Inhalt

Speicherverwaltung

- Zuweisung von Speicher an Prozesse
- Schutz vor unerlaubtem Zugriff auf OS-reservierten Bereich
- **Belegungstabelle (Memory Management Unit – MMU):** Speichert freie und belegte Speicherbereiche
- **Seite**: Block von x Bytes, die zusammengefasst sind

Direkte Speicherbelegung

- **Ein Programm**: Prozess erhält den gesamten Speicher
- **Mehrere Programme**: Zuordnung erfolgt über Speicherbelegungstabelle
- Wird ein freier Platz gesucht, wird die gesamte Tabelle auf eine passende Anzahl aufeinanderfolgender Nullen durchsucht

Speicherbelegungsstrategien

Kriterien

- Möglichst wenig Verschnitt
- Restblöcke sollen noch eine „nutzbare“ Größe haben
- Möglichst schnelles finden von freiem Speicher

Strategien

- **First-Fit**: Erster passender, freier Speicherplatz wird gewählt
- **Best-Fit**: Am besten passender Speicherplatz wird gewählt
  ➔ Wenig Verschnitt
- **Worst-Fit**: Am schlechtesten passender Speicherplatz wird gewählt
  ➔ Viel Verschnitt
- **Next-Fit**: Nächster Platz an dem der angeforderte Speicher passt wird gewählt
  ➔ Nächste Suche beginnt an dieser Stelle
- **Halbierung**: Speicher wird iterativ halbiert
  ➔ Verschiedengroße Blöcke entstehen
  ➔ Es wird immer ein kompletter Block belegt

Probleme

- **Fragmentierung**: Speicher hat viele kleine, unbrauchbare Stücke
- Belegungstabelle benötigt ebenfalls Platz

Virtuelle Speicherbelegung

- **Logischer Adressraum**: Adressraum, auf den die Befehle eines Programms referieren
- **Physischer Adressraum**: Adressraum, in dem sich das Programm bei der Abarbeitung befindet
- Beide Adressräume werden in gleichgroße Seiten eingeteilt
- **Seitentabelle**: Dient zur Transformation von virtuellen in physische Seitenrahmen. Übersetzt virtuelle Adressen in reale Adressen.
  - Enthält:
    - Für welche virtuelle Seite welche physische Seite verwendet werden soll
    - Bei nicht verwendeten Seiten, dass keine reale Seite dafür verwendet wird
    - Bei Auslagerung, wo in einer Programm-/Bibliotheks-/Auslagerungsdatei der Inhalt gespeichert ist

Seitentabelleneintrag

Aufbau

- **Seitenrahmennummer**: Physische Adresse im Arbeitsspeicher, auf die der Eintrag verweist
- **Present-Absent-Bit**: Im RAM(1) oder ausgelagert(0)
- **Protection-Bits**: Regelt Zugriff auf die Seite
    - z.B.: 1 Bit: 0 -> Lesen und Schreiben – 1 -> Schreiben
- **Modified-Bit (M-Bit):** Wird gesetzt, wenn auf eine Seite geschrieben wird
    - Beim Auslagern wird dadurch entschieden, ob die Version auf der Festplatte aktualisiert werden muss oder ob diese noch aktuell ist
    - Wurde es geändert?
- **Referenced-Bit (R-Bit):** Wird bei jedem Zugriff auf die Seite gesetzt
    - Hilft beim entscheiden welche Seite ausgelagert werden soll
    - Wurde es benutzt?

Adressabbildung

- **Virtuelle Adresse**: Seitennummer + Offset
- **Reale Adresse**: Basisadresse der realen Seite + Offset
- **Länge des Offsets**: Größe der Seite
- **Länge der Seitentabelle**: Anzahl der Bits für die Seitennummer/Basisadresse
    - z.B.: Seite mit 1024 Byte -> 2^{10} -> 10 Bit

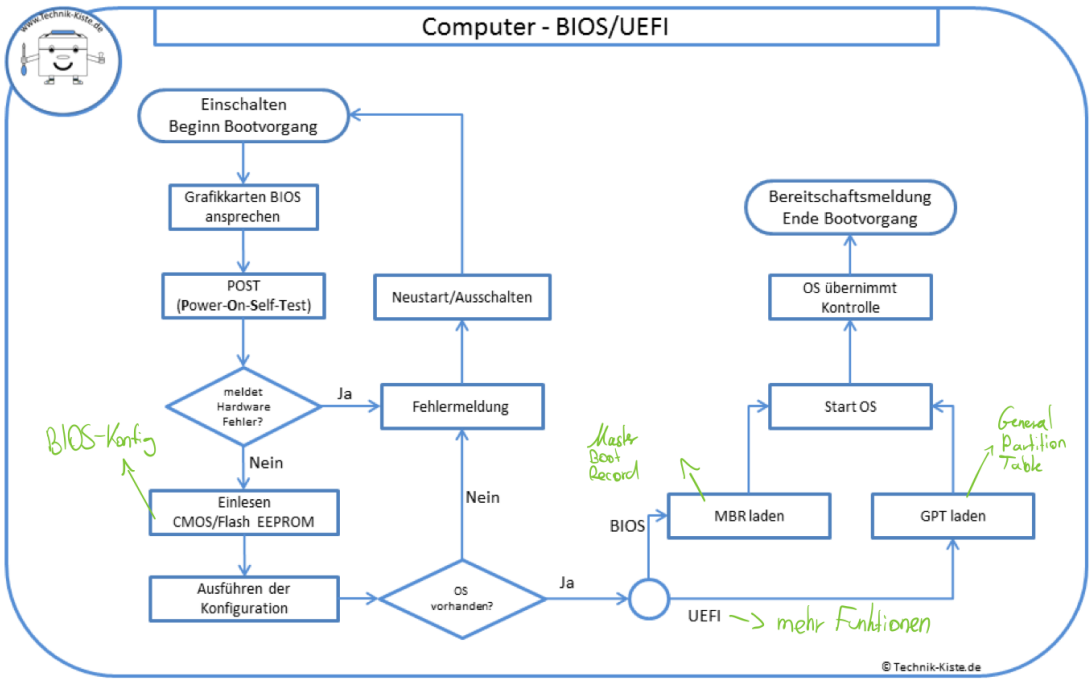
Swapping

- Kein freier Arbeitsspeicher -> Daten werden ausgelagert
- Adressen von ausgelagerten Seiten werden nicht in der Seitentabelle gespeichert
  ➔ Es kommt zum Seitenfehler -> OS greift auf eigene Tabellen zurück

Seitenfehler

- Prozess spricht Adresse an, die nicht im RAM geladen ist
  ➔ Seitenfehler entsteht
  ➔ OS übernimmt Behandlung
- Mögliche Ursachen:
    - Seite ist ausgelagert
    - Prozess greift das erste Mal auf die Seite zu
    - Seite ist ungültig bzw. Zugriff nicht erlaubt (Segmentation Fault)

Bootvorgang



BIOS: Master Boot Record (MBR)

- **Bootloader**: Ruft Bootloader oder Bootmanager auf
- **Datenträgersignatur**: Identifikation des Datenträgers, der Bootinstruktionen enthält
- **Schutzabstand**
- **Partitionstabelle**: Partitionen auf dem physischen Laufwerk
- **Bootsektorsignatur**: 0x55AA als Ende des MBR

UEFI: General Partition Table (GPT)

LBA: Logical Block Index z.B.: 1LBA = 512 Byte

- **LBA0 – Protective MBR**: 512 Byte Platzhalter für MBR
- **LBA1 – GPT Header**:
  - Position des Headers
  - Position des Backup-Headers
  - Anzahl und Größe der Partitionseinträge
  - CRC-Prüfsumme
- **LBA2 – LBA34**: Partitionseinträge
- **Ab LBA34**: Eigentliche Partitionen
- **In den letzten 34 LBAs**: Alles gespiegelt

Vergleich: MBR vs. GPT

	Master Boot Record (MBR)	**General Partition Table (GPT)**
Max. Festplattengröße	2TB	18 ExaByte
Primäre Partitionen	4	Unbegrenzt
Sicherheit	Keine Prüfsumme, nur ein Datensektor	Datensektor mit Prüfsumme und Backup
Standardisierung	Kein Standard; Lose Vereinbarung	Exakt definiert durch EFI

Datenträgerverwaltung

- **Unter Windows**: diskmgmt.msc (GUI) oder diskpart (CLI)
- **Einfachste Variante**: Basisdatenträger
    - **Partitionierung**: Einteilung in Untereinheiten (Volumes)
        - Wird in MBR/GPT geschrieben
    - **Laufwerksbezeichnung**: Name und Laufwerksbuchstabe
    - **Dateisystem**: Art, wie Dateien auf dem Datenträger abgelegt werden

Dynamische Datenträgerverwaltung

- **Logical Volume Manager (LVM):** kümmert sich um Verwaltung der logischen Datenträger
- **Physical Volume**: Physisches Laufwerk (HDD / SSD)
- **Physical Partition**: Physische Partition auf einem Laufwerk
- **Logical Volume**: Logisches Laufwerk, das sich aus mehreren physischen Partitionen zusammensetzen kann
- **Filesystem**
- **Mounting-Point**: Ort, an dem ein Laufwerk eingegliedert wird

Unter Windows

- **Einfaches Volume**: zusammenhängender Bereiche einer physischen Festplatte
- **Übergreifendes Volume**: besteht aus Bereichen mehrere physischer Festplatten – max. 32
- **Stripesetvolume**: Wie RAID 0
    - Bestandteile auf Festplatten aufgeteilt
    - Beschleunigung von Lese- und Schreibvorgängen
    - Keine Redundanz
- **Gespiegeltes Volume**: Wie RAID 1
    - Daten auf Festplatten dupliziert
    - Fehlertoleranz
    - Beschleunigung von Lesevorgängen

Dateisysteme

Aufgaben

- Physische Belegung von Speichereinheiten
- Zuordnung von Speichereinheiten zu logischen Dateien
- Benennung der logischen Dateien
- Zugriffsberechtigung regeln
- Führen von Dateiattributen (schreibgeschützt, versteckt…)
- Verwalten von Metadaten (Größe, letzter Zugriff)
- Bereitstellen standardisierter Zugriffsschnittstellen (open, read, write…)

Arten der Speicherung

Kontinuierliche Speicherung

- Daten einer Datei werden aneinanderhängend in den Speicher geschrieben
- Aufteilung in Blocks
- Probleme
    - Freien Speicherplatz finden
    - Fragmentierung
    - Erweiterung schwierig
    - Größe von Dateien ggf. nicht im Voraus bekannt

Verkettete Speicherung

- Dateien werden in Form einer verketten Liste gespeichert
- Start jeder Datei wird in File Allocation Table gespeichert
- Probleme
    - Fragmentierung
    - Schlecht für random accesses
    - Fehleranfällig

Indizierte Speicherung

- Adressen der Speicherblöcke werden in einer Indextabelle gespeichert
- Mehrere Stufen der Indizierung möglich
- Vorteile
    - Keine externe Fragmentierung
    - Random access sehr schnell
- Nachteil
    - Speicher-Overhead für die zusätzlichen Indextabellen

Baumsequentielle Speicherung

- Adressen werden in einer Baumstruktur gespeichert
- Nur unterste „Blätter“ enthalten Daten
- Vorteil
    - Schneller Zugriff auf Dateien

Beispiel NTFS

- Jede Datei hat einen Eintrag im Master File Table (MFT)
- Kleine Dateien sind direkt im MFT gespeichert
- Bei größeren Dateien steht die Adresse der Daten im MFT
- Bei Verzeichnissen wird weiter verzweigt

Unter Windows 10

- Mögliche Dateisysteme
    - NTFS (Standard)
    - FAT
    - FAT32
    - ReFS

Access Control Lists (ACLs) (NTFS)

- Zugriffsrechte können verwaltet warden
- Zugriffsrechte warden in Zugriffslisten (ACLs) gespeichert
- **ACL**: geordnete Liste von Zugriffseinträgen (Access Control Entries, ACEs)
- **ACE**: Access Control Entry
    - SID (Security Identifier): identifiziert User oder Gruppe
    - Spezifiziert Zugriffsrechte
    - Ein Bit, das besagt, ob das Recht vererbt wird

Registry

- Zentrale Datenbank zur Speicherung von Informationen von System und Software
- Einträge für OS, Anwendungen, Komponenten und Treiber
- Neue Einträge bei
    - Installation
    - Systemeinstellungsänderungen
    - Programmeinstellungen
    - Konfig-Änderungen
    - Manuelles erstellen
- Editieren über reg (CLI) oder regedit.exe (GUI)

Aufbau

- Hauptschlüssel & Views
    - **HKEY_LOCAL_MACHINE (Hauptschlüssel)**
    - **HKEY_USERS (Hauptschlüssel)**
    - HKEY_CLASSES_ROOT (View)
    - HKEY_CURRENT_USER (View)
    - HKEY_CURRENT_CONFIG (View)
- Unterschlüssel
    - z.B.: \SOFTWARE\7-Zip
- Wert: Eintrag unter Unterschlüssel
    - z.B.: \SOFTWARE\7-Zip\Path

Datentypen

- **REG_BINARY**: binäre Darstellung
- **REG_DWORD**: 8 Hex-Stellen
- **REG_QWORD**: 16 Hex-Stellen
- **REG_SZ**: Zeichenkette (String)
- **REG_Expand_SZ**: Zeichenkette mit Systemvariablen
- **REG_MULTI_SZ**: Array aus Zeichenketten

Netzwerkverwaltung

DNS: Domain Name System

- „Adressbuch des Internets“
- IP-Adressen schwer zu merken
  ➔ Domain-Namen wurden entwickelt
- Außerdem leichter wartbar, da beim benutzen eines Domain-Namen dem Nutzer nicht auffällt, wenn sich die IP-Adresse hinter dem Namen ändert
- **FQDN**: Fully Qualified Domain Name
- **NSLOOKUP**: Dienstprogramm zur “manuellen” Abfrage von Domain-Namen, z.B. für Debug

Schritte

1. Nutzer gibt Domain-Namen ein
2. Client sendet entsprechende DNS-Abfrage an DNS-Server
3. DNS-Server gleicht FQDN mit IP-Adresse ab
4. DNS-Server antwortet mit IP-Adresse des FQDN
5. Client verwendet die IP-Adresse für die tatsächliche Kommunikation mit dem Server

DHCP: Dynamic Host Configuration Protocol

- Automatisierte Zuweisung von Netzwerkeinstellungen wie IP-Adresse, Subnetzmaske, Gateway und DNS-Server
- Gegenstück ist die statische Adressierung
- DHCP-Netzwerkgeräte fordern beim Verbinden zum Netzwerk DHCP-Daten an
- Die DHCP-Daten haben eine definierte Gültigkeitsdauer (Lease-Dauer)
    - Nach Ablauf werden die Daten neu angefordert

Schritte

1. **Discover** (Broadcast): Client sendet DHCP-Discover beim booten bzw. beim herstellen einer Verbindung in einem Netzwerk
2. **Offer**: Ein DHCP-Server, der den Discover-Broadcast erhalten hat antwortet mit einem DHCP-Offer, in dem die Netzwerkdaten über eine bestimmte Lease-Dauer enthalten sind
3. **Request**: Da ggf. mehrere DHCP-Server auf den Discover ein Offer senden muss der Client ein Offer wählen und es mit einem entsprechenden Request bestätigen
4. **Ack**
    a. Wenn die angebotene Adresse aus dem Offer am Server noch verfügbar ist antwortet dieser mit einer entsprechenden Bestätigung
    b. Ist die angebotene Adresse nicht mehr verfügbar antwortet der Server mit einer negativen Bestätigung (**NAK**). Das DHCP-Verfahren beginnt am Client mit einem **Discover** von vorne.

CLI-Befehle

Befehl	Effekt
ipconfig	Zeigt alle Netzwerkadapter an
ipconfig /all	Ausführlicher Informationen zu den Netzwerkadaptern
ipconfig /release	Entfernen einer über DHCP bezogenen Adresse ohne Anforderung einer neuen
ipconfig /renew	Erneuern der über DHCP bezogenen IP-Adresse
ipconfig /registerdns	Erneuert die Registrierung des Clients am DNS-Server
ipconfig /displaydns	Zeigt den lokalen DNS-Cache an
ipconfig /flushdns	Löscht den lokalen DNS-Cache
hostname	Zeigt den Namen des Computers an
ping <DNS-Name>	Zeigt die IP-Adresse und Erreichbarkeit von <DNS-Name> an
pathping <IP-Adresse>	Zeigt die Erreichbarkeit und den Pfad zu <IP-Adresse> an
tracert <IP-Adresse>	Zeigt den Pfad zu <IP-Adresse> an
netstat	Zeigt aktuelle Rechnerverbindungen (TCP/UDP) an

Datensicherung & Systembackup

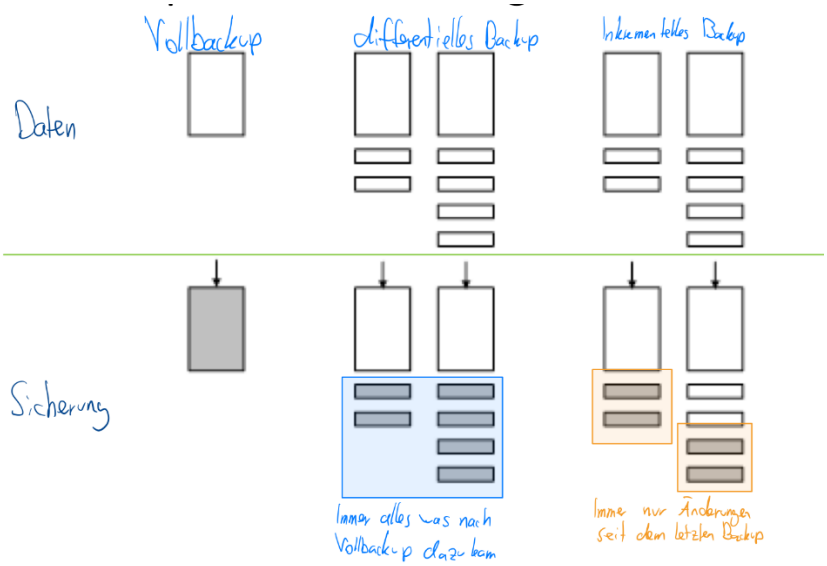
- **Gründe**: Virusbefall, fehlerhafter Systemzustand, Hardwareausfall
- **Kosten**: Hardware, Software, Personal
- Kriterien für Art der Sicherung
    - Häufigkeit der Sicherung
    - Häufigkeit der Wiederherstellung
    - Größe der Datenmenge
    - Dauer der Sicherung
    - Dauer der Wiederherstellung

Systemsicherung

- **Windows**: Wiederherstellungspunkte
    - Werden automatisch erstellt
    - Deinstalliert bei Wiederherstellung ggf. auch Programme

Userdatensicherung

Arten



Vollsicherung

- Alle Daten werden gesichert
- Einfache Wiederherstellung
- Große Datenmenge
- Lange Backupdauer

Differentielle Sicherung

- Alle Daten seit der letzten Vollsicherung werden gesichert
- Geringe Datenmenge
- Vollsicherung zur Wiederherstellung nötig
    - Aufwändige Wiederherstellung

Inkrementelle Sicherung

- Alle Daten seit der letzten inkrementellen Sicherung werden gesichert
- Noch geringere Datenmenge als bei differentieller Sicherung
- Alle Inkremente notwendig für Wiederherstellung
    - Noch aufwändigere Wiederherstellung

Verschlüsselung

- Benutzt Schlüssel um Nachrichten unleserlich zu machen
- Ohne Schlüssel kann die Nachricht nicht gelesen werden
- Rainbow-Table: Tabelle mit Hashwerten zu vorgegebenen Passwörtern

Arten

Symmetrische Verschlüsselung

- Selber Schlüssel beim ver- und entschlüsseln
- Beispiel: Caesar / Monoalphabetische Substitution
    - Buchstaben/Bytes werden durch einen anderen ersetzt
    - Leicht zu knacken durch Muster und Statistik
- Schneller als asymmetrische Verschlüsselung
- Beispiele: AES & DES
- **Schlüsselaustauschproblem**: beide Parteien benötigen den gleichen Schlüssel für ver- und entschlüsseln -> Übertragung muss auf sicherem Weg erfolgen
    - **Lösung**: Asymmetrische Verschlüsselung zum Austausch des Schlüssels

Asymmetrische Verschlüsselung

- Öffentlicher Schlüssel zum verschlüsseln
- Privater Schlüssel zum entschlüsseln
- Langsamer als symmetrische Verschlüsselung
- Sicherer Schlüsselaustausch
- Beispiele: RSA & DSA

Hybride Verschlüsselung

- Nutzt symmetrische und asymmetrische Verschlüsselung
- Effizienz: Symmetrische Verschlüsselung für Datenübertragung (schnell)
- Sicherheit: Asymmetrische Verschlüsselung für sicheren Schlüsselaustausch
- Ablauf
    - Daten werden mit symmetrischem Schlüssel verschlüsselt
    - Symmetrischer Schlüssel wird asymmetrisch verschlüsselt
- Beispiele: HTTPS & verschlüsselte Mails

Methoden der Verschlüsselung

- **Permutation am Eingang**: Durcheinanderwürfeln der Daten (Keine Statistik möglich)
- Veränderung des Schlüssels während des Verschlüsselungsvorgangs
    - Wenn eine Nachricht geknackt wird können nicht automatisch andere Nachrichten geknackt werden
- **Sicherheit der Verschlüsselung – Schlüssellänge**: Anzahl der möglichen Schlüssel
    - z.B.: 128 Bit Schlüssel -> 2^{128} Schlüssel möglich

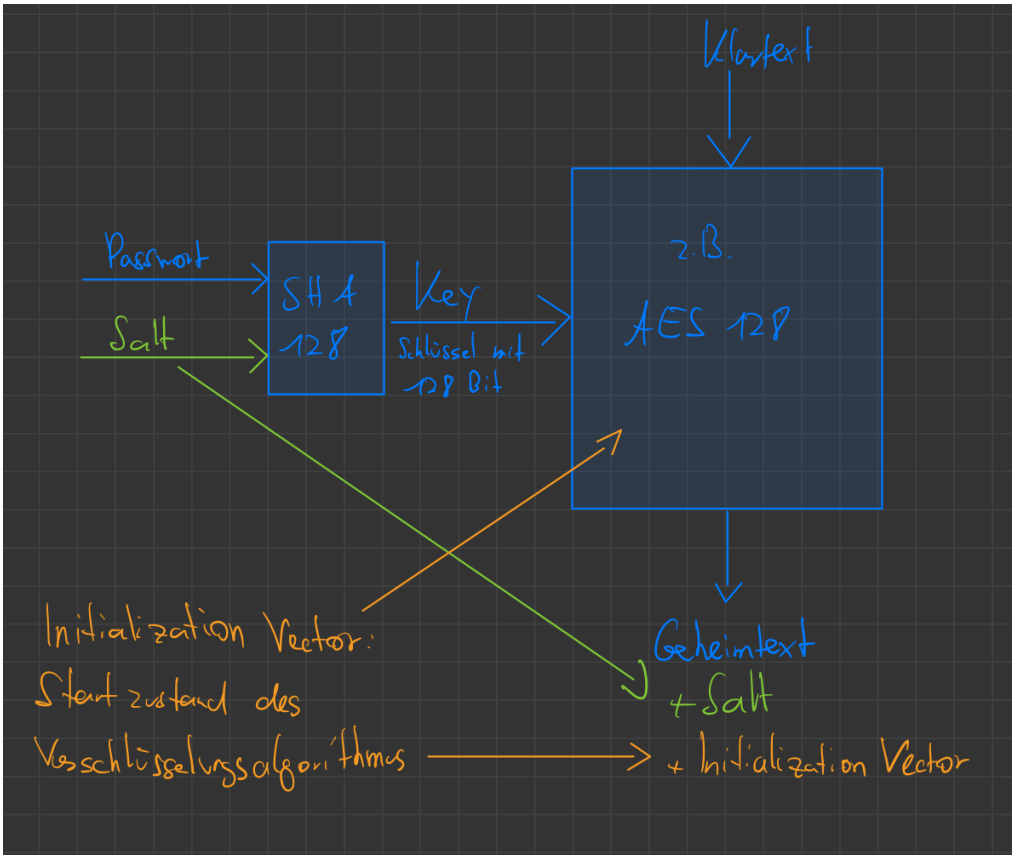
Schlüsselmöglichkeiten

- **Benutzerkennwort**
  - Probleme
    - Standardkennwörter
    - Kennwort ist hinterlegt
    - Kennwort wird vergessen
    - Länge ist begrenzt
- **Trusted Platform Module (TPM):** Chip auf Mainboard, der einen Schlüssel enthält
  - Verschlüsselung für Hardwarekonfiguration
- **Smartcard**
  - User identifiziert sich mit Smartcard
  - Smartcard stellt Schlüssel zur Verfügung
  - Verschlüsselung für einen User

Bitlocker

- **Festplattenverschlüsselung**: Komplettes Laufwerk wird verschlüsselt
- **Aktivierung**: Kontext-Menü am Laufwerk -> „Bitlocker aktivieren“
- **Schlüsselmöglichkeiten**: Kennwort, TPM, SmartCard
- Wiederherstellungsschlüssel wird bei Aktivierung generiert: Verwendung wenn regulärer Schlüssel nicht mehr verfügbar/defekt
- Eingabe des Schlüssels
  - Systempartition: Bei Start
  - Keine Systempartition: Bei Zugriff
- Verschlüsselung mit AES 128/256 Bit

AES: Advanced Encryption Standard



Zum Entschlüsseln notwendig:

- Passwort
- Salt
- Geheimtext
- Initialization Vector

EFS: Encrypting File System

- Dateiverschlüsselungssystem unter NTFS
- Kann auch nur einzelne Dateien verschlüsseln
- EFS verwendet sowohl symmetrische als auch asymmetrische Verschlüsselung
- Nach Aktivierung wird ein File Encryption Key (FEK) generiert
- Datei wird mittels DES/AES + FEK symmetrisch verschlüsselt
- FEK wird mittels RSA + Userkennwort asymmetrisch verschlüsselt