Checkliste: Das Firmennetz

Abhaken und Uhrzeit eintragen. So weißt du später genau, wer wann was getan hat.

Bemerkt am _____ um _____ Uhr → **72 Stunden enden am _____ um _____** Uhr

Bis dahin muss geklärt sein, ob eine Meldung an die Datenschutzaufsicht nötig ist (wenn personenbezogene Daten betroffen sind). Für Unternehmen nach NIS2: Frühwarnung an das BSI binnen 24 Stunden.

Jetzt sofort

- ☐ Betroffene Rechner und Bereiche vom Netz trennen, nicht ausschalten. Im Zweifel die Verbindung ins Internet kappen. ___:___ Uhr
- ☐ Sicherungen schützen: Sicherungsspeicher sofort vom Netz trennen, nichts zurückspielen. ___:___ Uhr
- ☐ Krisenstab bilden: Geschäftsführung, IT, eine Person fürs Protokoll, eine für die Kommunikation. ___:___ Uhr
- ☐ Außerhalb der eigenen IT kommunizieren: private Handys, Telefon, eine Gruppe außerhalb der Firmenmail. ___:___ Uhr
- ☐ Cyberversicherung und IT-Dienstleister anrufen, Fachleute für die Analyse holen. ___:___ Uhr
- ☐ Polizei einschalten. Kein Kontakt mit den Erpressern im Alleingang, nichts zahlen ohne Abstimmung. ___:___ Uhr
- ☐ Nichts gelöscht, nichts neu installiert, kein Backup eingespielt, nicht mit Angreifern geschrieben, nichts gezahlt.

Das sagst du beim ersten Anruf

„Hier ist _____ von _____. Wir haben den Verdacht auf einen Angriff: mehrere Rechner sind betroffen, Dateien sind verschlüsselt oder es gibt eine Erpressernachricht. Bemerkt haben wir es am _____ um _____ Uhr. Betroffen sind _____. Bisher haben wir _____. Was sollen wir als Nächstes tun, und was sollen wir auf keinen Fall tun?“

Wichtige Nummern

Polizei bei akuter Gefahr	**110**
Polizei für Unternehmen: ZAC deines Bundeslands polizei.de, Suche „ZAC“	
Datenschutzaufsicht deines Bundeslands datenschutzkonferenz-online.de	
IT-Dienstleister / Hoster	
Cyberversicherung (Notfallnummer)	
Bank	
PLUTEX	**0800 100400800 · support@plutex.de**

Vorfallbogen

Ausfüllen und an IT-Dienstleister, Polizei, Versicherung oder Datenschutzbeauftragte weitergeben. Unbekanntes einfach offen lassen.

Was ist passiert?

Bemerkt am / um	
Bemerkt durch wen, wodurch	
Betroffene Geräte, Konten, Systeme	

Zu deiner Lage

Wie viele Rechner und Server sind betroffen, welche Standorte?	
Wortlaut der Erpressernachricht, Kontaktadresse, genannte Frist (Foto beilegen)	
Zustand der Sicherungen: getrennt? unversehrt? Stand von wann?	
Welche Abläufe stehen still (Lohn, Produktion, Kundenservice)?	
Hinweise, dass Daten kopiert wurden?	

Daten und Maßnahmen

Welche Daten können betroffen sein? (Kunden, Mitarbeitende, Zahlungen, Gesundheit)	
Ungefähr wie viele Personen?	
Was wurde schon getan? (mit Uhrzeit)	

Wer ist informiert?

	Name / Stelle	Datum, Uhrzeit	Aktenzeichen, Schadennr.
IT-Dienstleister / Hoster			
Polizei (ZAC)			
Cyberversicherung			
Datenschutzbeauftragte/r			
Datenschutzaufsicht			
Bank			

Diesen Bogen sorgfältig aufbewahren. Er hilft bei Anzeige, Versicherung und einer möglichen Meldung nach Art. 33 DSGVO.