

IT-Security in Projekten

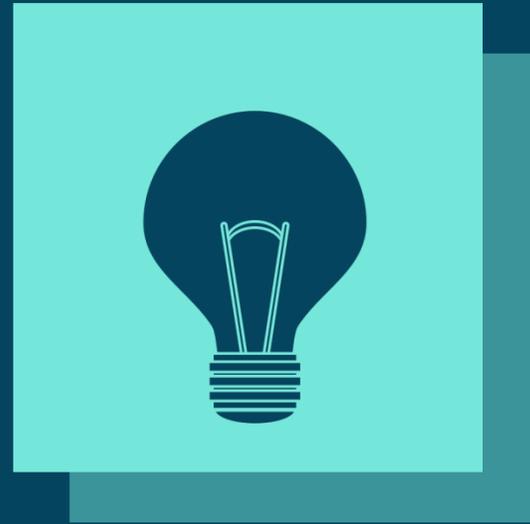
Was passiert, wenn's passiert?

Robert Wortmann

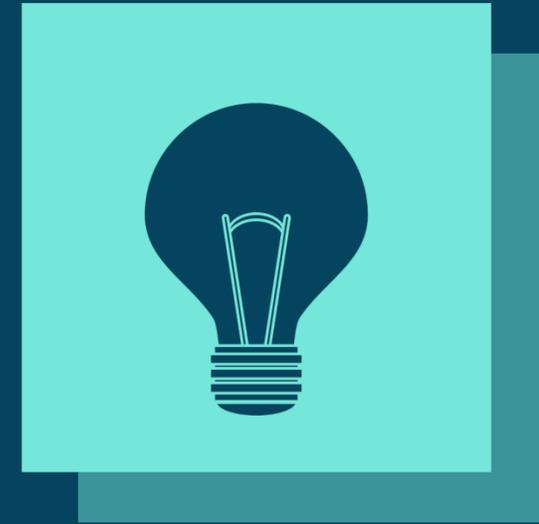
Aktuelle Sicherheitslage



Die Angriffslage hat sich für die meisten Unternehmen kaum geändert



Kriminelle Gruppen sind deutlich häufiger als Staatliche Akteure



KI spielt noch (!) keine übergeordnete Rolle

-
- 09/2022** Initiale Kompromittierung einer Cloud Umgebung abseits der IT
 - 12/2022** Angebot des Zugangs über Marktplatz im Darknet
 - 03/2023** Zugriff auf die Umgebung, laterale Verbreitung über unbekanntem VPN Tunnel
 - 04/2023** Erzeugung weiterer Persistenzen auf ungeschützten Clients, Credential Dump und Daten Exfiltrierung
 - 04.04.2023** Meldung Cobalt Strike Beacons durch Trend Micro
 - 05.04.2023** Verschlüsselung der Daten
 - 06.04.2023** Einleitung Incident Response

Learnings

Security by design

Security muss ab dem ersten Tag der Projektplanung ein wichtiger Faktor sein, der zugleich allerdings kein Bremsklotz sein darf. Egal, ob Auswahl einer Software oder der eigentlichen Steuerung des Projekts, Security muss in allen Köpfen verankert sein.

Compliance ist nicht gleich Sicherheit

Compliance ist wichtig, darf allerdings niemals mit operativer Sicherheit verwechselt werden. Es gilt in jedem Falle: Check-Box Security ist keine Security. Hinter fast jeder Anforderung steckt eine Intention.

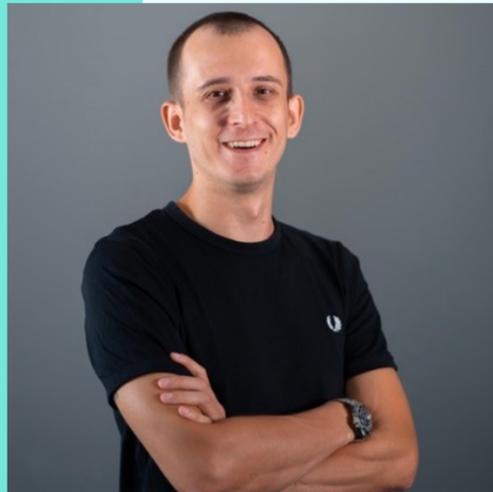
Reporting

Egal, ob Projektleitung oder nicht technische Führungsebene, Sicherheit muss greifbarer gemacht werden, sodass Investitionen nachhaltig Bestand haben.

Basics

IT-Sicherheit ist oftmals einfacher als man denken mag. Das Pareto Prinzip sollte dabei helfen einen möglichst Risiko-basierten Ansatz zu finden.

Kontakt



ROBERT WORTMANN

Podcast: Breach FM der Infosec Podcast

Mail: robert@thewortmann.com

LinkedIn: <https://www.linkedin.com/in/robert-wortmann-28091315a/>