NOTFALL · CHECKLISTE

Die erste Stunde. Minute für Minute vorbereitet.

Ein Sicherheitsvorfall beginnt selten zur Bürozeit. Diese Checkliste gibt der ersten Stunde eine feste Struktur – unabhängig davon, ob es Ransomware, ein kompromittiertes Konto oder ein Datenabfluss ist. Vorher ausfüllen, im Ernstfall abarbeiten.

VORHER AUSFÜLLEN	IM ERNSTFALL	ZIEL DER STUNDE
Namen, Nummern und Vertretungen im Kasten unten eintragen	Von oben nach unten abarbeiten, Uhrzeiten mitschreiben	Lage klären, Ausbreitung stoppen, Fristen nicht verlieren

VOR DEM ERNSTFALL AUSFÜLLEN

INCIDENT LEAD (NAME / MOBIL) .....

VERTRETUNG (NAME / MOBIL) .....

IT-NOTFALL EXTERN (NUMMER) .....

GESCHÄFTSLEITUNG (NAME / MOBIL) .....

DATENSCHUTZ (NAME / MOBIL) .....

KOMMUNIKATION (NAME / MOBIL) .....

T+0 bis T+5 Melden und bestätigen

UHRZEIT

- [ ] **Uhrzeit der Kenntnisnahme notiert** – ab hier laufen alle gesetzlichen Fristen
- [ ] **Erste Plausibilitätsprüfung:** echter Vorfall oder Fehlalarm
- [ ] **Meldung an den Incident Lead** über die hinterlegte Nummer, nicht per E-Mail
- [ ] **Kein Alleingang:** keine Systeme abschalten, keine Dateien löschen, nichts „schnell reparieren“

T+5 bis T+15 Krisenstab und Rollen aktivieren

UHRZEIT

- [ ] **Krisenstab einberufen** – physisch oder über einen Kanal außerhalb der betroffenen Umgebung
- [ ] **Protokoll eröffnet** – jede Entscheidung mit Uhrzeit und verantwortlicher Person
- [ ] **Rollen zuweisen:** Leitung, Technik, Kommunikation, Recht und Datenschutz, Protokoll
- [ ] **Externe Unterstützung alarmiert**, wenn eigene Kapazität oder Forensik-Erfahrung fehlt

T+15 bis T+30 Eindämmen, ohne Spuren zu zerstören

UHRZEIT

- [ ] **Betroffene Systeme isolieren** – vom Netz trennen, aber eingeschaltet lassen
- [ ] **Backups vom Netz nehmen** und gegen Löschung schützen
- [ ] **Kompromittierte Konten sperren** und Sitzungen zentral beenden
- [ ] **Beweissicherung anstoßen:** Arbeitsspeicher, Images, Logdateien – vor jeder Bereinigung

T+30 bis T+45 Bewerten und Meldepflichten klären

UHRZEIT

- [ ] **Was ist betroffen:** Systeme, Standorte, Konten, Daten, Geschäftsprozesse
- [ ] **Personenbezogene Daten betroffen?** Dann läuft zusätzlich die 72-Stunden-Frist der DSGVO
- [ ] **Versicherung und Rechtsbeistand** informiert
- [ ] **Ist der Vorfall „erheblich“** im Sinne von NIS2 – wer entscheidet das, und bis wann
- [ ] **Meldeentwurf beginnen**, auch wenn noch nicht alle Fakten vorliegen (Erstmeldung darf unvollständig sein)
- [ ] **Datenabfluss geprüft** – nicht nur Verschlüsselung, auch Exfiltration

T+45 bis T+60 Kommunizieren und stabilisieren

UHRZEIT

- [ ] **Interne Sprachregelung** steht: was dürfen Mitarbeitende sagen, was nicht
- [ ] **Notbetrieb definiert:** welche Prozesse laufen analog weiter, wer entscheidet
- [ ] **Nächster Lagebericht terminiert** mit fester Uhrzeit und festem Teilnehmerkreis
- [ ] **Externe Kommunikation vorbereitet**, aber erst nach Freigabe der Geschäftsleitung
- [ ] **Ablösung organisiert** – ein Vorfall dauert Tage, nicht Stunden. Schichten jetzt planen
- [ ] **Protokoll gesichert** und an einem Ort abgelegt, der vom Vorfall nicht betroffen ist

WAS DIE ERSTE STUNDE AM HÄUFIGSTEN RUINIERT

- ✕ Systeme **neu aufsetzen**, bevor Beweise gesichert sind
- ✕ **Keine Zeitstempel** – später ist die Fristwahrung nicht belegbar
- ✕ Die **Meldepflicht** erst nach der technischen Analyse anfassen
- ✕ Kommunikation über die **kompromittierte E-Mail-Umgebung**
- ✕ Alle reden mit, aber **niemand entscheidet** – Rolle „Leitung“ nicht besetzt
- ✕ **Keine Ablösung** geplant – nach acht Stunden entscheidet Erschöpfung

Der Unterschied zwischen Chaos und Kontrolle ist selten Technik, sondern Vorbereitung: ausgefüllte Kontaktliste, geübter Ablauf, vorab geklärte Zuständigkeit. Wer den Ablauf einmal im Jahr in einer Tabletop Exercise durchspielt, verliert im Ernstfall keine Stunde mit Organisation.

Diese Stunde lässt sich üben.

Wir erstellen Ihren Incident-Response-Plan, spielen ihn in einer Tabletop Exercise mit Ihrem Führungskreis durch und sichern die Reaktion vertraglich ab. Im Ernstfall genügt dann ein Anruf – Triage, Eindämmung, Forensik und Recovery kommen aus einer Hand.

Notfall-Hotline +49 89 45 24 24-112 · 24/7/365 · kontakt@argos.security

argos.security/kontakt