Checkliste: Eigenen Server oder vServer

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 Server vom Netz isolieren, etwa über die Firewall deines Anbieters, aber nicht ausschalten. ___:___ Uhr
- ☐ Beim Anbieter einen Snapshot oder ein Abbild des Servers anlegen lassen, bevor sich etwas ändert. ___:___ Uhr
- ☐ Protokolle und Konfiguration außerhalb des Servers sichern lassen. ___:___ Uhr
- ☐ Alle Zugangsdaten zum Kundenportal des Anbieters von einem sauberen Gerät ändern. ___:___ Uhr
- ☐ Deinen Anbieter informieren, besonders wenn er dich wegen Missbrauch angeschrieben hat. ___:___ Uhr
- ☐ Protokoll beginnen und klären, ob personenbezogene Daten auf dem Server lagen. ___:___ 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: unser Server verhält sich auffällig, etwa Spam-Versand, hohe Last oder eine Missbrauchsmeldung. 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

Anbieter, Servername und Vertragsnummer	
Missbrauchsmeldung erhalten? Datum und Referenz	
Welche Dienste liefen darauf (Websites, Mail, Datenbank)?	
Gespeicherte Zugänge zu anderen Systemen oder Kunden	
Abbild oder Snapshot angelegt? Wann, von wem?	

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.