Ransomware vorbeugen

Ransomware vorbeugen

Haben Sie in letzter Zeig den Begriff „Ransomware“ gehört?

Was ist Ransomware?

Das Bundesamt für Sicherheit in der Informationstechnik schreibt dazu folgendes:

„Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und eine Freigabe dieser Ressourcen erfolgt nur gegen Zahlung eines Lösegeldes (engl. ransom). Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung.“

Was können Sie als Internet- und E-Mail-Nutzer tun, um sich vor solchen Gefahren zu schützen?

Dazu empfielt das Bundesamt:

Behandlung von E-Mails / Spam auf dem Client (E-Mail-Programm auf Ihrem PC)
Viele E-Mails werden heutzutage als sogenannte HTML-E-Mails versendet. Damit diese im E-Mail-Programm korrekt dargestellt werden können, nutzt der E-Mail-Client jedoch die gleichen Mechanismen zur Darstellung wie der Web-Browser. Aufgrund der Größe der Darstellungskomponenten und der Vielzahl an Funktionen, enthalten diese jedoch häufig Schwachstellen, welche bei Web-Browsern durch zusätzliche Sicherheitsmaßnahmen eingedämmt werden. Dieser umgebende Schutz ist bei E-Mail-Programmen in der Regel weniger ausgeprägt. Die größte Schutzwirkung bietet in diesem Fall die Darstellung von E-Mails als Textdarstellung (oft als „Nur-Text“ bzw. „reiner Text“ bezeichnet im Gegensatz zur Darstellung als „HTML-Mail“). Ein weiterer sicherheitstechnischer Vorteil dieser Darstellung ist, dass Webadressen in der Textdarstellung nicht mehr verschleiert werden können (In einer HTML-E-Mail könnte ein Link mit der Bezeichnung „www.bsi.de“ z. B. in Wahrheit auf die Adresse „www.schadsoftwaredownload.de“ verweisen). Mindestens sollte die Ausführung

aktiver Inhalte bei Verwendung von HTML-Mails unterdrückt werden. Somit würden entsprechende, schadhafte Skripte (vergl. „Angriffsfläche minimieren“) nicht mehr ausgeführt werden können.

Präventionsmaßnahmen

Folgende Einstellung sollten für den Umgang mit MS-Office-Dokumenten-Makros (MIME/HTML-Kodierung betrachten) auf dem Client konfiguriert werden:

•JS/VBS: automatisches Ausführen bei Doppelklick verhindern
•Makros im Client (per Gruppenrichtlinie) deaktivieren
•Vertrauenswürdige Orte für Makros im AD konfigurieren
•Signierte Makros verwenden

Grundsätzlich sollten Makros, die in einer Institution genutzt werden, digital signiert sein und nur die Ausführung von Makros mit festgelegten digitalen Signaturen erlaubt werden.

Auch kann man durch eine entsprechende Konfiguration das Nachladen der Ransomware durch einen Dropper in einer E-Mail verhindern oder zumindest erschweren:

•Ausführung von Programmen (per Gruppenrichtlinie) nur aus nicht durch den Benutzer beschreibbaren Verzeichnissen (Execution Directory Whitelisting), was die effektivste Maßnahme zum Schutz vor Malware darstellt
•Entkopplung von Browser und APC (ReCoBS / Terminal-Server, Surf-VM, …

Nicos-EDVDienst hilft Ihnen gerne bei der Vorbeugung, Wartung und der Installation von Antivirus-Programmen.