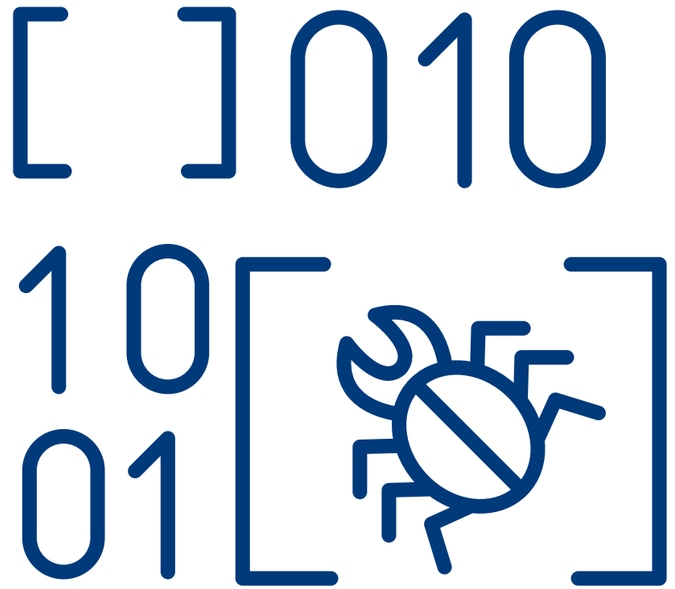
HACKING:

Schwachstellen oder Sicherheitslücken eines Systems werden identifiziert und ausgenutzt, um sich mit Hilfe eines Entschlüsselungsprogramms, wie z.B. Passwortalgorithmen oder gestohlenen Benutzerinformationen, Zugang zu den dortigen Daten zu verschaffen.



RANSOMWARE:

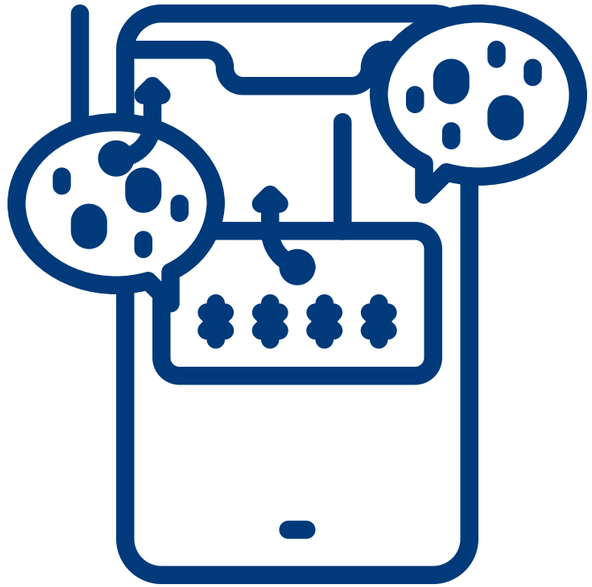
Durch eine Sicherheitslücke wird sogenannte Malware auf ein betroffenes System geladen. Hacker:innen können so Zugriff auf alle Daten erlangen und auf diese Weise das System lahmlegen. Mit der Drohung, Daten entweder nicht mehr freizugeben oder sensible Informationen zu veröffentlichen, ist die Freigabe der Systeme an eine Lösegeldforderung oder ähnliche Erpressung gebunden. Die Programme, die benutzt werden, um die betroffenen Systeme anzugreifen, nennt man deswegen Ransomware (engl. ‚ransom' - Lösegeld).

PHISHING:

Phishing-Attacken treten besonders in der elektronischen Kommunikation auf. Usern werden E-Mails mit bösartigen Links zugesendet mit dem Ziel, sensible und wertvolle Informationen durch das unbewusste Zutun der End-Users zu erlangen. Durch den Aufruf eines mit Malware hinterlegten Phishing-Links erhalten Hacker die Kontrolle über das System der End-User und können es so extern steuern und verschlüsseln. Das Wort ‚pishing' ist ein Neologismus von ‚fishing', engl. für ‚Angeln'.

SPEAR PHISHING:

Diese Form des Phishings basiert auf einer personalisierten Attacke, bei der die trügerischen E-Mails durch gesammelte Daten (bspw. von Social Media) mit mehr Glaubwürdigkeit versehen werden, um ein Infiltrieren wahrscheinlicher zu machen.



WASSERLOCH-ATTACKE:

Bei dieser Attacke wird das Verhalten von Usern durch Spysoftware beobachtet und oft besuchte Seiten, die IT-Sicherheitslücken aufweisen, werden mit Malware versehen.