Merkblatt Ransomware

Bei Ransomware (auch *„Erpressungstrojaner“* oder *„Verschlüsselungstrojanern“* genannt) handelt es sich um eine bestimmte Familie von Schadsoftware (Malware), welche Dateien auf dem Computer des Opfers sowie auf verbundenen Netzlaufwerken (Network shares) verschlüsselt und somit für das Opfer unbrauchbar macht. Die Ransomware zeigt danach dem Opfer einen „Sperrbildschirm“ an, wobei dieser das Opfer auffordert, eine bestimmte Summe in Form von Bitcoins (eine Internetwährung) an die Angreifer zu bezahlen, damit die Dateien wieder entschlüsselt werden. Die Landschaft von erpresserischer Schadsoftware weitet sich ständig aus und die aktuellen Versionenbesitzen ein viel grösseres Schadenpotential als die ersten Versionen, welche nur den Bildschirm blockierten ohne Daten zu beschädigen. Einfallstor für solche Verschlüsselungstrojaner sind insbesondere verseuchte E-Mail und gehackte Webseiten.

Auswirkung und Gefahren

- Unbrauchbarmachen von Daten auf dem Computer
- Finanzieller Schaden bei Bezahlung des Lösegeldes

Präventive Massnahmen

- **Erstellen Sie regelmässig eine Sicherungskopie (Backup) Ihrer Daten**: Die Sicherungskopie sollte offline, das heisst auf einem externen Medium wie Beispielsweise einer externen Festplatte gespeichert werden. Stellen Sie daher sicher, dass Sie das Medium, auf welche Sie die Sicherungskopie erstellen, nach dem Backup-Vorgang vom Computer trennen. Ansonsten werden bei einem Befall durch Ransomware möglicherweise auch die Daten auf dem Backup-Medium verschlüsselt und unbrauchbar.
- **Halten Sie Ihre Software aktuell:** Sowohl Betriebssysteme als auch alle auf den Computern installierte Applikationen (z. B. Adobe Reader, Adobe Flash, Sun Java etc.) müssen konsequent auf den neuesten Stand gebracht werden. Falls vorhanden, am besten mit der automatischen Update-Funktion.
- **Seien Sie vorsichtig im Umgang mit E-Mails:** Seien Sie immer vorsichtig bei verdächtigen E-Mails, bei E-Mails, welche Sie unerwartet bekommen, oder welche von einem unbekannten Absender stammen. Befolgen Sie hier keine Anweisungen im Text, öffnen Sie keinen Anhang und folgen Sie keinen Links.
- **Verwenden Sie stets einen aktuellen Virenschutz:** Falls Sie einen kostenpflichtigen Virenschutz verwenden, stellen Sie sicher, dass Sie das Abonnement jeweils wieder für ein zusätzliches Jahr verlängern. Ansonsten wird der Virenschutz nutzlos.
- **Eine Personal Firewall muss installiert sein und aktuell gehalten werden.**

Massnahmen nach einem erfolgreichen Angriff

- Im Falle einer Infektion empfehlen wir den Computer sofort von allen Netzwerken zu trennen. Danach ist eine Neuinstallation des Systems und das Ändern aller Passwörter unumgänglich.
- Nachdem der erfolgten Säuberung des Computers, können, sofern vorhanden, die Backup-Daten wieder zurückgespielt werden. Wenn kein Backup der Daten vorliegt, ist es empfehlenswert, die verschlüsselten Daten zu behalten und zu sichern, damit Sie sie allenfalls später noch entschlüsseln können, sollte hierzu eine Lösung gefunden werden.
- In jedem Falle empfiehlt MELANI den Vorfall der Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) zur Kenntnis zu bringen und Anzeige bei der lokalen Polizeidienststelle zu erstatten.
- Verzichten Sie darauf, ein Lösegeld zu bezahlen, da dies die kriminellen Infrastrukturen stärkt und dies somit den Kriminellen ermöglicht, weitere Opfer zu erpressen. Ausserdem gibt es keine Garantie die Schlüssel für die Entschlüsselung zu bekommen.

Massnahmen für KMUs

Für Unternehmen empfiehlt MELANI zusätzlich zu den oben genannten Massnahmen folgendes:

- Sie können den Schutz Ihrer IT-Infrastruktur vor Schadsoftware (wie Beispielsweise Ransomware) durch die Verwendung von Windows AppLocker[1] zusätzlich stärken. Durch den Einsatz von Windows AppLocker können Sie definieren, welche Programme auf den Computer in Ihrem Unternehmen ausgeführt werden dürfen.
- Durch die Verwendung des Microsoft Enhanced Mitigation Experience Toolkit (EMET)[2] können Sie verhindern, dass sowohl bekannte wie auch unbekannte Sicherheitslücken in Software, welche in Ihrem Unternehmen eingesetzt werden, ausgenutzt und beispielsweise für die Installation von Schadsoftware (Malware) verwendet werden kann.
- Blockieren Sie den Empfang von gefährlichen Email Anhängen auf Ihrem E-Mail-Gateway. Zu solche gefährlichen E-Mail-Anhängen zählen unter anderem:

.js (JavaScript)
.jar (Java)
.bat (Batch file
.exe (Windows executable
.cpl (Control Panel)
.scr (Screensaver)
.com (COM file)
.pif (Program Information File)
.vbs (Visual Basic Script)
.ps1 (Windows PowerShell)

Stellen Sie sicher, dass solche gefährliche E-Mail-Anhänge auch dann blockiert werden, wenn diese in Archiv-Dateien wie Beispielsweise ZIP, RAR oder aber auch in verschlüsselten Archive-Dateien (z.B. in einem Passwortgeschützen ZIP) an Empfänger in Ihrem Unternehmen versendet werden.

[1] https://technet.microsoft.com/en-us/library/dd759117.aspx
[2] https://support.microsoft.com/en-us/kb/2458544

Zusätzlich sollten sämtliche E-Mail-Anhänge blockiert werden, welche Makros enthalten (z.B. Word, Excel oder PowerPoint Anhänge, welche Makros enthalten).

Konsultieren Sie das MELANI Merkblatt IT-Sicherheit für KMUs und das 10-Punkte Programm zur Erhöhung der IT-Sicherheit auf dem KMU Portal des Bundes: Sicherheitsvorkehrungen für die IT-Infrastruktur KMU.

Merkblatt IT-Sicherheit für KMUs:
https://www.melani.admin.ch/it-sicherheit-fuer-kmus

Sicherheitsvorkehrungen für die IT-Infrastruktur:
https://www.kmu.admin.ch/kmu/de/home/praktisches-wissen/kmu-betreiben/infrastruktur-und-it/fachgerechte-it-infrastruktur/it-sicherheit.html

Sie finden dieses Merkblatt auch Online unter folgender Web-Adresse:
https://www.melani.admin.ch/ransomware