# Wie funktioniert TPM / BitLocker

# Einführung

- Thema: Verschlüsselung mit TPM und BitLocker
- Überblick:
  - Was ist Verschlüsselung?
  - Das Trusted Platform Module (TPM)
  - BitLocker-Funktionsweise
  - Vorteile und Sicherheitsaspekte

https://www.youtube.com/watch?v=L1sz6cm47Os

# Grundlagen der Verschlüsselung

- Definition: Umwandlung von Daten in unlesbaren Code, der nur mit dem richtigen Schlüssel wieder lesbar wird
- Zweck: Schutz sensibler Daten vor unbefugtem Zugriff
- Arten der Verschlüsselung:
  - Symmetrische Verschlüsselung (gleicher Schlüssel)
  - Asymmetrische Verschlüsselung (öffentlicher/privater Schlüssel)
- Herausforderung: Sichere Speicherung und Verwaltung von Schlüsseln

# Was ist TPM (Trusted Platform Module)?

- Definition: Hardware-Sicherheitschip auf dem Motherboard
- Funktionen:
  - Sichere Speicherung von kryptografischen Schlüsseln
  - Hardware-basierte Schlüsselgenerierung
  - Integritätsmessung des Systems
- Versionen: TPM 1.2, TPM 2.0 (neuer Standard)
- Merkmale: Manipulationssicher, vom Betriebssystem isoliert

# BitLocker - Überblick

- Definition: Microsoft-Technologie zur Festplattenverschlüsselung
- Integriert in: Windows 10/11 Pro, Enterprise und Education
- Hauptzweck: Schutz vor Offline-Angriffen und Datendiebstahl
- Verschlüsselung: AES mit 128-Bit oder 256-Bit Schlüssellänge

# Zusammenspiel von BitLocker und TPM

- Funktionsweise:
  - TPM speichert den BitLocker-Schlüssel sicher
  - System-Integritätsprüfung bei jedem Start
  - Automatische Entsperrung bei normalem Systemzustand
- Vorteile:
  - Transparenz für Benutzer
  - Schlüssel bleibt vor Software-Angriffen geschützt
  - Erkennung von Boot-Sektor-Manipulationen

# Aktivierung von BitLocker

- Voraussetzungen:
  - Kompatibles Windows-System
  - TPM 1.2 oder 2.0
  - UEFI mit Secure Boot (empfohlen)
- Aktivierungsprozess:
  - Systemsteuerung oder PowerShell
  - Wahl der Authentifizierungsmethode
  - Erstellung eines Wiederherstellungsschlüssels

# Folie 7: BitLocker-Authentifizierungsmethoden

- TPM-only: Automatische Entsperrung (wenn System unverändert)
- TPM + PIN: Zusätzlicher Schutz durch Benutzer-PIN
- TPM + USB-Schlüssel: Physischer Schlüssel erforderlich
- TPM + PIN + USB-Schlüssel: Mehrstufige Authentifizierung
- Ohne TPM: Kennwort oder USB-Schlüssel (weniger sicher)

Sicherheitsaspekte

# Sicherheitsaspekte

- Schutz vor:
  - Offline-Angriffen auf die Festplatte
  - Cold Boot-Angriffen (teilweise)
  - Diebstahl von physischen Geräten
- Einschränkungen:
  - Kein Schutz gegen Schadsoftware im laufenden System
  - Mögliche Angriffe auf TPM (selten, aber möglich)
- Best Practices: Regelmäßige Updates, starke PINs

# Wiederherstellung und Management

- Wiederherstellungsoptionen:
  - Wiederherstellungsschlüssel (48-stellige Nummer)
  - Microsoft-Konto oder Active Directory-Sicherung
- Management in Unternehmen:
  - Group Policy-EinstellungenMicrosoft
  - BitLocker Administration and Monitoring (MBAM)
  - Zentralisierte Schlüsselverwaltung

# Zusammenfassung

- TPM: Hardware-Sicherheitsbasis für Schlüsselspeicherung
- BitLocker: Vollständige Festplattenverschlüsselung in Windows
- Zusammenspiel: Sicherer, benutzerfreundlicher Datenschutz
- Vorteile: Transparente Sicherheit bei minimaler Benutzerinteraktion
- Fazit: Wesentlicher Bestandteil moderner Datensicherheit