Ransomware (Verschlüsselungstrojaner)

Kriminelle nutzen unterschiedliche Strategien, um Geld von unwissenden Opfern zu erbeuten. Ein beliebtes Vorgehen ist das Verschlüsseln von Dateien des Benutzers, der erst nach Zahlung eines «Lösegelds» wieder Zugriff darauf erhält – vielleicht …!

So schützen Sie sich vor Ransomware:

- **Erstellen Sie regelmässig eine Sicherungskopie (Backup) Ihrer Daten.**
  Stellen Sie sicher, dass Sie das Medium, auf welche Sie die Sicherungskopie erstellen, nach dem Backup-Vorgang vom System trennen. Ansonsten werden bei einem Befall durch Ransomware möglicherweise auch die Daten auf dem Backup-Medium verschlüsselt.
- **Halten Sie installierte Software und Plug-ins immer aktuell.**
  Stellen Sie sicher, dass sämtliche installierte Software, Apps sowie auch Web-Browser Plug-ins stets auf dem aktuellsten Stand sind. Verwenden Sie, wenn immer möglich, die automatische Update-Funktion der jeweiligen Software.
- **Seien Sie vorsichtig bei verdächtigen E-Mails.**
  Vorsicht ist bei allen E-Mails angebracht, welche Sie unerwartet erhalten, selbst wenn diese von einem scheinbar bekannten Absender stammen. Befolgen Sie keine Anweisungen im Text, öffnen Sie keinen Anhang und folgen Sie keinen Links.
- **Verwenden Sie ein Virenschutzprogramm.**
  Das Virenschutzprogramm muss mit automatischen Updates immer auf dem neusten Stand gehalten werden. Ansonsten besteht die Gefahr, dass neu entwickelte Schadsoftware nicht erkannt wird.

Funktionsweise

Es ist schnell passiert: Das Öffnen eines schädlichen E-Mail-Anhangs oder einer infizierten Website genügt unter Umständen, damit sich ein Verschlüsselungstrojaner auf dem eigenen System einnisten und unaufhaltsam Daten unbrauchbar machen kann, indem er sie löscht oder verschlüsselt.

Wurden Dateien auf dem System durch Ransomware verschlüsselt, zeigt diese dem Opfer einen Sperrbildschirm an. Dieser fordert das Opfer auf, eine bestimmte Geldsumme in Form einer Kryptowährung an die Angreifer zu überweisen, damit diese die verschlüsselten Dateien wieder freigeben und letztere somit wiederverwendet werden können (Erpressung). Durch die Verwendung einer Internetwährung wird die Nachverfolgung der Urheberschaft erschwert.

Die Kriminellen nehmen bei der Verbreitung von Ransomware vor allem Unternehmen ins Visier, da diese über sehr viele geschäftskritische Daten verfügen und daher eher bereit sind, zur Abwendung eines existenziellen Datenverlusts hohe Lösegeldsummen zu bezahlen. Eine Infektion mit einem Verschlüsselungstrojaner und damit verbundener Datenverlust kann aber genauso gut Privatanwender treffen.

Vorgehen im Schadenfall

Die wichtigste Massnahme passiert vor dem Schadenfall: Das regelmässige Erstellen von Sicherheitskopien (Backups) der Daten! Natürlich ist eine allfällige Infektion des Systems lästig und mit Aufwand (Neuinstallation) verbunden. Aber das Entscheidende ist, dass so die persönlichen Daten gerettet werden – auch vor anderen Bedrohungen. Weitere Informationen hierzu finden Sie unter «Schritt 1 – Sichern der Daten (https://www.ebas.ch/1-sichern-der-daten/) ».

Vom Zahlen der Lösegeldforderung wird ausdrücklich abgeraten! Es gibt absolut keine Garantie, dass Opfer wieder Zugang zu den verschlüsselten Dateien erhalten. Zudem finanziert eine Zahlung das Geschäftsmodell der Kriminellen und erlaubt diesen damit, die Angriffe mit Ransomware fortzuführen und weitere Opfer zu schädigen.

So gehen Sie im Schadenfall vor:

- **Schalten Sie Ihr Gerät «hart» aus.**
  Wenn Sie Unregelmässigkeiten auf Ihrem System feststellen und den Verdacht haben, dass eine Ransomware oder generell eine Malware am Werk ist, schalten Sie Ihr Gerät «hart» aus! «Hart» ausschalten heisst, dass Sie Ihrem Gerät den Strom nehmen – ziehen Sie also umgehend das Stromkabel heraus oder drücken Sie mindestens 5 Sekunden auf den Einschaltknopf Ihres Geräts. Nur so können Sie möglichst viele Ihrer Daten retten. Einem Smartphone und Tablet können Sie nicht so einfach den Strom nehmen, diese Geräte sollten Sie «normal» herunterfahren.
- **Säubern Sie Ihr Gerät mit einem Live-System.**
  Falls möglich und für Sie durchführbar, starten Sie Ihr Gerät mit einem Live-System wie beispielsweise «Desinfec't (https://www.heise.de/download/product/desinfect-71642) » von «c't». Von dort scannen, säubern und sichern Sie Ihre Daten erneut. Andernfalls bringen Sie Ihr Gerät zu einem Fachmann, welcher das für Sie erledigt.
- **Wenden Sie falls bekannt Entschlüsselungsroutinen an.**
  Ob für eine Ransomware bereits Entschlüsselungsroutinen bekannt sind, können Sie auf Webseiten wie www.nomoreransom.org (https://www.nomoreransom.org/de/index.html) nachlesen und diese von dort auch herunterladen und anwenden.
- **Ändern Sie alle Ihre Passwörter.**
  Weitere Informationen dazu finden Sie unter «Schritt 4 – Schützen der Online-Zugänge (https://www.ebas.ch/4-schuetzen-der-online-zugaenge/) ».
- **Informieren Sie die Behörden.**
  Informieren Sie das Nationale Zentrum für Cybersicherheit (NCSC) über das Meldeformular (https://www.report.ncsc.admin.ch/de/) und erstatten Sie bei der lokalen Polizeidienstelle Anzeige.

Breachstortion

Eine neuere Angriffsstrategie, die der mit Ransomware sehr ähnlich ist und häufig kombiniert wird, ist die sogenannte «Breachstortion». Hierbei geht es nicht primär um die Verschlüsselung der Daten, sondern es wird damit gedroht, sensible Informationen zu veröffentlichen und damit den Ruf des Opfers (meist ein Unternehmen) zu schädigen. Zur Wahrung der Reputation soll das Opfer eine bestimmte Geldsumme an die Angreifer überweisen.

Diese Strategie setzt auf die Angst des Opfers und soll der Lösegeld-Forderung des Angreifers zusätzlich Nachdruck verleihen – falls das Opfer nicht bereit ist, die für die Entschlüsselung der Daten geforderte Geldsumme zu überweisen.

Bei Ransomware handelt es sich um eine bestimmte Familie von Malware (Schadsoftware). Diese verbreitet sich üblicherweise über schädliche E-Mail-Anhänge oder infizierte Webseiten. Einmal installiert, verschlüsselt Ransomware Dateien auf dem Computer des Opfers sowie auf allfällig verbundenen Netzlaufwerken und Speichermedien (beispielsweise USB-Sticks). Die verschlüsselten Dateien werden dadurch für das Opfer unbrauchbar.