7

# Notfallplan erstellen

## VERANTWORTLICHKEITEN FESTLEGEN

- ☐ Ihre Planung muss folgende Aspekte umfassen: Definition der technischen und organisatorischen Rollen, Klärung von Verantwortlichkeiten jedes Einzelnen, Festlegung von Zuständigkeiten und die Einbeziehung externer Dienstleister.
- ☐ Bestimmen Sie Beauftragte für die in einem Notfall erforderlichen Aufgabenbereiche (Notfallteam). Eine Konzentration vieler Zuständigkeiten in einer Rolle ist zu vermeiden.

## NOTFALLPLAN ERSTELLEN

- ☐ Fertigen Sie eine Liste mit allen Ansprechpersonen an und treffen Sie Vorabsprachen mit diesen. Ein Kommunikationsplan sollte auch Handynummern eines Notfallteams und beispielsweise eine eigene Notfall-E-Mail-Erreichbarkeit enthalten, da betriebliche Festnetztelefone und E-Mail-Konten bei Cyberangriffen oft auch betroffen und nicht funktionsfähig sind. Denken Sie außerdem an Kundenadressen.
- ☐ Erstellen Sie einen Notfallplan (Vorfallreaktionsplan), der auflistet, was in der jeweiligen Situation zu tun ist, um so schnell wie möglich wieder handlungsfähig zu sein. Der Notfallplan sollte Kontaktdaten von zu informierenden externen Stellen und bestehende Meldepflichten enthalten (z. B. § 33 DSGVO – möglichst binnen 72 Std.).
- ☐ Dokumentieren Sie Leitlinien, Rollen und Zuständigkeiten für eine zeitnahe, professionelle und angemessene Reaktion auf alle Sicherheitsvorfälle.

## ÜBEN UND BEREITHALTEN

- ☐ Halten Sie den Notfallplan und die Kommunikationslisten physisch (ausgedruckt) bereit, damit diese den Beschäftigten auch bei einem IT- Ausfall zur Verfügung stehen.
- ☐ Führen Sie regelmäßig Übungen durch, damit Sie im Ernstfall schnell und richtig reagieren können.

Stand April 2024

Baden-Württemberg
MINISTERIUM DES INNEREN, FÜR DIGITALISIERUNG UND KOMMUNEN

POLIZEI
BADEN-WÜRTTEMBERG
LANDESKRIMINALAMT
BADEN-WÜRTTEMBERG

Hochschule Aalen

CSBW CYBER SICHERHEITS AGENTUR
BADEN-WÜRTTEMBERG