Checkliste: Das Microsoft-365- oder Google-Konto

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 ändern und alle Sitzungen und Geräte abmelden. ___:___ Uhr
- ☐ Zwei-Faktor-Anmeldung einschalten oder neu einrichten, fremde Geräte und Apps entfernen lassen. ___:___ Uhr
- ☐ Weiterleitungen, Postfachregeln und verbundene Apps prüfen, fotografieren und dann entfernen lassen. ___:___ Uhr
- ☐ Freigaben von Dateien und Ordnern an fremde Adressen prüfen lassen. ___:___ Uhr
- ☐ Die Person informieren, die euer Konto verwaltet, etwa den IT-Dienstleister. ___:___ Uhr
- ☐ Protokoll beginnen. Anmeldeprotokolle des Kontos sichern lassen, bevor sie ablaufen. ___:___ 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: jemand hat Zugriff auf unser Microsoft-365- oder Google-Konto, etwa mit heimlichen Weiterleitungen. 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

Betroffene Konten und wer sie verwaltet	
Gefundene Weiterleitungen, Regeln, fremde Apps oder Geräte (Foto beilegen)	
Zeitraum fremder Anmeldungen laut Protokoll	
Freigaben von Dateien an fremde Adressen	
Besonders schutzwürdige Daten im Konto (Gesundheit, Bank, Ausweise)?	

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.