Cyber-Notfall: Die ersten 24 Stunden

Ein Cyberangriff trifft viele KMU unvorbereitet. Was Sie in den ersten Stunden tun – und was Sie lassen –, entscheidet oft über die Höhe des Schadens und über Ihren Versicherungsschutz.

SOFORT In der ersten Stunde

1. **Betroffene Geräte vom Netz trennen, aber nicht ausschalten.** Netzwerkkabel ziehen, WLAN deaktivieren, externe Datensicherungen abhängen, damit sie nicht mitverschlüsselt werden. Spuren im Arbeitsspeicher können für die Aufklärung wichtig sein.
2. **Notfallteam alarmieren.** Geschäftsleitung, IT-Partner und Ihren Versicherungsbroker – am besten per Telefon, nicht über möglicherweise kompromittierte E-Mail-Konten.
3. **Nichts löschen, nichts neu aufsetzen.** Fotografieren Sie Bildschirmmeldungen und Erpresserschreiben. Beweise sind für Forensik, Polizei und Versicherung nötig.
4. **Kein Lösegeld zahlen, keinen Kontakt mit den Angreifern aufnehmen.** Das Bundesamt für Cybersicherheit rät grundsätzlich davon ab. Entscheiden Sie nichts ohne Fachleute, Polizei und Versicherer.

STUNDE 1–4 Schaden begrenzen

5. **Schaden dem Versicherer melden.** Viele Cyberversicherungen bieten eine Notfall-Hotline und vermitteln IT-Forensiker. Klären Sie vor grösseren Ausgaben, ob der Versicherer zustimmen muss.
6. **Passwörter ändern – von einem sauberen Gerät aus.** Zuerst E-Mail, E-Banking und Administratorkonten.
7. **Bank informieren**, wenn Zahlungen manipuliert oder ausgelöst worden sein könnten. Je schneller, desto eher lässt sich eine Überweisung stoppen.
8. **Protokoll führen – von Anfang an.** Wer hat wann was festgestellt und unternommen? Das hilft bei Meldungen und bei der Schadenregulierung.

BIS STUNDE 24 Melden und informieren

9 **Meldepflichten prüfen.** Welche gelten, sehen Sie im Kasten unten.

10 **Strafanzeige bei der Kantonspolizei erstatten.** Sie ist oft Voraussetzung für die Schadenregulierung.

11 **Mit einer Stimme kommunizieren.** Informieren Sie zuerst Ihre Mitarbeitenden, dann – falls nötig – Kunden und Partner. Eine Person spricht nach aussen, ohne Spekulationen.

Meldepflichten in der Schweiz

- **Datenschutz (Art. 24 DSG):** Führt der Vorfall voraussichtlich zu einem hohen Risiko für betroffene Personen, melden Sie ihn so rasch als möglich dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). Bei Ransomware ist je nach Umständen von einem hohen Risiko auszugehen. Betroffene Personen informieren Sie, wenn es zu ihrem Schutz nötig ist.
- **Kritische Infrastrukturen:** Seit dem 1. April 2025 müssen Betreiberinnen kritischer Infrastrukturen Cyberangriffe innerhalb von 24 Stunden dem Bundesamt für Cybersicherheit (BACS) melden. Alle anderen Unternehmen können Vorfälle freiwillig melden.
- **Versicherung:** Die meisten Policen verlangen eine unverzügliche Schadenmeldung. Prüfen Sie die Frist in Ihren Bedingungen.

Ihre Notfallnummern – jetzt ausfüllen, ausdrucken, aufhängen

Wer	Name und Telefon
IT-Partner	
Notfall-Hotline Versicherer	
Geschäftsleitung	
Ihr Broker	360 I Fokus GmbH · Martir Hoxha · +41 44 885 33 55
Polizei-Notruf	117

15 Minuten Zeit. Ein guter Kaffee. Vielleicht eine langfristige Zusammenarbeit.

Wie gut ist Ihre Firma vorbereitet? Testen Sie es mit dem kostenlosen FOKUS-Check Cyber oder rufen Sie uns an.

+41 44 885 33 55 · info@360-fokus.ch · 360-fokus.ch

Dieses Merkblatt dient der allgemeinen Information und ersetzt keine Rechts- oder IT-Beratung im Einzelfall.