

RANSOMWARE CHECKLISTE

- Gerät vom Netz trennen**
- Umfang der Infektion feststellen**
- Ransomware identifizieren**
- Ransomware entfernen**
- Netzwerkaktivität prüfen**
- Notfallplan umsetzen**
- Backups einspielen**
- Dateien nicht löschen**

RANSOMWARE CHECKLISTE

Gerät vom Netz trennen

Trennen Sie bei einer Infektion betroffene Geräte sofort vom Netz. Entfernen Sie zudem Speichermedien wie USB Sticks .

Umfang der Infektion feststellen

Stellen Sie fest welche Hosts, Netze oder IoT Geräte betroffen sind und isolieren Sie alle infizierten Systeme schnellstmöglich.

Ransomware identifizieren

Wenn Sie wissen womit Sie es zu tun haben (Art der Ransomware, Verbreitungsmechanismus etc.) können Sie effektiver reagieren.

Ransomware entfernen

Ransomware falls möglich entfernen, dabei aber Kopien der betroffenen Systeme zur Analyse sichern.

Netzwerkaktivität prüfen

Wurden die Daten nur verschlüsselt oder sind auch Daten aus dem Netzwerk abgeflossen?

Notfallplan umsetzen

Bezahlen oder nicht? Für beides gibt es gute Argumente. Statt darüber zu diskutieren, sollte man im Ernstfall aber auf den Plan setzen.

Backups einspielen

Betroffene Daten über zuvor angelegte (und getestete!) Backups wiederherstellen.

Dateien nicht löschen

Falls Sie nicht bezahlen: löschen Sie betroffene Dateien nicht, sondern kopieren Sie sie auf eine externe Festplatte. Eventuell gibt es zu einem späteren Zeitpunkt ein Entschlüsselungstool.