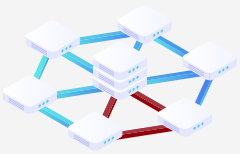
kramer & crew
Der IT-Regisseur.

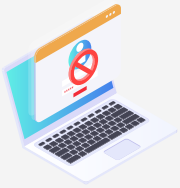
TECHNISCHE SOFORTMAßNAHMEN
BEI RANSOMWARE-FÄLLEN

Dos

Unterbrechung der Verbindung des Unternehmensnetzwerkes nach außen.



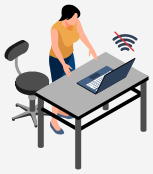
Bei Ransomware oder vermutetem Datenabfluss betroffene Netzwerkabschnitte sofort isolieren.



Sperren der betroffenen Admin- und Nutzer-Accounts.

Dokumentation der festgestellten Unregelmäßigkeiten mit Datum und Uhrzeit.

Geschäftsführung/ Vorstand sowie weitere relevante Bereiche informieren.



Mit Schadsoftware betroffene Systeme unverzüglich vom Netzwerk isolieren.

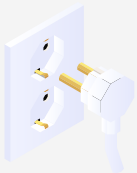
Falls keine Offline-Backups vorhanden sind, Backups sofort vom Netzwerk isolieren.

Bereithalten der Netzwerk- und Systemübersicht.

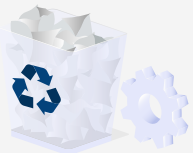
Zusammenstellung eines Krisenteams und Verantwortlichkeiten festlegen.

Information an die Cyber-Versicherung, falls eine besteht.

Don'ts



Keine Unterbrechung der Stromversorgung der IT-Systeme.



Keine Löschung der betroffenen Daten.

Keine Veränderungen an den betroffenen Systemen durchführen.

Keine Wiederherstellung bzw. kein Einspielen von Backups vor einer IT-forensischen Untersuchung.

Den Anweisungen in dem Erpresserschreiben nicht nachgehen.

Schnell handeln.
Richtig reagieren.
Jeder Schritt zählt.

0800 0060528