Checkliste: Den einzelnen PC

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

- ☐ Den PC vom Netz trennen: Kabel ziehen, WLAN aus. Nicht ausschalten, solange er nicht weiter verschlüsselt. ___:___ Uhr
- ☐ Die Erpressernachricht fotografieren. Nicht antworten, nichts zahlen, keine Links öffnen. ___:___ Uhr
- ☐ Externe Festplatten und USB-Sticks abziehen, Sicherungen nicht anschließen. ___:___ Uhr
- ☐ Prüfen lassen, ob andere Rechner oder Netzlaufwerke betroffen sind. Wenn ja: Kapitel Firmennetz. ___:___ Uhr
- ☐ IT-Dienstleister anrufen, Protokoll beginnen. ___:___ Uhr
- ☐ Von einem sauberen Gerät die Passwörter ändern, die auf diesem PC benutzt wurden. ___:___ 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: ein Rechner zeigt eine Erpressernachricht oder Dateien lassen sich nicht öffnen. 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**

NOTFALLBLATT SEITE 2 · GEHACKT – WAS JETZT?

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

Rechner: Name, Standort, wer arbeitet daran	
Wortlaut der Erpressernachricht, Kontaktadresse, Frist (Foto beilegen)	
Verbundene Netzlaufwerke, Cloud-Ordner, USB-Festplatten	
Sicherung vorhanden und getrennt? Stand von wann?	
Verdächtige Mail oder Download davor: Absender, Datum, Betreff	

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.