

# Threat Model

- "Gefahrenmodell": Analyse möglicher Bedrohungsszenarien für ein System / eine Gruppierung, um Sicherheitsbedürfnisse zu identifizieren und umzusetzen.
- Mögliche Akteure, von denen man schützen möchte: Strafverfolgungsbehörden und Geheimdienste (In- / Ausland?), Hacker mit Gewinnabsicht (Ransomware), Konzerne
- Mögliche Einfallstore: Hausdurchsuchung, Staatstrojaner, Anfrage an Internetanbieter / Hostinganbieter / Google etc, reguläre Schadsoftware

# Server

- Computer, der einen Service über das Netzwerk bereitstellt
- z.B. Mail-Server, Matrix-Server, Website, Cloud-Speicher, Streaming-Dienst
- Kann bei einem Cloud-Provider (Hetzner, Google, Njalla) oder zuhause stehen
- Meistens mit Linux betrieben

# Router

- Netzwerkgerät, das Datenpakete zwischen verschiedenen Netzwerken weiterleitet.
- Vergibt IP-Adressen für das lokale Netz
- Bsp: WLAN-Router

# IP-Adresse

- Eindeutige Nummer, die jedem Gerät in einem Netzwerk zugewiesen wird.
- Quasi die Koordinaten eines Geräts im Netz
- Globale IP-Adressen werden durch den ISP (Internetanbieter) vergeben, lokale IPs durch den Router.
- IPv4-Adressen (z.B. 192.168.1.1) und IPv6-Adressen (z.B. 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

# Browser

- Software, die den Zugriff und die Anzeige von Webseiten ermöglicht.
- z.B. Google Chrome, Mozilla Firefox, Microsoft Edge.

# Cookie

- Eine kleine Textdatei, die von einer Webseite auf dem Computer eines Nutzers gespeichert wird, um Informationen über den Besuch zu speichern.
- Werden für Personalisierung von Webseiten, die Speicherung von Sitzungseinstellungen und das Tracking von Nutzerdaten verwendet
- Nicht alle Cookies sind problematisch, gespeicherter Login läuft auch über Cookies

# Vulnerability

- Bei einer Vulnerability (Sicherheitslücke) handelt es sich um eine Schwachstelle in einem System, die ausgenutzt werden kann, um unbefugten Zugriff oder Schaden zu verursachen.
- Software-Bugs, Konfigurationsfehler, Schwachstellen in Netzwerken.
- Seriöse / Große Software-Anbieter sammeln sie im CVE-System und beheben
- Geheimdienste und Kriminelle kaufen oft gefundene Schwachstellen von Hackern, um sie zu nutzen ohne sie zu veröffentlichen

# OSINT

- Bei OSINT (Open Source Intelligence) handelt es sich um die Sammlung und Analyse von Informationen aus öffentlich zugänglichen Quellen.
- Informationen werden u.a. über Social Media (v.a. Twitter), Nachrichtenartikel, öffentliche Datenbanken, Informationsfreiheitsanfragen, Satellitenbilder gesammelt
- z.B. Kollektiv "Bellingcat"



# BIOS

## Basic Input/Output System

- Wird beim Starten des Computers geladen
- Startet den Bootloader des Betriebssystems
- BIOS-Einstellungen werden mit einer herstellerabhängigen Tastenkombination beim Start aufgerufen.

# UEFI

## Unified Extensible Firmware Interface

- Der Nachfolger von BIOS
- Bietet eine grafische Benutzeroberfläche
- Bietet erweiterte Sicherheitsfunktionen wie Secure Boot
- Die allermeisten Computer der letzten 10 Jahre haben UEFI.
- Relevant: Manche Betriebssysteme benötigen LEGACY-BOOT (BIOS-Kompatibilität)

# Betriebssystem

- Steuert die Hardware und führt Anwendungen aus
- Beispiele: Windows, macOS, Linux

# Partition

## Partitionierung von Festplatten

- Unterteilung einer Festplatte in mehrere Abschnitte
- Ermöglicht die Installation mehrerer Betriebssysteme auf derselben Festplatte
- Beim Start des Systems wird zuerst die 1. Partition, die Boot-Partition geladen.
- Wird beim Installieren des Betriebssystems angelegt / modifiziert.
- Kann mit Programmen wie Gnome Disks oder GParted verändert werden.

# Bootprozess

## Vom Einschalten bis zum Betriebssystem

1. **Power-On Self-Test (POST)**
2. **BIOS/UEFI Initialisierung**
3. **Bootloader laden (bei Linux meistens GRUB)**
4. **Betriebssystemkernel starten**
5. **Systemdienste und Benutzeroberfläche laden**

# Linux

## Ein freies Betriebssystem

- Open-Source
- Weniger Ressourcenverbrauch als Windows => Läuft auch auf älteren Geräten
- Verschiedene Distributionen wie Ubuntu, Fedora, Debian, openSUSE

## Open Source / Freie Software

- Software, deren Quellcode öffentlich zugänglich und frei nutzbar, veränderbar und verteilbar ist.
- Entwickler sind oft Hobbyisten, aber auch viele Unternehmen veröffentlichen open-source Software.
- Beispiele: Linux, Firefox, Android (teilweise), Krita, LibreOffice

# TPM

## Trusted Platform Module

- Ein Sicherheitschip auf dem Mainboard
- Speichert kryptographische Schlüssel
- Unterstützt Funktionen wie Festplattenverschlüsselung und sichere Bootprozesse



# Sicherheitslücke

- Schwachstelle in Soft- oder Hardware
- Kann durch Fehler im Code oder fehlerhafte Konfiguration entstehen

# Exploit

- Ausnutzen einer Sicherheitslücke
- Kann Zugriff oder Manipulation von Daten erlauben

# Responsible Disclosure

- Verantwortungsbewusste Offenlegung von Sicherheitslücken
- Hacker informiert den betroffenen Anbieter zuerst
- Gibt dem Anbieter Zeit zur Behebung der Lücke
- Veröffentlichung der Lücke erst nach einer festgelegten Frist oder nach Behebung

# Zero-Day vulnerability

- Sicherheitslücke, die dem Entwickler meist nicht bekannt ist und für die kein Fix verfügbar ist
- Kann von Konzernen, Strafverfolgungsbehörden und Geheimdiensten auf dem Schwarzmarkt eingekauft werden.

