Sicherheit oder Komfort?
Eine Geschichte über E-Mail-Spam und Ransomware

„Sicherheit oder Komfort?“ ist eine der zentralen Fragen, der sich IT-Verantwortliche heute stellen müssen. Soll ich Web-Sicherheit deaktivieren um die Geschwindigkeit von Facebook zu erhöhen? Müssen wir wirklich die Microsoft Office-Makros deaktivieren wo unsere Finanzabteilung sie doch so häufig verwendet? Der Software Installer stürzt immer wieder ab, vielleicht sollten wir die AV-Lösung deaktivieren, so lange er läuft?

Die Antworten auf diese Fragen bergen viel Sprengstoff in sich – für die Usability, die internen Prozesse und natürlich für die Sicherheit der Firmendaten. Sophos stellt einige der möglichen Szenarien vor.

Die Bedrohung
Drahtzieher der kriminellen Machenschaften ist ein Hacker, den wir im folgenden Ghost nennen. Er hat mehrere Namen, dafür aber kein Gesicht. Sein Aufenthaltsort ist (und bleibt meistens) unbekannt, ein männlicher Weißer um die dreißig – vielleicht. Ghost ist ein Cyber-Krimineller, der in den letzten Jahren erfolgreich Geld und persönlichen Daten von Internetusern gestohlen hat. Dabei ist er wirklich kein Computer-Experte. Seine Programmierkenntnisse sind begrenzt und sein Wissen über Sicherheitssysteme nur mittelmäßig. Das hindert ihn nicht daran, seinen Lebensunterhalt erfolgreich mit Straftaten im Cyberspace zu verdienen.

Als Mittel der Wahl für seinen nächsten Angriff hat Ghost eine Ransomware ausgewählt, einen TorrentLocker. Die Zustellung erfolgt über eine Spam-Kampagne per E-Mail. Er entscheidet sich für die USA, Großbritannien, Australien und Kanada, da diese wohlhabenden Länder die größte Rendite versprechen.

Mit Hilfe der Tor-Software, taucht Ghost ins Dark Web und nimmt Kontakt zu einer Malware-as-a-Service (MaaS) Organisation auf. Für einen geringen monatlichen Betrag erhält er nun Zugriff auf die TorrentLocker Ransomware. Zusätzlich kann er über das Botnet der MaaS-Organisation Hunderttausende von Spam-E-Mails mit Microsoft Word oder Excel-Anhänge versenden. Öffnet der Benutzer die Anhänge mit den versteckten Makros, wird die Ransomware heruntergeladen. All dies wird unterstützt mit einem technischen 24/7 Support, falls Ghost mal Fragen hat oder Hilfe braucht. Seine Aktivitäten zielen auf Büros, Fabriken und Heimanwender, also so ziemlich jeden mit einer gültigen E-Mail-Adresse. Seinen Angriff startet er in den frühen Morgenstunden.

Die Verteidigung
Der Held unserer Geschichte ist Frank, Anfang 30, einziger IT-Administrator in einem mittelständischen Unternehmen irgendwo in Deutschland. Er ist verantwortlich für alles Digitale im Haus, von Storage und Netzwerken bis hin zu Home Office

Lösungen und dem defekten Drucker in der Buchhaltung. Frank weiss, dass Sicherheit aus mehreren Ebenen besteht. Je mehr Ebenen vorhanden sind, desto schwieriger ist es für Kriminelle, Malware einzuschleusen. Um möglichst viele Risiken auszuschließen, setzt auf folgende:

1. E-Mail-Schutz
Die erste Ebene in Franks Abwehrkette ist eine E-Mail-Gateway-Appliance. Diese nutzt eine Anti-Spam-Technologie, die unangeforderte und unerwünschte E-Mails herausfiltert. Er nutzt DKIM und SPF. DKIM ermöglicht das Anfügen einer digitalen Signatur an gesendete E-Mails. Diese sorgt zum einen dafür, dass der Empfänger sich auf den korrekten Absender verlassen kann, zum anderen kann sie eingehende E-Mails blockieren. Kriminelle haben so keine Möglichkeit, über die E-Mail-Domain eine gültige digitale Signatur zu erstellen und zu senden. Ein SPF-Eintrag ist eine Liste aller offiziellen E-Mail-Server, die eine Organisation verwendet. So wird überprüft, ob eine gesendete E-Mail von einem geprüften Server kam, oder nicht.

Hinweis:
SPF-Einträge beinhalten in der Regel entweder -all oder ~ all. Die Option -all bedeutet: „Diese Liste ist endgültig und keine anderen Server gelten als valide Versender meiner E-Mails." Mit anderen Worten: Der SPF-Eintrag ist auf dem neuesten Stand und jede E-Mail, die von einem anderen Server kam, ist demnach nicht von Ihnen. ~ all ist ein so genanntes Soft-Fail, das bedeutet „meine Server-Liste ist womöglich doch nicht vollständig." Soft-Fails können verwendet werden, wen SPF-Einträge modifiziert und getestet werden. Beenden Sie daher die Einträge möglichst mit -all.

2. IT-Sicherheitsregeln
Kürzlich bemerkte Frank einen Anstieg von Spam mit Microsoft Office-Anhängen; diese Dokumente führen beim Öffnen automatisch Makros aus, die eine Malware herunterladen. Hier gibt es zwei mögliche Lösungsansätze:
1) Makros können vollständig deaktiviert werden. Die automatische Ausführung wird gestoppt, der Benutzer muss sie manuell akzeptieren, bevor sie ausgeführt werden.
2) Der Microsoft Office Viewer. Diese Anwendung lässt die Anwender sehen, wie die Dokumente aussehen, ohne Word oder Excel zu öffnen. Die Viewer-Software unterstützt Makros überhaupt nicht, eine versehentliche Aktivierung ist also unmöglich.

3. Benutzerschulung
Die schwierigste aller Sicherheitsebenen ist: der User selbst. Seine Reaktionen sind am wenigsten berechenbar. Oh, ein Nigerianischer Prinz schreibt mir? Na, was der wohl will? Ich soll dem Paketzusteller meine Adresse und E-Mail bestätigen? Na klar, sonst kommt das Päckchen ja nicht!
Die Sicherheit müssen die User immer im Blick haben – sei es durch starke Passwörter, oder einfach durch die Kenntnis der vielen Bedrohungsarten, die es gibt. Frank hat sich entschieden, ein Sicherheitstraining aufzubauen, einschließlich E-Mail und Passwort-Tipps, Trainingsvideos, Poster und gelegentliche Tests mit kleinen Gewinnspielen.

4. Endpoint-Scanning
Frank weiß, dass es eigentlich egal ist, wie ausgefeilt sein E-Mail-Schutz ist, denn es gibt zahlreiche Möglichkeiten, bösartige Dateien in sein Netz zu bekommen. Es

könnte über File-Sharing-Dienste wie Dropbox, FTP, mobile Geräte oder den berühmten USB-Stick auf dem Parkplatz sein. Neuerdings sorgt Frank sich sogar um mögliche Drohnenangriffe.

Ein Web-Gateway-Appliance kann zwar viel Schutz bieten, einen hundertprozentigen jedoch nicht. Dort setzt der EndpointScan an. Ihn mögen die Nutzer aufgrund der häufig auftretenden Verlangsamung des Rechners am wenigsten. Egal, denkt Frank. Folgende Möglichkeiten gibt es:

On-Access-Scans
Dies ist der Kern der meisten Endpoint-Schutzprodukte. On-Access-Scanning prüft jede Datei, kurz bevor sie verwendet wird. Die Malware wird identifiziert, die Aktivierung verhindert und angrenzende Lösungen gewarnt.

Host Intrusion Prevention
Dieses System ist auch bekannt unter Namen wie Verhaltensüberwachung oder HIPS. Hat eine Datei den On-Access-Scanner passiert und verhält sich auffällig, kann ein HIPS diese Aktivitäten überwachen und stoppen. Diese Sicherheitsfunktion kann dabei helfen sich vor neuer Malware zu schützen, die noch niemand zuvor gesehen hat.

Live-Schutz
Angesichts der Menge an schädlichen Aktivitäten ist ein Schutz vor neuen Bedrohungen besonders wichtig. Selbst wenn Anti-Viren-Software mehrmals täglich aktualisiert wird, bleibt das Infektionsrisiko. Live-Schutz sammelt Informationen über eine Datei und verifiziert diese über einen Cloud-Service.

Web Protection und Malicious Trafic Detection
Gängige Praxis bei einem Malwareangriff ist es, diesen in mehrere Segmente aufzuspalten. Man unterscheidet:
1. Die Lieferung – in diesem Fall über Spam.
2. Den Download – ein kleines Programm zum Start der nächsten Etappe.
3. Die Ausführung – die eigentliche Malware, die den Schaden anrichtet.
Ein Downloader ist eine Miniatur-Malware, die nichts weiter tut als den eigenen Webserver anzurufen, um von dort herunterzuladen, was der Angreifer an Schadsoftware hinterlegt hat. Dies bedeutet, dass die Kriminellen ihre Angriffe über Spam ausführen können, ohne Malware mitzuschicken. Es ist sogar möglich, die Art der Malware im Verlauf der Attacke zu verändern.

Web Protection und Malicious Trafic Detection überwacht, zu welchen Webseiten der Computer eine Verbindung herstellt. Wird eine mit Malware-Verbreitung in Verbindung gebracht, wird die Verbindung blockiert.

Memory-Scanning
Wird die Malware bereits auf dem Computer ausgeführt, hilft ein Memory Scanning dabei, weiteren aktiven Malware-Code zu finden und loszuwerden. Überprüft werden sollte auch die Liste der aktiven Programme. Cyber-Kriminelle kennen jedoch eine Vielzahl von Tricks, mit denen Malware in der Prozessliste verborgen bleibt, so dass nur eine direkte Untersuchung der Memory helfen kann. Einige Malwarearten löschen sich bei Aktivität selbst von der Festplatte, so dass ein „Disc-only“-Scan vielleicht nicht hilft.

Unsere Tipps zum Endpoint-Scanning:
• Stellen Sie sicher, dass Ihre Endpoints regelmäßig aktualisiert werden.
• Überprüfen Sie, dass dies auch korrekt geschieht.
• Aktivieren Sie alle Live-Schutzfunktionen in Ihrem Produkt, um auch gegen die neuesten Bedrohungen gewappnet zu sein.
• Aktivieren Sie HIPS, Behaviour Monitoring und MemoryScanning, wenn Ihr Produkt diese Funktionen unterstützt.
• Aktivieren Sie Web Protection and Malicious Traffic Detection, um Downloader von ihrer Malwarequelle zu trennen.
• Prüfen Sie, ob die Verwendung von Wechseldatenträgen wie USB-Sticks begrenzt werden kann.
• Verwenden Sie Application Control um die Nutzung von ungenehmigter Software wie Torrent Clients, Keyloggern u.a. zu unterbinden.

Web Gateway-Schutz
Frank nutzt ein Unified Threat Management (UTM) Produkt, um Web-Richtlinien, Firewall, Netzwerk-Traffic und Serverschutz zu verwalten. Die bisherige Firewall-Regel, die den gesamten Datenverkehr in beide Richtungen erlaubte, hat er entfernt.

In den ersten Wochen seiner Tätigkeit erlaubte er den meisten Verkehr. Über einige Wochen hinweg prüfte er, was die Nutzer wirklich brauchten und schloss, was nicht benötigt wurde. Er aktiviert Intrusion Protection und nutzte die erweiterten Funktionen wie Port-Scanning um zu erkennen, wenn Kriminelle sein Netzwerk auf Schwachstellen hin testen würden. Er ermöglichte Traffic Flooding Protection um seine Server gegen einen DDoS-Angriff zu wappnen. Franks UTM-Lösung kommuniziert auch mit seinen Endpoints. Das hat den Vorteil, dass seine Policies einen Computer im Falle einer Infektion automatisch vom Internet oder internen Servern trennen können.
Im Falle einer Malware-Attacke könnten alle infizierten Computer schnell gestoppt und unter Quarantäne gestellt werden, um größeren Schaden vom Netzwerk abzuwenden.

11. Sicherheitsberechtigungen
Bei Frank gilt das Prinzip des geringsten Privilegs: wenn Benutzer nicht auf eine bestimmte Ressource oder Server im Netzwerk zugreifen müssen, dann erteilt er diese Erlaubnis auch nicht.

Wie viele andere hat auch Frank sich schon mit den Konsequenzen von Ransomware beschäftigen müssen. Die Vorgehensweise ist perfide:

• Ein Benutzer aktiviert eine infizierte Datei
• Diese holt und startet die Ransomware
• Diese kontaktiert einen Server und holt sich einen einzigartigen Encryption Schlüssel
• Dann beginnt sie, alles Vorhandene zu verschlüsseln: mobile und stationäre Festplatten, Netzwerkfreigaben und vieles mehr
• Der User bittet die IT um Hilfe
• Ein System-Admin verbringt dann viel Zeit damit, den Computer wieder herzustellen und die verlorenen Daten aus dem Backup zu holen

Verschlüsselt wird grundsätzlich alles: Bilder, Dokumente, Videos, die letzte Präsentation in der Stunden Arbeit stecken, die Bitcoin-Brieftasche und sogar die Minecraft-Kreationen.

Verantwortliche sollten darauf achten, mindestens eine Sicherung offline zu haben. Ist das Backup-Laufwerk angeschlossen, werden die hier befindlichen Daten ebenso verschlüsselt.

Hinweis:
Bei der Fehlersuche in Folge einer Ransomware-Infektion, bei der Server-Dateien verschlüsselten wurden, kann es schwierig sein, die infizierten User zu identifizieren, die den Schaden verursacht haben. Nutzen Sie den Windows-Explorer und stellen Sie auf die „Details"-Ansicht. Dann fügen Sie die Spalte „Owner" hinzu. Hier finden Sie häufig den Usernamen, der die Verschlüsselung verursachte.

Zusammenfassung
Kundige Anwender machen das Netzwerk für alle sicherer. Informationen über das „Wie" und mögliche Konsequenzen ihres Tuns helfen dabei, die Vorteile der Sicherheit verständlicher zu machen und zu verdeutlichen, welche Unannehmlichkeiten entstehen können.

Dies wird sich auch auf die Sicherheit in ihrem Heimnetzwerk auswirken. Niemand will seine Urlaubsbilder verschlüsselt sehen, nur weil er leichtsinnig auf den falschen Anhang geklickt hat.

Autor: Sascha Pfeiffer, Principal Security Consultant bei **Sophos**

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-30-55248198
sophos@tc-communications.de