

Heute eintragen, damit Sie im Ernstfall nicht suchen müssen

IT-Dienstleister (Name, Telefon): _____

Wer entscheidet, wenn die Geschäftsführung nicht erreichbar ist: _____

Cyber-Versicherung (Notfallnummer, Policennummer): _____

Anwalt oder Datenschutzbeauftragter: _____

Zentrale Ansprechstelle Cybercrime der Polizei (Ihr Bundesland): _____

Wo steht das Backup, und wie wird es vom Netz getrennt: _____

Die erste Stunde · Ausbreitung stoppen

- ☐ **Netzwerk trennen.** Kabel ziehen, WLAN abschalten. Wenn unklar ist, welche Geräte betroffen sind: das ganze Unternehmen vom Internet trennen, Stecker am Router oder an der Firewall.
- ☐ **Geräte nicht ausschalten, nichts neu starten.** Im Arbeitsspeicher liegen die Spuren, die später zeigen, was passiert ist.
- ☐ **Backup vom Netz nehmen, sofort.** NAS oder Sicherungsserver trennen. Was nicht erreichbar ist, kann nicht verschlüsselt werden.
- ☐ **Anrufen, nicht mailen.** Ihre E-Mail kann mitgelesen sein. Den IT-Dienstleister per Telefon erreichen.
- ☐ **Im Betrieb Bescheid sagen.** Niemand meldet sich irgendwo an, niemand öffnet Anhänge, niemand versucht, „schnell noch“ etwas zu retten.

Die ersten Stunden · verstehen, was passiert ist

- ☐ **Liste anlegen, was betroffen ist und was nicht:** Rechner, Server, Cloud, Buchhaltung. Mit Handyfotos der Bildschirme – für Versicherung, Anzeige und Helfer.
- ☐ **Erpresserbotschaft fotografieren.** Nicht antworten, nicht auf eigene Faust verhandeln, am ersten Tag auf keinen Fall zahlen.
- ☐ **Davon ausgehen, dass Daten kopiert wurden,** bis jemand das Gegenteil belegt. Das ändert die Meldepflichten.

Noch am ersten Tag · melden und informieren, mit Anwalt oder Datenschutzbeauftragtem

- ☐ **Datenschutzbehörde:** Wenn personenbezogene Daten betroffen sein könnten, gilt eine Frist von 72 Stunden – ab dem Moment, in dem Sie den Vorfall bemerkt haben.
- ☐ **Versicherung:** sofort melden. Viele Versicherer stellen dann eigene Spezialisten.
- ☐ **Polizei:** Anzeige bei der Zentralen Ansprechstelle Cybercrime Ihres Bundeslandes.
- ☐ **Wichtige Kunden und Partner anrufen:** Mails von Ihnen gerade nicht öffnen.
- ☐ **Wenn Ihr Unternehmen unter NIS2 fällt:** Meldung an das BSI.

Ab Tag zwei · wiederherstellen, aber richtig

- ☐ **Nur aus einer sauberen Sicherung wiederherstellen,** die vor dem Vorfall liegt und nicht erreichbar war.
- ☐ **Erst die Ursache, dann der Neustart:** offener Fernzugang, altes Passwort, Rechner ohne Updates. Solange die Tür offen ist, kommen die Angreifer wieder.