10
IT-Notfallmaßnahmen für Geschäftsführer

Der Erste-Hilfe-Plan bei Hackerangriffen,
Ransomware & Datenverlust.

SELBACH CONSULTING

Ein Leitfaden von Daniel Selbach

Wenn der Bildschirm schwarz wird oder Daten verschlüsselt sind, zählt jede Minute. Diese 10 Schritte müssen Sie sofort einleiten...

1 Netzwerkverbindung sofort trennen (nicht ausschalten!)

Ziehen Sie sofort das LAN-Kabel und deaktivieren Sie das WLAN am betroffenen Gerät, um die Ausbreitung im Netzwerk zu stoppen. **Schalten Sie den Rechner jedoch nicht aus (Stecker ziehen)**, da sonst wichtige Spuren im Arbeitsspeicher für die spätere forensische Analyse verloren gehen.

2 Interne IT oder externen Dienstleister alarmieren

Kontaktieren Sie umgehend Ihre IT-Abteilung oder Ihren externen IT-Dienstleister. Wichtig: Nutzen Sie dafür einen alternativen Kommunikationsweg (z. B. das private Smartphone oder Telefon), da Ihr E-Mail-System bereits von den Angreifern mitgelesen werden könnte.

3 Beweise sichern

Fotografieren Sie Fehlermeldungen, Erpresserschreiben (Ransomware-Notes) oder auffällige Aktivitäten auf den Bildschirmen mit Ihrem Smartphone. Diese Informationen sind für die IT-Forensiker und die Polizei später von unschätzbarem Wert.

4 Kritische Passwörter ändern (Sicheres Gerät nutzen)

Ändern Sie sofort die Zugangsdaten für zentrale Systeme (z. B. Microsoft 365, Server-Admin, Online-Banking). **Zwingend beachten:** Tun Sie dies ausschließlich von einem Gerät, das nicht mit dem infizierten Firmennetzwerk verbunden ist (z. B. über Ihr Smartphone im Mobilfunknetz).

5 Mitarbeiter sofort informieren

Informieren Sie Ihr gesamtes Team (z. B. über eine Durchsage oder Messenger). Die klare Anweisung muss lauten: Niemand darf mehr auf Links klicken, USB-Sticks einstecken, Mails öffnen oder sich an Systemen anmelden, bis offizielle Entwarnung gegeben wird.

6 Keine Alleingänge bei Lösegeldforderungen

Wenn Sie Opfer von Ransomware (Erpressungstrojanern) geworden sind: Zahlen Sie niemals sofort Lösegeld und nehmen Sie nicht auf eigene Faust Kontakt zu den Erpressern auf! Es gibt keine Garantie für eine Entschlüsselung und Sie machen sich als "zahlungsbereites Opfer" nur noch attraktiver.

7 Backups prüfen und physisch trennen

Trennen Sie Ihre Backup-Laufwerke sofort physisch vom Netz, falls das noch nicht geschehen ist. Prüfen Sie mit der IT, ob die letzten Datensicherungen unbeschädigt sind. Spielen Sie jedoch **niemals** Backups zurück, bevor die Sicherheitslücke nicht zu 100 % gefunden und geschlossen ist.

8 Notfallbetrieb (Business Continuity) starten

Aktivieren Sie Ihren analogen Notfallplan. Können Kernprozesse (z. B. Produktion, Logistik) vorübergehend manuell oder mit Stift und Papier aufrechterhalten werden? Informieren Sie wichtige Kunden oder Partner proaktiv und transparent über mögliche Verzögerungen.

9 DSGVO-Meldepflichten prüfen (72-Stunden-Regel)

Wenn der Verdacht besteht, dass personenbezogene Daten (Kundendaten, Mitarbeiterdaten) abgeflossen oder unbrauchbar gemacht wurden, müssen Sie dies in der Regel innerhalb von 72 Stunden der zuständigen Datenschutzbehörde melden. Ziehen Sie sofort Ihren Datenschutzbeauftragten hinzu.

10 Polizei (ZAC NRW) einschalten

Erstatten Sie in jedem Fall Anzeige. Für Unternehmen aus unserer Region ist die "Zentrale Ansprechstelle Cybercrime" (ZAC NRW) des Landeskriminalamts der beste erste Kontaktpunkt. Die Experten dort helfen unbürokratisch und kennen die aktuellsten Vorgehensweisen der Hacker-Gruppierungen.

Warten Sie nicht auf den Notfall.

Sie haben nun einen klaren Plan für den Ernstfall. Doch das beste Szenario ist, dass Sie diese Checkliste niemals aus der Schublade holen müssen. Ein durchschnittlicher Cyberangriff kostet ein mittelständisches Unternehmen schnell zehntausende Euro – Stillstand und Reputationsverlust noch nicht eingerechnet. Prävention ist immer günstiger als die Schadensbegrenzung.

Wissen Sie aktuell, wo die größten Einfallstore in Ihrer IT-Infrastruktur liegen?

Ihr Fundament für echte Sicherheit: Der CyberRisikoCheck

Beenden Sie den Blindflug. Als BSI-qualifizierter Berater liefere ich Ihnen mit dem **CyberRisikoCheck nach DIN SPEC 27076** objektive Fakten statt vager Vermutungen.

- **Minimaler Aufwand:** Nur ein 1- bis 2-stündiges Interview (vor Ort in Düsseldorf/NRW oder digital).
- **Maximale Klarheit:** Eine ungeschönte Standortbestimmung Ihrer IT-Sicherheit – ohne Fachjargon.
- **Offizieller Nachweis:** Sie erhalten einen anerkannten DIN-Bericht, mit dem Sie Ihre Sorgfaltspflicht gegenüber Banken, Kunden und Versicherungen belegen können.
- **Priorisierter Plan:** Sie bekommen konkrete Handlungsempfehlungen für die dringendsten Schwachstellen, damit Sie Ihr Budget gezielt einsetzen.

Ihre Investition: Einmalig 399 € *(statt regulär 599 €)*.

Jetzt kostenloses Erstgespräch im Kalender sichern

Daniel Selbach | IT-Sicherheitsberatung & KI-Berater Meisenweg 80, 40468 Düsseldorf
Tel: 0211/54571740 E-Mail: info@selbach-consulting.de Web: www.selbach-consulting.de