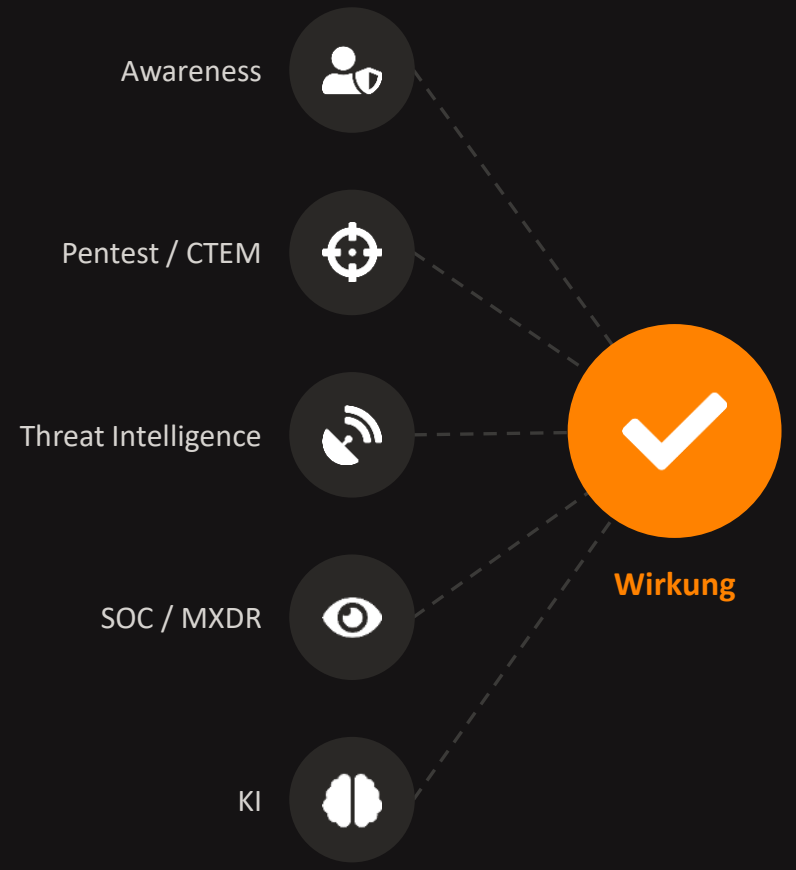
CYBER SAMURAI
WE SERVE AND PROTECT

CYBER DEFENSE HORIZONS 2026

Vom Signal zur Wirkung

Wie aus Security-Bausteinen belastbare Abläufe werden



Gerd Boving
Geschäftsführer, Cyber Samurai GmbH

AKTUELLER FALL · BERLINER LANDESVERWALTUNG

Der Angriff war leise. Die Folgen sind laut.

5 Tage

unbemerkter Datenabfluss

7. – 12. August 2026

≈ 5,8 TB

Daten im Darknet veröffentlicht

1,44 Mio. Dateien (Angabe der Täter)

1

Betriebsstörung als erster Hinweis

Domain Controller – kein Security-Alarm

Betroffen: zwei Senatsverwaltungen (Stadtentwicklung · Mobilität/Verkehr). Laut Berichten u. a. Personaldaten, Verträge, Passwörter und Unterlagen mit KRITIS-Bezug.

Quellen: berlin.de, Berliner Datenschutzbeauftragte, heise online, Security-Insider (Stand 01.10.2026). ***Täterangaben nicht unabhängig verifiziert.***

CHRONOLOGIE

Zwischen Abfluss und Erkennung liegt die Lücke

Erkennungslücke Isolation erst 2 Tage nach Ende des Abflusses

7.–12.08.
Datenabfluss läuft verdeckt

13.08.
Störung am Domain Controller – CERT prüft

14.08.
Zwei Senatsverwaltungen vom Landesnetz getrennt

Mitte Aug.
Rhysida bekennt sich, fordert 30 BTC (≈ 2 Mio. €)

28.08.
„Berlin lässt sich nicht erpressen“

04.09.
Daten im Darknet veröffentlicht

Seitdem: Passwortwechsel, Prüfung von rund 12.000 Systemen, Steuerungseinheit zur Information Betroffener (ab 06.09.)

Quellen: berlin.de, heise online, Security-Insider, eGovernment (Stand 01.10.2026).

ANATOMIE DES ANGRIFFS

Fünf Schritte – fünf verpasste Signale – Mögliches Angriffsszenario

01

Erstzugang

Phishing-Mail; Nutzer führt per „ClickFix/TerminalFix“ selbst Befehl aus

Verpasstes Signal
Mitarbeitende melden nicht

02

Zugangsdaten

Klartext-Passwörter in Dokumenten und im Quelltext von Fachverfahren

Verpasstes Signal
Kein Credential-Hunting

03

Bewegung

Anmeldung mit gültigen Konten – kein Einbruch nötig

Verpasstes Signal
Anomalie nicht erkannt

04

Exfiltration

Terabytes über mehrere Tage aus dem Netz geleitet

Verpasstes Signal
Kein Volumenalarm

05

Erkennung

Aufgefallen über Betriebsstörung, nicht über Detection

Verpasstes Signal
Kein 24/7-Monitoring

Darstellung nach öffentlich bekannten Informationen (BSI, Tagesspiegel, Security-Insider, ad-hoc-news); Ermittlungen laufen, Details können sich ändern.

DIE EIGENTLICHE LEHRE

Nichts an diesem Angriff war neu

Nov. 2023	FBI / CISA / MS-ISAC warnen vor Rhysida: Regierungsstellen als Ziel, Erstzugang über gültige Zugangsdaten, Gegenmaßnahmen benannt.
2025	„ClickFix“ öffentlich beschrieben: gefälschte Fehlermeldung, Nutzer startet den Schadcode selbst.
Sep. 2026	BSI ordnet die Variante „TerminalFix“ dem Berliner Fall zu.

Das Wissen war da.

Es fehlte die Verbindung.

- Signal
- Maßnahme
- Verantwortung
- Nachweis

Quellen: CISA Advisory AA23-319A (aktualisiert 2025), Expel (Okt. 2025), BSI via Security-Insider (18.09.2026).

ZUSAMMENSPIEL

Jeder Schritt war von mindestens zwei Disziplinen abdeckbar

	Erstzugang	Zugangsdaten	Bewegung	Exfiltration	Erkennung
Awareness	●	○			○
Pentest / CTEM	○	●	●	○	○
Threat Intelligence	●	●	○	○	○
SOC / MXDR	○	○	●	●	●
KI	○		○	○	●

● primäres Signal ○ unterstützendes Signal

Einzeln hat jede Disziplin blinde Flecken. Zusammen entsteht ein Netz.

DIE REALITÄT

Fünf Disziplinen. Fünf Reports. Null Wirkung?

- **Awareness-Report** geht an HR / ISB
- **Pentest-PDF (80 Seiten)** liegt in der IT – nächstes Jahr dieselben Findings
- **Threat-Intel-Feed** läuft in ein ungelesenes Postfach
- **SOC-Tickets** ohne Wissen über offene Schwachstellen
- **KI-Pilot** im Innovation Lab, ohne Bezug zum Betrieb

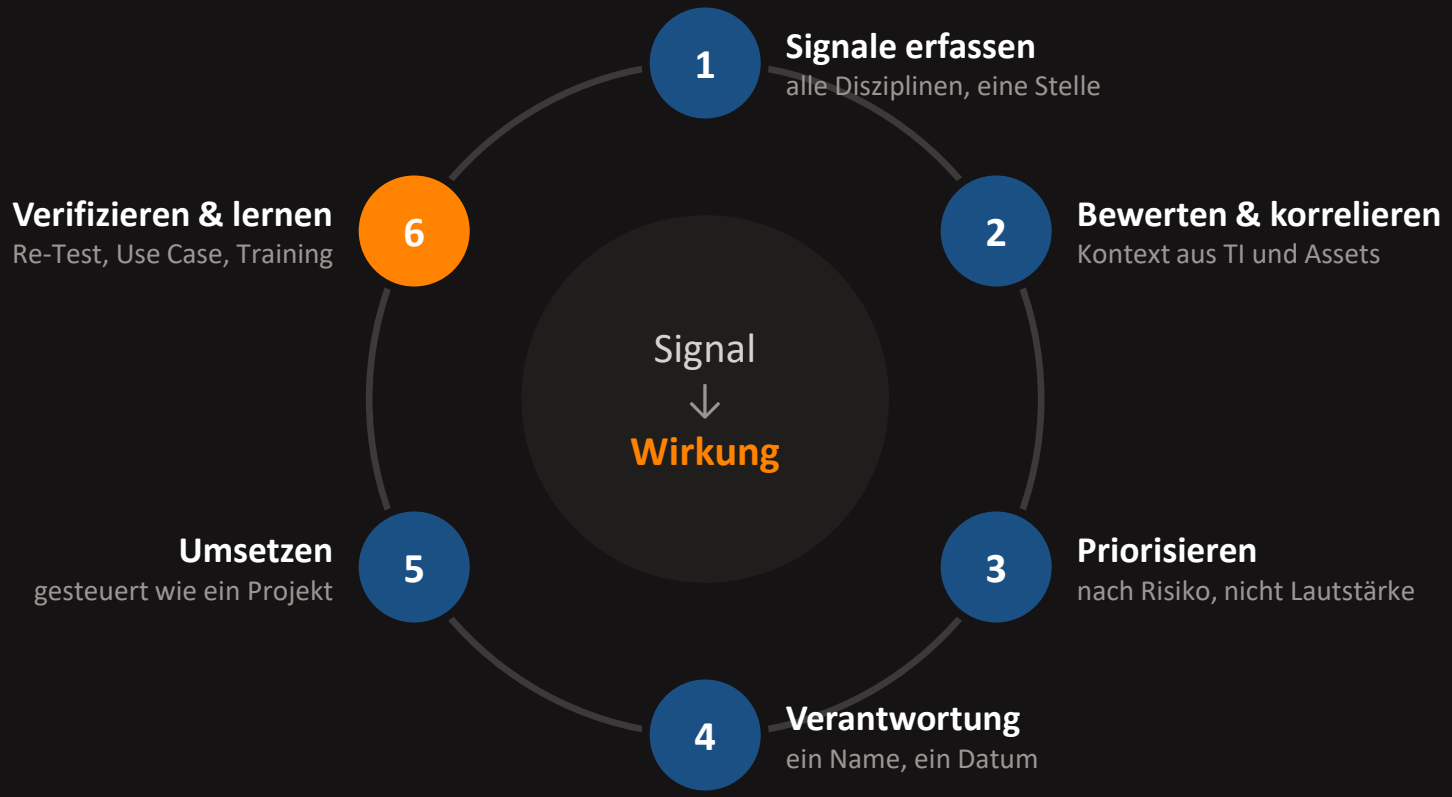
Die Folge

- ✕ keine gemeinsame Priorisierung
- ✕ keine klaren Owner
- ✕ keine Nachverfolgung
- ✕ kein Nachweis der Wirkung

Signale ohne Wirkung sind teure Dokumentation.

DAS CYBER-SAMURAI-MODELL

Der Wirkungskreislauf



Was den Unterschied macht

Ein Backlog
Findings aus Awareness, Pentest, TI und SOC in einer Liste

Ein Steuerungsboard
Status, Owner und Fristen für alle sichtbar

Eine Sicht
Management-Reporting mit Wirkungs-KPIs

GEDANKENEXPERIMENT

Derselbe Angriff – im verbundenen Modell

1

Threat Intelligence

Warnung: Rhysida nutzt ClickFix gegen Behörden → Ticket im Backlog

2

Awareness

Gezielte ClickFix-Simulation + Melde-Button; Meldungen gehen ins SOC

3

Pentest / CTEM

Credential-Hunting & MFA-Check; Fix mit Owner, danach Re-Test

4

SOC / MXDR

Use Cases: Kommandozeile, PowerShell, Upload-Volumen

5

KI + Analyst

KI korreliert Meldung, Shell und Upload – Analyst dämmt ein

Ziel: Erkennung nicht erst nach Tagen – Abfluss stoppen, bevor er Terabytes erreicht.

PRIORISIERUNG

Nach Wirkung priorisieren – nicht nach Score

Ausnutzbarkeit
Wie leicht kommt ein Angreifer daran?

Geschäftswirkung
Was steht still, was fließt ab?

Bedrohungsrelevanz
Nutzen relevante Gruppen das gerade aus?

CVSS allein ist kein Prioritätsmaß.



VERANTWORTLICHKEITEN

Ein Name pro Maßnahme

Aufgabe	Geschäfts-führung	CISO / ISB	IT-Betrieb	Fach-bereiche	Cyber Samurai
Risikoakzeptanz & Budget	A	R	I	C	C
Backlog priorisieren	I	A	C	C	R
Technische Umsetzung	I	A	R	I	C
Detection & Response 24/7	I	A	C	I	R
Awareness-Kampagnen	I	A	I	C	R
Re-Test & Wirkungsnachweis	I	A	C	I	R

Beispielhafte Rollenverteilung – wird je Kunde im Kick-off festgelegt.

Legende

- **A** Accountable – entscheidet
- **R** Responsible – führt aus
- **C** Consulted – berät
- **I** Informed – wird informiert

NIS2: Die Leitung billigt Risikomanagement-Maßnahmen und überwacht ihre Umsetzung (§ 20 Abs. 1 NIS-2-Richtlinie).

STEUERUNG

Ein Rhythmus. Wenige, ehrliche Kennzahlen.

Wöchentlich
Ops-Sync SOC · IT · ISB

Monatlich
Security Steering: Backlog & Fristen

Quartalsweise
Management-Review für die GF

MTTD
Zeit bis zur Erkennung

Melderate
Phishing-Simulationen gemeldet

Use-Case-Abdeckung
relevante Angriffstechniken detektierbar

MTTR
Zeit bis zur Eindämmung

Time-to-Fix
Offene Tage kritischer Findings

Closed-Loop-Quote
Findings per Re-Test geschlossen

Die Closed-Loop-Quote misst nicht Aktivität, sondern Wirkung.

KÜNSTLICHE INTELLIGENZ

KI ist Verstärker – kein Autopilot

Wo KI hilft

Triage & Korrelation
Alarme sortieren, Zusammenhänge erkennen

Übersetzen
Technik in Management-Sprache zusammenfassen

Priorisierungsvorschläge
Findings mit TI-Kontext anreichern

Awareness
Inhalte zielgruppengerecht aufbereiten

Leitplanken

Mensch entscheidet
über Maßnahmen, Systemeingriffe und Personen

Nachvollziehbar
Empfehlungen begründet und fachlich geprüft

Datenhoheit
klar geregelt, welche Daten in welche KI dürfen

Protokolliert
Logging und Kontrolle bei automatisierten Aktionen

AB MONTAG

Fünf Maßnahmen ohne Großprojekt

1. **MFA für jeden Fernzugang** — ohne Ausnahmen – auch für Dienstleister
2. **Kommandozeile & PowerShell protokollieren** — zentral & lange genug aufbewahren
3. **Alarm auf ausgehendes Datenvolumen** — Terabytes über Tage sind kein Rauschen
4. **Klartext-Passwörter suchen & entfernen** — Dateiablagen, Wikis, Skripte, Quelltext
5. **Melde-Button + ClickFix-Awareness** — jede Meldung landet beim SOC

Für alle fünf gilt:

Ein Verantwortlicher.
Ein Datum.
Ein Re-Test.

CYBER SAMURAI

Signale haben Sie genug.

Sorgen wir für Wirkung.

Awareness · Pentesting & CTEM · Threat Intelligence · SOC / MXDR · KI – gesteuert aus einer Hand.

Gerd Boving
Geschäftsführer · Cyber Samurai GmbH
gerd.boving@cyber-samurai.net

Informationssicherheit ISO/IEC 27001