Ablauf eines Ransomware-Angriffs

Taktiken, Techniken und Prozeduren: Aus dem Logbuch eines Angreifenden

HiSolutions Know-how to go

Lisa Lobmeyer

Agenda

1. Motivation von Ransomware-Angriffen
2. Ransomware-Angriffe in der Praxis
3. Lessons Learned

1. Funktionsweise von Ransomware-Angriffen

Beispiel für aktuelle Fälle

Sophos-Bericht
State of ransomware

66%

wurden Opfer eines Ransomware-Angriffs
(78% Anstieg gegenüber 2020)

812.360 $

durchschnittliche Lösegeldzahlung
(480% Anstieg gegenüber 2020)

73%

konnten durch Backups Daten wiederherstellen

1,4 Mio. $

durchschnittliche Kosten zur Behebung
der Angriffs-Folgen

Studienhintergrund:

- 5.600 IT-Entscheider
- 31 Länder
- 100-5.000 Mitarbeiter
- Jan/Feb 2022 für 2021

46% | 4%

zahlen das Lösegeld | konnten dadurch alle Daten wiederherstellen

1 Monat

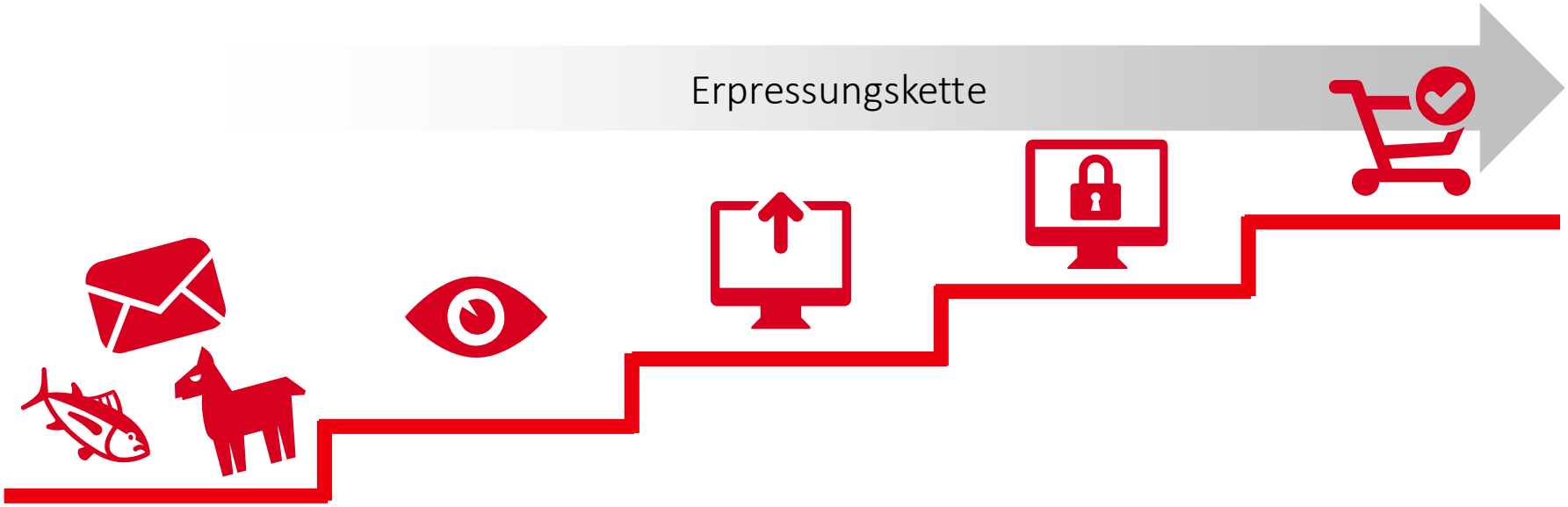
durchschnittliche Zeit bis zur kompletten Wiederherstellung

https://www.sophos.com/de-de/whitepaper/state-of-ransomware

Motivation hinter Cyber-Angriffen

- Erpressung – finanzielle Motivation
- Hacking aus Spaß und Neugier
- Frust oder Rache – persönliche Motivation
- Ressourcen
- Behinderung von Wettbewerbern
- Betrug – Onlinehandel oder CEO-Fraud
- Spionage

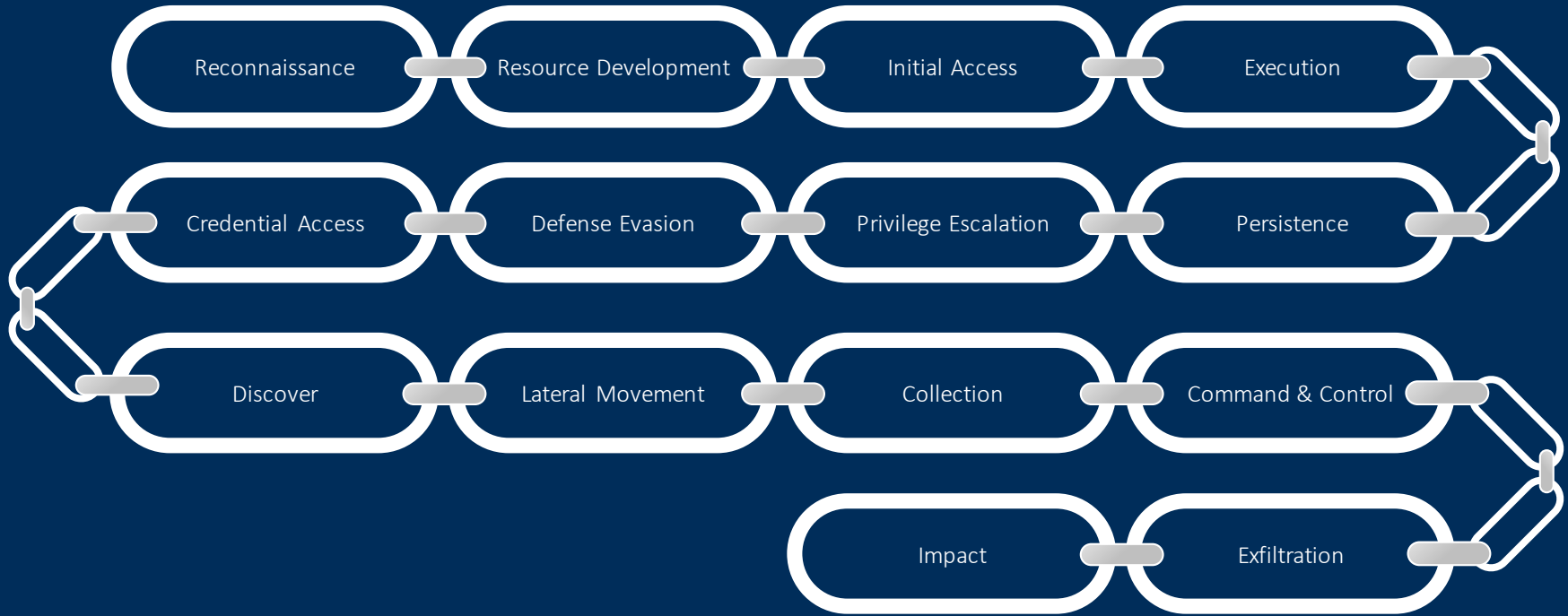
Das Geschäftsmodell: Ransomware as a Service



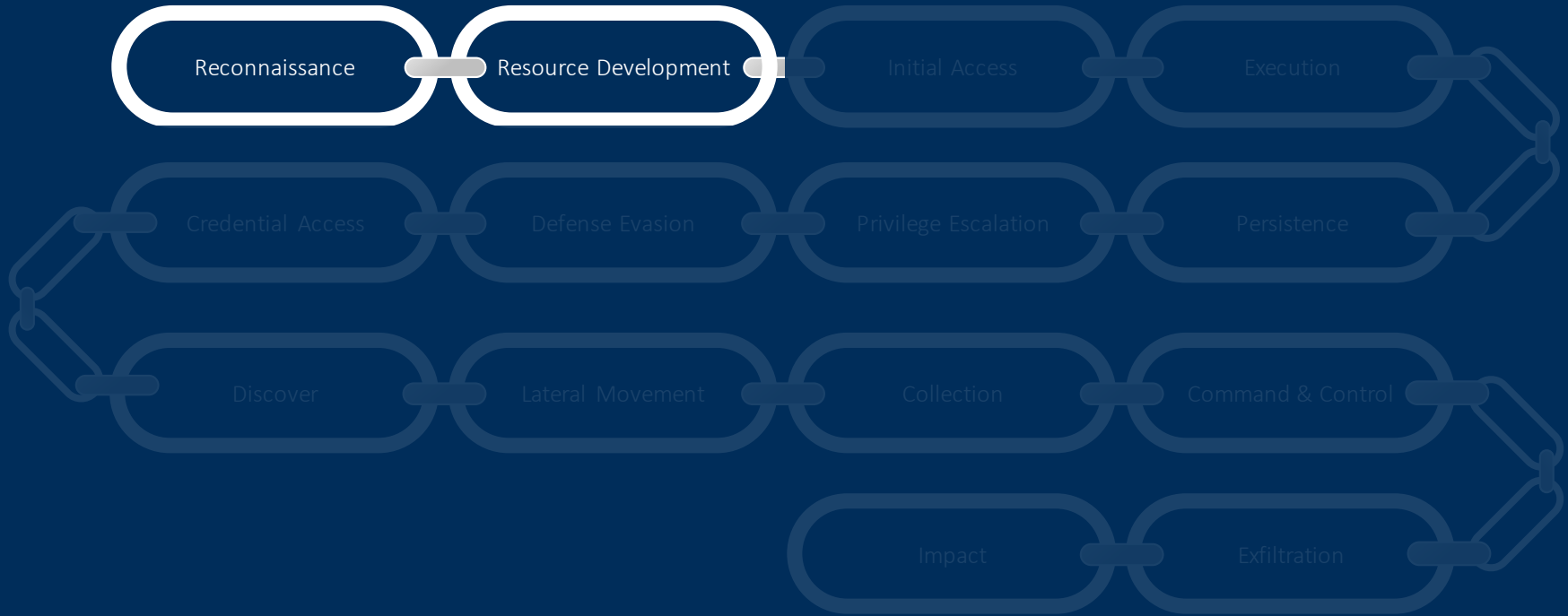
Initialer Zugriff	Auskundschaften des Ziels	Datenabzug	Verschlüsselung	Daten-veröffentlichung/ -verkauf

2. Ransomware-Angriffe in der Praxis

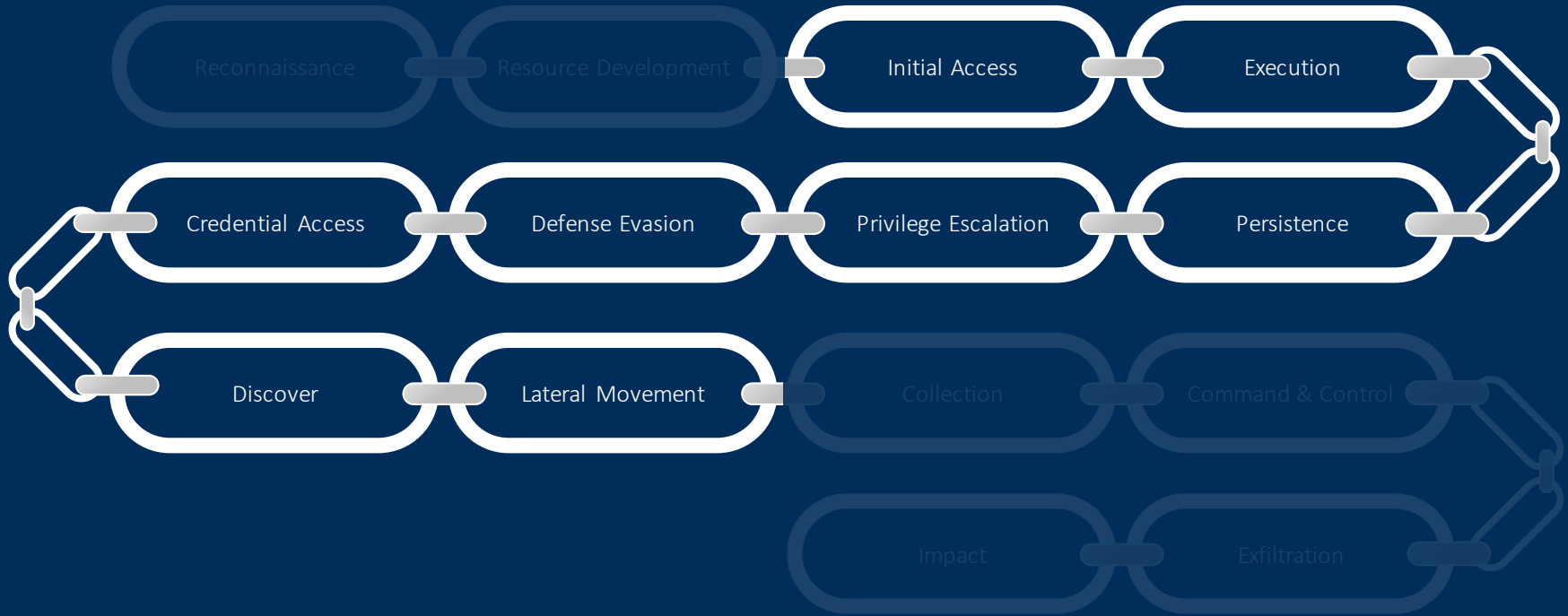
Cyber Kill Chain nach MITRE ATT&CK



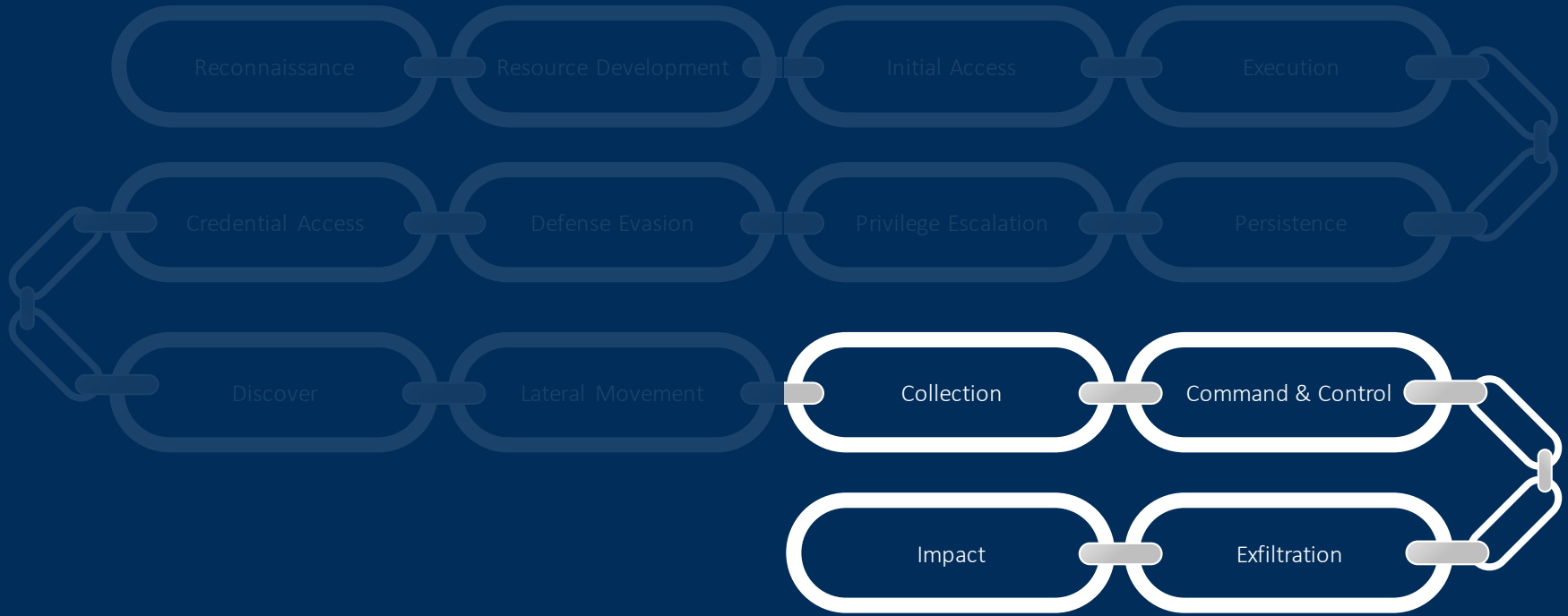
Cyber Kill Chain nach MITRE ATT&CK: Vorbereitende Schritte



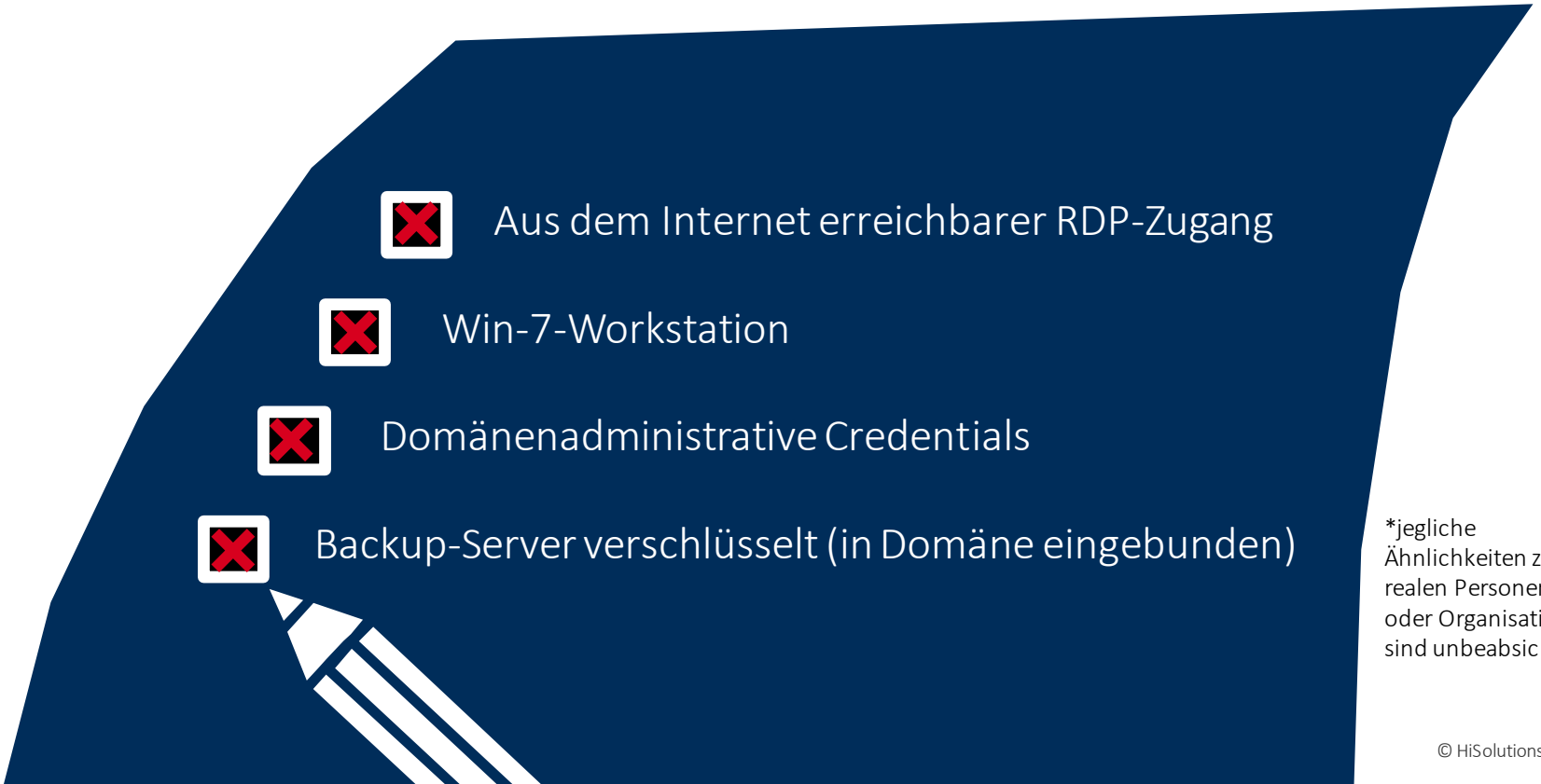
Cyber Kill Chain nach MITRE ATT&CK: Kompromittierung



Cyber Kill Chain nach MITRE ATT&CK: Ausführung zur Zielerreichung

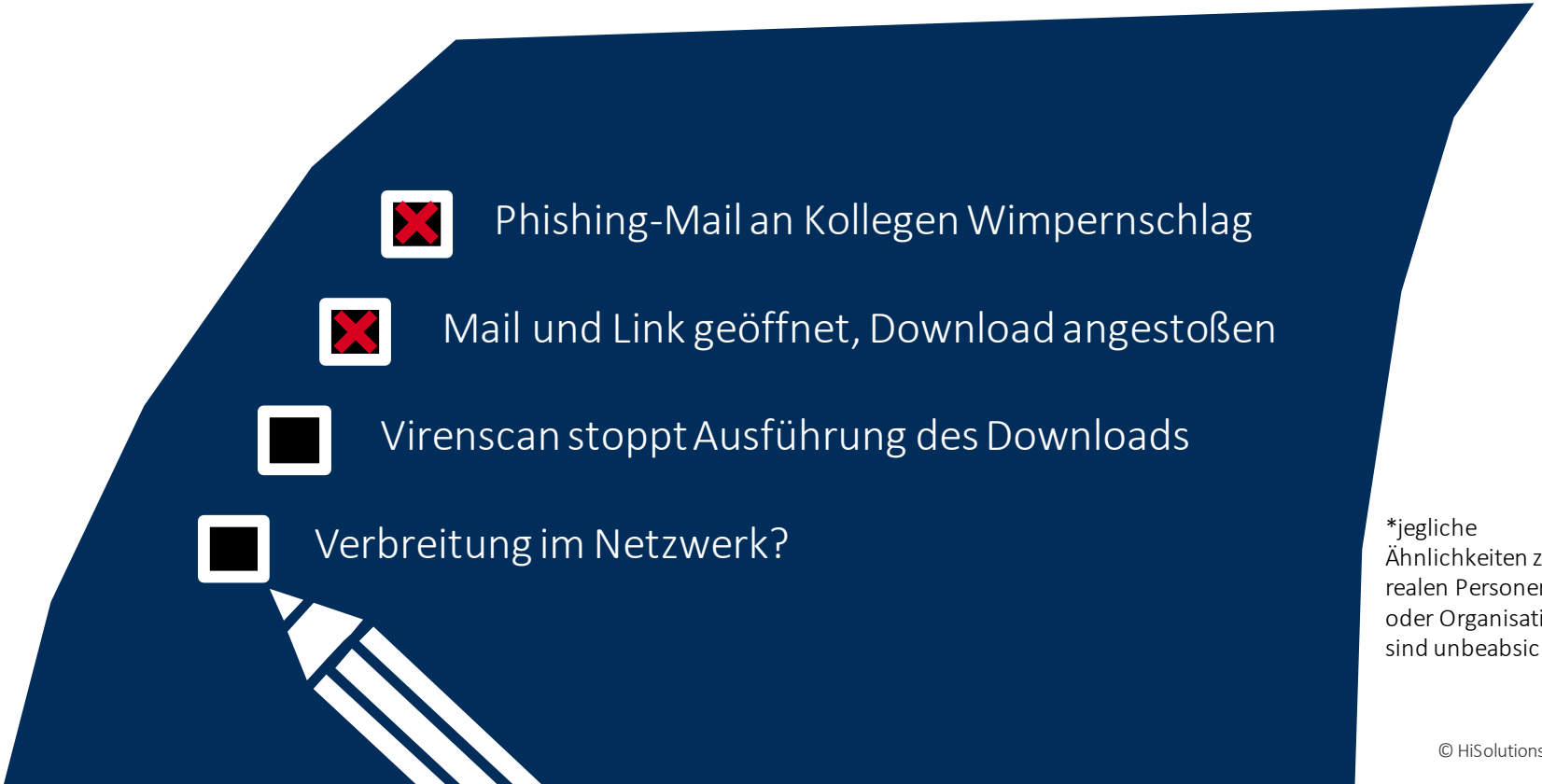


Fallbeispiel 1
Organisation Wolkenbruch: Vollverschlüsselung



*jegliche Ähnlichkeiten zu realen Personen oder Organisationen sind unbeabsichtigt

Fallbeispiel 2
Unternehmen Sonnenschein: Phishing-Mail mit/ohne Nachwirkung



*jegliche Ähnlichkeiten zu realen Personen oder Organisationen sind unbeabsichtigt

Fallbeispiel 3
Organisation Gewittersturm: Vollverschlüsselung mit nutzbaren Backups

*jegliche Ähnlichkeiten zu realen Personen oder Organisationen sind unbeabsichtigt

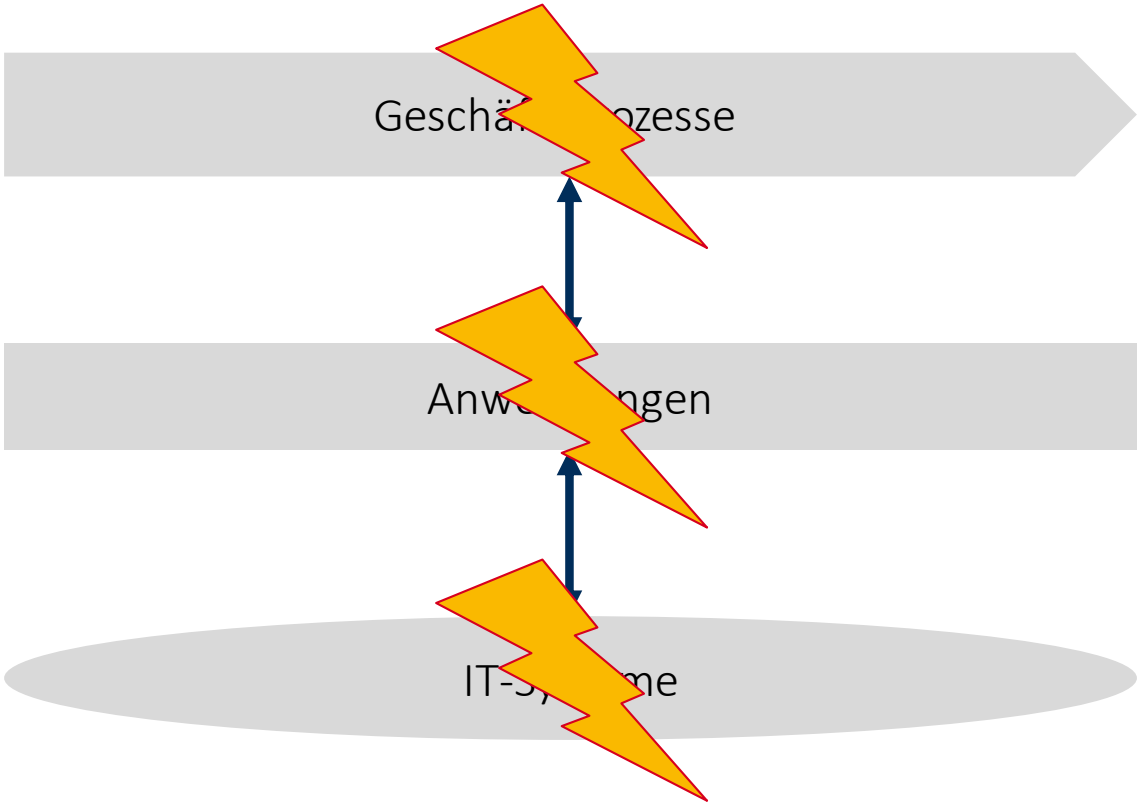
3. Lessons Learned?

Reaktion auf Vorfälle zur Abfederung des Falls

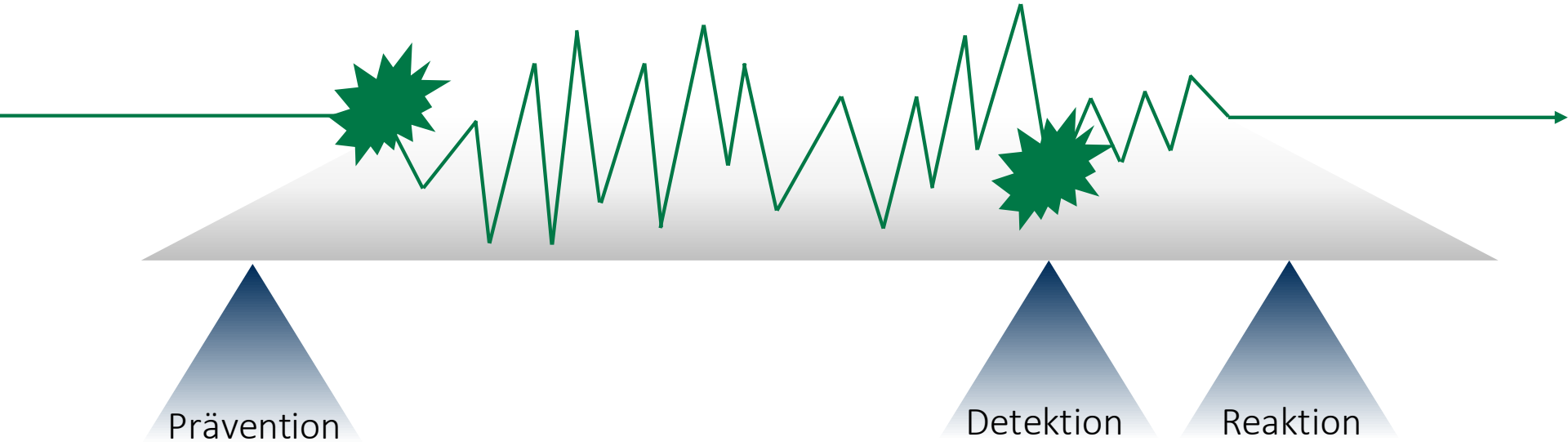
Vorbereitung: Reaktion auf Ransomware

- Ransomware-sichere Backups (https://research.hisolutions.com/2021/03/schutz-gegen-ransomware-hisolutions-selbsthilfe-offline-backup/)
- Definierte Eskalationsketten
- Krisenstab
- Wiederanlaufpläne & Notfallpläne/BCM
- Dokumentierte Passwörter/Notfalllisten
- Vertrag mit einem Incident-Response-Dienstleister

Auswirkungen von Cyber-Angriffen: Definition kritischer Prozesse



Schutz vor Cyber- und Ransomware-Angriffen



Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com