VAPS Applied Security

WHITEPAPER · 16 MASSNAHMEN, JEDE MIT BELEG

Sicherheit ist kein Bauchgefühl.
Das hier ist der Beweis.

Für jede der 16 wichtigsten Sofortmaßnahmen zeigen wir, welches konkrete Risiko sie schließt – belegt mit einer öffentlich prüfbaren Quelle – überwiegend vom BSI, vom BKA und aus Gesetzen. Keine Framework-Folklore, keine gefühlte Priorität.

- **8 technische Stellschrauben**
- **8 organisatorische Regeln ohne zusätzliches Tool**
- **Kurz-Check von außen, ohne Systemzugriff**

202,4 Mrd. €
geschätzter Schaden für die deutsche Wirtschaft 2025
Quelle: BKA, Bundeslagebild Cybercrime 2025

1.041
angezeigte Ransomware-Angriffe 2025, 10 % mehr als im Vorjahr
Quelle: BKA, Bundeslagebild Cybercrime 2025

119
neue Schwachstellen pro Tag, 24 % mehr als im Vorjahr
Quelle: BSI, Die Lage der IT-Sicherheit in Deutschland 2025

Jetzt Lücken finden – bevor es andere tun

AUSGANGSLAGE

Warum genau diese 16 Maßnahmen

Ransomware trifft laut BKA vor allem Unternehmen und öffentliche Einrichtungen. Die folgenden 16 Maßnahmen orientieren sich überwiegend an Empfehlungen des BSI. Wo nur Herstellerdokumentation oder keine Behördenquelle existiert, ist das gekennzeichnet.

119

neue Schwachstellen pro Tag im Berichtszeitraum Juli 2024 bis Juni 2025

Quelle: BSI, Die Lage der IT-Sicherheit in Deutschland 2025

4,5 %

des Bruttoinlandsprodukts entspricht der geschätzte Schaden durch Cyberkriminalität 2025

Quelle: BKA, Bundeslagebild Cybercrime 2025

+10 %

mehr angezeigte Ransomware-Angriffe 2025 als im Vorjahr

Quelle: BKA, Bundeslagebild Cybercrime 2025

TECHNISCHE MASSNAHMEN

Acht technische Stellschrauben

01

MFA / PASSWORDLESS

Das Passwort allein reicht nicht

Das BSI empfiehlt Zwei-Faktor-Authentisierung für Fernzugänge (VPN) und immer für privilegierte Konten.

Quelle: BSI, Top 10 Ransomware-Maßnahmen (Nr. 2 und 6)

02

LEGACY-AUTH BLOCKIEREN

Die Hintertür, die niemand abgeschlossen hat

Veraltete Anmeldeprotokolle unterstützen keine Mehr-Faktor-Authentisierung und umgehen den zweiten Faktor.

Quelle: Microsoft Learn, Conditional Access (Herstellerdokumentation, keine Behördenquelle)

03

AUTOMATISCHES PATCH-MANAGEMENT

Ungepatcht ist ein Haupteinfallstor

Laut BSI zählt die Ausnutzung meist schon behobener Schwachstellen zu den drei häufigsten Ransomware-Einstiegswegen.

Quelle: BSI, Top 10 Ransomware-Maßnahmen (Nr. 1)

04

SPF / DKIM / DMARC

Drei Standards gegen gefälschte Absender

Das BSI empfiehlt Unternehmen mit eigener Domain SPF, DKIM und DMARC gegen gefälschte Absenderidentitäten – ohne Mehrfacheinträge im DNS.

Quelle: BSI-CS 155 „Upgrade für die E-Mail-Sicherheit“, Version 1.00 vom 05.05.2025

05

ADMIN-KONTEN TRENNEN

Das Kronjuwel ist auch der Köder

Das BSI rät: Admin-Konten nur für Administration nutzen, nicht für E-Mail und Surfen – dafür gibt es normale Benutzerkonten.

Quelle: BSI, Top 10 Ransomware-Maßnahmen (Nr. 6)

06

BACKUP (OFFLINE)

Ein Backup, das der Angreifer nicht erreicht

Laut BSI ist ein Offline-Backup, das nach der Sicherung vom Netz getrennt wird, die wichtigste Vorsorge – Wiederherstellung praktisch testen.

Quelle: BSI, Top 10 Ransomware-Maßnahmen (Nr. 8)

07

ZUGRIFFSRECHTE-REVIEW

Rechte regelmäßig auf Bedarf prüfen

Der IT-Grundschutz verlangt, die Dokumentation der Benutzer, Benutzergruppen und Rechteprofile regelmäßig zu überprüfen.

Quelle: BSI, IT-Grundschutz-Kompendium, ORP.4.A2

08

NETZWERK SEGMENTIEREN

Schäden auf ein Segment begrenzen

Laut BSI begrenzt starke Netzwerksegmentierung den Schaden: Ransomware erreicht nur die Systeme in unmittelbarer Nähe.

Quelle: BSI, Top 10 Ransomware-Maßnahmen (Nr. 7)

ORGANISATORISCHE MASSNAHMEN

Acht Regeln ohne zusätzliches Tool

09

EIN-SEITEN-NOTFALLPLAN

Ein Blatt Papier, wenn alles verschlüsselt ist

Das BSI empfiehlt Notfallplanung für den Worst Case: Abläufe regelmäßig üben, Kontakte und Telefonnummern auf Papier vorhalten.

Quelle: BSI, Top 10 Ransomware-Maßnahmen (Nr. 10)

10

MELDEWEGE OHNE ANGST

Melden darf keine Angst machen

Phishing ist laut BSI seit Jahren eines der häufigsten Einfallstore. Wer weiß, wohin er meldet, und nichts fürchten muss, meldet früher.

Quelle: BSI, Lage der IT-Sicherheit in Deutschland 2025 (Phishing); Empfehlung: VAPS

11

PASSPHRASEN STATT SONDERZEICHEN

Länger schlägt komplizierter

Der IT-Grundschutz rät von zeitgesteuerten Passwortwechseln ab. Laut LfD Niedersachsen zählt die Länge mehr als der Zeichenvorrat.

Quelle: BSI, ORP.4.A22 und ORP.4.A23; LfD Niedersachsen, Passwort-Handreichung

12

ONBOARDING-/OFFBOARDING-CHECKLISTE

Der Austritt gehört in eine Checkliste

Der IT-Grundschutz regelt Einstellung und Austritt (ORP.2) und den Entzug von Berechtigungen (ORP.4.A2). Das LSI Bayern bietet eine Checkliste.

Quelle: BSI, ORP.2 und ORP.4.A2; LSI Bayern, Checkliste Personalwechsel

13

ROLLEN & ANSPRECHPARTNER

Im Ernstfall zählt jede Minute Klarheit

Das BSI empfiehlt, wichtige Telefonnummern und Ansprechpartner für den Ernstfall vorab festzulegen und offline vorzuhalten.

Quelle: BSI, Top 10 Ransomware-Maßnahmen (Nr. 10)

14

MICRO-LEARNING

Wissen, das im Alltag ankommt

Das BSI empfiehlt, Mitarbeitende praktisch zu E-Mail-Risiken zu schulen. Kurze, regelmäßige Lerneinheiten sind unsere Umsetzungsempfehlung.

Quelle: BSI, Top 10 (Nr. 3) und ORP.3; Umsetzungsform: VAPS

15

NDA

Vertraulichkeit schriftlich regeln

Personalsicherheit ist Teil des IT-Grundschutzes (ORP.2). Verschwiegenheit schriftlich regeln – Ausgestaltung mit Rechtsberatung klären.

Quelle: BSI, IT-Grundschutz-Kompendium, ORP.2 Personal; Handlungsempfehlung: VAPS

16

DATENSCHUTZ

72 Stunden – ab Kenntnis läuft die Uhr

Datenpannen sind unverzüglich, möglichst binnen 72 Stunden nach Kenntnis, zu melden. Datenschutzbeauftragter in der Regel ab 20 Beschäftigten mit Datenverarbeitung.

Quelle: Art. 33 Abs. 1 DSGVO; § 38 Abs. 1 BDSG

NÄCHSTER SCHRITT

16 Maßnahmen kennen ist der erste Schritt. Sie umsetzen der zweite.

Der Kurz-Check zeigt in wenigen Tagen, wie Sie bei genau diesen Punkten heute stehen – von außen, ohne Systemzugriff, ohne Vorlaufzeit.

BAUSTEIN 1

Kurz-Check

Passiver Außenblick auf Ihre Angriffsfläche – MFA-Lücken, offene Legacy-Auth, fehlendes DMARC inklusive.

BAUSTEIN 2

Deep Scan

Tiefergehende Prüfung Ihrer Umgebung – über den Außenblick des Kurz-Checks hinaus.

BAUSTEIN 3

Assessment

Strukturierte Bewertung Ihrer organisatorischen Sicherheitsmaßnahmen – Ampel-Reporting statt Bauchgefühl.

BAUSTEIN 4

ISaaS Information Security as a Service

Kontinuierliche Unterstützung, fester Beratungsrahmen, monatlicher aktiver Sicherheitsscan und jährliche Prüfung Ihrer Baseline.

Bei Fragen wenden Sie sich an sales@vaps.de