

Verdacht auf einen IT-Sicherheitsvorfall?

Seltene Meldungen, verschlüsselte Dateien, ein Klick auf einen verdächtigen Link oder ein Gerät, das sich merkwürdig verhält – handeln Sie sofort:

1

Ruhe bewahren

Panik führt zu Fehlern. Niemand bekommt Ärger, wenn er schnell meldet.

2

Arbeit einstellen

Am betroffenen Gerät nichts mehr öffnen, speichern oder löschen.

3

Vom Netz trennen

Netzwerkkabel ziehen, WLAN ausschalten – das Gerät aber eingeschaltet lassen.

4

Sofort melden

An die unten eingetragene Stelle – telefonisch, nicht per E-Mail vom betroffenen Gerät.

5

Notieren

Was haben Sie gesehen, wann, an welchem Gerät? Fotos vom Bildschirm helfen.

Im Notfall melden an: _____

Diese Angaben helfen beim Melden

- Wer meldet – und wie sind Sie erreichbar?
- Welches Gerät oder System ist betroffen (Name, Standort)?
- Was ist passiert? Wortlaut von Meldungen, Absender verdächtiger E-Mails
- Wann ist es aufgefallen – und was wurde schon unternommen?

Bitte nicht

- ✗ Lösegeld zahlen oder mit Erpressern Kontakt aufnehmen
- ✗ Gerät ausschalten, neu aufsetzen oder Daten löschen – nur nach Anweisung
- ✗ Externe Festplatten oder Backups an das betroffene Gerät anschließen
- ✗ Verdächtige E-Mails oder Anhänge an Kollegen weiterleiten
- ✗ Den Vorfall aus Scham verschweigen

Typische Fälle – was jetzt zu tun ist

Link geklickt oder Passwort eingegeben

Passwort sofort an einem anderen, sicheren Gerät ändern und den Vorfall melden.

Erpresser-Bildschirm oder verschlüsselte Dateien

Gerät vom Netz trennen, eingeschaltet lassen, sofort melden. Nichts bezahlen.

Gerät verloren oder gestohlen

Sofort melden, damit Konten gesperrt und Daten aus der Ferne gelöscht werden können.

Ungewöhnliche Zahlungsaufforderung

„Chef“ oder Lieferant verlangt eilig eine Überweisung? Rückruf über die bekannte Nummer – nie über die Angaben in der Nachricht.

Wichtige Kontakte – bitte eintragen

Interne IT / Notfall-
verantwortliche

IT-Dienstleister

Geschäftsführung

Datenschutz-
beauftragte

Cyber-Versicherung
Hotline, Policennummer

Polizei

ZAC beim LKA · Notruf 110

Personenbezogene Daten betroffen?

Verletzungen des Datenschutzes müssen in der Regel innerhalb von 72 Stunden der Aufsichtsbehörde gemeldet werden (Art. 33 DSGVO).

Unter NIS2 registriert?

Erhebliche Sicherheitsvorfälle gehen an das BSI: Frühwarnung in 24 Stunden, Meldung in 72 Stunden, Abschlussbericht nach einem Monat.