strategyc.

IT-NOTFALLKARTE

Verdacht auf Angriff oder Datenverlust? So handeln Sie.

TYPISCHE WARNZEICHEN

- Dateien lassen sich nicht mehr öffnen
- Anmelde-Anfragen, die Sie nicht ausgelöst haben
- Zugangsdaten auf verdächtiger Seite eingegeben
- Lösegeldforderung auf dem Bildschirm
- E-Mails in Ihrem Namen, die Sie nicht kennen
- Computer verhält sich auffällig ungewöhnlich

SOFORT, IN DIESER REIHENFOLGE

1 Ruhe bewahren

Überlegt handeln. Hektische Schritte richten oft zusätzlichen Schaden an.

2 Vom Netzwerk trennen

Kabel ziehen, WLAN aus. Das Gerät **nicht ausschalten** und nicht neu starten.

3 Nichts löschen

Keine Dateien, E-Mails oder Meldungen löschen. Sie sind wichtige Spuren.

4 Kein Lösegeld zahlen

Nicht auf Forderungen antworten, **nichts zahlen**, keinen Kontakt aufnehmen.

5 Sofort melden

Interne Ansprechperson und IT-Dienstleister informieren, auch bei bloßem Verdacht.

6 Alles notieren

Was ist wann an welchem Gerät passiert? Bildschirm mit dem Handy fotografieren.

WEN SIE INFORMIEREN

ZUERST INTERN

Interne Ansprechperson

Name

Telefon

Vertretung

IT-DIENSTLEISTER

Ihr IT-Dienstleister

Firma

Telefon

Erreichbarkeit

POLIZEI

LKA NRW, Cybercrime

0211 939-4040

cybercrime.lka@polizei.nrw.de

Zentrale Ansprechstelle Cybercrime für Unternehmen. Anzeige nach Absprache mit der Geschäftsleitung. **Bei akuter Gefahr: Notruf 110.**

72 h
DATENSCHUTZ

Personenbezogene Daten betroffen? Dann muss die Geschäftsleitung als Verantwortliche prüfen, ob die Datenpanne innerhalb von 72 Stunden der Datenschutz-Aufsichtsbehörde gemeldet werden muss (in NRW: LDI NRW). Die Frist beginnt, sobald die Panne bekannt ist.