Erstmaßnahmen-Checkliste: Die ersten 60 Minuten

Zwischen Entdeckung und Eintreffen externer Hilfe vergehen Stunden – in denen erfahrungsgemäß genau die Fehler passieren, die Forensik zerstören: **Server ausschalten, neu starten, Backups überschreiben, Anmeldung mit Domain-Admin auf kompromittierten Systemen.** Diese Checkliste gibt dem Admin nachts um drei eine abarbeitbare Reihenfolge – und dokumentiert zugleich, was getan wurde.

Warum dieses Dokument?

Die ersten 60 Minuten entscheiden, ob Beweise erhalten bleiben und ob sich der Angreifer weiterbewegen kann. Eine vorgedruckte Reihenfolge verhindert die typischen Panik-Fehler – und jede abgehakte Zeile ist zugleich Dokumentation.

Wann brauchen Sie es?

Sofort bei jedem Verdacht, noch bevor externe Hilfe eintrifft – gedacht für die Person, die den Vorfall entdeckt oder als Erste alarmiert wird.

Wo aufbewahren?

Ausgedruckt im Notfallordner neben Kontaktliste (IR-01) und Logbuch (IR-03): Tresor, Pforte, Bereitschaftstasche. Bei Ransomware ist die digitale Ablage nicht erreichbar.

Die vier Grundregeln der ersten Stunde

1. **Trennen, nicht ausschalten** – Netzkabel/WLAN/Port, Zustand fotografieren
2. **Alarmieren** – Kaskade nach IR-01, telefonisch – nicht per E-Mail
3. **Backups schützen** – vom Netz trennen, Replikation stoppen
4. **Dokumentieren** – jede Maßnahme mit Uhrzeit ins Logbuch IR-03

Grundregel: Keine Anmeldung mit privilegierten Konten auf verdächtigen Systemen – jede Anmeldung liefert dem Angreifer möglicherweise frische Zugangsdaten.

So sieht ein ausgefüllter Eintrag aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg (fiktiv) · Vorfall MM-2026-001: Ransomnote auf TS-02, Freitag 04:15 Uhr

Erl.	Maßnahme	Uhrzeit	Durchgeführt von	Bemerkung
☑	2. Nicht ausschalten, nicht neu starten – betroffene Systeme nur vom Netz trennen, Zustand fotografieren	04:22	M. Yilmaz	TS-02 Netzwerkkabel gezogen; Foto der Ransomnote per privatem Handy (IMG_0041)
☑	4. Backups prüfen und sofort vom Netz trennen / Replikation stoppen	04:31	M. Yilmaz	Veeam-Repository per Switchport deaktiviert; letzte Sicherung Do 23:00 intakt

⚠ **Warum nicht ausschalten?** Im Arbeitsspeicher liegen Schlüssel und Spuren, die das IR-Team braucht – ein ausgeschalteter Server verliert diese flüchtigen Beweise unwiederbringlich. Die Trennung vom Netz stoppt den Angreifer genauso, erhält aber den Zustand.

Halbjährliche Prüfung: ☐ Punkte an eigene Umgebung angepasst ☐ Offline-Kopien am Ort ☐ mit IT-Bereitschaft geübt
Geprüft am: _____ von: _____

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

UNTERNEHMEN	STAND / VERSION	VERANTWORTLICH	ORT DER OFFLINE-KOPIE	NÄCHSTE PRÜFUNG

INCIDENT-NR.	DATUM	BLATT-NR.

SOFORTMASSNAHMEN – IN DIESER REIHENFOLGE ABARBEITEN

Erl.	Maßnahme	Uhrzeit	Durchgeführt von	Bemerkung
☐	**1.** Ruhe bewahren, Logbuch beginnen (IR-03), Uhrzeit notieren			
☐	**2.** Nicht ausschalten, nicht neu starten – betroffene Systeme nur vom Netz trennen (Kabel/WLAN/Switchport); Zustand fotografieren (Bildschirm, Ransomnote)			
☐	**3.** Alarmierungskette auslösen (IR-01) – telefonisch, nicht per E-Mail			
☐	**4.** Backups prüfen und sofort vom Netz trennen, Replikation stoppen – bevor sie verschlüsselt oder überschrieben werden			
☐	**5.** Keine Anmeldung mit privilegierten Konten (Domain-Admin!) auf verdächtigen Systemen			
☐	**6.** Isolations-Matrix anwenden (IR-15): Was wird getrennt, wer entscheidet?			

⚠ **Uhrzeiten von EINER Referenzuhr nehmen** (z. B. Ihr Mobiltelefon) und jede Zeile sofort ausfüllen – nicht abends aus dem Gedächtnis. Die Checkliste wird später Teil der Beweiskette.

SOFORTMASSNAHMEN (FORTSETZUNG)

Erl.	Maßnahme	Uhrzeit	Durchgeführt von	Bemerkung
☐	**7.** Externe Zugänge sperren: VPN, RDP, Wartungszugänge von Dienstleistern			
☐	**8.** Kommunikation nicht über potenziell kompromittierte Systeme (E-Mail!) – Ersatzkanal aus IR-01 nutzen			
☐	**9.** Kein Kontakt zu Erpressern, nichts löschen, keine Lösegeld-Entscheidung ohne Krisenstab			
☐	**10.** Beweise sichern: nichts „aufräumen“, keine Virenscans mit automatischer Löschung starten			

UNTERNEHMENSSPEZIFISCHE PUNKTE (BEI DER VORBEREITUNG ERGÄNZEN)

Erl.	Maßnahme	Uhrzeit	Durchgeführt von	Bemerkung
☐				
☐				
☐				
☐				
☐				

NOTIZEN