Threat Model

- "Gefahrenmodell": Analyse möglicher Bedrohungszenarien 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, Njala) 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 behoben
- 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"