Security Awareness

Mensch vs. Trojaner 1:0

Die Heise Gruppe wurde Opfer der Schadsoftware Emotet. Was wir daraus lernen können: 1. Niemand ist davor sicher. 2. Besser kann man kommunikativ mit einem Schadensfall nicht umgehen. 3. Ein Schadenfall ist sehr teuer. 4. Security Awareness zahlt sich aus.

Man könnte annehmen, dass ein Verlag, in dem sich so viel IT-Know-how vereint, bestens gegen derartige Angriffe geschützt sein müsste. Gleiches könnte man wohl auch von der Informationsverarbeitung im Bankensektor annehmen – und es wäre ebenso falsch! Denn IT-Know-how allein reicht nicht aus, es muss in konkrete organisatorische Vorgaben und Prozesse gegossen werden. Und auch diese schützen nur, wenn Informationssicherheit im Unternehmen gelebt wird, wenn Informationssicherheit zu einem Teil der Unternehmenskultur geworden ist.

In diesem Artikel soll beispielhaft an dem „Banking-Trojaner" Emotet und der Heise Gruppe gezeigt werden, welche Methoden moderne Trojaner nutzen, um einen Zugang zu Ihrem Unternehmensnetzwerk zu erlangen[1].

Bericht der Infektion von Heise

Am Montag, den 13. Mai 2019 wurde einem Mitarbeiter von Heise eine E-Mail zugestellt, welche sich auf eine real existierende Geschäftsbeziehung bezog. Es wurde darum gebeten, falls sich Daten geändert haben sollten, diese doch bitte zu ändern. Zu diesem Zweck befand sich im Anhang eine Word-Datei. Die E-Mail war unauffällig. Weder fiel sie durch übliche Rechtschreib- noch durch Logikfehler auf, wie man sie bei Phishing-E-Mails oft beobachten kann. Es schien sich um eine reguläre Kommunikation mit einem Geschäftspartner zu handeln. Mit dem Öffnen der Word-Datei wurde jedoch das Ausführen von Makros bestätigt, die dann den Schadcode aus dem Internet nachgeladen haben. Der nun mit Emotet infizierte Rechner des Mitarbeiters begann sofort, auch die Rechner von Kollegen anzugreifen und zu infizieren.

Dieses löste in Folge mehrere Alarme in der Anti-Viren-Software aus, woraufhin die Systemadministratoren die betroffenen Systeme reinigten. Zunächst schien es, als ob das Problem damit unter Kontrolle sei, bis am Mittwoch, den 15. Mai 2019 die Firewall Alarmmeldungen erzeugte. Mehrere Rechner hatten Verbindung mit einem Emotet Command- & Control-Server hergestellt. Die Systemadministratoren versuchten diese Verbindungen zu blockieren und die infizierten Rechner zu isolieren. Gegen Mittwochabend zeichnete sich ab, dass dieses Wettrennen nicht zu gewinnen war. Sie führten einen kompletten Lockdown der Systeme und Netzwerke durch. Der normale Geschäftsbetrieb kam vollständig zum Erliegen.

Ab Donnerstag begann dann eine systematische Analyse der Netzwerke mit forensischen Methoden im Rahmen des Incident-Response-Prozesses. Dabei wurde offensichtlich, dass das Ausmaß der Infektion zu umfangreich war, um es mit den internen Fachkräften bewältigen zu können. Es wurden externe Berater engagiert, um bei der Analyse zu unterstützen. Ergebnis war: Mindestens fünf verschiedene Versionen von Emotet haben mehr als 100 Rechner infiziert. Das Active Directory war derart beschädigt, dass es neu aufgebaut werden musste.

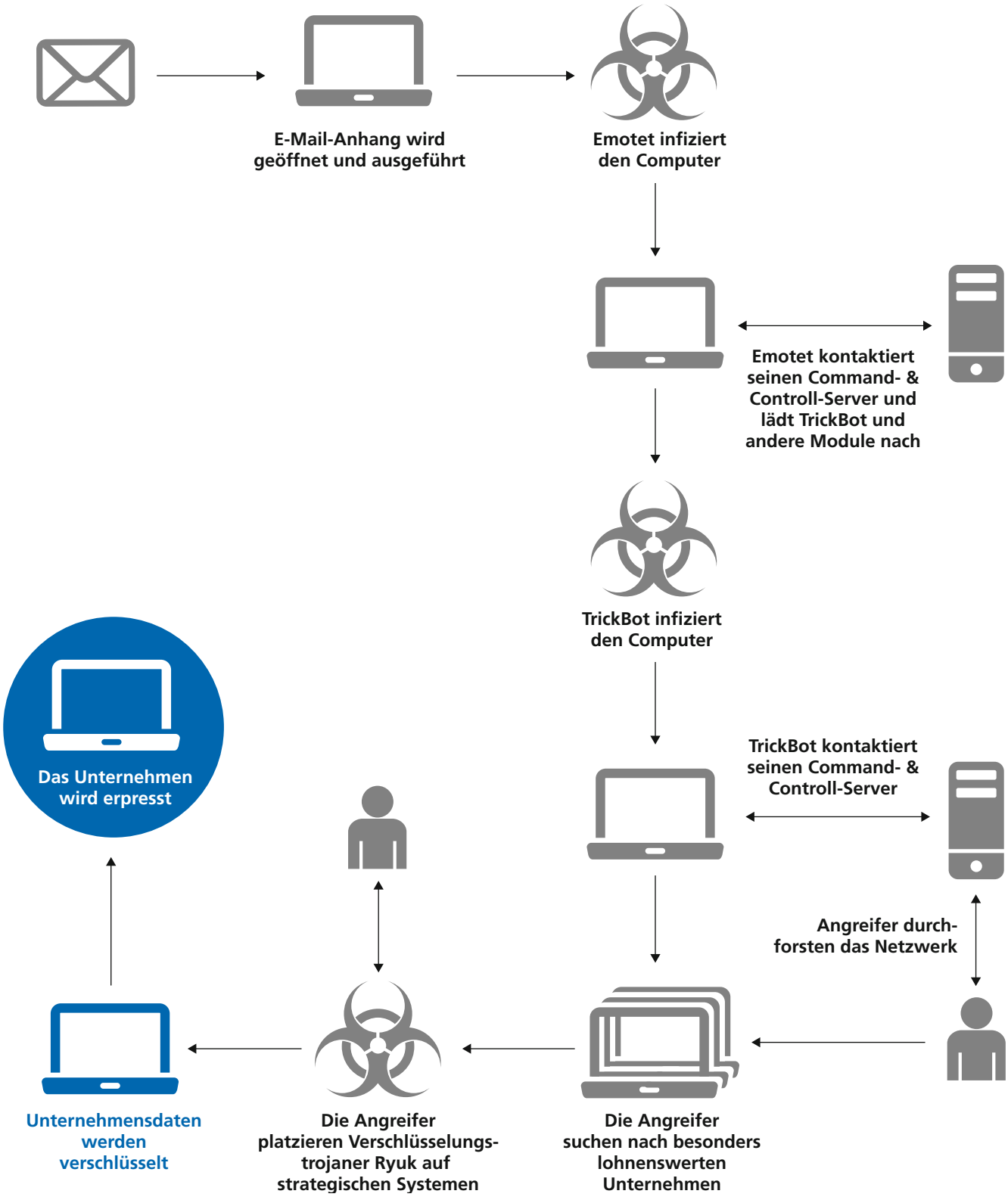
Der Wiederaufbau dauerte mehrere Tage an. Die Kosten: ca. 50.000 EUR zzgl. Umsatzeinbußen durch Produktionsausfälle sowie Kosten für verbesserte Security.

Die Wirkweise von Emotet und Co.

Wie aber konnte ein Trojaner wie Emotet trotz Viren-Scanner, Firewalls, fein abgestimmter Berechtigungsstrukturen sowie Mitarbeitersensibilisierung so erfolgreich ein ganzes Unternehmensnetzwerk infiltrieren? Die Antwort: Auch die Angreifer werden geschickter und rüsten auf.

Emotet ist nicht neu. Erstmals wurde dieser Trojaner im Juni 2014 identifiziert. Damals waren hauptsächlich Kunden österreichischer und deutscher Banken betroffen. Da Emotet den Kommunikationspartnern vortäuscht, das jeweilige Gegenüber zu sein, kann er nahezu beliebige Änderungen im Datenstrom vornehmen, ohne dass der Kunde oder die Bank etwas davon bemerken. Denn anders als beim Phishing handelt es sich beim Kunden-PC und der Onlinebanking-Webseite um die echten Systeme dieser Kommunikationsverbindung. >

[1] https://www.heise.de/security/meldung/Emotet-bei-Heise-Aufzeichnung-des-heisec-Webinars-jetzt-verfuegbar-4464045.html


E-Mail-Anhang wird geöffnet und ausgeführt
Emotet infiziert den Computer
Emotet kontaktiert seinen Command- & Controll-Server und lädt TrickBot und andere Module nach
TrickBot infiziert den Computer
TrickBot kontaktiert seinen Command- & Controll-Server
Angreifer durch-forsten das Netzwerk
Das Unternehmen wird erpresst
Unternehmensdaten werden verschlüsselt
Die Angreifer platzieren Verschlüsselungs-trojaner Ryuk auf strategischen Systemen
Die Angreifer suchen nach besonders lohnenswerten Unternehmen

AUTOR UND ANSPRECHPARTNER

Florian Brüderle
Beauftragter Informationssicherheit & Datenschutz,
E-Mail: florian.bruederle@dz-cp.de

Emotet wurde seitdem immer weiter entwickelt, bis er seit Ende 2018 auch in der Lage ist, E-Mails auszulesen und zu verwenden. Wie schon im konkreten Fall bei der Heise Gruppe beschrieben, versendet Emotet nun E-Mails mit authentisch aussehenden, aber frei erfundenen Inhalten an Personen, mit denen der infizierte Rechner bereits in Kontakt steht. Dabei werden die Signatur der ausgelesenen E-Mail, der Betreff und der Absender stimmig eingesetzt, so dass auch sensibilisierte Mitarbeiter Schwierigkeiten haben, dies als Angriff zu erkennen. Dieses sogenannte „E-Mail-Harvesting" ist der Klasse automatisierter und für den massenhaften Einsatz konzipierter APT-Angriffe (Advanced Persistent Threat) zuzuordnen.

Unter APT-Angriffen versteht man komplexe, zielgerichtete Angriffe auf lohnende Infrastrukturen. Dabei nehmen die Angreifer über einen langen Zeitraum großen, oft auch personellen Aufwand auf sich, um möglichst lange in dem Netzwerk des Opfers handlungsfähig zu bleiben. Ein in der Öffentlichkeit wahrgenommener APT war der Angriff auf den deutschen Bundestag zwischen Dezember 2014 und Mai 2015.

Nun handelt es sich bei APTs wie den oben beschriebenen und dem Angriff auf Heise zwar um unterschiedliche Angriffs- und auch Gefährdungsklassen. Der Hauptunterschied ist die hohe Automatisierung von Emotet, die zwar erstaunlich geschickt vorgeht, menschlichen Angreifern aber immer noch weit unterlegen ist. Dies ist aber kein Grund, solche Angriffe als weniger bedrohlich einzustufen. Denn zum einen können sich Gruppen, die einen APT planen, bekannter Schädlinge wie Emotet bedienen, um im Falle der frühen Entdeckung als „normale" Infektion eingeordnet zu werden. Zum anderen besitzt Emotet einen weiteren Angriffsmechanismus.

Sobald Emotet einen Computer infiziert hat, kontaktiert er seinen Command- & Control-Server. Der lädt im Hintergrund weitere Module und sogar Banking-Trojaner, wie etwa TrickBot, nach.

TrickBot wurde 2016 entwickelt und zählt zu den derzeit modernsten Banking-Trojanern. Emotet übernimmt in dieser Symbiose dann mehr die Verbreitung über das bereits beschriebene E-Mail-Harvesting. Er agiert also wie ein Wurm und unterstützt dadurch die Verbreitung von TrickBot. Sobald TrickBot installiert ist, nimmt dieser ebenfalls Verbindung zu seinem Command- & Control-Server auf und könnte damit der Beginn eines APT sein. Denn ab diesem Moment beginnen die Eigentümer des Command- & Control-Servers das Netzwerk des Opfers zu untersuchen.

Bei besonders interessanten und lukrativen Opfern werden die Angreifer dann auch manuell tätig. Sie analysieren das Netzwerk, identifizieren Backupsysteme, löschen Backups und platzieren Verschlüsselungstrojaner. Im Falle einer Emotet-/TrickBot-Infektion würde dann der Verschlüsselungstrojaner Ryuk zum Einsatz kommen. Da sich aber zuvor bereits Emotet umfassende Rechte im Active Directory des Unternehmens gesichert hat und die TrickBot-Administratoren gegebenenfalls manuell das Netzwerk untersucht haben, hat die Verschlüsselung mittels Ryuk meist katastrophale Folgen für das Unternehmen.

Die Entschlüsselung muss dann teuer bezahlt werden: Die Höhe der Summe hängt von der Finanzkraft des Opfers ab. Eine Bank müsste also tiefer in die Tasche greifen als eine Privatperson. Aber auch die Nationalität kann eine Rolle spielen. Der IT-Sicherheitsexperte Linus Neumann berichtete kürzlich in seinem Podcast „Logbuch Netzpolitik (Folge 307)", wie mittels russischer Sprachkenntnisse und eines russischen Passes ein mit dem Verschlüsselungstrojaner GandCrap verschlüsselter PC kostenlos entschlüsselt werden konnte.

Schutzmaßnahmen gegen solche Angriffe

Nach all den bedrohlichen Berichten: Kann man sich vor Emotet und Co. überhaupt schützen? Die gute Nachricht: Ja, es gibt zahlreiche Maßnahmen, die das Risiko einer Infektion verringern.

Es gibt aber nicht die „eine" wirksame Lösung. Heise hat aus dem Angriff gelernt und sechs Verteidigungslinien definiert, in denen sie sich verbessern wollen:

1. Security Awareness
2. Perimetersicherheit: Die zentralen Fragen in diesem Punkt lauten: Nutzen wir geeignete Firewalls, Web- und E-Mail-Filter? Ist es wirklich notwendig, dass wir Office-Dokumente mit Makros erhalten? Und arbeiten unsere Nutzer noch mit lokalen Administratorrechten?
3. Netzwerksicherheit: Netzwerk- und Rechtemanagement ist zentral bei der Verteidigung, deshalb die Frage: Ermöglichen wir unseren IT-Administratoren Weiterbildungen auf höchstem Niveau und haben sie in der täglichen Arbeit die notwendigen zeitlichen Ressourcen, dieses Wissen anzuwenden?
4. Monitoring: Monitoringsysteme helfen die Integrität des Netzwerkes zu überwachen. Aber auch hier benötigt man gut geschultes Personal mit ausreichend zeitlichen Ressourcen. Ansonsten droht man in einer Flut von Fehlalarmen unterzugehen, die kaum mehr jemand ernst nimmt.
5. Backups: Emotet, TrickBot und Ryuk verschlüsseln alles, auch und gerade Online-Backups. Machen sie daher offline Backups auf externen Datenträgern und testen sie diese regelmäßig.
6. Notfallmanagement: Bereiten Sie sich auf den Ernstfall vor. Denn mit kühlem Kopf und einem Plan kann man jede Krise meistern. Es ist nicht die Frage, ob sie angegriffen werden, sondern wann.

Punkt 1 der Liste, Security Awareness, ist insbesondere hervorzuheben. Wie sieht es bei Ihnen aus: Was tun Sie im Unternehmen ganz konkret für Ihre Security Awareness?

Bei einem Angriff mit Emotet, TrickBot, Ryuk sind jene Unternehmen gut geschützt, deren MitarbeiterInnen den Trick durchschauen und den verhängnisvollen Anhang nicht öffnen.

Tragischerweise ist Mitarbeitersensibilisierung genau der Bereich, den Unternehmen oft mit ungenügenden finanziellen Ressourcen ausstatten. Und lassen Sie uns Klartext reden: Web Based Trainings sind nur ein kleiner Bestandteil einer wirksamen Security-Awareness-Strategie. Nicht vergessen: Wir sprechen hier von unserer 1. Verteidigungslinie.

Deshalb betrifft Mitarbeitersensibilisierung nicht nur die normalen Computernutzer, sie richtet sich zunächst an das Management. Die Botschaft lautet: Informationssicherheit kostet Geld. Die meisten betroffenen Unternehmen erhöhen erst nach einem Vorfall ihr Budget für Informationssicherheit. Klug, wenn man es bereits zuvor getan hat und kein Opfer geworden ist.

Der nächste Adressat von Security Awareness ist die IT-Abteilung. Hier ist die Botschaft: Wir haben Probleme, und wir müssen uns ständig verbessern. Dies betrifft nicht zwangsläufig Hard- und Software. Zu oft arbeiten Administratoren mit zu hohen Rechten oder umgehen gar lästige technische Richtlinien wie globale Passwortrichtlinien. Administratoren sollten sich ständig bewusst sein, dass sie auch nur User sind. Angesichts ihrer Rechte in den Systemen sind aber gerade sie besonders gefährliche und vor allem lohnenswerte Ziele.

Und last but not least richtet sich Security Awareness an alle Mitarbeiter mit folgender Botschaft: Ich bin wichtiger Teil der Informationssicherheit meines Unternehmens. Nur mit meiner Hilfe kann das Unternehmen effektiv geschützt werden!

Fazit

Wenn alle sechs Verteidigungslinien greifen, dann wird Ihr Unternehmen zwar dennoch irgendwann angegriffen werden, aber die Auswirkungen werden erträglich sein. Stellen Sie sich die Alternative vor. Alle Ihre Unternehmensdaten, auch Ihre Backups sind unwiederbringlich verloren. Eventuell werden durch Sie auch noch Kunden oder Geschäftspartner infiziert. Können Sie den Schaden für Ihr Unternehmen beziffern? Angesichts dieses Szenarios erscheint es gar nicht mehr so schlimm, sich proaktiv auf Angriffe dieser Art vorzubereiten, oder? ▬