Checkliste: Das Mailkonto

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

- ☐ Von einem sauberen Gerät das Passwort des Postfachs ändern und alle Sitzungen abmelden. ___:___ Uhr
- ☐ Zwei-Faktor-Anmeldung einschalten, wenn dein Anbieter sie bietet. ___:___ Uhr
- ☐ In den Einstellungen nach Weiterleitungen, Filtern und Abwesenheitsnotizen suchen, die du nicht angelegt hast. Fotografieren, dann entfernen lassen. ___:___ Uhr
- ☐ Kunden und Geschäftspartner warnen, wenn aus deinem Postfach Mails mit Rechnungen oder Links verschickt wurden. ___:___ Uhr
- ☐ Bei geänderter Bankverbindung in Rechnungen sofort die Bank anrufen. Überweisungen lassen sich manchmal noch zurückholen. ___:___ Uhr
- ☐ Protokoll beginnen und den Mailanbieter informieren. ___:___ 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: aus unserem Postfach wurden Mails verschickt, die wir nicht geschrieben haben. 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

Betroffene Mailadresse und Anbieter	
Gefundene Regeln oder Weiterleitungen: Ziel-Adresse (Foto beilegen)	
Empfänger der gefälschten Mails	
Fehlüberweisung: Betrag, Empfänger-IBAN, Datum, Bank des Zahlenden	
Auf welchen Geräten wird das Postfach genutzt?	

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.