Cheat Sheet: Cybersecurity

CODIALIST

Asset

Aspekte eines Produktes, die wertvoll sind und vor unberechtigten Zugriffen geschützt werden müssen.

- Personenbezogene Daten
- Intellectual Property
- Verfügbarkeit der Funktion

Die Identifizierung von Assets ist ein wichtiger Schritt bei der Erstellung einer effektiven Cybersecurity-Strategie. Der Schritt ist hilfreich, um ein angemessenes Sicherheitslevel festzulegen (bei sensiblen Assets muss ein höheres Sicherheitslevel erreicht werden). Assets sind bei sicherheitskritischen Anwendungen auch oft der Link zur Risikoanalyse.

Threat

Potenzielle Bedrohung, die darauf abzielt ein Produkt zu beschädigen oder zu beeinträchtigen bzw. die Assets eines Produktes zu kompromittieren.

- Tampering
- Denial-Of-Service Angriff
- Information Disclosure

Bedrohungen können von externen (oder auch internen) Angreifern (Hackern) ausgehen, aber auch versehentlich durch menschliche Fehler verursacht werden. Um Bedrohungen effizient und möglichst vollständig zu erfassen, empfiehlt sich ein methodisches Vorgehen (z.B. STRIDE, Attack Trees, OCTAVE).
Threats sollten dabei eher als „Konzept eines Angriffs“ verstanden werden und nicht als konkrete „technische Schwachstelle/technische Umsetzung eines Angriffs“.

Vulnerability

Konkrete technische Schwachstelle im Produkt, die von einem Angreifer genutzt werden kann, um das Produkt zu schädigen, beeinträchtigen oder zu kompromittieren.

- SQL Injection
- Buffer-Overflow
- Schwachstellen Drittanbieter-Komponenten
- Insecure Default Settings
- Unzureichende Verschlüsselung

Schwachstellen werden von Entwicklern oft unabsichtlich im Code hinterlassen (z.B. Buffer Overflow) oder sind in Drittanbieter-Komponenten enthalten. Angreifern können diese z.B. durch Reverse Engineering entdecken.
Die Identifizierung, Bewertung und Behebung von Schwachstellen ist daher ein wichtiger Bestandteil der Cybersecurity auf dem Weg zu einem sicheren Produkt.
Eine besondere Bedeutung hat auch das „Vulnerability Scanning“ - während der Entwicklung und auch danach, da viele Schwachstellen erst im Laufe der Zeit bekannt werden.

Incident Scenario

Threat  —nutzt→ **Vulnerability**  —zur Kompromittierung von→ **Asset** 

 **Sicherheitsmaßnahmen**

z.B. manipuliertes Software- Image gelangt via Update-Over-The-Air auf ausgelieferte Geräte (z.B. Insulin-Pumpe)

z.B. Sicherheitslücke, die das Hinterlegen verfälschter Software Images auf dem Over-The-Air-Update Server ermöglicht

z.B. Funktionalität des Gerätes (steht dann auf Grund des manipulierten Software-Images nicht mehr zur Verfügung)

z.B. Prüfung der Signatur des Software Images bevor Update auf dem Gerät installiert wird.