• RANSOMWARE-VERDACHT · SOFORT HANDELN

Notfall-Karte: Erstreaktion in 60 Minuten

Zum Aushang im Serverraum. Was in der ersten Stunde zählt – ruhig, in der richtigen Reihenfolge, ohne Beweise zu vernichten.

ITS AG · 24/7-NOTDIENST
06021 / 49649-222

BSI SERVICE-CENTER
0800 274 1000

Die ersten 60 Minuten – Schritt für Schritt

1. **Ruhe bewahren, Krisenteam zusammenrufen**
   Nicht überstürzt handeln. Verantwortliche (Geschäftsführung, IT, Dienstleister) informieren und einen festen Ansprechpartner bestimmen.
2. **Isolieren – nicht ausschalten**
   Betroffene Systeme vom Netz trennen: Netzwerkkabel ziehen, WLAN aus, Switch-Ports deaktivieren. Geräte **nicht** herunterfahren – der Arbeitsspeicher enthält wichtige Spuren.
3. **Dokumentieren**
   Erpressernachricht und Bildschirm mit dem Smartphone fotografieren. Uhrzeiten und betroffene Systeme notieren. Über einen Kanal *außerhalb* des kompromittierten Netzes kommunizieren (Mobiltelefon).
4. **Umfang prüfen**
   Nicht nur das Offensichtliche. Ist der Verzeichnisdienst (Active Directory / Domaincontroller) betroffen, gilt das gesamte Netz als kompromittiert.
5. **Backups schützen**
   Offline- und unveränderbare Sicherungen sofort vom Netz nehmen bzw. sichern. Angreifer suchen gezielt danach. Sauberen Stand *vor* dem Eindringen identifizieren.
6. **Hilfe holen**
   IT-Dienstleister / ITS-Notdienst anrufen. Cyber-Versicherung früh informieren (Frist beachten – sonst drohen Leistungskürzungen).
7. **Meldepflichten beachten**
   Datenschutz-Meldung binnen 72 Stunden, ggf. NIS2-Meldung binnen 24 Stunden, Strafanzeige bei der Polizei (Details auf Seite 2).

✓ Richtig

- Netzwerkverbindung trennen (Kabel/WLAN), Gerät **eingeschaltet** lassen
- Vorfall fotografieren und protokollieren (Zeiten, Systeme)
- Forensische Sicherung erstellen, *bevor* etwas wiederhergestellt wird
- Über getrennten Kanal kommunizieren (Mobiltelefon)
- Frühzeitig Dienstleister, Versicherung und Behörden einbinden

✕ Vermeiden

- System sofort **herunterfahren** – vernichtet flüchtige Spuren
- Sofort einen Virenscan starten – überschreibt Beweise
- Mit Admin-Konten an verdächtigen Systemen anmelden
- Lösegeld- oder Leak-Seite der Täter öffnen
- Vorschnell zahlen – keine Garantie, finanziert die Täter, ggf. strafbar

Wen benachrichtigen? (Kontakte eintragen)

Geschäftsführung / Krisenstab	_____
IT-Dienstleister · ITS AG 24/7-Notdienst	**06021 / 49649-222**
BSI Service-Center Mo–Do 8–17, Fr 8–16 Uhr · kostenlos	**0800 274 1000**
Polizei – ZAC Cybercrime Zentrale Ansprechstelle des LKA (Strafanzeige)	_____
Datenschutz-Aufsicht Meldung nach Art. 33 DSGVO binnen 72 h	_____
Cyber-Versicherung Schadennummer / Hotline	_____

Meldefristen im Blick:
· DSGVO (Art. 33): Meldung an die Aufsichtsbehörde binnen **72 Stunden** ab Kenntnis – die Frist läuft auch am Wochenende.
· NIS2 (falls betroffen): Frühwarnung binnen **24 h**, Bestätigung binnen **72 h**, Abschlussbericht binnen **1 Monat** an das BSI.

Erste Stunden danach

Einfallstor schließen, *bevor* Systeme wieder ans Netz gehen. Alle privilegierten Passwörter zurücksetzen, MFA erzwingen, Verzeichnisdienst aus sauberem Backup neu aufbauen. Wiederanlauf nach Geschäftskritikalität (Verzeichnis → E-Mail → ERP → Arbeitsplätze). Über Wochen erhöhte Wachsamkeit.

Im Ernstfall sind wir rund um die Uhr erreichbar

Hängen Sie diese Karte gut sichtbar im Serverraum aus. Noch besser: Lassen Sie es gar nicht so weit kommen. Mit einem **EDV-Notfallplan**, geprüften Backups und proaktivem Monitoring der ITS AG sind Sie vorbereitet – bevor der Ernstfall eintritt.

24/7-Notdienst	Kostenfrei	Notfallplan anfragen
06021 / 49649-222	**0800 - 72 38 7 88**	**info@its-gruppe.de**

Quellen (Auswahl): BSI, „Ransomware – Erste Hilfe bei einem schweren IT-Sicherheitsvorfall“ · BSI Checkliste Technik · Art. 33 DSGVO · BSIG (NIS2-Umsetzung), Meldepflichten §32.