingabeaufforderung
  - Startprotokollierung aktivieren
  - Videomodus mit niedriger Auflösung aktivieren
  - Frühen Start des Treibers der Antischadsoftware deaktivieren

- Aufrufen der erweiteten Startoptionen:
  - STRG + F8 (beim Bootvorgang)
  - Mit gedrückter SHIFT-Taste auf „Neu starten“ klicken
  - `shutdown.exe /r /o /t 0`

Troubleshooting mit einem Systemwiederherstellungspunkt

- Schnappschuss des Systems
- Betrifft
  - Systemdateien
  - Registry-Einstellungen
  - Installierte Programme

Troubleshooting mit einem Systemwiederherstellungspunkt

- Erstellt bei
  - Installation nicht signierter Treiber
  - u.U. Windows Update
  - Div. andere Installationen
  - Täglich
- Sinnvoll nach
  - Instabilität nach Treiberinstallation
  - Instabilität nach Softwareinstallation
- Persönliche Daten werden nicht gesichert!

Systemstartoptionen

- Abgesicherter Modus
  - Nur die notwendigsten Treiber werden geladen
  - Verwenden, wenn normaler Systemstart nicht möglich
  - I.A. weitere Troubleshooting-Massnahmen erforderlich

Systemstartoptionen

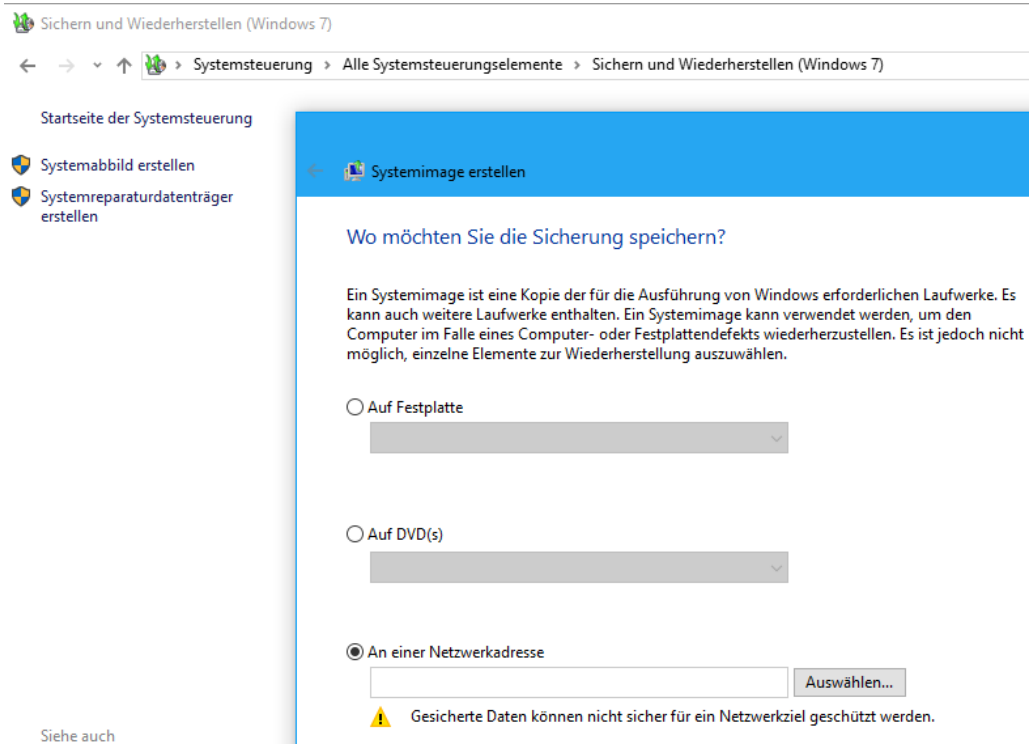
- VGA-Modus
  - 640x480, aber mit dem Original-Grafikkarten-Treiber
  - Verwenden, wenn eine Einstellung des Grafikkartentreibers zu keiner Bilddarstellung führt. (z.B. Wiederholfrequenz)

Reparaturmöglichkeiten in der Shell

- `bootrec`
- `regedit`
  - Mit „Struktur laden“ ist Bearbeitung der offline-Registry möglich
- `chkdisk`
- Dateioperationen (`copy`, `del`, . . .)

Rücksichern einer Image-Sicherung

- Verwenden, wenn keine andere Reparaturmethode zum Erfolg führt
- Systemabbild muss vorher einmal erstellt worden sein!
- Irreführend zu finden unter: Systemsteuerung | Sichern und Wiederherstellen (Windows 7)



REGISTRY

Registrierung

- Zentrale Datenbank, die u.a. folgende wichtige Informationen enthält
  - Systemhardware
  - Installierten Programmen und Einstellungen
  - Benutzerprofil-Informationen
- Besteht aus Schlüsseln und Werten
- Speicherorte
  - %SYSTEMROOT%\SYSTEM32\CONFIG
  - Benutzerprofil (NTUSER.DAT)

Hauptschlüssel der Registry

- HKEY_CLASSES_ROOT (HKCR)
- HKEY_CURRENT_USER (HKCU)
- HKEY_USERS (HKU)
- HKEY_LOCAL_MACHINE (HKLM)
- HKEY_CURRENT_CONFIG

HKEY_CLASSES_ROOT

- Enthält alle Daten, die in Windows zur Unterstützung registrierter Dateitypen und Bibliotheken benötigt
  - Icons
  - Befehle (Öffnen, Drucken, etc.)
  - Konfigurationsdaten für Programme

HKEY_CURRENT_USER

- Einstellungen für den aktuell angemeldeten Benutzer
- Aus dem Zweig HKU bei der Anmeldung übernommen
- HKU-Registry Teil wird bei der Anmeldung aus NTUSER.DAT geladen

HKEY_USERS

- Userspezifische Daten aller Benutzer, deren Profil zur Zeit benötigt wird.
- Beispiele
  - Aktueller Benutzer (Link von HKCU)
  - Dienstbenutzer (SYSTEM)
  - Sekundäre Anmeldungen

HKEY_LOCAL_MACHINE

- Informationen über Treiber, Installierte Hardware, Software-Einstellungen, …
- Enthält folgende Unterschlüssel
  - HARDWARE (installierte HW + Parameter)
  - SOFTWARE
  - SYSTEM
    - CurrentControlSet
      - Control (Computername,Dateisystem,etc.)
      - Services (Dienste)

Typen von Registrierungswerten

- String (REG_SZ)
- Multistring (MULTI_SZ)
- Expandable-String (REG_EXPAND_SZ)
- Binary (REG_BINARY)
- DWORD (REG_DWORD) (32-Bit-Wert)
- QWORD (REG_QWORD) (64-Bit-Wert)

Registrierungseditor

- `regedit.exe`
  - Ändern von Registrierungseinträgen
  - Umbenennen von Schlüsseln und Werten
  - Neue Schlüssel und Werte einfügen
  - Löschen von Einträgen
  - Suchen
  - Favoriten
  - Drucken
  - Export/Import
  - Berechtigungen