IKARUS security software

Notfallplan Ransomware

1. Ruhe bewahren

- **Angreifer vorerst ignorieren** - keinen Kontakt aufnehmen!
- **SOFORT Notfallteam / Hilfe** für Lageeinschätzung und Gegenmaßnahmen organisieren
- Versuchen Sie NIE ohne ausreichende Expertise Gegenmaßnahmen zu ergreifen! Vermeiden Sie Schnellschüsse, das erschwert spätere Hilfeleistungen unter Umständen sehr.

Hilfreiche Stellen:
https://bundeskriminalamt.at/602/
https://www.onlinesicherheit.gv.at/Themen/Erste-Hilfe/Meldestellen.html
https://www.wko.at/Content.Node/kampagnen/cyber-security-hotline/index.html

2. Status Quo erfassen

Überblick über die direkten Auswirkungen verschaffen:

- Welche **Systeme** sind betroffen?
- Welche **Ransomware-Variante** wurde eingesetzt? https://www.nomoreransom.org/crypto-sheriff.php?lang=de
- Mit welchen **Ausfällen** ist zu rechnen?
- Wer muss wann und wie **informiert werden**?
- Schulen/Spitäler/Ärzte sollten umgehend die Ransomware-Betreiber-Seite kontaktieren.

3. Bewusstsein schaffen

- Ihre IT-Infrastruktur ist **kompromittiert**.
- Der Angreifer kann Ihre Maßnahmen eventuell **mitverfolgen/mitlesen**.
- Der Angreifer ist wahrscheinlich **seit Tagen / Wochen** in Ihren Netzen aktiv und gut informiert.
- Vermutlich wurden **Daten gestohlen**, die veröffentlicht oder Dritten zugänglich gemacht werden.

Die Infrastruktur wird im Regelfall gemietet. Das heißt, es sind NICHT die Ransomware oder der Dienstleanbieter, die angreifen. **Jeder kann diese Werkzeuge nutzen!**

4. Befallene Systeme trennen

- **Identifizieren** Sie jene Bereiche Ihres Netzwerkes, die noch nicht infiziert wurden
- **Isolieren** Sie infizierte Bereiche so schnell wie möglich, um eine Ausbreitung zu verhindern.
- Denken Sie dabei auch an **externe Datenanbindungen** wie Festplatten, Cloud-Anbindungen oder andere Schnittstellen.

5. Ransomware entfernen

- Computer im **abgesicherten Modus** mit Netzwerkbetrieb neu starten (während des Starts wiederholt die Taste F8 drücken, bis das Menü „Erweiterte Startoptionen“ erscheint)
- System vollständig mit seriöser, **aktueller Anti-Malware-Software** prüfen und gefundene Bedrohungen löschen bzw. Expert*innen hinzuziehen
- Als Administrator in die Eingabeaufforderung den Befehl „sfc / scannow“ eingeben, um **Systemdateien zu scannen** und gefundene Probleme zu reparieren

6. Sicherheitslücken schließen

- **Einfallstor** aufdecken, gegebenenfalls mithilfe forensischer Fachkräfte. Solange Sie dies nicht erfolgreich tun ist die Chance groß, dass der Angreifer sofort wieder kommt.
- Erkennen, wo und wie sich die Angreifer **festgesetzt** haben
- **Neueste Updates und Sicherheitspatches** für gesamte Software einspielen

7. Backups überprüfen

- Vor einer Wiederherstellung **Sicherungskopie der verschlüsselten Dateien** erstellen, um weitere Schäden oder Verluste zu vermeiden
- Dateien nur aus sicheren, sauberen **Backups** wiederherstellen, wenn die Malware restlos aus dem Netzwerk entfernt wurde
- Nicht rekonstruierbare Daten aus **anderen Quellen** (Kunde, alten Systeme) wiederbeschaffen

8. Vorfall melden und Anzeige erstatten

- **Rechtlichen Vorgaben** zur Meldung des Vorfalls und Informationen Betroffener beachten
- **Partner und Kunden** bei besonders kritischen Daten **telefonisch kontaktieren**
- **Mitarbeitende** über den Vorfall und darüber, welche Informationen sie an Dritte weitergeben können oder sollen, informieren
- **Anzeige** bei der nächsten Polizeidienststelle erstatten