KVB
Kassenärztliche Vereinigung Bayerns

Notfallkarte Verschlüsselungstrojaner – Verdacht oder bestätigter Vorfall

Ihr System verhält sich auffällig

(Langsam, reagiert nicht, Fehlermeldungen wie zum Beispiel „System ausgelastet“, Programme starten nicht oder stürzen ab)

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

IT Dienstleister bestätigt Verschlüsselungstrojaner

Geräte noch nicht komplett verschlüsselt

- Geräte hart ausschalten (Netzstecker am Gerät ziehen, Akku aus Laptop entfernen, Ein-/Ausschalter fünf Sekunden gedrückt halten)
- Achtung: Geräte können dadurch beschädigt werden!

Geräte bereits komplett verschlüsselt

- vom Netzwerk trennen (Netzwerkkabel entfernen oder WLAN abschalten)
- gegebenenfalls die komplette Praxis vom Internet trennen, wenn alle Geräte betroffen sind

Info an alle Mitarbeitenden

- Festlegen: Wer kümmert sich um was?

Dokumentation

- Was ist passiert?
- Was wurde zuletzt vorher gemacht?
- Welche Maßnahmen wurden beschlossen und umgesetzt?
- Bilder mit dem Handy machen (Bildschirminhalte, Fehlermeldungen), dabei Geräte vom Netzwerk / Internet getrennt lassen.

Meldung bei Behörden

- Lokale Polizeibehörde
  https://www.polizei.bayern.de/suche/dst/index.html
- Zentrale Anlaufstelle Cybercrime Bayern (ZAC)
  https://www.polizei.bayern.de/kriminalitaet/internetkriminalitaet/002464/index.html
- Gegebenenfalls Datenschutzbehörde (wenn personenbezogene Daten manipuliert, zerstört, gestohlen, verschlüsselt wurden, gibt es Melde- und Informationspflichten!)
  https://www.lda.bayern.de/de/index.html

Wiederinbetriebnahme

- Prüfen, ob Schlüssel für diesen Trojaner verfügbar
  https://www.nomoreransom.org/de/index.html
  https://id-ransomware.malware-hunterteam.com/
- Festplatten ausbauen und verwahren (gegebenenfalls später wiederherstellbar)
- Backups prüfen, ob aktuell, unverschlüsselt, nicht von Ransomware befallen
- alle Systeme prüfen, betroffene komplett neu installieren
- Active Directory/Domänen neu aufsetzen, insbesondere „Golden Tickets“ inaktivieren
- Änderung aller Logindaten
  - Infrastruktur (Router, Switches, VPN...)
  - Anwendungen (Computer, Praxisverwaltungssoftware...)
  - Sonstige Dienste (Online-Banking, E-Mail, Webseiten...)

Nacharbeiten

- Systeme überwachen
- Verbesserungsmaßnahmen (technisch und organisatorisch) zur Verhinderung erneuter Vorfälle

Link IT-Forensiker

- Bundesamt für Sicherheit in der Informationstechnik
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.pdf

Mit freundlicher Unterstützung der Kassenärztlichen Vereinigung Westfalen-Lippe

Stand: Mai 2026 Gestaltung: KVB Kommunikation