

Lehren aus dem Hackerangriff auf die Berliner Verwaltung

Sieben Fragen an Ihre **Angriffserkennung**

Sieben Tage hatte die Ransomware-Gruppe Rhysida Zugriff auf zwei Berliner Senatsverwaltungen. 5,79 Terabyte flossen ab, bevor jemand reagierte. Keine der Ursachen ist Berlin-spezifisch. Prüfen Sie mit dieser Liste, ob Ihre Organisation den Angriff früher gesehen hätte.

So nutzen Sie die Checkliste: Gehen Sie die sieben Fragen gemeinsam mit IT-Leitung und Geschäftsführung durch. Jeder Punkt, den Sie nicht abhaken können, markiert eine Stelle, an der ein Angreifer heute unbemerkt bliebe. Die Auswertung finden Sie auf Seite 2.

1

Sehen wir alles?

Ist jedes Netz und jedes System an unsere Angriffserkennung angebunden, auch Altsysteme, Zukäufe und die IT von Fachabteilungen?

- ☐ Ein vollständiges Inventar aller Netze und Systeme existiert und ist jünger als zwölf Monate.
- ☐ Jedes Segment liefert Logs oder Telemetrie an SOC oder SIEM.
- ☐ Ausnahmen („vorübergehend“) sind dokumentiert, befristet und haben eine verantwortliche Person.

In Berlin: Zwei Senatsverwaltungen waren nie in die zentrale ITDZ-Umgebung migriert. Das seit 2022 bestehende SOC sah ihre Netze nicht.

2

Reicht bei uns ein Passwort?

Ist jeder Fernzugang mit Multi-Faktor-Authentifizierung gesichert: VPN, RDP, Cloud-Konsolen, Admin-Portale, Dienstleisterzugänge?

- ☐ MFA für alle externen Zugänge, ohne Ausnahme für Dienstleister oder Notfallkonten.
- ☐ Kein Klartext-Passwort in Dateien oder Mails, ein Passwortmanager ist für alle Mitarbeitenden im Einsatz.
- ☐ Getrennte Administrationskonten, privilegierte Zugänge laufen über Privileged Access Management.

In Berlin: Rhysida arbeitet mit gestohlenen Zugangsdaten über VPN. Im Netz lag eine Datei „Passwort.docx“ mit Klartext-Passwörtern wie „Sonnenschein13“.

3

Erkennen wir Angriffe mit Bordmitteln?

Schlägt unsere Erkennung an, wenn jemand mit PowerShell, PsExec und Remote Desktop arbeitet, die Active-Directory-Datenbank ausliest und Protokolle löscht?

- ☐ Endpoint Detection and Response mit Verhaltensregeln auf allen Servern und Clients, nicht nur Signaturen.
- ☐ Alarme für ntdsutil, wevtutil, gehäufte Domänenabfragen und neue geplante Aufgaben sind definiert und getestet.
- ☐ Alarme werden rund um die Uhr bewertet, auch nachts und am Wochenende.

In Berlin: Die Gruppe nutzte laut CISA-Advisory AA23-319A ausschließlich Windows-Bordmittel. Kein Virens Scanner schlägt darauf an.

4

Messen wir, was unser Netz verlässt?

Würde uns auffallen, wenn heute Nacht ein Terabyte Daten nach außen fließt?

- ☐ Eine Baseline des normalen ausgehenden Verkehrs je Segment ist vorhanden.
- ☐ Abweichungen bei Volumen, Ziel oder Uhrzeit lösen einen Alarm aus.
- ☐ Network Detection and Response oder Flow-Analyse deckt auch Segmente ohne Agent ab: OT, Altsysteme, Insellösungen.

In Berlin: 5,79 Terabyte in fünf Tagen, rechnerisch mehr als ein Terabyte pro Tag. Ausgewertet hat das niemand.

5

Begrenzt unsere Segmentierung den Schaden?

Kommt ein Angreifer von einem einzelnen Büro-Client aus an Personalakten, Verträge und Notfallpläne?

- ☐ Netzzonen mit kontrollierten Übergängen: Verwaltung, Fachanwendungen, Server, OT.
- ☐ Berechtigungen nach Minimalprinzip, mindestens jährlich rezertifiziert.
- ☐ Datenklassifizierung ist umgesetzt: Vertrauliches liegt getrennt, verschlüsselt und mit eigener Zugriffskontrolle.

In Berlin: Ein Einstieg reichte für eine KRITIS-Analyse der Trinkwasserversorgung, das CBRN-Rahmenkonzept und rund 46.500 Verträge.

6

Können wir reagieren, nicht nur erkennen?

Wer entscheidet um 22 Uhr über eine Netztrennung, und wie schnell passiert sie?

- ☐ Ein Playbook regelt Entscheidungsbefugnis und Ablauf der Isolation, auch außerhalb der Geschäftszeiten.
- ☐ Meldekettens stehen: NIS2 mit Erstmeldung binnen 24 Stunden, Datenschutz binnen 72 Stunden.
- ☐ Krisenkommunikation ist vorbereitet und wurde in den letzten zwölf Monaten geübt.

In Berlin: Zwischen erstem Verdacht und Netztrennung lagen nach Medienberichten bis zu sieben Tage. Am 19. August hieß es „nichts Sensibles“, neun Tage später bestätigte der Senat die Erpressung.

7

Ist unser Security-Budget eine bewusste Risikoentscheidung?

Weiß die Geschäftsleitung, welches Risiko sie mit gestrichenen oder verschobenen Erkennungsmaßnahmen trägt?

- ☐ Risiken aus Budgetentscheidungen sind dokumentiert und von der Leitung gebilligt (§ 38 BSIg).
- ☐ Angriffserkennung ist im Budget geschützt und keine Verschiebemasse.
- ☐ Die Leitung erhält jährlich Kennzahlen zu Erkennungs- und Reaktionszeit.

In Berlin: Im Haushalt 2025 fielen zwei Millionen Euro für die Eindringungserkennung komplett weg. Sachverständige hatten 2023 und 2025 im Innenausschuss gewarnt.

Auswertung: Wie viele Punkte konnten Sie nicht abhaken?

0 bis 3 offen

Sie würden einen Angriff vermutlich früh sehen. Schließen Sie die offenen Punkte in den nächsten 90 Tagen und testen Sie die Erkennung mit einem Red-Team-Szenario.

4 bis 10 offen

Ein Angreifer mit gültigen Zugangsdaten hätte bei Ihnen Tage. Priorisieren Sie Sichtbarkeit aller Netze, MFA für jeden Fernzugang und Alarmer auf ausgehenden Verkehr.

11 oder mehr offen

Sie stehen dort, wo Berlin am 7. August 2026 stand. Klären Sie zuerst, wer im Ernstfall die Netztrennung anordnet, dann die Erkennung.

Wissen Sie, was in Ihrem Netz gerade passiert?

Wir prüfen gemeinsam mit Ihnen, welche Systeme heute außerhalb Ihrer Angriffserkennung liegen und wie Sie die Zeit bis zur Reaktion auf Stunden verkürzen.

Die vollständige Analyse des Berliner Falls lesen Sie auf axians-secure.de/blog.

Gespräch vereinbaren