SOPHOS
Security made simple.

Zur Verfügung gestellt von:

SanData | Die IT-Gruppe

Sofortmaßnahmen gegen Krypto-Trojaner

Von **Michael Veit**, Security Consultant

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.

Woher kommt die aktuelle Infektionswelle mit Krypto-Trojanern?

Obwohl in den meisten Unternehmen umfangreiche Sicherheitsmechanismen wie Virenscanner, Firewalls, IPS-Systeme, 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 Entschlüsselungswerkzeug 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 Form von Bitcoins) innerhalb eines Zeitfensters von z.B. 72 Stunden gezahlt werden kann, um ein passendes Entschlüsselungstool mit dem – nur auf dem System des Angreifers zu findenden – privaten Schlüssel zu erhalten

Dies ist nur ein Beispiel, wie eine solche Infektion ablaufen kann. Referenzen auf detaillierte Analysen einzelner konkreter Schädlinge habe ich im Anhang zusammengestellt.
Die dort beschriebenen Schädlinge nutzen teilweise andere/weitere Infektionswege, Verschlüsselungsverfahren und Kommunikationsmechanismen.

Warum sind diese Angriffe so erfolgreich?

Die Gründe für den Erfolg dieser Infektionen sind vor allem:

1. 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

2. 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..“)

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 bewusst machen, 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 Konsquenzen bei Nicht-Umsetzung wären und wie man diese Maßnahmen so umsetzt, dass sie den Benutzer nur soweit nötig betreffen.

Was sollte ich sofort machen?

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.

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.

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“ klicken kann).

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.

Endpoint-Virenschutz richtig konfigurieren

Konfigurieren Sie Ihren Virenscanner nach den empfohlenen „Best Practices".

Wenn Sie **Sophos Endpoint Protection** per Sophos Enterprise Console verwalten, dann stellen Sie sicher, dass in der AV-Policy aller Workstations und Fileserver/Terminalserver Folgendes eingestellt ist:

- On-Access-Scan: an
  - Scannen beim Lesen, Schreiben, Umbenennen: an
  - Systemspeicher scannen: an
- Download-Scans: an
- Erkennung schädlichen Verhaltens: an
- Erkennung schädlichen Datenverkehrs: an
- Erkennung von Pufferüberläufen: an

Wenn Sie **Sophos Cloud Endpoint Protection** einsetzen, dann muss für alle User eingestellt sein:

- Echtzeit-Scan: an

Wenn Sie **Sophos Cloud Server Protection** einsetzen, konfigurieren Sie für Ihre Server

- Echtzeit-Scans – lokale Dateien..: alle Schalter an
- Echtzeit-Scans – Internet: alle Schalter an
- Echtzeit-Scans-Optionen:
  - Erkennung schädlichen Verhaltens: an
  - Live-Schutz: an
- Aktivieren Sie die „Server Lockdown" Funktionalität

Email-Gateway richtig konfigurieren

Zunächst muss auf dem Email-Gateway ein Virenscan sowie ein SPAM-Scan von allen ein- und ausgehenden E-Mails eingerichtet sein, konfiguriert nach den Best Practices des Herstellers.

Wenn Ihr Email-Gateway eine Sandboxing-Technologie zur Analyse von Anhängen bereitstellt, dann aktivieren Sie diese Funktion. Die Sophos Email Appliance stellt diese Funktion ab der Version 4.0 bereit, die Sophos UTM ab der Version 9.4.

Konfigurieren Sie Ihr Email-Gateway außerdem so, dass von aus dem Internet eingehenden E-Mails keine ausführbaren Anhänge durchgelassen werden, inkl. Office-Dokumente, VBS, JavaScript, Java, ActiveX, CHM.

Sophos empfiehlt konkret die Quarantäne von Dateitypen, die typischerweise folgende Endungen haben (.ade, .adp, .bas, .bat, .chm, .cla, .class, .cmd, .com, .cpl, .exe, .hlp, .hta, .inf, .ins, .js, .jse, .lnk, .msc, .msi, .mst, .ocx, .pcd, .pif, .reg, .scr, .sct, .shb, .shs, .url, .vb, .vbs, .vbe, .wsf, .wsh, und .wsc). Wichtig ist auch, dass unverschlüsselte Archive nach diesen Dateien gescannt werden und ggf. die Archive in Quarantäne gestellt werden.

Bei der **Sophos Email Appliance** gibt es hierfür die vordefinierte Regel „Threat Protection -> SophosLabs Suspect Attachments to all".

E-Mails mit diesen Typen von Anhängen sollten in eine Quarantäne gestellt werden und der Empfänger sollte benachrichtigt werden, dass eine entsprechende E-Mail in der Quarantäne ist (z.B. durch Ersetzen des ursprünglichen Anhangs durch eine Textnachricht, dass sich der Anhang in Quarantäne befindet und wie man jetzt vorgehen soll).

Je nach E-Mail-Lösung und Organisation sowie erfolgter Schulung der Mitarbeiter können die E-Mails aus dieser Quarantäne entweder von den E-Mail-Administratoren oder den ursprünglichen Empfängern der E-Mail freigegeben werden – nachdem der betreffende Empfänger verifiziert hat (z.B. durch Telefonanruf beim Absender der E-Mail), dass es sich um eine valide E-Mail handelt.

Web-Gateway konfigurieren

Konfigurieren Sie Ihr Web-Gateway so, dass alle Downloads auf Viren gescannt werden und dass bekannte Webadressen und Mechanismen zur Kommunikation mit Command & Control-Servern geblockt werden. In jedem Fall aktivieren Sie das Scannen von SSL-Verbindungen. Wenn Ihr Web-Gateway eine **Sandboxing**-Technologie zur Analyse von Downloads bereitstellt, dann aktivieren Sie diese Funktion.

Die **Sophos UTM** konfigurieren Sie wie folgt:

- ATP: Network Protection -> Advanced Threat Protection: an
- Webfilter-Profil -> Filteraktion -> Antivirus -> Antivirenscan: Zweifachscan
- Webfilter-Profil -> Filteraktion -> Antivirus -> Sandstorm: an (ab UTM 9.4)
- Webfilter -> HTTPS -> Entschlüsseln und Scannen
- Webfilter-Kategorien sperren:
  - Anonymisierer
  - Browser-Exploits
  - Gefährliche Downloads
  - Bösartige Sites
  - Phishing
  - SPAM-URLs
  - Programmdaten werden anonymisiert (engl: Anonymizing Utilities)

Die **Sophos XG/SF-OS Firewall** konfigurieren Sie wie folgt:

- ATP: Auf dem Dashboard -> Klick in der rechten Spalte auf „Advanced Threat Protection“ -> Configure -> „Advanced Threat Protection: an“
- Web Content Filter -> Scanning: Dual Anti-Virus
- In jeder relevanten Policy-Regel -> Malware-Scan -> Decrypt & Scan HTTPS: an
- In jeder relevanten Policy-Regel -> Webfilter-Policy mit gesperrten Kategorien:
  - Anonymizers
  - Command & Control
  - Phishing & Fraud
  - SPAM URLs

Die **Sophos Web Appliance** konfigurieren Sie wie folgt:

- Global Policy -> HTTPS Scanning: an
- Global Policy -> Sandstorm: an
- Webfilter-Kategorien sperren: Proxies & Translators
  Alle anderen bösartigen URLs (Phishing, Spyware, SPAM, High Risk Sites) werden standardmäßig blockiert und Virenscan ist aktiviert.

Firewall/Intrusion Prevention System konfigurieren

Ein dediziertes oder in eine Firewall/UTM integriertes IPS sollte so konfiguriert sein, dass die Command & Control-Kommunikation blockiert wird.

In der **Sophos UTM** blockieren Sie per IPS Policy:

- Network Protection -> Intrusion Prevention -> Angriffsmuster
  - Schadsoftware

In der **Sophos XG/SF-OS Firewall** blockieren Sie per IPS Policy:

- Policies -> Intrusion Prevention Category
  - Malware Communication

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?“).

Was sollte ich zusätzlich langfristig machen?

Bewusstsein/Schulung der Mitarbeiter (Teil 2)

Zusätzlich zu den oben beschriebenen Sofortmaßnahmen für Mitarbeiter, die bei ihrer täglichen Arbeit mit solchen Sicherheitsgefahren und -maßnahmen konfrontiert sind, müssen alle Mitarbeiter regelmäßig IT-Sicherheits-Schulungen erhalten. Der Erfolg dieser Maßnahmen sollte auch regelmäßig überprüft werden.

Sophos stellt Ihnen mit dem im Anhang referenzierten Trainingshandbuch „IT Security DOs und DON'Ts" sowie dem „Schreckxikon" mit der Beschreibung von Angriffsmethoden und Gefahren im Internet dafür kostenlose Tools zur Verfügung.

Segmentierung des Firmennetzwerkes

Während sich die aktuellen Krypto-Trojaner (noch) nicht innerhalb eines Firmennetzwerkes über Netzwerkschwachstellen verbreiten, so ist das bei zukünftigen Varianten durchaus denkbar – wie ehemals Conficker, der sich durch einen Fehler in einer Windows-Netzwerkkomponente von einem einzigen infizierten Rechner im Firmennetz in Windeseile im gesamten internen Netzwerk ausbreiten konnte.

Zudem helfen alle oben gezeigten Sicherheitsmaßnahmen am Gateway nichts, wenn ein unbefugt ins Netzwerk eingebrachter Rechner (privates Notebook, Rechner eines Dienstleisters, Firmen-Notebook mit veraltetem Virenschutz) diese Maßnahmen unterwandern kann. Gegen die Gefahr eines unerlaubten Gerätes im Netzwerk können beispielsweise NAC-Lösungen helfen, die nur bekannten Rechnern den Zugriff aufs Netzwerk erlauben.

Generell sollte also auch beim Netzwerkdesign das Prinzip gelten, dass jedes System nur auf die Ressourcen Zugriff erhält, die für die Erfüllung seiner Aufgaben notwendig sind.

Im Bereich des Netzwerkes bedeutet das auch, dass man funktionale Bereiche über eine Firewall voneinander trennt wie z.B. die Client- und Servernetze. Auf die jeweiligen Zielsysteme und Dienste darf nur zugegriffen werden, wenn dies tatsächlich notwendig ist. Von den Workstations auf die Backupserver darf dann beispielsweise nur über den von der Backuplösung benötigten Port zugegriffen werden, nicht aber per Windows-Dateisystemzugriff.

In der Konsequenz muss auch über den Einsatz einer Client Firewall auf Workstations und Servern nachgedacht werden, da es typischerweise keinen Grund gibt, dass Workstations oder Server außer über dediziert bekannte Dienste untereinander kommunizieren müssen. So können auch Infektionswellen innerhalb eines Netzes verhindert werden.

Verschlüsselung von Unternehmensdaten

Durch die geeignete Verschlüsselung von Unternehmensdokumenten kann verhindert werden, dass Schädlinge unverschlüsselten Zugriff auf vertrauliche Dokumente erlangen. Das verhindert Schaden durch den Abfluss von geschäftsrelevanten Dokumenten.

Security als System betrachten

In vielen Unternehmen laufen Security-Komponenten (z.B. Firewall, VPN, IPS, Endpoint Security, Verschlüsselung, Web-Security, Email-Security, Mobile Management, WLAN Management) parallel nebeneinander her, ohne dass diese Komponenten miteinander kommunizieren, Ereignisse korrelieren und automatische Gegenmaßnahmen bei möglichen Sicherheitsvorfällen auslösen können.

Wenn diese Security-Komponenten aber miteinander kommunizieren und bei möglichen Sicherheitsvorfällen automatisch Aktionen zur Absicherung des Gesamtsystems auslösen können, also als System agieren, dann kann dadurch die Gesamtsicherheit der Infrastruktur deutlich erhöht werden. Mit der Strategie **Synchronized Security** verfolgt Sophos genau diesen Ansatz.

Security-Analysewerkzeuge einsetzen

Auch wenn alle oben genannten Maßnahmen umgesetzt sind, kann nicht mit hundertprozentiger Sicherheit gewährleistet werden, dass es in Zukunft keine Sicherheitsvorfälle/Infektionen auf Unternehmensrechnern geben wird. Wenn dieser Fall aber eintritt, dann müssen schnellstmöglich die Quelle der Infektion sowie mögliche Auswirkungen auf andere Systeme des Unternehmenssysteme identifiziert und eingeschränkt werden. Dadurch können die Aufwände zur Identifikation und Bereinigung der betroffenen Systeme und zur Wiederherstellung der Funktionsfähigkeit der IT-Infrastruktur drastisch verkürzt werden. Außerdem können durch die Indentifikation der Quelle und der Methode der Infektion mögliche Schwachstellen im Sicherheitskonzept identifiziert und geschlossen werden.

Für diese Zwecke gibt es spezielle Analyse-Werkzeuge („Root Cause Analysis/Source of Infection"-Tools), die umso effektiver sind, je mehr diese mit den im Unternehmen im Einsatz befindlichen IT-Security-Systemen kommunizieren und interagieren (siehe den vorigen Abschnitt „Security als System").

IT Security Best Practices

Viele der in dem Dokument vorgeschlagenen Maßnahmen sind „Best Practices" in der IT Security und sollten in Unternehmen eigentlich längst etabliert sein, ebenso wie andere, hier nicht erwähnte Maßnahmen wie z.B. starke Passwörter. Wir empfehlen regelmäßige Security Check-Ups/Health Checks, um mögliche Sicherheitsdefizite zu identifizieren und Sie auf dem aktuellen Stand zu halten bezüglich technischer und organisatorischer Möglichkeiten zum Schutz Ihrer IT-Infrastruktur.

Referenzen

Technisches Whitepaper zur Ransomware

Informationen zu Locky

Informationen zu aktueller Ransomware

Best Practices gegen Trojaner Troj/DocDl

IT Security DOs und DON'Ts

Schreckxikon

Zur Verfügung gestellt von:

SanData | Die IT-Gruppe

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

Oxford, GB | Boston, USA

02/16.NP.wpde.simple

SOPHOS