computerforensic&more

Die erste Stunde.

Sieben Entscheidungen, die nach einem Ransomware-Angriff über Schaden, Wiederanlauf und Aufklärung bestimmen. Ausdrucken, ins Krisenhandbuch legen, neben den Serverraum hängen.

01 Isolieren, nicht abschalten. ☐

Netzwerk trennen, Systeme eingeschaltet lassen. Abschalten nur als bewusste Entscheidung, mit Uhrzeit festgehalten.

02 Backups vom Netz. ☐

Sicherungen sofort trennen. Nichts zurückspielen und nichts neu aufsetzen, bevor das Einfallstor geklärt ist.

03 Kein Kontakt zum Angreifer. ☐

Erpressernachricht fotografieren. Nicht antworten, keine Links öffnen. Ob verhandelt wird, entscheidet die Geschäftsführung.

04 Getrennt kommunizieren. ☐

Nicht über E-Mail oder Teams des Unternehmens. Privilegierte Konten gelten als kompromittiert. Sperren, nicht löschen.

05 Zeitleiste beginnen. ☐

Wer hat was wann bemerkt und getan, an welchem System. Jede Uhrzeit mit Zeitzone.

06 Versicherung zuerst. ☐

Cyberversicherung informieren, bevor Dienstleister beauftragt werden. Viele Polizzen verlangen das.

07 Meldepflichten prüfen. ☐

Personenbezogene Daten betroffen? Meldung an die Datenschutzbehörde binnen 72 Stunden (Art. 33 DSGVO). NIS-Einrichtung? Frühwarnung an das Bundesamt für Cybersicherheit binnen 24 Stunden (NISG 2026).

INCIDENT RESPONSE · SOFORTHILFE

Computerforensic & more GmbH

+43 (664) 144 83 63

IHRE NUMMERN · VORAB AUSFÜLLEN

KRISENLEITUNG

VERTRETUNG

CYBERVERSICHERUNG, HOTLINE

POLIZZENNUMMER

IT-DIENSTLEISTER

DATENSCHUTZ UND RECHT