DFIR (Digital Forensik – Incident Response)

Cyberangriffe verstehen, analysieren und eindämmen

Agenda

- Einführung in die Bedrohungslage
- Was ist DFIR?
- Typische Angriffswege
- Anlauf eines Incident Response-Falls
- Forensische Analyse in der Praxis
- Lessons Learned & Handlungsempfehlung

Warum sprechen wir heute über DFIR?

Die Bedrohungslage verändert sich massiv

- Ransomware-Angriffe nehmen weiterhin stark zu
- Angreifer arbeiten professionell und automatisiert
- KMU stehen zunehmend im Fokus
- Backups allein reichen nicht mehr aus

FACT: „Viele Unternehmen merken erst Tage oder Wochen später, dass ein Angreifer bereits aktiv war. Genau hier setzt DFIR an.“

Was bedeutet DFIR?

Digital Forensic

- Digitale Spurensicherung
- Analyse kompromittierter Systeme
- Rekonstruktion des Angriffsverlaufs
- Beweissicherung

Incident Response

- Schnelle Reaktion auf Sicherheitsvorfälle
- Eindämmen des Schadens
- Wiederherstellung des Betriebs
- Verhindern weiterer Angriffe

Fakt: ***„DFIR verbindet Technik, Prozesse und Krisenmanagement.“***

Typischer Ablauf eines Cyberangriffs

Initial Access

- Phishing
- Schwache Kennwörter
- Zugriff mittels VPN

Typischer Ablauf eines Cyberangriffs

Privilege Escalation

- Backdoors
- Scheduled Tasks
- RMM-Tools

Typischer Ablauf eines Cyberangriffs

Persistence

- Credential Dumping
- Pass-the-Hash

Typischer Ablauf eines Cyberangriffs

Lateral Movement

- PsExec
- RDP
- SMB

Typischer Ablauf eines Cyberangriffs

Data Exfiltration

- Daten werden in ein rar-archiv gepackt
- Upload meist auf filebin

Typischer Ablauf eines Cyberangriffs

Ransomware Deployment

- Verschlüsselung von 17.000 Dateien pro Minute
- Ablage der Ransomnote
- Löschen von Log-Dateien

Warum klassische Security oft nicht reicht

Typische Probleme in Unternehmen

- Fehlende Netzwerksegmentierung
- Lokale Administratorrechte
- Unzureichendes Monitoring
- Kein 24/7 Security Monitoring
- Fehlende Logdaten
- Backup ohne Offline-Kopie

„Der Angreifer war bereits 18 Tage im Netzwerk bevor die Verschlüsselung startete.“

Der Incident Response Prozess

Strukturierte Reaktion auf Sicherheitsvorfälle

Die 6 Phasen:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

Fokus:

- Geschwindigkeit
- Kommunikation
- Dokumentation
- Priorisierung

„Das Ziel ist nicht nur die technische Bereinigung, sondern die schnelle Stabilisierung des Geschäftsbetriebs.“

Beispiele aus der Praxis

Ausgangslage:

- Mitarbeiter hat schwaches Kennwort
- Bruteforce-Attacke auf das VPN-Portal
- VPN-Zugang missbraucht

Was der Angreifer tat:

- Domain-Admin Rechte erlangt
- Backupserver Deaktiviert
- Daten Exfiltriert
- Ransomware verteilt

Folgen:

- Produktionsausfall
- Verschlüsselte Systeme
- Datenschutzvorfall
- Hohe Wiederherstellungskosten

„In vielen Ransomware-Fällen vergehen zwischen der ersten Kompromittierung und der eigentlichen Verschlüsselung mehrere Tage oder sogar Wochen – genug Zeit für Angreifer, sich unbemerkt im gesamten Netzwerk auszubreiten."

Was machen Forensiker konkret

Analysebereiche:

- RAM-Analyse
- Windows Event Logs
- Registry-Artefakte
- Netzwerkverkehr
- Benutzeraktivitäten
- Malware-Analyse

Typische Tools:

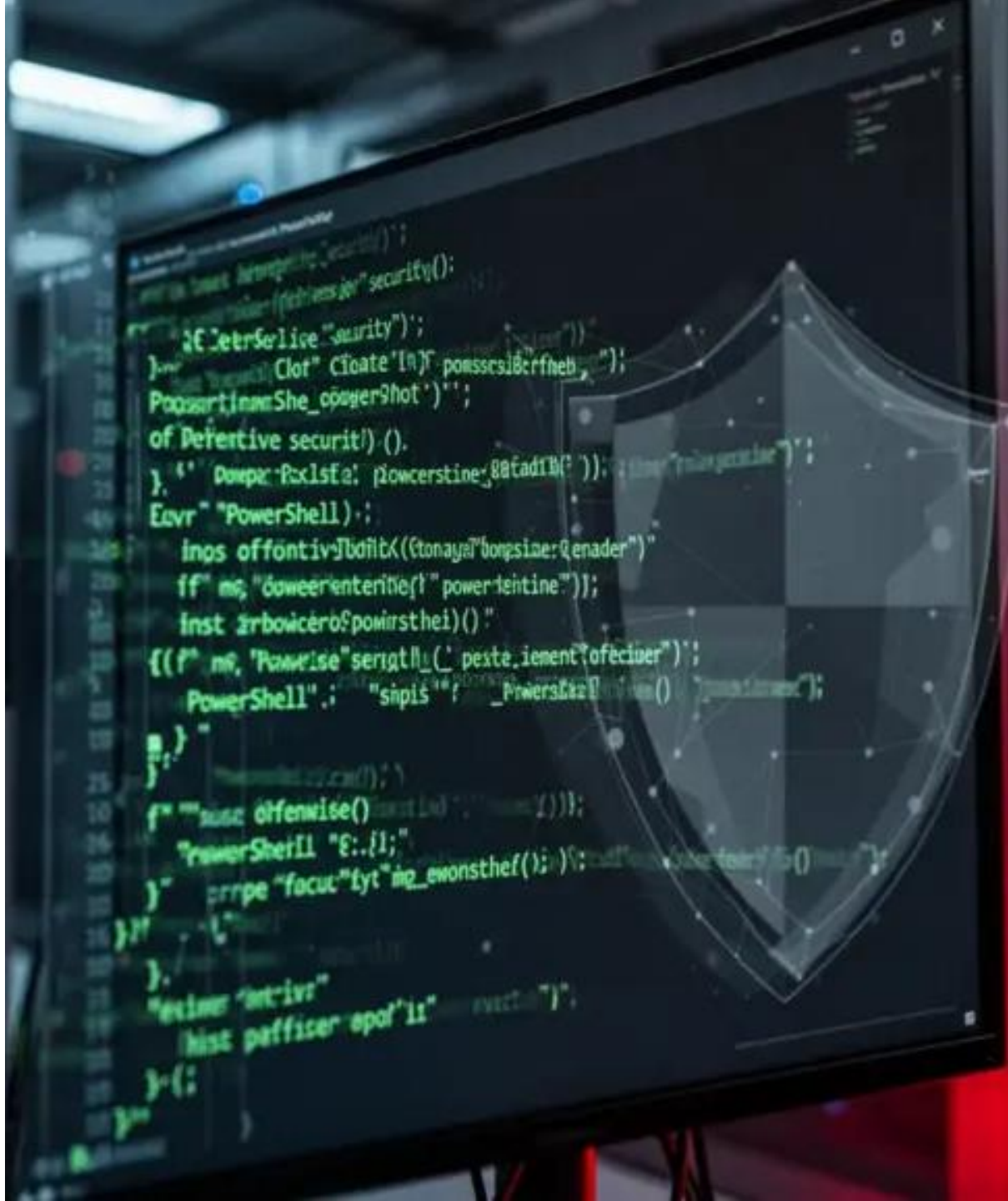
- Cyber Triage (Für die Erstaufnahme)
- Magnet Axiom Cyber
- FTK Imager
- Spezialisierte Hardware mit Writeblocker

ZIEL: *„Vollständige Angriffsrekonstruktion“*

Typische Artefakte eines Angreifers

Woran erkennt man Kompromittierung?

- Ungewöhnliche Powershell-Befehle
- Neue lokale Benutzer
- Verdächtige Scheduled Tasks
- RDP-Anmeldungen nachts
- LSASS-Zugriffe
- RMM-Tools



Herausforderungen im Ernstfall

Technische Herausforderungen:

- Zeitdruck
- Verschlüsselte Systeme
- Fehlende Logs
- Komplexe Infrastruktur

Organisatorische Herausforderungen:

- Kommunikation
- Managementdruck
- Versicherungen
- Datenschutzbehörden
- Kundenkommunikation

„Cybersecurity ist nicht nur IT – sondern Business Continuity“

Wie Unternehmen sich vorbereiten sollten

Technische Maßnahmen:

- MFA Überall
- Netzsegmentierung
- DER/XDR
- Immuntable Backups
- Zentrales Loggin
- PAM-Lösungen

Organisatorische Maßnahmen:

- Incident Response Plan
- Notfallkontakte
- Übungen/Tabletop
- Awareness Trainings
- Externe DFIR-Partnerschaft

Der Faktor Zeit

Warum schnelle Reaktion entscheidend ist

Durchschnittliche Auswirkungen:

- Höhere Kosten bei später Erkennung
- Lange Ausfallzeiten
- Größerer Datenverlust
- Höhere regulatorische Risiken

„Jede Stunde zählt“

Initial Access

Erster erfolgreichen Zugriff eines Angreifers auf ein System oder Netzwerk, z. B. durch Phishing, gestohlene Zugangsdaten oder das Ausnutzen einer Schwachstelle.

Detection

Das Erkennen verdächtiger oder bösartiger Aktivitäten in einem System oder Netzwerk durch Monitoring und Sicherheitsmechanismen.

Encryption

Die Verschlüsselung von Daten durch Angreifer, sodass diese für das Unternehmen unzugänglich werden und meist nur gegen Lösegeld wiederhergestellt werden sollen.

Zukunft von DFIR

Entwicklung und Trends

- KI-gestützte Angriffe
- Living-off-the-Land-Techniken
- Cloud Forensics
- Saas-Kompromittierung
- MDR & Soc as a Service
- Automatisierte Incident Response

Fazit

- Cyberangriffe sind heute eine reale Geschäftsbedrohung
- Prävention allein reicht nicht aus
- Schnelle Reaktion minimiert Schäden
- DFIR schafft Transparenz im Ernstfall
- Vorbereitung entscheidet über den Schaden

„Es geht nicht mehr um die Frage ob – sondern wann ein Sicherheitsvorfall eintritt.“


ho.Systeme

Björn Hagedorn
Teamlead Cyber Security

Kreisstraße 10

33790 Halle (Westf.)

Telefon: 05201 97177 – 337

E-Mail: bjoern.hagedorn@hosysteme.de