



8 Praxistipps gegen Verschlüsselungstrojaner:
So bleiben Sie für einen Angriff gewappnet.

✓ 1. Sicherheitsbackups erstellen.

Trotz aller Sicherheitsmassnahmen ist Ihr Unternehmen nie komplett gegen Verschlüsselungstrojaner geschützt. Deswegen ist es umso wichtiger regelmässig Sicherheitsbackups zu erstellen. Im Falle eines Angriffs sollten Sie das Gerät möglichst rasch herunterfahren und von Ihrem Netzwerk trennen (Netzwerkkabel ausziehen), bevor es andere Geräte befällt. Zudem ist es besonders wichtig die Datensicherung in einem externen Rechenzentrum oder eigenem Speichermedium zu erstellen. Weiter empfehlen wir Ihnen diese Backups nach einem geregelten Zeitplan automatisch zu generieren. Der Zyklus dazwischen sollte so angesetzt werden, dass Sie einen Datenverlust ohne grosse Schäden verkraften.

✓ 2. Patches konsequent installieren.

Kennen Sie das Gefühl, wenn Sie unter Zeitdruck stehen und auf Ihrem Bildschirm eine lästige Updatemeldung erscheint und Sie diese schnell wegdücken? Genau das sollten Sie in Zukunft nicht mehr tun, denn diese Software-Patches schliessen wichtige Sicherheitslücken, die Hacker gerne als Schleusen für Verschlüsselungstrojaner nutzen. Zudem empfehlen wir Ihnen möglichst neue Software Versionen zu nutzen, weil die Hersteller diese immer zuerst absichern.

✓ 3. Mitarbeitende sensibilisieren.

Bekanntlich sind die Mitarbeitenden das schwächste Glied in der Sicherheitskette. Hacker nutzen gerne das natürliche Verhalten und Vertrauen von Menschen aus und entwickeln immer wie raffiniertere Taktiken. Dazu gehören beispielsweise professionell gestaltete Phishing-E-Mails oder angebliche Sicherheitsbackups, die schwer von Originalen zu unterscheiden sind. Deswegen sollten Sie Ihre Mitarbeitenden über die bestehenden Risiken gründlich aufklären und das richtige Verhalten im Ernstfall schulen.

✓ 4. Ohne Adminrechte arbeiten.

Grundsätzlich benötigen viele Programme Administratorenrechte, um installiert zu werden. Das gilt natürlich auch für Schadprogramme in Form von Verschlüsselungstrojaner. Um diesen Vorteil zu nutzen, sollten Sie den Benutzerprofilen nur die Rechte, die zur Erfüllung der jeweiligen Aufgaben absolut erforderlich sind, zuweisen. Dieses Prinzip können Sie nicht nur für die Endnutzerebene ausschöpfen, sondern auch bei der Laufwerkberechtigung anwenden. Somit senken Sie das Risiko bei falscher Anwendung auf ein Minimum.

✓ 5. Netzwerke voneinander trennen.

Mit einer Aufteilung Ihres Netzwerkes begrenzen Sie die Zahl der Geräte die ein Verschlüsselungstrojaner befallen kann. Um ein Netzwerk effektiv zu segmentieren, werden Netzwerkbereiche und Anwendung logisch gruppiert. Mittels dynamischer Zugriffskontrolle, können Sie verhindern, dass ein Angreifer Ihr ganzes Netzwerk infizieren kann. Denn nur über die Benutzerkonten mit Lese- und Schreibrechte können die Dateien durch eine Schadsoftware verschlüsselt werden. Das ermöglicht Ihnen beispielsweise wichtige Geschäftsbereiche- und Daten zu separieren und nur den zuständigen Personen zugänglich zu machen.

✓ 6. Skriptblocker einsetzen.

Um das Surfen im Internet abzusichern, können Sie einen modernen Skriptblocker auf Ihrem Webbrowser installieren. Mit dem kann ein schädlicher Code auf den Webseiten meist nicht mehr ausgeführt werden. Ein toller Nebeneffekt ist, dass lästige Werbung vom Skriptblocker auch unterbunden wird.

✓ 7. Effektive Schutzmauer.

Verschlüsselungstrojaner und andere Schädlinge können sich über viele Wege einschleusen. Deshalb empfehlen wir Ihnen nebst den beschriebenen Massnahmen eine umfangreiche Schutzmauer aufzubauen. Die ParCom Sicherheitslösung für Ihr Netzwerk setzt die neue Technologie von Next-Generation-Firewalls ein, die verdächtige Verbindungen blockiert, Malware eindämmt und automatisch löscht. Zusätzliche Dienste sperren den Zugriff auf böartige und riskante Websites und blockieren infizierte E-Mails. Mit dieser mehrschichtigen Verteidigung decken Sie vielerlei Sicherheitsmassnahmen in zahlreichen Bereichen Ihres Netzwerkes ab.

✓ 8. Im Fall der Fälle richtig reagieren.

Werden Sie trotzdem zum Opfer eines Angriffes, zahlen Sie in erster Linie kein Lösegeld. Mit einer Zahlung unterstützen Sie zum einen den Markt, zum anderen haben Sie keine Garantie, dass Sie Ihre Daten zurückbekommen. Als erstes sollten Sie Ihren Computer vom Netzwerk trennen und herunterfahren. Prüfen Sie anschliessend, ob andere Geräte betroffen sind. Danach müssen Sie Ihren Computer neu aufsetzen und sämtliche Passwörter ändern. Abschliessend können Sie Ihr Backup auf den Computer einspielen.