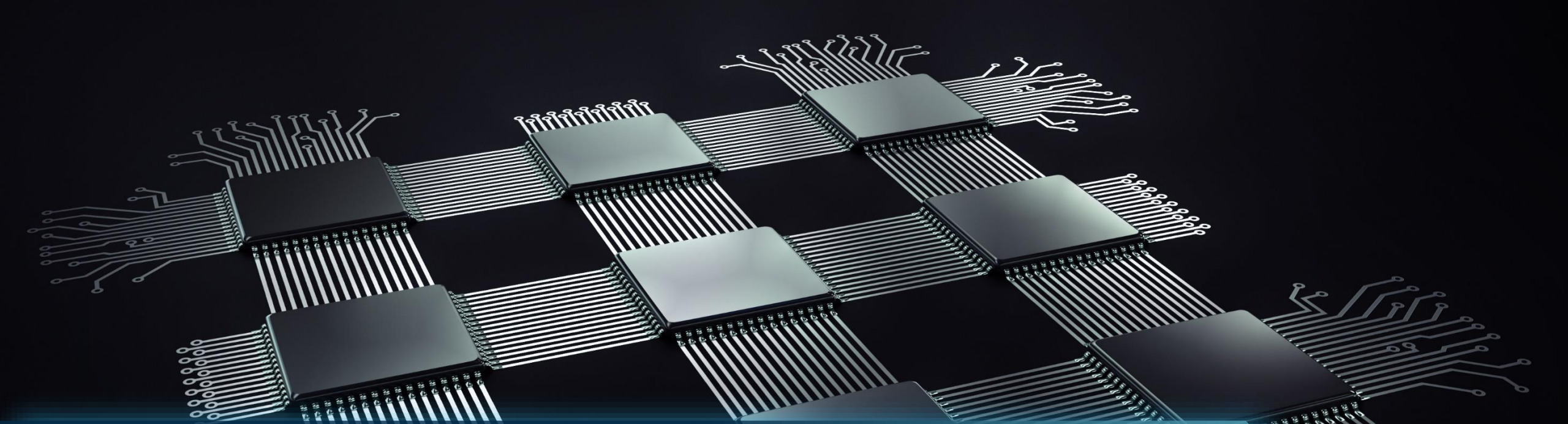
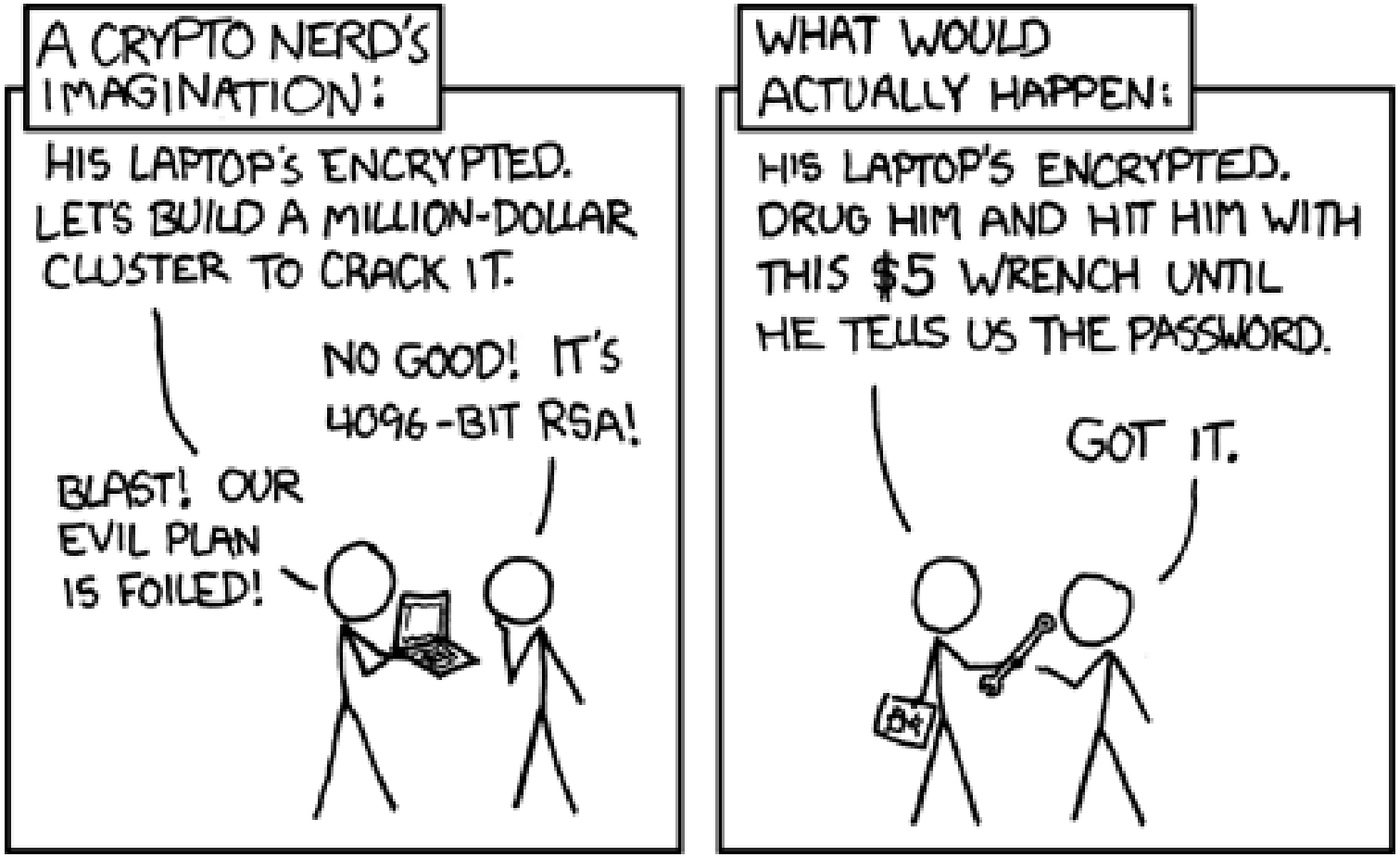


Operation System Security

04 – Festplatten Verschlüsselung

SECURNITE



OSSEC 05 – Festplatten Verschlüsselung

Wiederholung: Speicher

Exkurs: ATA Sicherheitsfunktionen

Festplatten Verschlüsselung

Methoden zur Schlüsselbereitstellung

Exkurs: Externe Festplatten

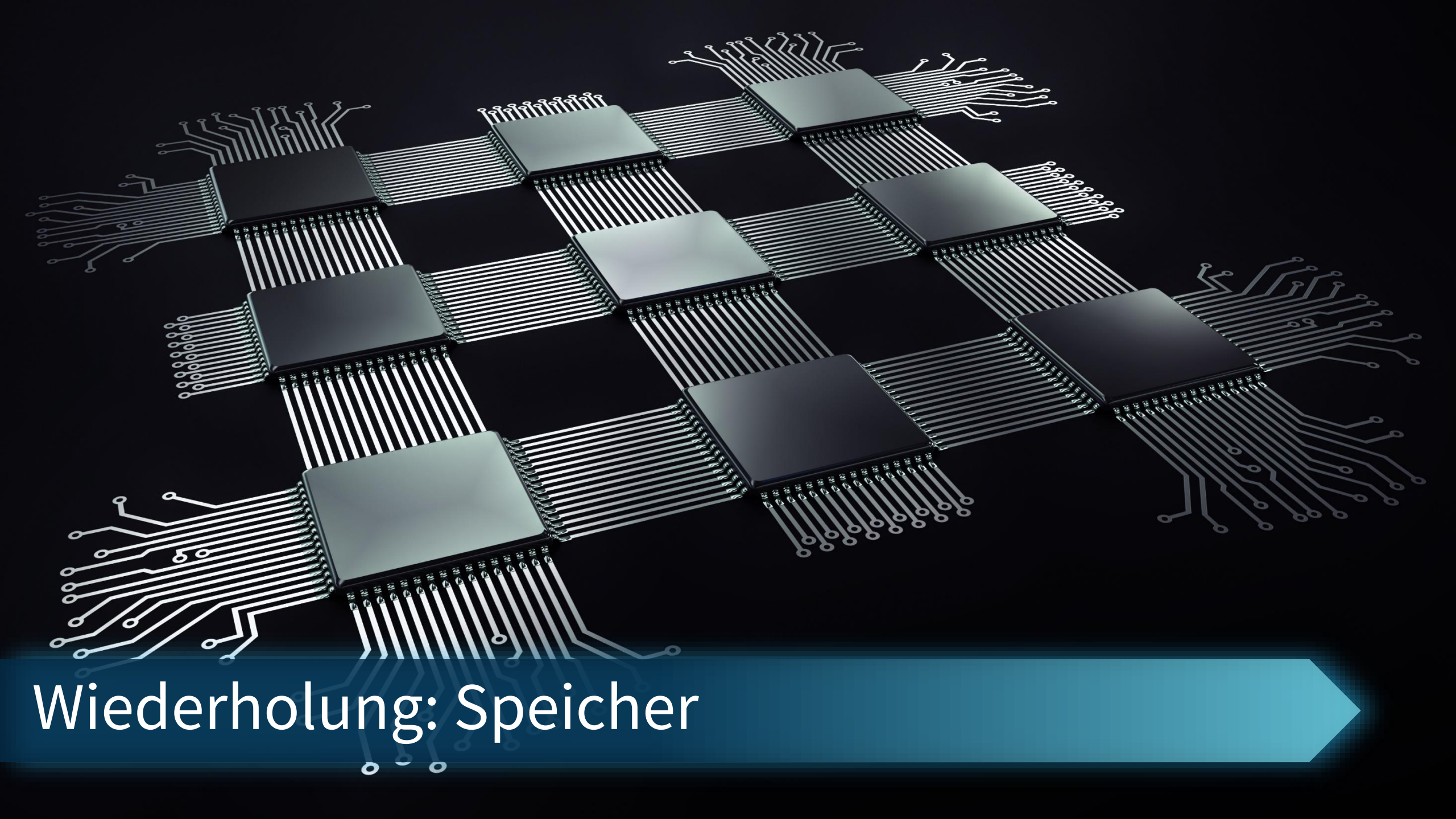
Angriffe auf verschlüsselte Festplatten

Exkurs: Mobile Device Management

Vor und Nachteile von Festplatten Verschlüsselung

Betriebssystemlösungen zur Festplatten Verschlüsselung

SECURNITE



Wiederholung: Speicher

Repetition: Speicher

Sekundärer Speicher

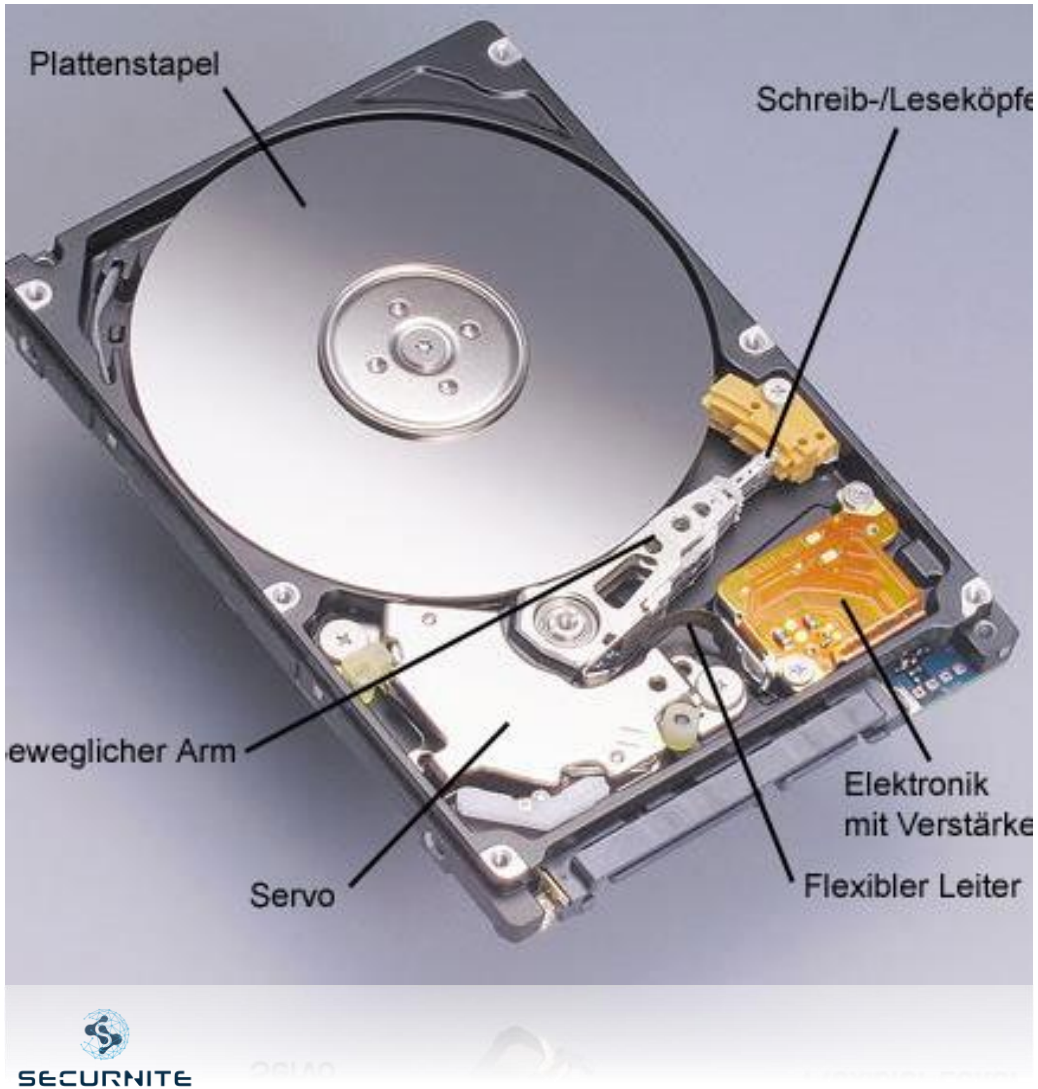
- Speichert Informationen **permanent**
- Kostengünstig
- Langsamere **Zugriffszeiten**
- Beispiele: HDD / SDD, USB Sticks

Tertiärer Speicher

- Speichert Informationen **permanent** und über **sehr lange Zeit**
- Sehr kostengünstig
- Sehr langsame **Zugriffszeiten**
- Meist für **Backup** und **Transfer**
- Beispiel: Tapes

SECURNITE

Repetition: Festplatten



- **Magnetisches** Speichermedium
- Daten werden auf Oberfläche **rotierender Scheiben** geschrieben
- **Direktadressierbares** Speichermedium
  - kein linearer Durchlauf erforderlich, um zu einer bestimmten Speicherstelle zu gelangen
  - Unterschied zu **Tertiärem Speicher**

Repetition: Festplatten

- **Schreiben:** hartmagnetische Beschichtung der Scheibenoberfläche wird berührungslos **magnetisiert**
- **Speichern**: verbleibende Magnetisierung (Remanenz)
- **Lesen:** berührungsloses Abtasten der Magnetisierung der Plattenoberfläche

SECURNITE

Repetition: Festplatten

- **Datenhaltung**
  - **CKD** (count key data): unterschiedlich lange Datenblöcke.
  - **FBA** (fix block architecture): gleich lange Datenblöcke (512 oder 4096 Byte gross)

- Es werden immer **ganze Blöcke** gelesen / geschrieben

SECURNITE

Repetition: Festplatten

- Gängige Schnittstelle: **SATA**
  - V1 mit 1.2 Gbit lesen / schreiben
  - V2 mit 2.4 Gbit lesen / schreiben

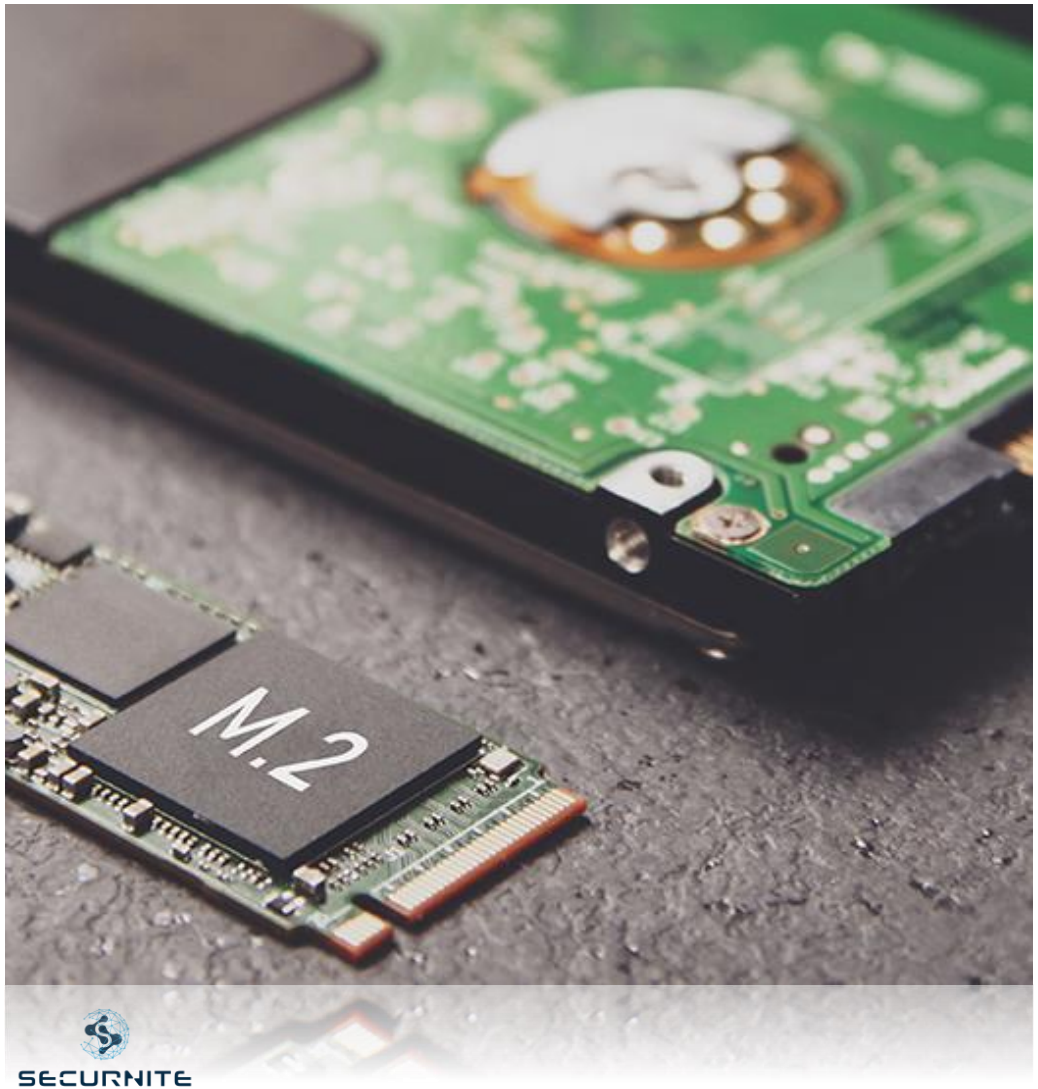
Repetition: SSD

- viel höhere Geschwindigkeiten als herkömmliche Festplatten

- Gängige Schnittstelle: **SATA** (**S**eriell **A**dvanced **T**echnology **A**ttachment)
  - V3 mit 4.8 Gbit lesen / schreiben
  - V3.2 mit 6.0 Gbit lesen /schreiben

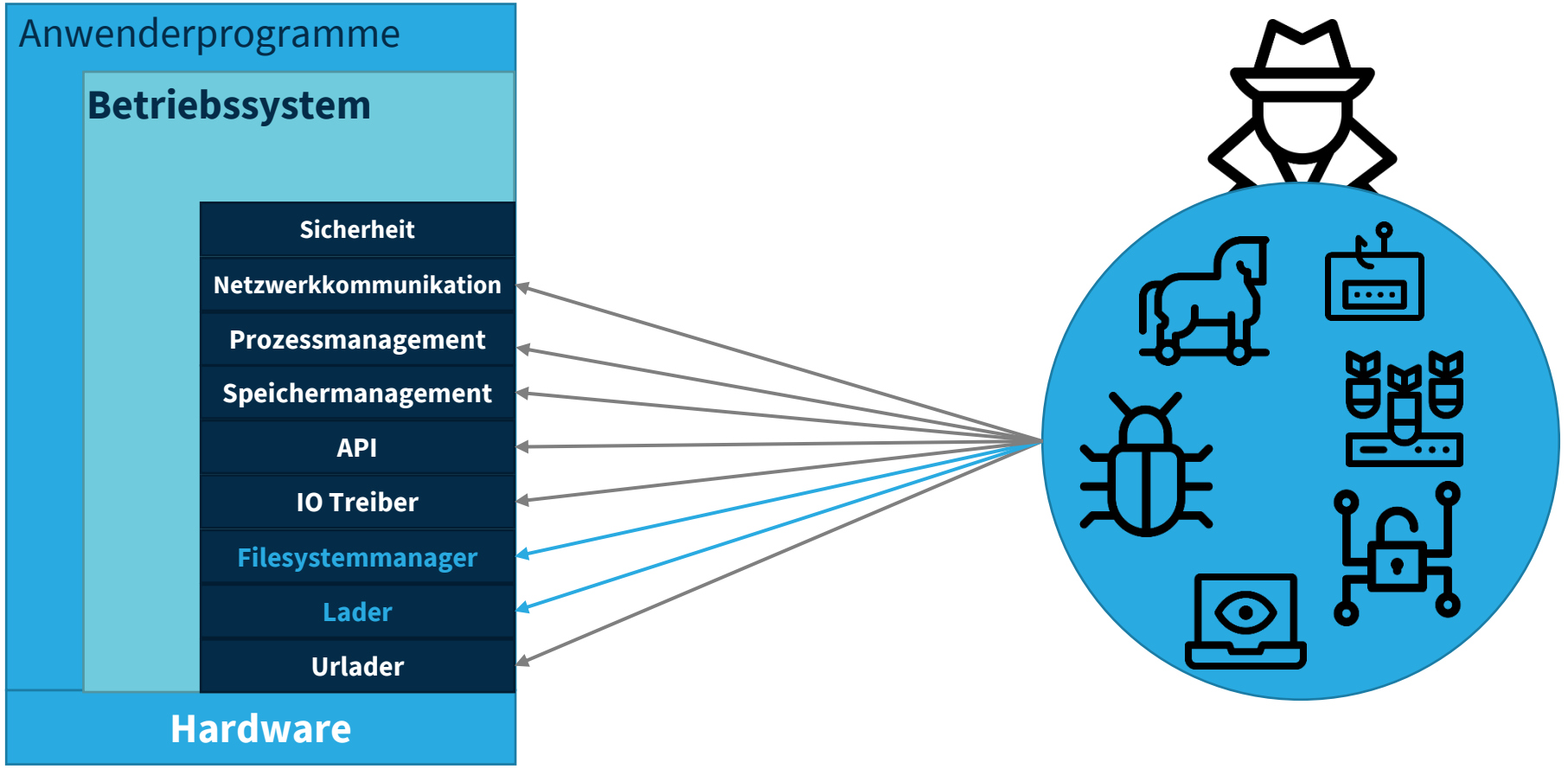
- **Engpass**: in der Praxis maximal 550 MByte pro Sekunde lesen und schreiben

Repetition: SSD



- **Massnahme**: SSD-Speicher über PCI-Express
  - Steckkartenformat: Next Generation Form Factor (NGFF) / M.2)
  - Bis zu 32 GBit/s lesen / schreiben
  - deutlich teurer als SATA-SSDs gleicher Kapazität
  - PCIe-Steckplätze nur in stationären Rechnern vorhanden

Angriffsvektoren auf das Filesystem



Exkurs: ATA Sicherheitsfunktionen

Exkurs: ATA Sicherheitsfunktionen

- **Security Feature Set** schützt die auf einer Festplatte vor unbefugtem Zugriff
- Bestandteil der ATA-Spezifikation
- Zwei 32 Bit lange Passwörter: **„User Passwort“** und **„Master Passwort“**
- Aktiviert durch ATA-Kommando *Security Set Password*
- Kommando *Security Unlock* + Passwort **entsperrt** die Platte vorübergehend
- Nach dem nächsten **Cold Boot** ist die Platte automatisch wieder verriegelt
- Kommando *Security Disable* + Passwort schaltet die Sperre dauerhaft ab

Die Daten auf der Festplatte sind durch diese Sicherheitsfunktion nicht verschlüsselt.

SECURNITE

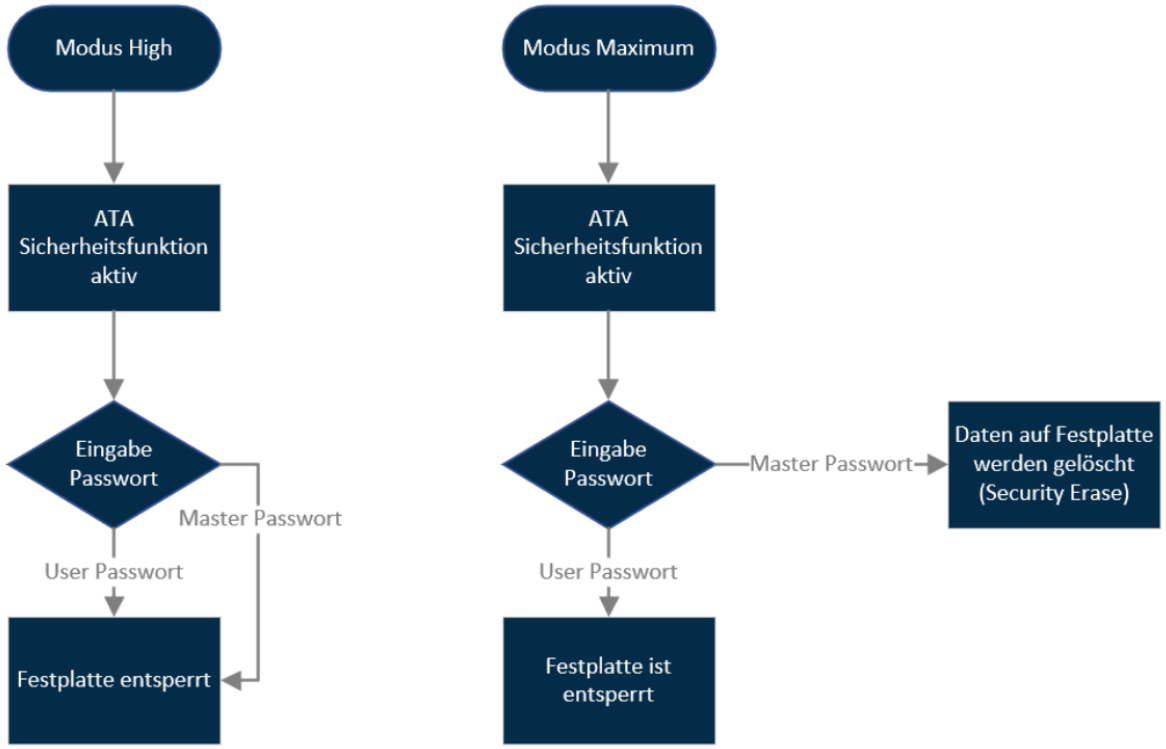
Exkurs: ATA Sicherheitsfunktionen

- Zwei **Sicherheitsstufen** „High“ und „Maximum“
  - „**High**“: Entsperren / Abschalten mit **User-** und **Master-Passwort** möglich
  - „**Maximum**“: Entsperren nur mit **User-Passwort**, Master-Passwort entsperrt aber führt zum **Verlust** aller Daten (Security erase)
- Beim **BIOS/UEFI Setup** wird Passwort initial vergeben
- BIOS/ UEFI fragt Passwort bei jedem Einschalten ab
- Bei Erfolg werden die **Sicherheitseinstellungen** (z.B. Passwort setzen / entfernen) zum Schutz **eingefroren** (bis zum nächsten Start), damit das Passwort nicht durch z.B. Malware gesetzt/ geändert wird

Die BIOS / UEFI Hersteller müssen dieses Einfrieren implementieren. Viele Hersteller haben das zur Einführung des Features versäumt, was es **Angreifern** ermöglicht, durch Malware **unbemerkt** ein **Festplattenpasswort** zu **aktivieren**!

SECURNITE

Exkurs: ATA Sicherheitsfunktionen



- Das Master Passwort wird im „**Maximum**“ Modus verwendet, falls der Benutzer sein Passwort **vergessen** hat

Dadurch werden alle Daten auf der Festplatte (Security Erase) **gelöscht**

Festplatten Verschlüsselung

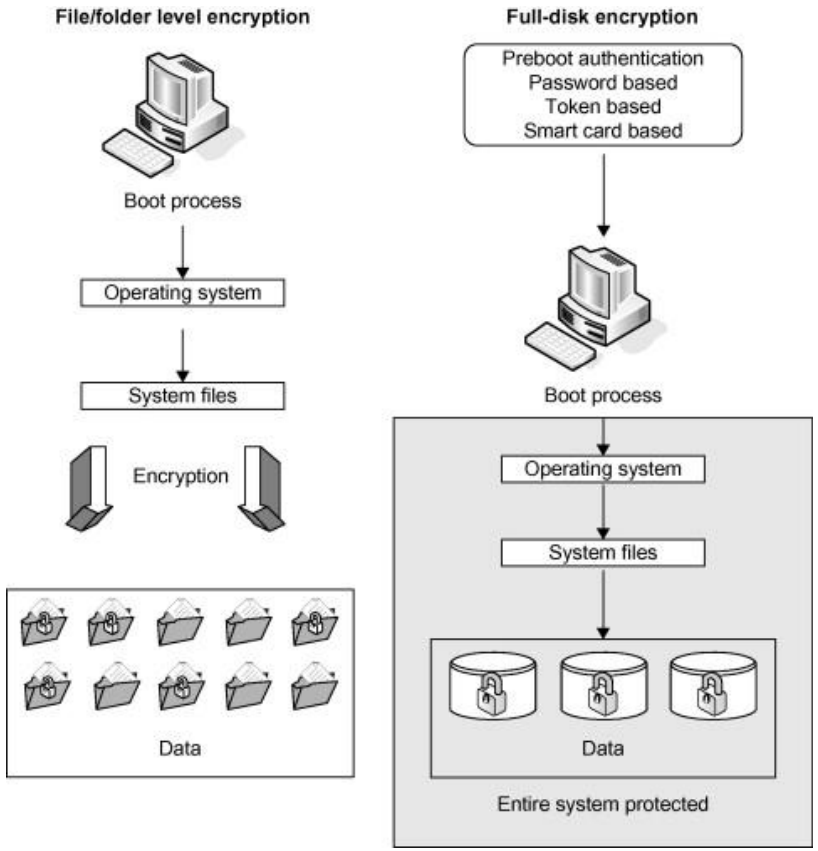
Zielsetzung der Festplatten Verschlüsselung

- **Full Disk Encryption** (FDE) schützt die auf einer Festplatte oder einer Festplatten-partition gespeicherten Informationen vor unbefugtem Zugriff
- Auch Daten des **Betriebssystems** sind verschlüsselt
- Auslesen der Festplatten mithilfe eines **externen** Geräts ist ohne Schlüssel nicht möglich
- Für den Zugriff auf die Daten oder das Booten des Rechners ist **Authentifizierung** mit Kennung oder spezieller Hardware (z.B. TPM) nötig
- Ver- und Entschlüsseln der Daten automatisch beim **Lesen** und **Schreiben**

Festplattenverschlüsselung bietet keinen Schutz für gebootete Rechner, die mit einem Netzwerk verbunden sind!

SECURNITE

Full disk encryption

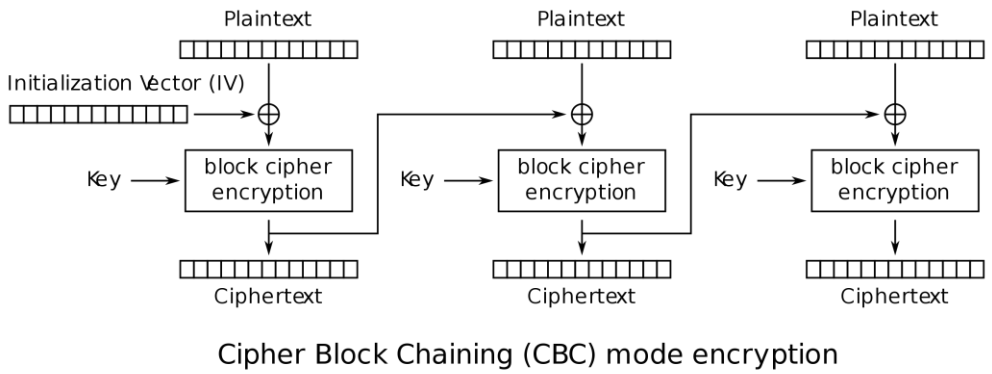


Für alle gängigen **Betriebssysteme** existieren Lösungen

- direkt von den **Herstellern** des Betriebssystems integrierte Lösungen
- Anwendungen **externer Anbieter**

Mechanismus: idR. **AES** mit 256 Bit Schlüssel im CBC Modus → schnell, hohes Mass an Sicherheit, wird durch gängige Hardware unterstützt

CBC Mode



Cipher Block Chaining (CBC) mode encryption

Quelle: https://de.wikipedia.org/wiki/Cipher_Block_Chaining_Mode

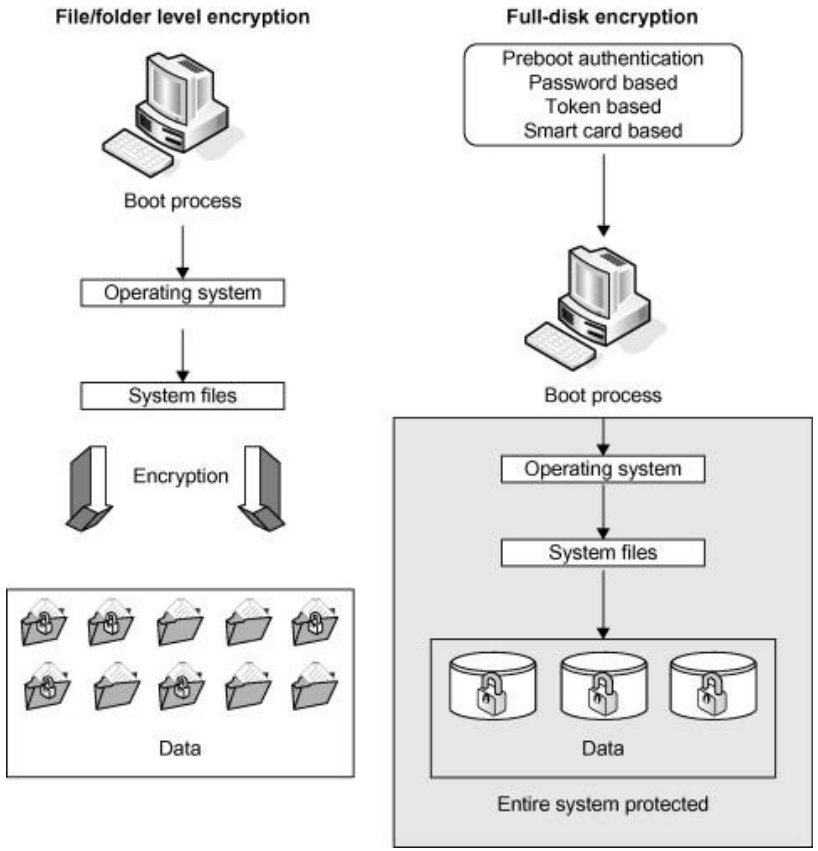
Klartextblock wird mit vorherigen Chiffretextblock **XOR-verknüpft**

Identische Klartextblöcke werden zu **verschiedenen Chiffretextblöcken** verschlüsselt (wenn Vorläuferblock unterschiedlich ist)

Um bei zwei **gleichen** ersten Klartextblöcken unterschiedliche Chiffretextblöcke zu erhalten, wird ein **Initialisierungsvektor** (IV) eingesetzt

IV ist Block mit **Zufallsdaten**, der das fehlende Ergebnis des nicht existenten vorhergehenden ("nullten") Chiffretextblocks kompensiert

Full disk encryption

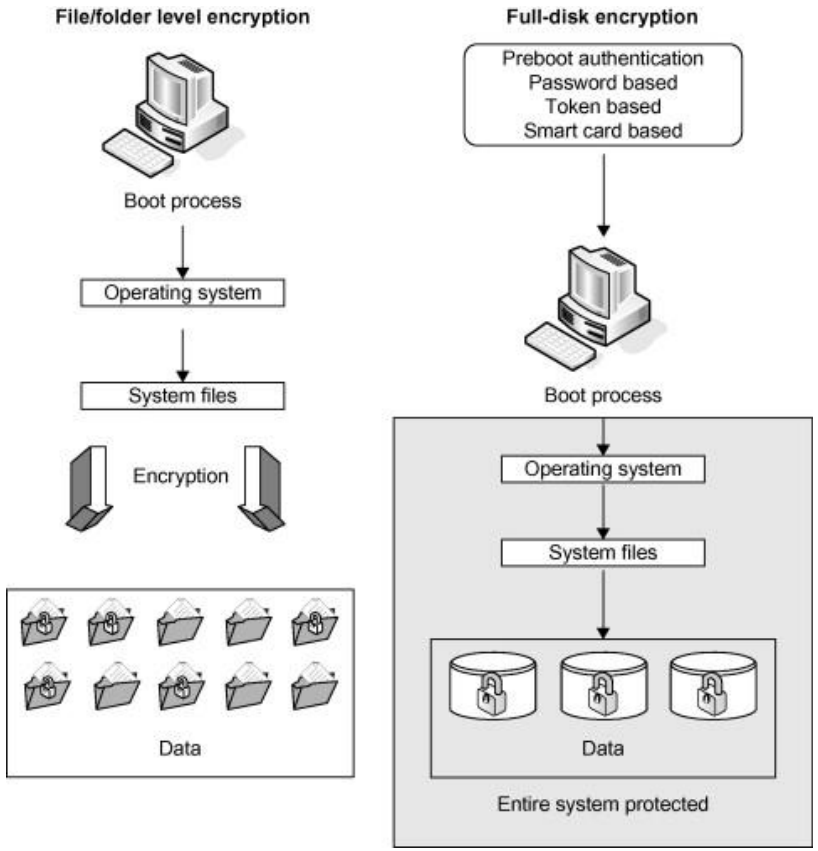


Beim **Lesen** entschlüsselt Software die Daten

Auf der **Festplatte** bleiben Daten **verschlüsselt**

Für die Nutzer und Anwendungen ist die Festplattenverschlüsselung **transparent**

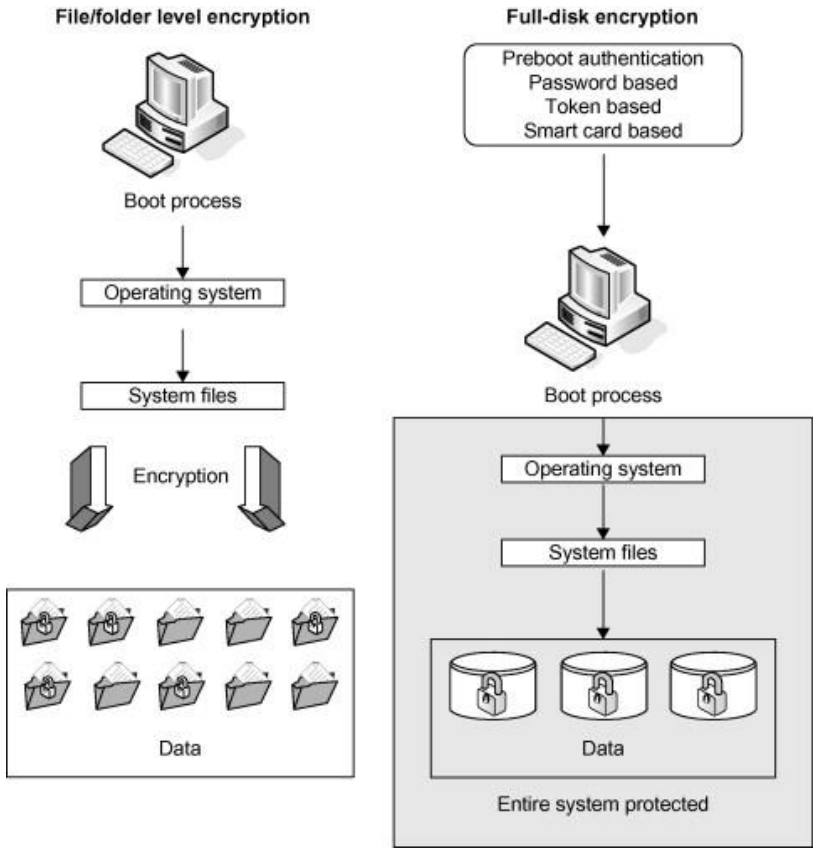
Full disk encryption



Sowohl **Inhalt** der Dateien als auch **Dateinamen** sind verschlüsselt

Durch die Verschlüsselung der Dateinamen (z.B. im Fall von Diebstahl) sind **keine Rückschlüsse** auf die Inhalte der Dateien möglich

Full disk encryption



Verschlüsselung für **komplette Festplatte** oder eine **Partition** aktiv

Zum **Booten**, muss das Betriebssystem entschlüsselt werden:

- **Authentifizierung** im Pre-Boot-Prozess
- **Passwort-** oder **Hardware-basiert**
- Schlüssel freigegeben → Daten beim **Startprozess** entschlüsselt und **lesbar**

Methoden zur Schlüsselbereitstellung

Hardwarebasierte FDE

Bereitstellen des Schlüssels

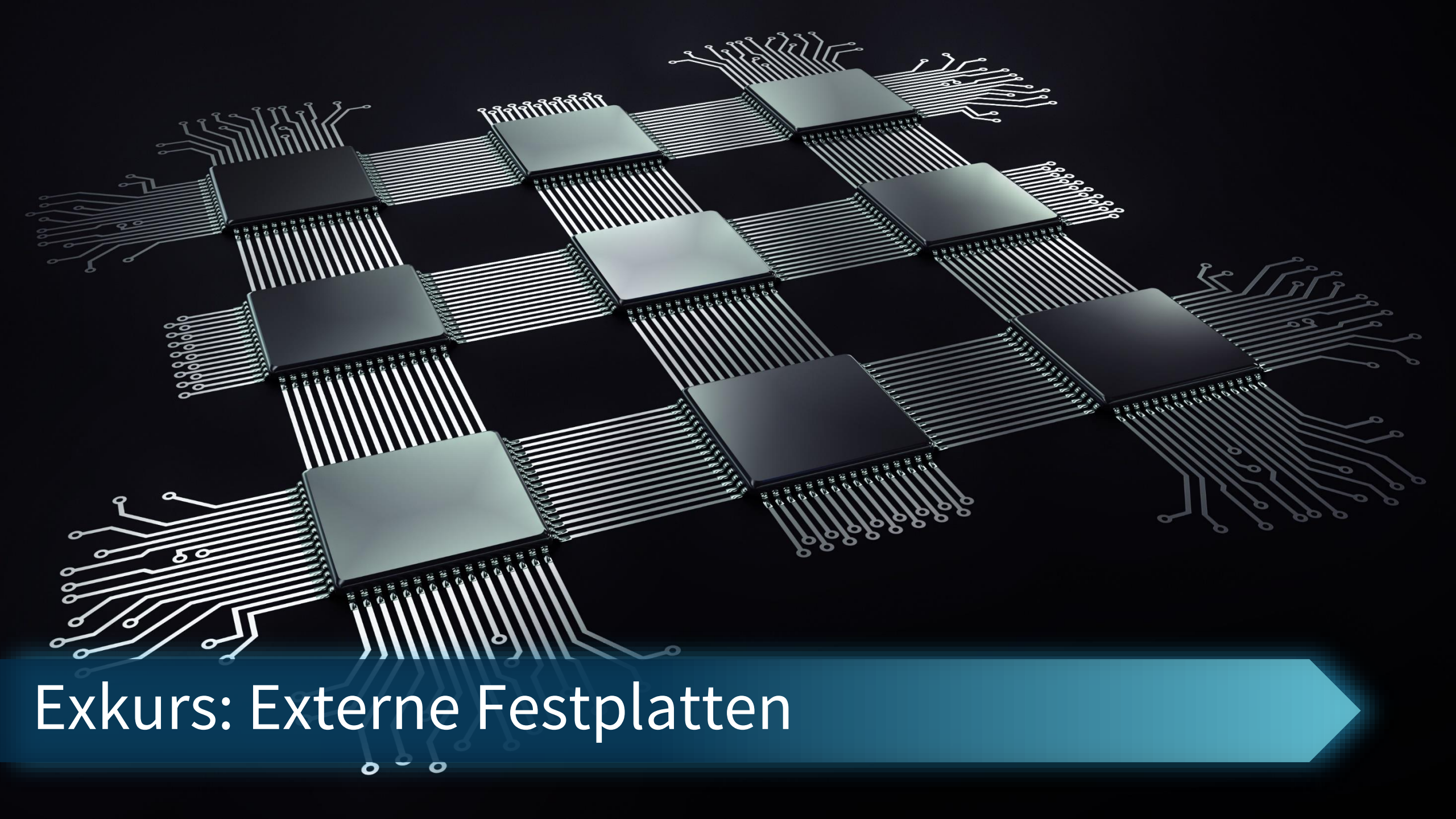
Verschiedene Methoden ermöglichen **sichere Speicherung** der Schlüssel und **Verifizieren** der **Integrität** des MBR

- Eingabe eines vorab eingestellten **Passworts**
- Verwenden eines **TPM Chips**
- Im Motherboard integrierter **Chip** nach Trusted Computing Spezifikation

Hardware basierte FDE

Bereitstellen des Schlüssels

- **Externe** Speicher
  - USB Stick
  - Dongle, z.B für SmartCards
  - Auch serielle oder parallele Schnittstellen für alte Systeme verfügbar



Exkurs: Externe Festplatten

Enclosed Hard Disk FDE

Externe verschlüsselte Festplatten

können **vollständige Verschlüsselung** selbst bereitstellen

Vorteil: Zusätzlich Ausgereifte Sicherheitsfeatures

- Keypad
- Einbruchssichere Chassis
- Self-destruct bei brute force Angriffen

Enclosed Hard Disk FDE

Externe verschlüsselte Festplatten

Nachteil: Bei Beschädigung der Festplatte Daten oft unwiderruflich verloren, da sie ohne Erzeugen des Schlüssels nicht zu entschlüsseln sind

Gruppenübung: HDD

(15 Minuten)

Recherchieren Sie das Grundprinzip und die Funktionalität von HDDs.
Stellen Sie die Ergebnisse in einer Präsentation vor (max. 5 Minuten). Gehen Sie besonders auf folgende Aspekte ein:

- Welche Fehlfunktionen können bei HDD auftreten?
- Welche Auswirkungen haben Vibrationen auf HDD?

Betriebssystemlösungen zur Festplatten Verschlüsselung

Lösungen

Windows

- Seit Windows 2000
  - verschlüsseltes Dateisystem EFS
  - verschlüsselt auf Ebene einzelner **Nutzer**
  - **nicht** für Verschlüsselung des Betriebssystems an sich **geeignet**

- Seit Vista: **BitLocker**
  - Programm, das unabhängig von den Nutzern das Betriebssystem schützt

Lösungen

Windows - BitLocker

- Verwendet eigene **Systempartition** mit notwendigen Daten zum **Starten** des Computers und zum **Laden** der verschlüsselten Betriebssystemdaten
- Kann zur Verwendung einer **PIN** Eingabe, **externe Schlüsselbereitstellung** oder Schlüsselverwaltung mittels **TPM Chip** konfiguriert werden
- **AES** Verschlüsselung mit 128 oder 256 Bit (standard)

Lösungen

MacOS – FileVault 2

- Moderne MacOS Versionen verwenden FileVault2 zur **Verschlüsselung** des **Home** Verzeichnisses

- Speicherung in einem mit XTS-AES verschlüsseltem **sparse image** mit Schlüssel Länge von 256bit

Linux - Dateisystem basierte Verschlüsselung

- **eCryptFS**
  - Kryptographisches Dateisystem, welches die Verschlüsselungs-informationen im **Datei Header** speichert
  - Entschlüsselung durch **Linux Kernel Keyring**
  - Dateien können so einfach **zwischen Hosts ausgetauscht** werden
  - Heute nicht mehr Standard

Lösungen

Linux - Dateisystem basierte Verschlüsselung

- **EncFS**
  - Kryptographisches Dateisystem im **User Space**
  - benötigt **keine** speziellen **Berechtigungen**
  - Verwendet **FUSE** und **Linux Kernel Module** zur Bereitstellung des Dateisystem Interface
  - **Open Source**

Linux – Block Level Verschlüsselungen

- Anstelle des Dateisystems wird die **gesamte Festplatte** auf **Blockebene** verschlüsselt
- Ein auf Block Level Verschlüsselung aufgesetztes **Dateisystem** ist automatisch auch **verschlüsselt**
- Nicht nur **Dateiinhalt**, alle **Daten**, inklusive freiem **Speicher**, **Dateinamen** und **Ordnerstruktur** sind verschlüsselt

Linux – Block Level Verschlüsselungen

- **Loop AES**
  - Verschlüsselungs-Package für das Dateisystem für **komplette Partition** oder **virtuelles Laufwerk**
  - Verwendet **Loop Kernel Modul** und **AES** Verschlüsselung mit wahlweise 128, 196 oder 256 Bit Schlüssel

Linux – Block Level Verschlüsselungen

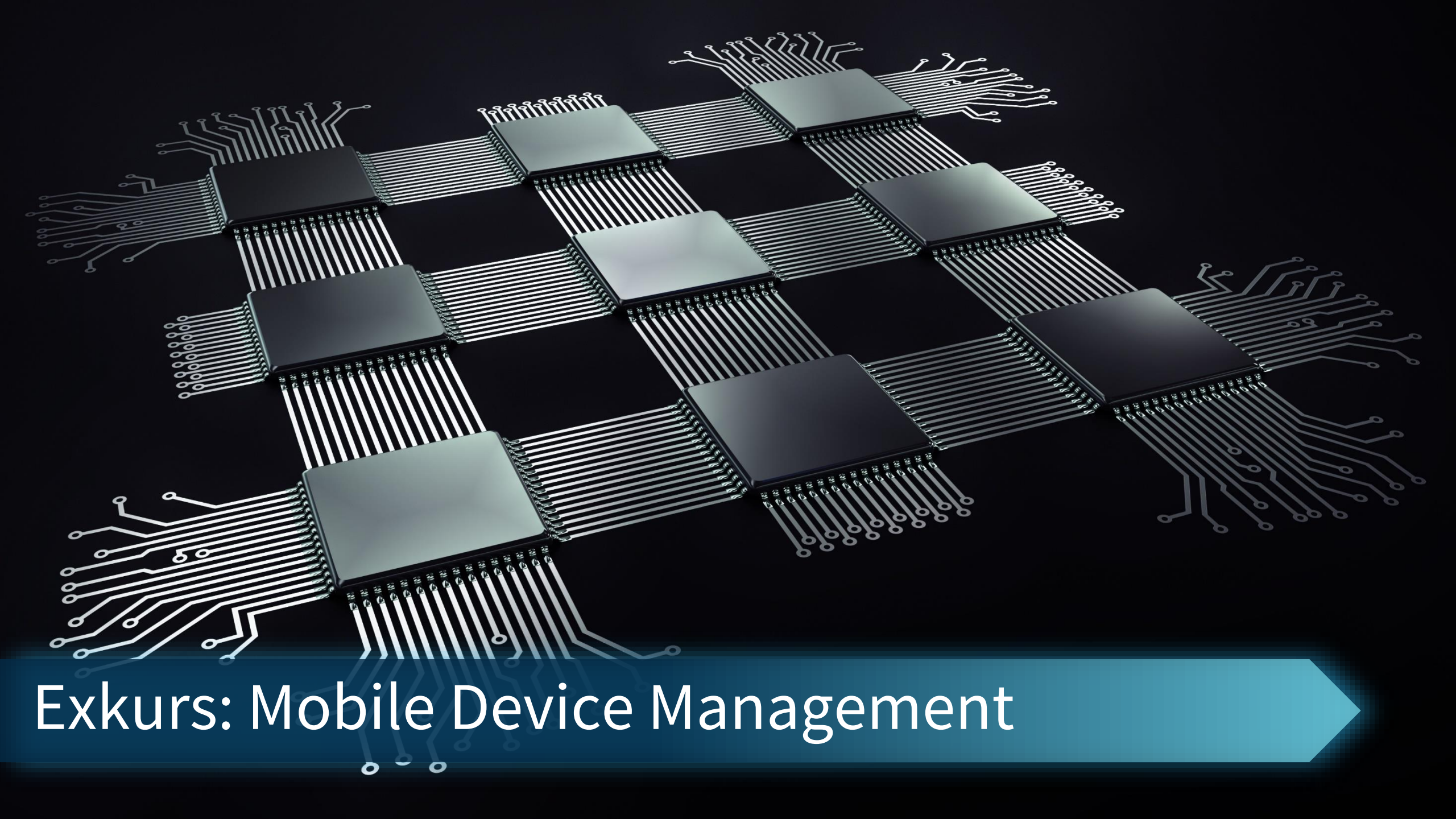
- **VeraCrypt**
  - Linux Version der freien Open Source Software VeraCrypt basierend auf **TrueCrypt** Source Code
  - Verschlüsselung des **gesamten Systems**, einzelnen **Partitionen** oder **Containern** möglich

Linux – Block Level Verschlüsselungen

- **DM Crypt mit LUKS**
  - DM Crypt ist Teil des Linux Device Mappers und verwendet die **Crypto API** des Kernels
  - Verschlüsselung der **gesamten Festplatte**, einzelner **Partitionen** oder des **LVM** möglich

Linux – Block Level Verschlüsselungen

- **Linux Unified Key Setup (LUKS) Erweiterung**
  - **Erweitert DMCrypt** verschlüsselte Daten um einen **Header** mit **Metadaten**, indem **Schlüsselinformationen** sowie Informationen zum **Verschlüsselungsalgorithmus** gespeichert werden
  - **Partitionen** und **Container** können so nach Passwort Abfrage einfach **eingebunden** werden



Exkurs: Mobile Device Management

Gruppenübung: Fernlöschung bei MDM

(20 Minuten)

- Diskutieren Sie wie Mobile Device Management Lösungen die Fernlöschung von Daten umsetzen
- Stellen Sie die Ergebnisse in einer Präsentation vor (max. 5 Minuten). Gehen Sie besonders auf folgende Aspekte ein:
  - **Warum** brauche ich Fernlöschung?
  - Was ist das **Besondere** an Fernlöschung?
  - Welche **Herausforderungen** habe ich bei Fernlöschung?

Angriffe auf verschlüsselte Festplatten

Schutz durch verschlüsselte Festplatten

Infizierung des Master Boot Records (MBR) durch ein Bootkit

- **TPM Chips** schützen auch vor Manipulation des Boot Environment
- Verifizieren der angeschlossenen Hardware über **Hashes** von System Variablen
- Ohne TPM Chips kann ein Angreifer ein eigenes **Bootkit** im MBR installieren und das Boot Verfahren anpassen

Angriffe auf verschlüsselte Festplatten

Hot Swapping bei Verschlüsselungschip auf Festplatte

- Sobald das System **gebootet** hat, sind alle Daten auf der Festplatte verfügbar, auch im System Ruhezustand
- Ein Angreifer kann die Festplatte von der Schnittstelle **trennen,** ohne die **Stromversorgung** zu unterbrechen
- Nach Einsetzen in ein **neues System** sind alle Daten auszulesen

Angriffe auf verschlüsselte Festplatten

Weitere Angriffe

- Bei **partieller Verschlüsslung**: Wiederherstellen des Passworts aus der **Auslagerungsdatei** der Festplatte

- **Keylogger**: Ausspähen des Schlüssels

- Auslesen des **Hauptspeichers** (vgl. OSSEC-02)
    - durch DMA
    - durch die Ausnutzung physikalischer Eigenschaften des DRAM

Angriffe auf verschlüsselte Festplatten

Weitere Angriffe

- **Wörterbuch-** oder **Brute-Force-Angriff**
- Ausnutzung von **Schwachstellen**
  - **Seitenkanalattacken** (z.B. bei TrueCrypt, Bitlocker): Messen der Zeiten, die für Ver- und Endschlüsselung von Daten benötigt wird ermöglicht Rückschlüsse auf den generierten Schlüssel
  - Lesen und Schreiben der **Keyfiles**
- **Social Engineering**

Vor- und Nachteile von Festplatten Verschlüsselung

Vor- und Nachteile

Nachteile

Performance des Systems wird ggf. beeinträchtigt

Massnahme: Hardware mit AES Unterstützung

Vorteile

- **Auslesen** ohne Schlüssel nicht möglich

- Verhindert:
  - **Ausbauen** der Festplatte und **Verbinden** mit externen Systemen
  - **Booten** eines gestohlenen Rechners per externen Medien (USB-Sticks)