Incident Response und Forensik

Das 1x1 der Vorfallsreaktion: Reaktion und Aufklärung nach Cyber-Angriffen

HiSolutions Know-how To Go

Lena Morgenroth

Agenda

1. Möglichkeiten forensischer Analyse im Rahmen von IR
2. Kernpunkte für die Vorbereitung auf den Ernstfall

1. Möglichkeiten forensischer Analyse im Rahmen von IR

Forensik zur Ermittlung des Rollback-Datums

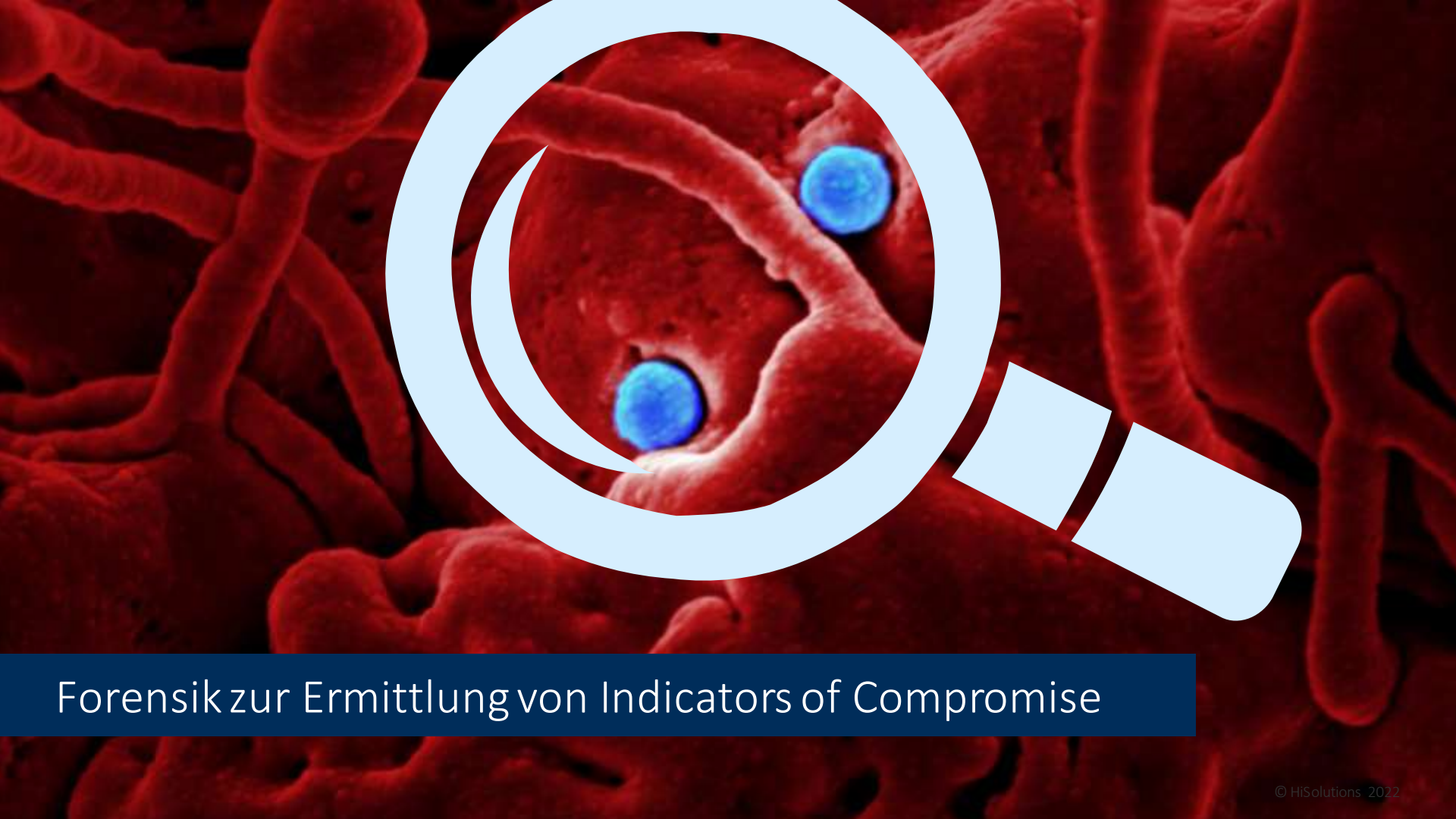
Forensik zur Ermittlung des Rollback-Datums

Mögliches Szenario:

- Ransomware-sicheres Backup mit Sicherungspunkten bis zu 6 Monaten in die Vergangenheit
- Konkreter Verdacht für das Einfallstor: im Internet exponierter RDP-Server
- sicherheitsrelevante Logs der letzten 6 Monate vorhanden

Vorgehen:

- Untersuchung des möglichen „Patient Zero“, der Domain Controller, sowie weiterer ggf. von den Angreifenden zur Rechteausweitung benutzter Systeme
- Rekonstruktion der gesamten Angriffskette vom ersten Zugriff bis hin zur Verschlüsselung
- Ermittlung des Datums des ersten Zugriffs
- Entscheidung: Rollback zu einem Datum vor dem ersten Zugriff der Angreifenden



Forensik zur Ermittlung von Indicators of Compromise

Forensik zur Ermittlung von Indicators of Compromise (IoCs)

Mögliches Szenario:

- Frühzeitige Detektion des Angriffs bei noch laufender Verschlüsselung
- VPN-Verbindungen zu Außenstandorten als Sofortmaßnahme getrennt
- Server an den Standorten teilweise nicht verschlüsselt
- Viele Clients wegen Urlaubszeit länger nicht angeschaltet

Vorgehen:

- Untersuchung von Speicher und Festplattenimages kompromittierter Systeme sowie Logs von Sicherheitssystemen zur Identifikation von IoCs
- Gezielter Scan der Standort-Server und Clients auf fallspezifische, ggf. durch AV-Scanner noch nicht erkannte Spuren von Kompromittierung
- Entscheidung: Weiterbetrieb und Überwachung vs. Neuaufsetzen?

Forensik zur Untersuchung von Datenabfluss

Forensik zur Untersuchung von Datenabfluss

Mögliches Szenario:

- Ransomware wurde identifiziert
- Angreifende sind bekannt dafür, auch mit Veröffentlichung von Daten zu drohen
- Relevante Logs sind für den Angriffszeitraum und einige Zeit in der Vergangenheit vorhanden

Vorgehen:

- Abschätzung abgeflossener Datenmengen anhand von eigenen Netflow-Daten oder Logs des ISP
- Loganalyse zur Ermittlung von Zugriffen auf Daten in Postfächern, Cloud-Anwendungen, etc.
- Untersuchung von Systemen, die durch die Angreifenden verwendet wurden

Suche nach der Stecknadel im Heuhaufen - Nachweis oft nur per Zufallsfund

Grenzen forensischer Analyse

Recht

- Datenschutz
- Geheimschutz
- Vertragliche Regelungen

Fehlende Daten

- Deaktiviertes Logging
- Unzureichendes Logging
- Spuren durch Angreifer verwischt
- Systeme im Wiederanlauf überschrieben

Aufwand/Kosten

- Untersuchung teils mehr Aufwand als Neuaufsetzen
- „Vollständige“ Untersuchung von Systemen zur Freigabe als „nicht kompromittiert“ sehr aufwändig

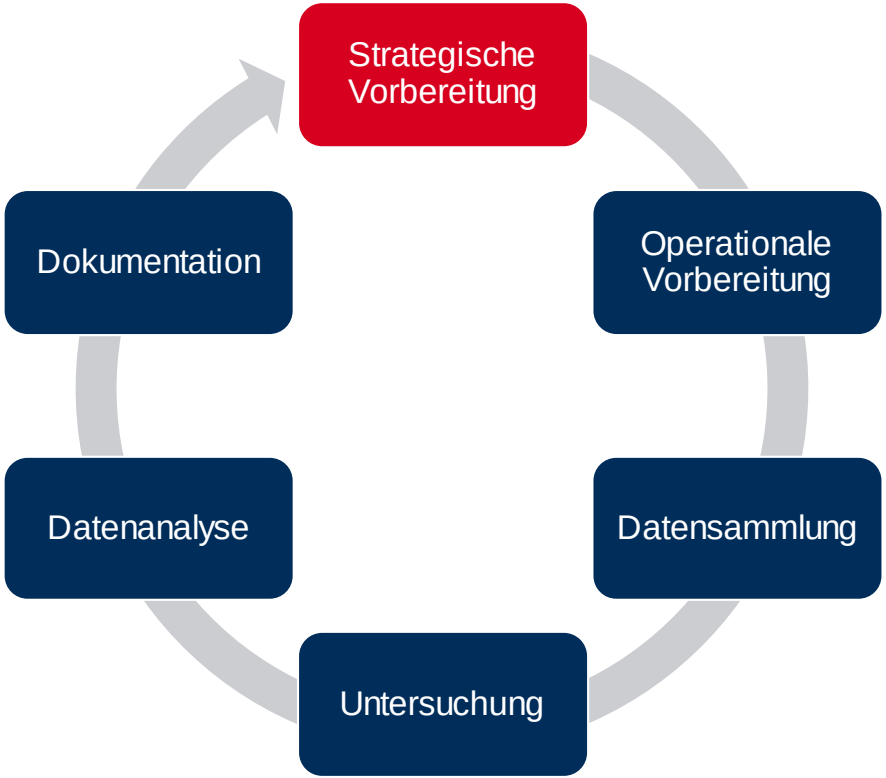
Strategien zur Vorgehensweise: Ermittlungsstrategie

Faktoren, die strategiebestimmend sind:

- Wie kritisch sind die betroffenen Systeme?
- Wichtigkeit der gestohlenen oder beschädigten Daten.
- Wer sind die vermutlichen Täter?
- Ist der Vorfall bereits an die Öffentlichkeit gelangt?
- Wie weit ist der Täter bereits gekommen?
- Welche Skills werden beim Täter vermutet?
- Welche Downtime ist zu verkraften?
- Vermuteter finanzieller Gesamtverlust.

2. Kernpunkte für die Vorbereitung auf den Ernstfall

Forensikprozess nach BSI



5 Kernpunkte für die Vorbereitung auf den Ernstfall

Für den Worst Case planen hilft auch dann, wenn es doch nicht so schlimm kommt.

➔ **Ransomware als Szenario in die Krisen-/Notfallplanung aufnehmen**

Was nicht da ist, kann nicht untersucht werden.

➔ **Cyber-Angriffe und ihre Timelines bei den Protokollierungsvorgaben mitdenken**

Forensik benötigt Entscheidungen und informiert Entscheiderinnen und Entscheider.

➔ **Schnittstellen zum Krisenstab/Notfallstab im Vorfeld klar definieren**

5 Kernpunkte für die Vorbereitung auf den Ernstfall

Jede Klärung im Vorfeld entlastet im Schadensfall.

➔ **Beteiligte und Prozesse für forensische Untersuchungen festlegen, vertragliche Regelungen treffen**

Forensik benötigt spezialisierte Kenntnisse.

➔ **Eigene Expertise aufbauen oder mögliche Dienstleister im Vorfeld identifizieren**

Schloßstraße 1 | 12163 Berlin

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

www.hisolutions.com