CYBER-NOTFALL · SOFORTMASSNAHMEN

Die ersten 60 Minuten

Ransomware, gehacktes Postfach, kompromittierter Server — der Notfallplan für Unternehmen ohne eigene IT-Abteilung

Bevor Sie irgendetwas tun

Nicht herunterfahren. Nicht neu starten. Nichts selbst „aufräumen“. Ein Neustart vernichtet flüchtige Spuren im Arbeitsspeicher, die später darüber entscheiden können, wie der Angreifer hereinkam — und in seltenen Fällen sogar, ob Daten wieder entschlüsselt werden können. Trennen Sie das Gerät vom Netz, aber lassen Sie es eingeschaltet.

MIN 0–5 Ausbreitung stoppen

- [ ] Netzwerkkabel ziehen bzw. WLAN am betroffenen Gerät deaktivieren — **Gerät eingeschaltet lassen**
- [ ] Externe Festplatten, USB-Medien und NAS/Backup-Systeme **physisch trennen** — *sonst werden sie mitverschlüsselt*
- [ ] VPN-Zugänge und Fernwartungszugänge (RDP, TeamViewer, AnyDesk) zentral deaktivieren
- [ ] Niemand meldet sich neu an betroffenen Systemen an — auch nicht „kurz zum Nachschauen“
- [ ] Ist ein Server betroffen: prüfen, ob weitere Systeme im selben Netz auffällig sind, bevor Sie diese anfassen

MIN 5–15 Zuständigkeit klären, Hilfe holen

- [ ] **Geschäftsführung sofort informieren** — *Abschalt- und Zahlungsentscheidungen sind Chefsache, auch haftungsrechtlich*
- [ ] **Eine Person** als Notfallleitung benennen. Alle Informationen laufen dort zusammen
- [ ] IT-Dienstleister anrufen (Nummer auf Seite 2)
- [ ] **Cyber-Versicherung anrufen, BEVOR Sie externe Dienstleister beauftragen** — *viele Policen verlangen eigene Partner; eigenmächtige Beauftragung kann die Deckung kosten*
- [ ] Ab jetzt: **jede Maßnahme mit Uhrzeit notieren** — auf Papier, nicht im betroffenen System

MIN 15–30 Beweise sichern, nicht reparieren

- [ ] Mit dem Handy fotografieren: Erpresserbildschirm, Fehlermeldungen, ungewöhnliche Fenster, Dateiendungen
- [ ] Betroffene Geräte eingeschaltet und unangetastet lagern, Zugang beschränken
- [ ] Backups prüfen — **nur von einem sauberen, nicht verbundenen Gerät aus**
- [ ] Von einem sauberen Gerät die Passwörter der zentralen Konten ändern: E-Mail-Administration, Cloud/Microsoft 365, Online-Banking, Domain-Verwaltung
- [ ] Nicht zahlen, nicht mit den Angreifern kommunizieren — erst nach Rücksprache mit Versicherung, Dienstleister und Polizei
- [ ] Bei Verdacht auf Kontozugriff: Bank informieren und Zahlungen prüfen — *Rechnungsbetrug folgt oft auf gehackte Postfächer*

MIN 30–60 Die rechtlichen Fristen laufen bereits

- [ ] **Sind personenbezogene Daten betroffen?** Kunden-, Mitarbeiter-, Bewerber-, Gesundheits- oder Zahlungsdaten — auch bloßer Zugriff ohne Abfluss zählt
- [ ] Wenn ja: Meldung an die zuständige **Landesdatenschutzbehörde binnen 72 Stunden ab Kenntnis** (Art. 33 DSGVO). Die Frist läuft ab dem Moment, in dem Sie den Vorfall bemerkt haben — nicht ab Feierabend
- [ ] Bei hohem Risiko für die Betroffenen: zusätzlich **die Betroffenen selbst informieren** (Art. 34 DSGVO)
- [ ] **NIS2 prüfen:** seit 06.12.2025 in Kraft, gilt aber nur für bestimmte Sektoren ab ca. 50 Mitarbeitern oder 10 Mio. € Umsatz. Falls betroffen: **Frühwarnung an das BSI binnen 24 Stunden**. Die meisten kleinen Betriebe fallen nicht darunter — die DSGVO-Pflicht gilt trotzdem
- [ ] Strafanzeige bei der **ZAC** (Zentrale Ansprechstelle Cybercrime) des jeweiligen Bundeslandes
- [ ] Mitarbeiter informieren: was zu tun ist **und** was nicht — keine Auskünfte nach außen, keine Posts, keine Weiterleitung verdächtiger Mails

Kevin Westmeier · westmeier.cloud · kevin@westmeier.cloud — Notfallblatt zum Ausfüllen auf Seite 2.

Ihr Notfallblatt

Ausfüllen, ausdrucken, aushängen — ein Notfallplan, den man erst im Notfall sucht, ist keiner.

Wen rufen wir an?

Diese Nummern müssen auch dann verfügbar sein, wenn kein einziges Firmensystem mehr läuft. Ausgedruckt, nicht nur im Handy.

ROLLE	NAME / ORGANISATION	TELEFON
Notfallleitung intern		
Stellvertretung		
IT-Dienstleister Auch außerhalb der Geschäftszeiten?		
Cyber-Versicherung Schadenshotline + Policennummer		
Datenschutzbeauftragte/r		
Rechtsanwalt / Kanzlei		
ZAC Polizei (Bundesland)		
Bank — Sperrhotline		
Wichtigste Kunden / Lieferanten		

Fünf Fragen, die Sie heute klären sollten — nicht im Notfall

Wenn Sie diese fünf Punkte beantworten können, sind Sie besser aufgestellt als die meisten Betriebe Ihrer Größe.

- ☐ **Wo liegt unser letztes Offline-Backup — und wann wurde zuletzt eine Rücksicherung getestet?**
  Ein Backup, das nie zurückgespielt wurde, ist kein Backup, sondern eine Hoffnung. Mindestens eine Kopie muss dauerhaft vom Netz getrennt sein.
- ☐ **Wer darf entscheiden, dass Systeme abgeschaltet werden — auch nachts und am Wochenende?**
  Wenn diese Frage erst im Ernstfall gestellt wird, vergehen im Schnitt die teuersten 30 Minuten des Vorfalls.
- ☐ **Haben wir eine Cyber-Versicherung — und was genau verlangt sie von uns im Schadensfall?**
  Meldefristen, vorgeschriebene Dienstleister und Dokumentationspflichten stehen in der Police, nicht im Internet.
- ☐ **Kommen wir an unsere Kunden- und Mitarbeiterkontakte, wenn alle Systeme verschlüsselt sind?**
  Ohne Kontaktdaten können Sie weder Betroffene informieren noch Ihr Geschäft am Laufen halten.
- ☐ **Wer spricht mit Kunden, Mitarbeitern und ggf. der Presse — und mit welcher Botschaft?**
  Schweigen und widersprüchliche Aussagen richten regelmäßig mehr Schaden an als der Angriff selbst.

> **Der häufigste Fehler:** Der Notfallplan liegt als Datei auf demselben Server, der gerade verschlüsselt wurde. Drucken Sie dieses Blatt aus und legen Sie es dorthin, wo es auch ohne Strom und ohne Netzwerk auffindbar ist.

Kevin Westmeier
IT-Administrator für Windows- und Linux-Serverumgebungen · Netzwerksicherheit
westmeier.cloud · kevin@westmeier.cloud