

Notfallplan Verschlüsselungstrojaner in der Praxis

(Verdacht oder bestätigter Vorfall)



Ausgangssituation:

Das IT-System arbeitet auffällig langsam oder reagiert nicht.
Fehlermeldungen, wie z.B. „System ausgelastet“; Programme starten nicht oder stürzen ab)



- ▶ Keine Anmeldung als Administrator an den verdächtigen Geräten!
- ▶ Auftrag an IT-Dienstleister zur Prüfung



Ergebnis der Prüfung negativ
(kein Verschlüsselungstrojaner):
▶ ggfs. Updates / Systemwartung durch
IT-Dienstleister

Ergebnis der Prüfung **positiv**
(Verschlüsselungstrojaner erkannt):



Geräte komplett verschlüsselt

Geräte noch nicht komplett
verschlüsselt



- ▶ vom Netzwerk trennen
(Netzwerkkabel entfernen oder WLAN ab-
schalten)
- ▶ Ggf. die komplette Praxis vom
Internet trennen, wenn alle
Geräte betroffen sind

- ▶ Geräte „hart ausschalten“
(Netzstecker am Gerät ziehen, Akku Lap-
top entfernen, Ein-/Ausschalter
5 Sekunden gedrückt halten)

Achtung: Geräte können dadurch
beschädigt werden!



- ▶ Info an das gesamte Praxisteam
- ▶ Festlegen: Wer kümmert sich um was?

Meldung bei Behörden

- ▶ Lokale Polizeibehörde
(<https://polizei.nrw/wachenfinder>)



- ▶ Zentrale Anlaufstelle Cybercrime
NRW (ZAC)
(<https://lka.polizei.nrw/artikel/das-cybercrime-kompetenzzentrum-beim-lka-nrw>)



- ▶ Ggf. Datenschutzbehörde (Wenn
personenbezogene Daten manipu-
liert, zerstört, gestohlen, ver-
schlüsselt wurden gibt es Melde-
und Informationspflichten!)
(<https://idi-fms.nrw.de/lip/action/invoke.do?id=Datenschutzverletzung>)



Wiederinbetriebnahme der IT-Systeme (durch IT-Dienstleister)

Prüfen, ob Schlüssel für diesen Trojaner verfügbar
(<https://www.nomoreransom.org>)
(<https://id-ransomware.malwarehunterteam.com>)



1. Festplatten ausbauen und verwahren (ggf. später wiederherstellbar)
2. Backups prüfen: Aktuell? Unverschlüsselt? Nicht von Ransomware befallen?
3. Alle Systeme prüfen, betroffene komplett neu installieren
4. Active Directory / Domänen neu aufsetzen, insbesondere „Golden Tickets“ inaktivieren
5. Änderung aller Logindaten
 - ▶ Infrastruktur (Router, Switches, VPN...)
 - ▶ Anwendungen (Computer, Praxisverwaltungssoftware...)
 - ▶ Sonstige Dienste (Online-Banking, E-Mail, Webseiten...)

Nacharbeiten

- ▶ Systeme überwachen
(weitere Auffälligkeiten)
- ▶ Notfallmaßnahmen evaluieren
- ▶ Verbesserungsmaßnahmen
(technisch und organisatorisch)
zur Verhinderung erneuter Vorfälle

Recherche-Tipp IT-Forensiker

Bundesamt für Sicherheit in der Informationstechnik
(www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.pdf?__blob=publicationFile&v=41#download=1)

