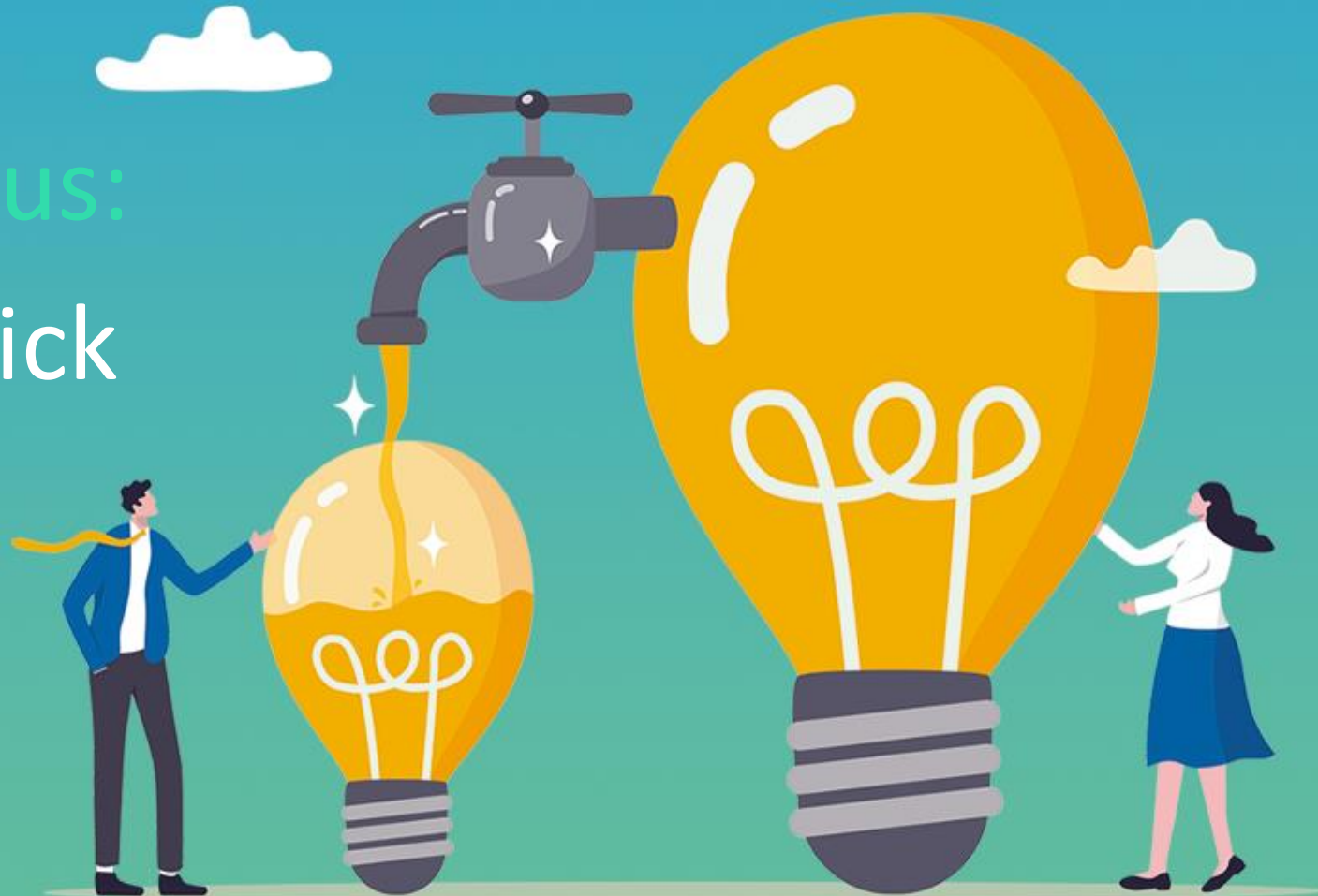


Technologie im Fokus:
Unser Jahresrückblick
und Ausblick





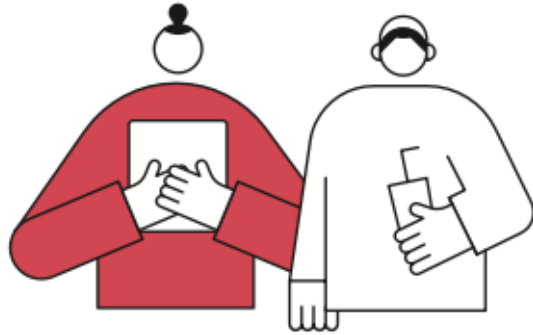
Agenda

1. Die Lage der IT-Sicherheit in DE
2. Frühzeitiges Erkennen von Cyberangriffen
3. KI, neue Angriffsfläche, neue Chance
4. Beyond SASE, Cyber-Resilienz und Digitalisierung

Die Lage der IT-Sicherheit in Deutschland 2023

Top-3-Bedrohungen je Zielgruppe:

Gesellschaft



Identitätsdiebstahl

Sextortion
Phishing

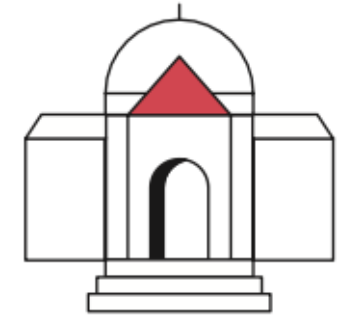
Wirtschaft



Ransomware

Abhängigkeit innerhalb der
IT-Supply-Chain
Schwachstellen, offene oder falsch
konfigurierte Onlineserver

Staat und Verwaltung



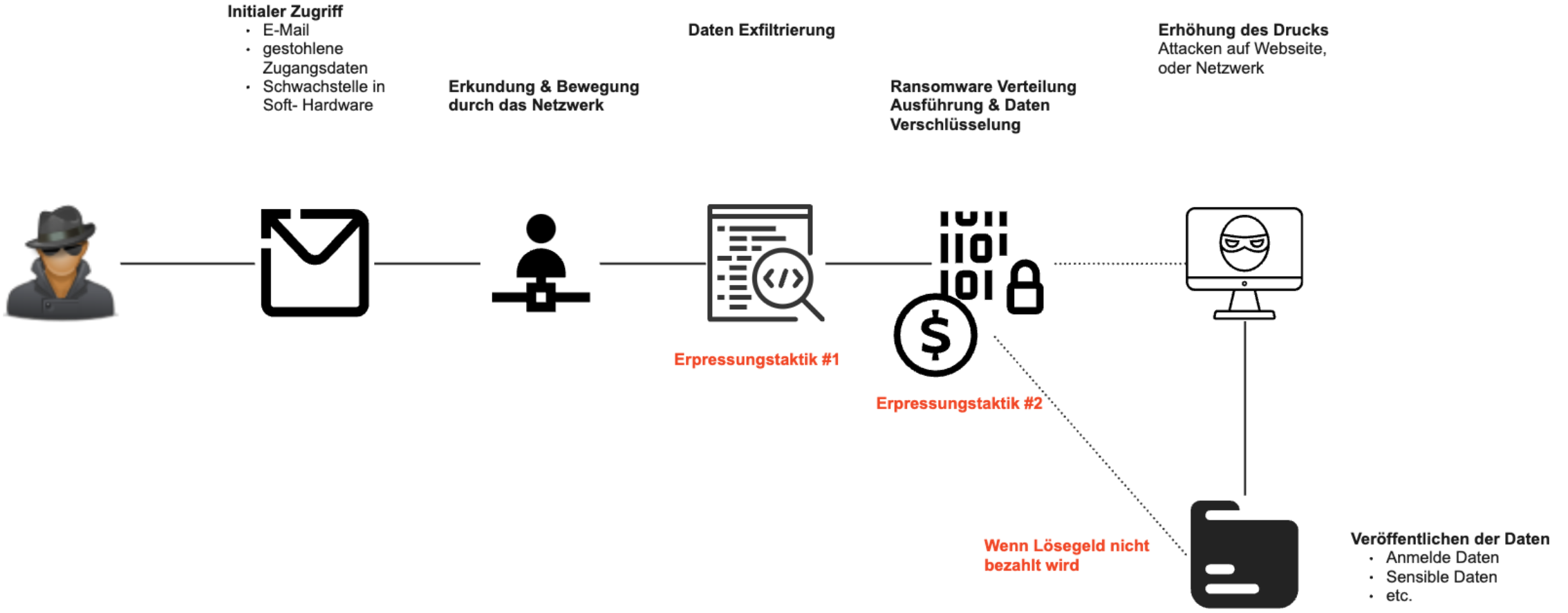
Ransomware

APT*
Schwachstellen, offene oder
falsch konfigurierte Onlineserver

**„Insgesamt zeigte sich im aktuellen
Berichtszeitraum
eine angespannte bis kritische Lage. Die
Bedrohung im
Cyberraum ist damit so hoch wie nie zuvor.“**

Quelle: BSI - Die Lage der IT-Sicherheit in Deutschland 2023

Einmal angegriffen, zweimal erpresst! Double-Extortion-Angriffe



Gültige Anmeldedaten waren der Hauptinfektionsvektor im Q2 2023



Quelle: Talos Report Q2 2023

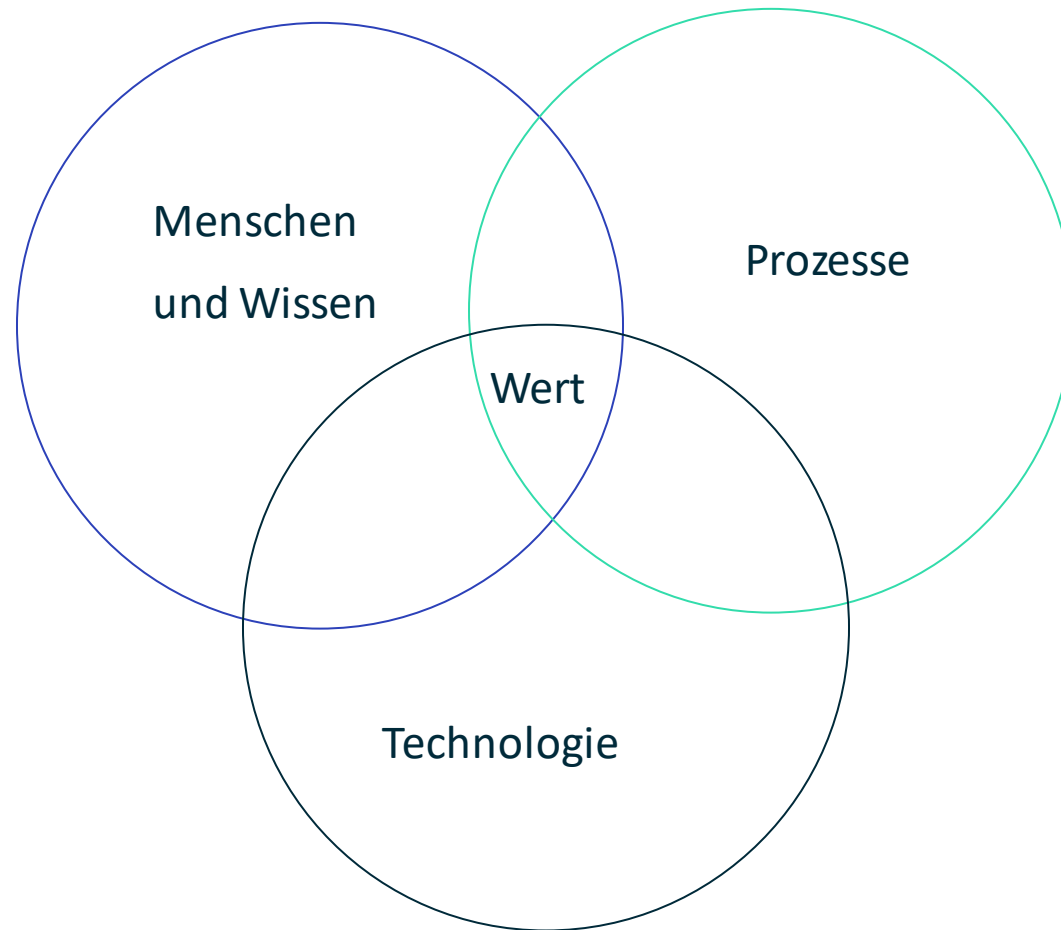
avodaq Advisory Abteilung

Frühzeitiges Erkennen von Cyberangriffen

Durchschnittlich dauert es 280 Tage, bis ein Unternehmen einen Datenverstoß entdeckt und darauf reagiert.

Quelle: IBM Cost of a Data Breach Report 2023

System zur Angriffserkennung



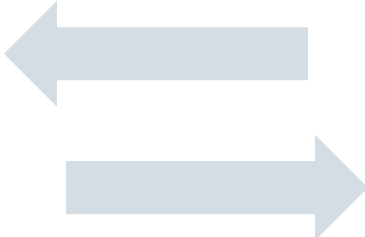
KI, neue Angriffsfläche, neue Chance

KI als Angriffsfläche

Sammlung von Unternehmensinformationen in einer einzigen, schwer abzusichernden Anwendung



Zugriffsrechte



Prompt Injections

Prompt Engineering



Adversarial Attacks

KI gestützte Deepfakes



Echter Doppelgänger?

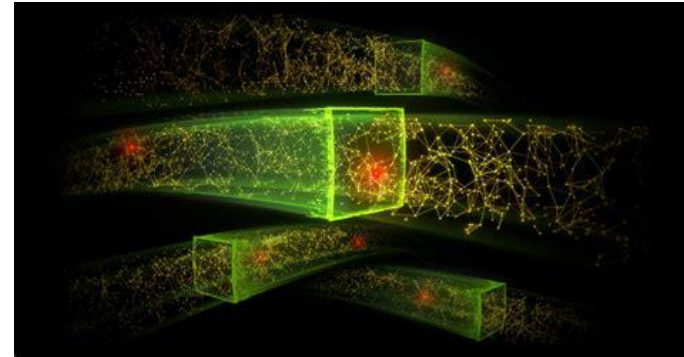


Deepfake

Chancen



Cisco AI Assistant



NVIDIA Morpheus

Beyond SASE, Cyber-Resilienz und Digitalisierung

Access



Managed
Endpoint



Unmanaged



On Premise,
Users, Devices
& Things

Secure



Services



Internet/SaaS



Private
Applications

Public/Private
Cloud



DC/Colo/
Branch

avodaq Fazit

Danke!

avodaq AG

info@avodaq.com

avodaq.com