HYPERSECURE IT

Die einfache Lösung für komplexe Cyber-Bedrohungen

Andreas Fuchs, Director Product Management

Oktober 2024

DriveLock

HYPERSECURE IT

Mit der HYPERSECURE Endpoint Protection Platform
bleiben **Angriffe** auf IT-Systeme da,
wo sie hingehören: **außen vor**.

Unsere Expertise

DriveLock

- Seit über 20 Jahren am Markt
- Ausgezeichnete und zertifizierte Lösung
- SMB bis Enterprise
- Eine Plattform, eine Konsole, ein Agent
- Cloud & On-premise
- Fokus: Kundenzufriedenheit
- Effizient, rentabel, aktuell, auf Knopfdruck

Herausforderungen

Digitalisierung

Fachkräftemangel

Gesetze & Regularien

Cyber-Kriminalität

Die Phasen vor und nach einem Angriff

DriveLock

Pre-Breach | Attack | Breach | Post-Breach

Identify → Protect → Detect → Respond → Recover

LEFT OF BOOM

Reducing the likelihood of an attack

BOOM

RIGHT OF BOOM

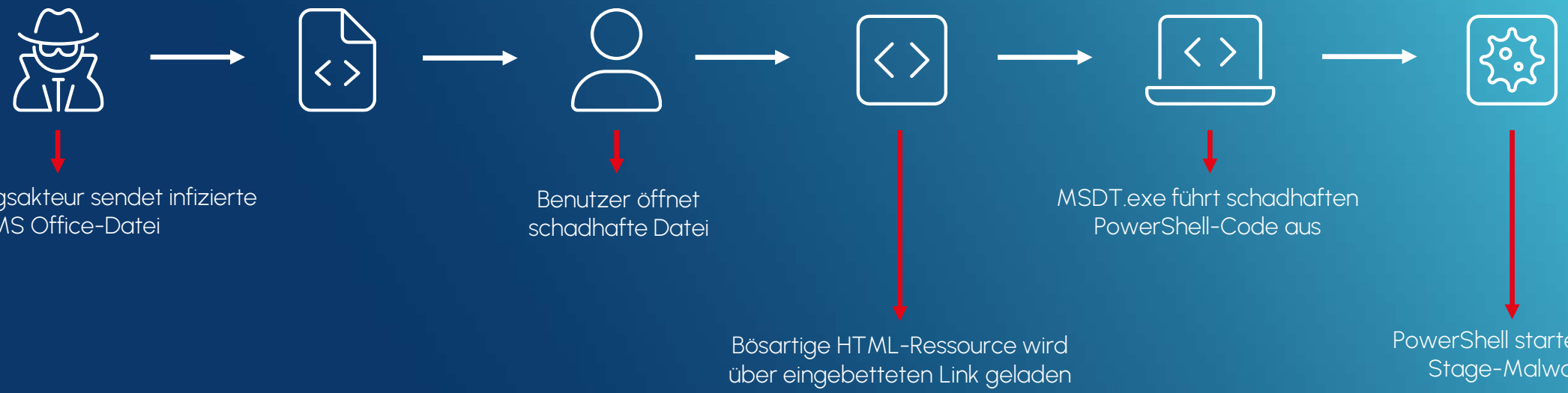
Reducing the impact of a successful attack

Months | Weeks | Days | Hours | Minutes | Minutes | Hours | Days | Weeks | Months

Reconnaissance → Weaponization → Delivery → Exploitation → Installation → Command & Control → Actions on Objectives

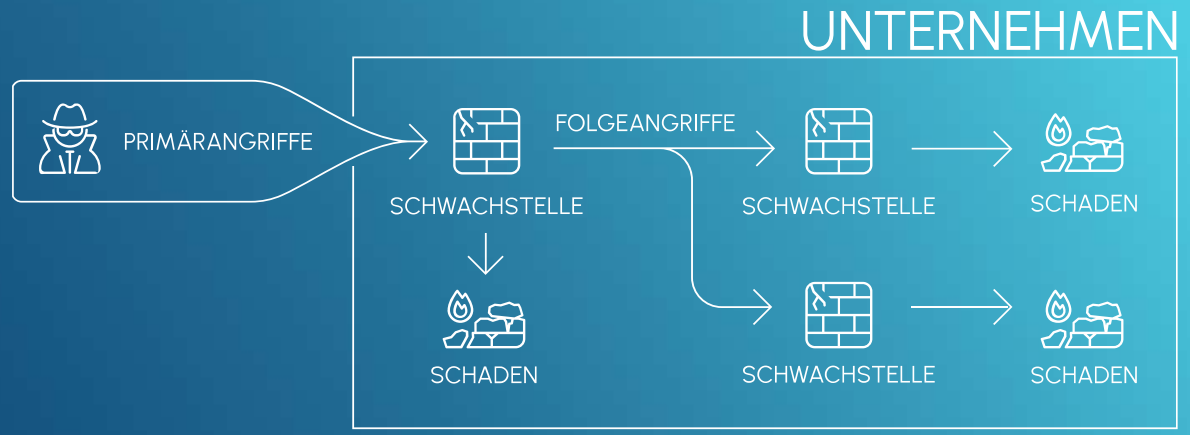
Praxisbeispiel

Follina (CVE-2022-30190) ist eine Microsoft Office Zero-Day-Schwachstelle. Es handelt sich um eine hochgradig gefährliche Schwachstelle, die Hacker für RCE-Angriffe (Remote Code Execution) ausnutzen können.



BSI nennt die größten Cyberbedrohungen

- Einschleusen von Schadsoftware
- Infektion mit Schadsoftware
- Menschliches Fehlverhalten und Sabotage
- Social Engineering und Phishing
- (D)DoS Angriffe
- Internetverbundene Steuerungskomponenten
- Einbruch über Fernwartungszugänge
- SW/HW Schwachstellen in der Lieferkette



Bildvorlage: BSI

https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.pdf

Angriffe rechtzeitig in der Kill Chain stoppen

Verhindern statt später entdecken!

Beispiele für Präventionsmaßnahmen

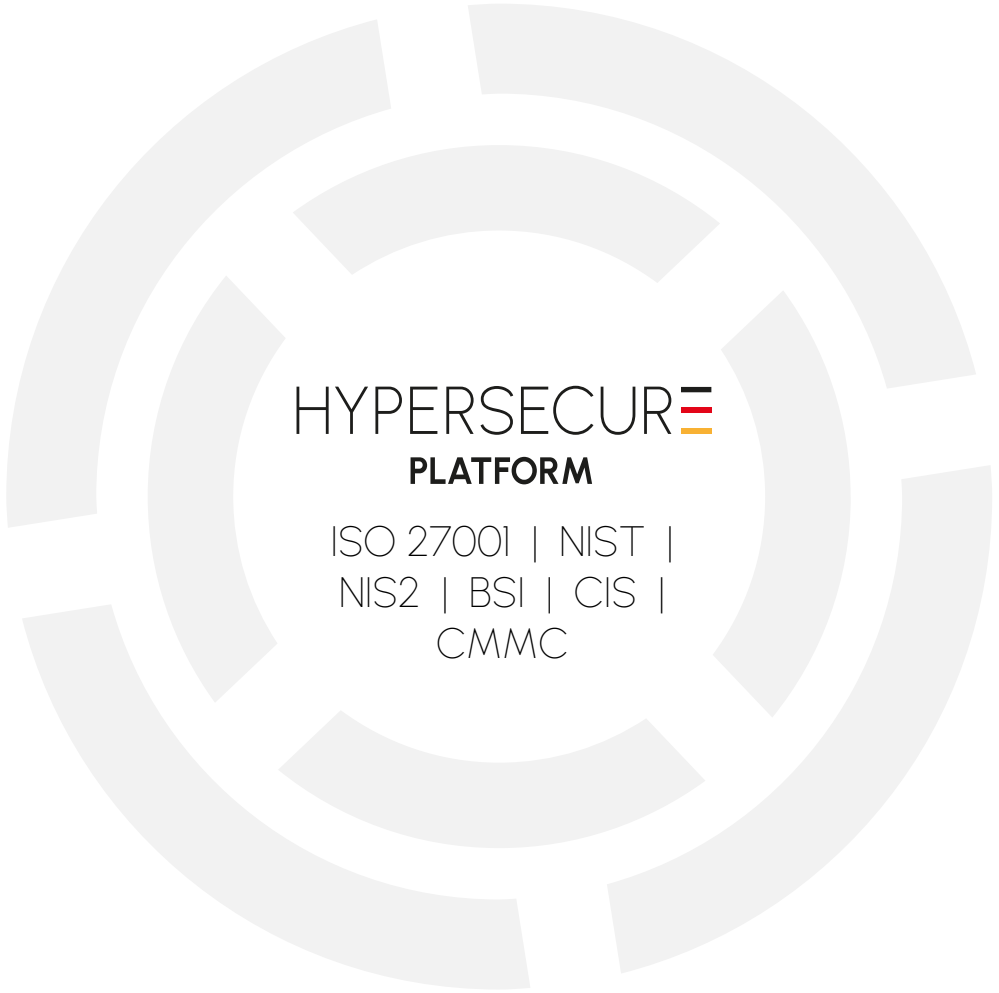
Szenario	Maßnahme
Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme	Device Control
Infektion mit Schadsoftware über Internet und Intranet (LotL)	Application Control
Menschliches Fehlverhalten und Sabotage	Security Awareness

https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.pdf

HYPERSECURE Platform

DAS ZIEL

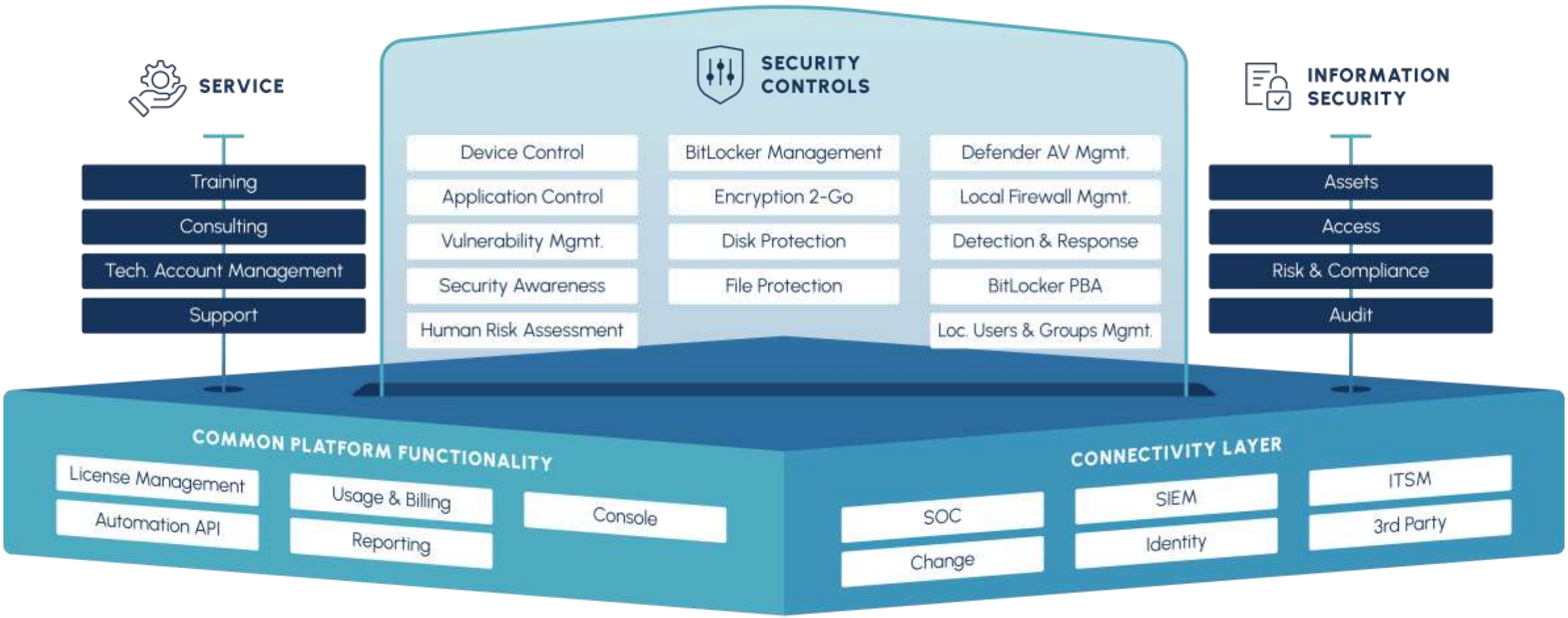
Angriffe verlangsamen, verhindern und es den Angreifern so teuer wie möglich machen!



Die Produkte

HYPERSECURE Platform

The HYPERSECURE Platform



NIS2 Risikomanagement (Art. 21 Abs. 2)

Richtlinien	Konzepte bzgl. Risikoanalyse und Sicherheit für Informationssysteme
Incident Management	Bewältigung von Sicherheitsvorfällen
Business Continuity	Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
Supply Chain	Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zw. den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern
Prevention & Detection / Vulnerability Management	Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen
Risk & Compliance	Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
DLP / Verschlüsselung	Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung
Awareness	Grundlegende Verfahren bzgl. Cyberhygiene und Schulungen bzgl. Cybersicherheit
Access Control	Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen
Zero Trust	Verwendung von Lösungen zur MFA oder kontinuierlichen Authentifizierung

NIS2 Art. 21 (2): https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555#d1e3335-80-1

Bereit für NIS2 ?

Machen Sie den Check!

https://www.drivelock.com/de/lp-nis2-compliance-check

DriveLock
DRIVELOCK.COM

Halle 9
Stand 241