NOTFALLKARTE · SICHERHEITSVORFALL

Cyberangriff: Erste Hilfe

Ruhe bewahren. Diese Karte Schritt für Schritt abarbeiten. Ausdrucken, laminieren, sichtbar aufhängen.

Phase 01 — Sofort stoppen

Minute 0 bis 15

1. **Befallene Geräte vom Netz trennen.** Netzwerkkabel ziehen, WLAN aus. **Nicht ausschalten**, im Arbeitsspeicher liegen Spuren.
2. **Kein Lösegeld zahlen.** Und keine weiteren Aktionen auf den befallenen Systemen ausführen.
3. **Nicht selbst aufräumen.** Veränderte oder gelöschte Dateien erschweren die Spurensicherung.

Phase 02 — Sichern und dokumentieren

Erste Stunde

4. **Alles fotografieren oder notieren.** Fehlermeldungen, Bildschirminhalte, Zeitpunkt des ersten Auffindens.
5. **Kritische Systeme prüfen.** Welche sind noch sauber? Sind die Backups isoliert und zugriffsgeschützt?
6. **Zugangsdaten ändern**, und zwar auf nicht befallenen Geräten: E-Mail, Admin-Konten, VPN.

Phase 03 — Melden und kommunizieren

Erste 24 Stunden

7. **Internen Krisenstab aktivieren.** CISO, IT-Leitung und Geschäftsführung informieren, jetzt, nicht morgen.
8. **BSI melden**, sofern meldepflichtig. Erstmeldung über das Meldeportal, Zugangsdaten vorher sichern.
9. **Externe Notfallhilfe rufen.** Forensik und, wenn nötig, Anwalt einschalten, bevor kommuniziert wird.

Phase 04 — Wiederherstellung

Erst nach der Analyse

10. **Erst wiederherstellen, wenn der Angriff verstanden ist.** Backup auf geprüfter Hardware einspielen, nicht auf demselben System.

MELDEFRISTEN NACH § 32 BSIG

24 h	72 h	1 Monat
Erstmeldung	Folgemeldung	Abschlussbericht

Die Frist läuft ab dem Moment der Kenntniserlangung, nicht ab dem Abschluss der Analyse. Im Zweifel höher einstufen, die Herabstufung in der Folgemeldung ist jederzeit möglich.

Notfallkontakte

Vor dem Ernstfall ausfüllen. Diese Liste muss auch ohne IT-Zugang erreichbar sein.

IT-Notfalltelefon intern		**Forensik-Dienstleister**	
IT-Leitung / CISO		**Rechtsanwalt (IT-Recht)**	
Geschäftsführung		**Cyberversicherung**	
Datenschutzbeauftragter		**BSI Lagezentrum**	+49 228 9582-444 (24/7)