

Merkblatt: Verhalten im Cyber-Schadenfall

Ein Cyber-Angriff erfordert schnelles, koordiniertes und besonnenes Handeln. Dieses Merkblatt fasst die wichtigsten Sofortmassnahmen zusammen, um Schäden zu minimieren und die Wiederherstellung zu beschleunigen.

1. Erste Schritte: Was ist allgemein bei einem Cyber-Schadenfall zu tun?

Netzwerktrennung: Trennen Sie betroffene Systeme sofort vom Netzwerk (WLAN deaktivieren, Netzkabel ziehen).
WICHTIG: Schalten Sie die Geräte NICHT aus, da sonst flüchtige Daten im Arbeitsspeicher verloren gehen, die für eine forensische Untersuchung wichtig sind.

IT-Partner: Benachrichtigen Sie umgehend Ihre IT-Fachverantwortlichen (intern und extern).

Versicherung: Melden Sie uns den Schadenfall, damit die Cyberversicherung informieren können (sofern versichert)

Meldewege & Eskalation: Informieren Sie die Geschäftsleitung und, falls vorhanden, Ihre Cyber-Versicherung. Stellen Sie eine Liste mit den internen Ansprechpartnern und den Kontaktdaten Ihres IT-Dienstleisters zusammen.

Passwörter ändern: Ändern Sie kritische Passwörter (Admin-Zugänge, E-Mail) von einem sauberen, nicht vom Vorfall betroffenen Gerät aus. Zweifaktoren Anmeldung «2FA» einrichten.

Journalführung: Notieren Sie die getroffenen Massnahmen sowie den genauen zeitlichen Ablauf des Cyber-Ereignisses seit der ersten Feststellung.

Beweissicherung (Screenshots / IoC): Machen Sie wo möglich Screenshots von Fehlermeldungen oder Erpresserschreiben. Sammeln Sie die vorhandenen Log-Daten und sichern Sie Beweismittel (Indicators of Compromise).

Kontakt sicherstellen: Stellen Sie Kommunikationswege sicher, falls die firmeninterne IT ausfällt (z. B. über sichere Messenger, private Handys oder Laptops).

Dokumentation: Organisieren Sie die IT-Dokumentation, Netzwerkpläne und das IT-Inventar für die externen Spezialisten.

2. Zusätzliche Massnahmen bei einem Betrugsfall (z. B. falsche Zahlungen)

Konto- und Kartensperrung: Lassen Sie kompromittierte Konten oder Kreditkarten bei Verdacht umgehend sperren.

Chargeback-Antrag: Bitten Sie Ihre Bank sofort, ein Chargeback (Rückbuchung) einzuleiten. Dies kann in der Regel telefonisch oder über das Online-Banking erfolgen. Geschwindigkeit ist hier essenziell.

Polizeimeldung: Melden Sie den Vorfall der Polizei (lokale Polizeistelle oder via Suisse ePolice). <https://www.suisse-epolice.ch/cybercrime-case>

3. Zusätzliche Massnahmen bei einem Datendiebstahl (Data Breach)

Meldung an Behörden: Je nach Schwere des Vorfalls und den geltenden gesetzlichen Bestimmungen (z.B. revDSG, DSGVO) ist es erforderlich, den Vorfall dem EDÖB (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter) zu melden.

Rechtliche Beratung: Ziehen Sie frühzeitig Fachexperten für IT-Recht und Datenschutz hinzu, um Ihre rechtlichen Pflichten abzuklären.

Krisenkommunikation: Koordinieren Sie die interne sowie externe Krisenkommunikation. Ziehen Sie ggf. PR-Spezialisten bei, um Reputationsschäden zu minimieren. Betroffene Kunden und Partner müssen transparent, aber rechtlich abgesichert informiert werden.

4. Zusätzliche Massnahmen bei Cyber-Erpressung (Ransomware)

Kein Lösegeld zahlen: Gehen Sie nicht auf Forderungen ein. Eine Zahlung garantiert weder die Entschlüsselung noch die Löschung gestohlener Daten und finanziert weitere Kriminalität.

Backups absichern: Prüfen Sie, ob unkorruptierte Offline-Backups vorhanden sind. Stellen Sie sicher, dass Backups nicht aus dem kompromittierten Netzwerk erreichbar sind, bevor Sie Wiederherstellungsversuche starten.

Beweissicherung für Strafverfolgung: Verändern Sie keine Daten auf den verschlüsselten Systemen, damit der Weg für eine professionelle forensische Untersuchung offenbleibt.

Meldung beim BACS: Benachrichtigen Sie das Bundesamt für Cybersicherheit (BACS, ehemals NCSC) via www.bacs.admin.ch. Dort erhalten Sie auch wertvolle Ersthilfe.

Noch keine Cyberversicherung?

Offertenanfrage für die KMU-Cyberversicherung: www.cyberbroker.ch