

IT-NOTFALLKARTE

Technisch

Sofortmaßnahmen

Keine Anmeldung als Admin, wenn Netzwerk noch aktiv

Vom Netzwerk trennen; Gerät anlassen

Arbeiten mit dem IT-System einstellen;
Weitere Maßnahmen nur nach Anweisung einleiten!



Tutorial

Organisatorisch



Verantwortliche im Betrieb informieren

Helfer informieren (z. B. IT-Dienstleister, ggf. Cyber-Versicherung)

Meldepflichten beachten (Datenschutz)



Grundsätzlich wird empfohlen:

Bei Erpressungsversuch ⇒ NICHT auf Lösegeldzahlungen einlassen
Für alle Cyber-Angriffe ⇒ Strafanzeige erstatten, hat in der Regel polizeiliche Maßnahmen zur Folge

Geschäftsbetrieb wiederaufnehmen

1.

Verantwortliche bestimmen

Wer?

Was?

Wann?

2.

Check Arbeitsfähigkeit

Jede Anwendung/
Jedes IT-System
überprüfen



System 1

- Nicht betroffen
- Auslagerungsfähig auf anderes System
- Nicht arbeitsfähig, Neuaufbau nötig
- Eingeschränkt arbeitsfähig (z. B. Laptop, Handy)

System 2

- ...

3.

Wiederherstellung des Datenbestands

Vorhandene saubere Backups, bzw. nicht-betroffene Daten

www.cyber-sicherheitsnetzwerk.sachsen.de

Eine Initiative der sächsischen Handwerkskammern, sächsischen Industrie- und Handelskammern, des Landeskriminalamts Sachsen und der Digitalagentur Sachsen

CHECKLISTE



Sofortmaßnahmen eingeleitet ?

Geschäftsführung informiert ?

IT-Notfallplan beachtet ?



NOTFALLKONTAKTE

Ansprechpartner IT-Sicherheit:

Geschäftsführung:

IT-Dienstleister:

BSI-Hotline:

0800-2741000

Weiterer Notfallkontakt:

www.cyber-sicherheitsnetzwerk.sachsen.de

Eine Initiative der sächsischen Handwerkskammern, sächsischen Industrie- und Handelskammern, des Landeskriminalamts Sachsen und der Digitalagentur Sachsen