1 Allgemeines

Dieses Dokument soll als Leitfaden dienen, wie Unternehmen und Behörden schnell und effektiv auf die aktuelle Bedrohungslage durch Krypto-Trojaner wie Cryptowall, TeslaCrypt oder Locky reagieren können. Zunächst werden die Mechanismen vorgestellt, mit denen diese Schädlinge in Unternehmen gelangen und wieso es trotz vorhandener Schutzmaßnahmen viele neue Infektionen gibt.

Anschließend werden konkrete Empfehlungen gegeben, wie mit kurzfristigen und langfristigen technischen und organisatorischen Maßnahmen der Bedrohung begegnet werden kann.

1.1 Woher kommt die aktuelle Infektionswelle mit Krypto-Trojanern?

1.2

Obwohl in den meisten Unternehmen umfangreiche Sicherheitsmechanismen wie Virenscanner, Firewalls, IPSSysteme, Anti-SPAM/Antiviren-Email-Gateways und Webfilter im Einsatz sind, registrieren wir aktuell weltweit eine große Anzahl von Infektionen von Unternehmensrechnern mit Verschlüsselungstrojanern wie Cryptowall, TeslaCrypt oder Locky. Im Zuge dieser Infektionen werden Dateien auf Rechnern und Netzlaufwerken verschlüsselt, um die Nutzer dieser Rechner zu erpressen, für das Entschlüsselungs-werkzeug einen Geldbetrag von typischerweise 200-500 USD zu zahlen.

Eine typische Infektion läuft dabei wie folgt ab:

- Ein Benutzer bekommt eine E-Mail, die angeblich von einem plausiblen Absender stammt, z.B. einem internen Scanner/Kopierer mit angehängtem gescannten Dokument, einem Paketdienst mit angehängten Zustellinformationen oder einem externen Unternehmen mit einer angehängten Rechnung
- Der Anhang der E-Mail enthält ein MS Word oder Excel-Dokument mit einem eingebetteten Makro. Wenn der Empfänger das Dokument öffnet, startet automatisch ein Makro, das folgende Aktionen ausführt:
- Es versucht, von einer Reihe nur für kurze Zeit existierenden Webadressen (Einweg-URLs) den eigentlichen Krypto-Trojaner herunterzuladen. Wenn eine Webadresse nicht erreichbar ist, wird die nächste angesprochen, so lange, bis der Trojaner erfolgreich heruntergeladen wurde.
- Das Makro führt den Trojaner aus
- Der Trojaner kontaktiert den Command & Control-Server des Herstellers, sendet Informationen über den infizierten Rechner und lädt einen für diesen Rechner individuellen öffentlichen Schlüssel herunter
- Mit diesem öffentlichen Schlüssel werden dann Dateien bestimmter Typen (Office-Dokumente, Datenbankdateien, PDFs, CAD-Dokumente, HTML, XML etc.) auf dem lokalen Rechner sowie auf allen erreichbaren Netzlaufwerken verschlüsselt.
- Häufig werden automatische Sicherheitskopien des Windows-Betriebssystems (Schattenkopien) gelöscht, um diese Art der Datenwiederherstellung zu verhindern
- Anschließend wird auf dem Desktop dem Benutzer eine Nachricht dargestellt, wie ein Lösegeld (oft in Formvon Bitcoins) innerhalb eines Zeitfensters von z.B. 72 Stunden gezahlt werden kann, um ein passendes Entschlüsselungstoolmit dem – nur auf dem System des Angreifers zu findenden – privaten Schlüssel zu erhalten

Dies ist nur ein Beispiel, wie eine solche Infektion ablaufen kann.

1.2 Warum sind diese Angriffe so erfolgreich?

Die Gründe für den Erfolg dieser Infektionen sind vor allem:

- Die Art der Angriffe**:**
    - Hochprofessionell agierende Produzenten der Krypto-Trojaner. Dazu gehört unter anderem auch, dass nach Zahlung der Erpressungssumme in der Regel tatsächlich ein Werkzeug zur Entschlüsselung bereitgestellt wird.
    - Geschicktes Social Engineering, um den Benutzer zum Ausführen der Installationsroutine des Trojaners zu bewegen (In der E-Mail steht etwas in der Art: „Wenn die Codierung des angehängten Word Dokuments fehlerhaft erscheint, aktivieren Sie bitte die Ausführung von Makros. Das geht wie folgt...“)
    - Nutzung von Technologien zur Infektion, die in vielen Unternehmen zugelassen sind und in denen bösartiger Code leicht verschleiert werden kann (Microsoft Office Makros, JavaScript, VBScript, CHM, Flash, Java)
    - Technologisch fortgeschrittene Schädlinge, die u.a.
        - durch Verschleierungsmechanismen auf dem infizierten System schwer zu identifizieren sind
        - diverse redundante Kommunikationsmechanismen nutzen
        - Public Key Verschlüsselungsverfahren nutzen, um ein für alle Infektionen nutzbares Entschlüsselungswerkzeug zu verhindern
- Die Situation in den betroffenen Unternehmen
    - Mangelhaftes Backupkonzept (keine zeitnahen Backups, Backups nicht offline/offsite)
    - Updates/Patches für Betriebssystem und Anwendungen werden nicht zeitnah eingespielt
    - Mangelhaftes Benutzer-/Rechtekonzept (Benutzer arbeiten als Administratoren und/ oder haben mehr Dateirechte auf Netzlaufwerken, als für ihre Aufgabe notwendig ist)
    - Mangelhafte Schulung der Benutzer („Welche Dokumente von wem darf ich öffnen?“, “Wie ist die Prozedur, wenn ein vom Typ eigentlich gesperrtes Dokument empfangen werden muss?“, „Wie erkenne ich eine Phishing-Email?“)
    - Sicherheitssysteme (Virenscanner, Firewalls, IPS, Email-/Web-Gateways) sind nicht vorhanden oder falsch konfiguriert. Dazu zählt auch fehlende Netzwerksegmentierung (Server und Workstations im gleichen Netz)
    - Unwissenheit der Administratoren im Bereich der IT-Sicherheit (.exe-Dateien werden in E-Mails zwar blockiert, nicht aber Office-Makros oder andere aktive Inhalte)
    - Falsche Prioritäten („Wir wissen, dass diese Vorgehensweise nicht sicher ist, aber unsere Leute müssen doch arbeiten.“)

1.3 Prioritäten setzen

Insbesondere der zuletzt beschriebene Punkt bezüglich der Prioritäten muss hinterfragt werden. Häufig werden mit dem Argument „Sicherheit stört die Benutzer nur, die müssen doch arbeiten“ viele sicherheitstechnisch sinnvolle Maßnahmen nicht umgesetzt. In vielen Fällen trifft das Argument zudem nicht zu, wenn die sicherheitstechnischen Maßnahmen sorgfältig geplant und angepasst an die Situation der Mitarbeiter und des Unternehmens umgesetzt werden.

In manchen Fällen wie dem Empfang per E-Mail und der internen Nutzung von Office-Dokumenten mit Makros muss man sich bewusstmachen, was für das Unternehmen wichtiger ist:

- Variante 1: Jeder Benutzer kann Office-Dokumente aus dem Internet empfangen und kann diese zudem mit Makros auf Unternehmensrechnern ausführen.
- Variante 2: Nur die Benutzer der Fachabteilungen, die mit Office-Makros arbeiten müssen (Auftragsbearbeitung, Buchhaltung, Vertrieb) bekommen per zentraler Richtlinie das Recht, Office-Makros auszuführen. Wenn Geschäftspartner eine E-Mail mit einem Office-Dokument an Empfänger im Unternehmen schicken, dann kommt diese E-Mail in eine Quarantäne. Der Empfänger wird darüber informiert und aufgefordert, sich beim Absender der E-Mail rückzuversichern, dass dieser die E-Mail tatsächlich geschickt hat. Wenn er das gemacht hat, kann der Mitarbeiter diese E-Mail selbsttätig aus der Quarantäne entlassen. Alternativ kann er den Geschäftspartner bitten, zukünftig alle Dokumente in ein passwortgeschütztes ZIP-Archiv einzupacken, dessen Passwort beide während dieses Gespräches ausmachen. Solche passwortgeschützte ZIP-Archive werden nie in E-Mail Quarantäne gestellt, die E-Mails kommen zukünftig immer sofort an und zudem ist die Übertragung per E-Mail jetzt auch noch verschlüsselt.

Vom Administrationsstandpunkt aus ist Variante 1 sicherlich am einfachsten. Bei Variante 2 muss man zunächst herausfinden, welche Fachabteilungen von Geschäftspartnern im Internet Office-Dokumente empfangen müssen, man muss die passenden Gruppenrichtlinien definieren und die Mitarbeiter der Fachabteilungen schulen. Trotzdem ist die Umsetzung von Variante 2 natürlich der sinnvollere Schritt, um mit technischen Maßnahmen und für den Mitarbeiter minimalen Änderungen im Arbeitsverhalten erheblich mehr Sicherheit zu erreichen.

Analog zu diesem Beispiel sollten die folgenden empfohlenen Maßnahmen immer unter dem Aspekt betrachtet werden, was die Konsequenzen bei Nicht-Umsetzung wären und wie man diese Maßnahmen so umsetzt, dass sie den Benutzer nur soweit nötig betreffen.

Was sollte ich sofort machen?

2.1 Allgemeine Handlungsempfehlungen

2.1.1 Backups offline/offsite

Ein Backup-Konzept muss berücksichtigen, dass nicht nur der Ausfall einer Hardware abgesichert ist (Stichwort: RAID1 ersetzt kein Backup) sondern auch der Online-Zugriff auf Sicherungen z.B. durch Verschlüsselungstrojaner auf Admin- Rechnern nicht möglich ist. Backups sollten zudem offsite d.h. auch räumlich getrennt aufbewahrt werden, um vor Umweltschäden (Feuer, Löschmitteln) geschützt zu sein.

2.1.2 Keine Adminrechte oder Rechte, die nicht benötigt werden

Jeder Benutzer sollte immer nur mit den Rechten arbeiten, die zur Erfüllung seiner Aufgabe notwendig sind. Es gibt nur sehr wenige bis keine Gründe, warum ein Mitarbeiter beim Arbeiten mit seinen Geschäftsanwendungen als Administrator angemeldet sein sollte oder warum dieser Mitarbeiter auf Netzlaufwerke zugreifen darf, die er nicht (mehr) zur Erfüllung seiner Aufgaben benötigt.

2.1.3 Patches und Updates einspielen

Nicht aktuelle Anwendungen und Betriebssysteme waren und sind der primäre Weg, über den Rechner mit Schadsoftware infiziert werden. Ein zentrales Update- und Patchmanagement muss für das zeitnahe Einspielen der Updates und Patches sorgen. Dies darf nicht dem Benutzer überlassen werden (der etwa bei Benachrichtigungen des lokalen Adobe oder Java-Updaters wiederholt auf „Später erinnern“ klickt).

2.1.4 Office-Makros per Gruppenrichtlinie deaktivieren

In einer ActiveDirectory Umgebung können Office-Makros per Gruppenrichtlinie zentral deaktiviert werden. Für die Mitarbeiter, die aufgrund ihrer Tätigkeit z.B. in der Buchhaltung oder im Vertrieb, diese Funktionalität benötigen, kann diese Funktion ebenso zentral freigeschaltet werden.

2.1.5 Bewusstsein/Schulung der Mitarbeiter

Alle technischen Maßnahmen bringen wenig, wenn die Mitarbeiter sich nicht der potentiellen Gefahren bewusst sind und nicht wissen, wie sie sich in bestimmten Situationen zu verhalten haben. Als Sofortmaßnahme müssen die Mitarbeiter geschult werden, die bei ihrer täglichen Arbeit mit solchen Sicherheitsgefahren und -maßnahmen konfrontiert sind („Wie erkenne ich eine Phishing-E-Mail?“, „Wie kann ich, obwohl Office-Dokumente in E-Mails gesperrt sind, trotzdem mit meinen Geschäftspartnern Daten austauschen?“).