Checkliste Datenpanne: die ersten 72 Stunden

Was in welcher Reihenfolge zu tun ist, wenn Daten verloren gehen oder ein Angriff läuft: eindämmen, bewerten, melden, informieren, dokumentieren.

1 Stunde 0 bis 4: Eindämmen
2 Stunde 4 bis 24: Bewerten
3 Bis Stunde 72: Melden
4 Danach: Aufräumen und lernen

Eine Datenpanne ist jeder Vorfall, bei dem personenbezogene Daten verloren gehen, unbefugt gelesen, verändert oder gelöscht werden: verschlüsselte Server, gestohlener Laptop, E-Mail an den falschen Empfänger, offener Aktenschrank. Die Meldefrist an die Aufsichtsbehörde beträgt 72 Stunden ab Kenntnis. Diese Liste hängt griffbereit, nicht auf dem betroffenen Server.

1 Stunde 0 bis 4: Eindämmen

- [ ] **Vorfall melden**
  an die intern zuständige Person; Uhrzeit der Kenntnis notieren, sie startet die 72 Stunden.
- [ ] **Ausbreitung stoppen**
  betroffene Geräte vom Netz trennen (nicht ausschalten, Spuren bleiben erhalten), Zugänge sperren, Passwörter der betroffenen Konten ändern.
- [ ] **IT-Dienstleister und ggf. Datenschutzbeauftragten einschalten**
  Telefonnummern stehen im Notfallplan.
- [ ] **Bei Erpressung oder Angriff**
  keine Zahlung ohne Beratung; Anzeige bei der Polizei (Zentrale Ansprechstelle Cybercrime des Landes) erwägen; Cyberversicherung informieren, oft mit eigener Hotline.

2 Stunde 4 bis 24: Bewerten

- [ ] **Was ist passiert?**
  Art des Vorfalls, Zeitraum, betroffene Systeme, Ursache soweit bekannt.

contrust in – André Walther · Beratender Betriebswirt · Südstr. 8, 08539 Rosenbach (Vogtland) · +49 37431 86 77 35 · info@contrust-in.de · contrust-in.de

- [ ] **Welche Daten, wie viele Personen?**
  Kategorien (Kunden, Beschäftigte, Bewerber), Datenarten (Kontakt, Bank, Gesundheit, Zugangsdaten), ungefähre Zahl.

- [ ] **Welches Risiko für die Betroffenen?**
  Identitätsdiebstahl, finanzieller Schaden, Rufschädigung, Diskriminierung. Kein Risiko (z. B. verschlüsseltes Gerät mit sicherem Schlüssel) heißt: dokumentieren, nicht melden.

- [ ] **Entscheidung dokumentieren**
  Meldung ja/nein, Information der Betroffenen ja/nein, mit Begründung und Unterschrift.

3 Bis Stunde 72: Melden

- [ ] **Meldung an die Aufsichtsbehörde**
  über das Online-Formular der zuständigen Behörde (Sachsen: datenschutz.sachsen.de). Inhalt: Art der Verletzung, Kategorien und Zahl der Betroffenen, Folgen, Maßnahmen, Kontaktstelle. Was noch unbekannt ist, wird nachgereicht.
  Art. 33 DSGVO, 72 Stunden ab Kenntnis

- [ ] **Information der Betroffenen bei hohem Risiko**
  unverzüglich, in klarer Sprache, mit Empfehlung, was sie tun sollen (Passwörter ändern, Kontobewegungen prüfen).
  Art. 34 DSGVO

- [ ] **Auftragsverarbeiter**
  Ist der Vorfall beim Dienstleister passiert, muss er Sie unverzüglich informieren; Sie bleiben meldepflichtig.

4 Danach: Aufräumen und lernen

- [ ] **Systeme bereinigen und wiederherstellen**
  aus sauberem Backup; Sicherheitslücke schließen, bevor der Betrieb wieder ans Netz geht.

- [ ] **Vorfall im Pannenregister dokumentieren**
  auch nicht gemeldete Vorfälle, mit Ablauf und Begründung.

- [ ] **Ursache abstellen**
  Schulung, Zwei-Faktor-Anmeldung, Rechtekonzept, Backup-Test; Maßnahme mit Termin und Verantwortlichem.

Intern zuständig (Name, Telefon)

IT-Dienstleister (Name, Telefon, Notfallnummer)

Datenschutzbeauftragter / Berater

Cyberversicherung (Police, Hotline)

Arbeitshilfe von contrust in – André Walther, Beratender Betriebswirt. Sie gibt den Stand zum genannten Datum wieder und ersetzt keine Rechts-, Steuer- oder Förderberatung. Die Details Ihres Falls klärt das Erstgespräch: contrust-in.de