Checkliste: Website, Webshop oder Online-Buchung

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

- ☐ Fotos von der veränderten Seite und von seltsamen Mails machen, mit Uhrzeit. ___:___ Uhr
- ☐ Von einem sauberen Gerät die Passwörter ändern: zuerst Mail, dann Hoster, dann Website-Verwaltung und Buchungssystem. ___:___ Uhr
- ☐ Deinen Hoster anrufen und um Sperren oder Wartungsseite bitten. Nichts selbst löschen oder neu installieren. ___:___ Uhr
- ☐ Den Anbieter des Buchungs- oder Shopsystems informieren und fragen, welche Daten betroffen sein können. ___:___ Uhr
- ☐ Protokoll beginnen: wann bemerkt, was getan, wen angerufen. ___:___ Uhr
- ☐ Prüfen lassen, ob personenbezogene Daten abgeflossen sind. Ab Kenntnis laufen 72 Stunden für eine mögliche Meldung. ___:___ 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: unsere Website wurde verändert und Kunden bekommen gefälschte Mails in unserem Namen. 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

Adresse der Website	
Hoster und Kundennummer	
Anbieter des Buchungs-, Shop- oder Formularsystems	
Welche Daten erfassen Formulare, Buchungen, Bestellungen?	
Gefälschte Mails an Kunden? Seit wann, an wie viele?	

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.