Hintergrundinformationen zu Trends bei Cyberattacken

Fünf Trends bei Cyberattacken von 2018 und warum man diese 2019 im Auge behalten sollte

- *Emotet, VPNFilter, Mobile Device Management, Kryptomining, Olympic Destroyer*
- *Aktuelle Angriffsarten und wie man sich davor schützt*

Der aktuelle Cisco Threat Report 2019 wirft einen Blick auf die Gefahrenlandschaft 2018 und analysiert einige der größten Bedrohungen des vergangenen Jahres, die von der Cisco Talos Threat Intelligence Group untersucht und veröffentlicht wurden.

„Es ist wichtig, aus den bisherigen Angriffen zu lernen, um zu erfahren, was sie uns über die zukünftigen Cyberattacken erzählen“, kommentiert Holger Unterbrink, Security Researcher, Cisco Talos Threat Intelligence. „Denn die Grundlage der meisten Bedrohungen sind bewährte Methoden und nicht unbedingt immer neue Techniken. Zudem sind weltweite Entwicklungen zu berücksichtigen, da sie eher früher als später auch in Deutschland zur Anwendung kommen.“

Eine Übersicht der wichtigsten Trends:

E-Mail ist nach wie vor der häufigste Angriffsvektor, wobei 2018 Bedrohungen von Kryptomining bis hin zur steigenden Gefahr durch Emotet zu sehen waren. Unternehmen sollten ihr Mail-System im Auge behalten und Mitarbeiter regelmäßig zu E-Mail-Sicherheit schulen. E-Mail wird einfach deswegen immer noch als primäre Verteilungsmethode für Malware verwendet, weil sie weiterhin die effizienteste Methode ist.

Geld spielt eine wichtige Rolle für die meisten erfolgreichen Bedrohungen von 2018. Somit ist die Umsatzgenerierung nach wie vor eine der wichtigsten Motivationen für Angreifer.

Dies ist zudem ein Grund, warum Ransomware durch bösartiges Kryptomining überholt wurde. Bei Ransomware zahlt nur ein kleiner Prozentsatz der Opfer das Lösegeld, und selbst dann handelt es sich um eine einmalige Zahlung.

Aus der Sicht von Unternehmen gibt es viele Gründe, sich Sorgen über bösartiges Kryptomining zu machen. Wie jede aktive Software auf einem Computer beeinträchtigt auch Kryptomining die Gesamtsystemleistung und erfordert zusätzliche Performance. Das mag nicht viel auf einem System ausmachen, aber wenn man die

Kosten über die Anzahl der Endpunkte in einem Unternehmen multipliziert, lässt sich ein spürbarer Anstieg der Energiekosten feststellen. Darüber hinaus kann es die Compliance beeinträchtigen, wenn Kryptominer in Unternehmensnetzwerken Einnahmen erzielen. Dies gilt insbesondere für die Finanzbranche, wo strenge Regeln für den Umsatz aus Unternehmensressourcen gelten – unabhängig davon, ob die Verantwortlichen vom Missbrauch Kenntnis haben oder nicht. Aber am beunruhigendsten ist es wohl, dass bösartiges Kryptomining von den betroffenen Netzwerk-Betreibern häufig nicht erkannt wird. Dies weist auf beträchtliche Sicherheitslücken in der Netzwerkkonfiguration oder den allgemeinen Security-Richtlinien hin. Solche Schwachstellen können Angreifer auch für andere Zwecke ausnutzen.

Der Banking-Trojaner Emotet hat sich im Laufe der Zeit zu einer modularen Plattform entwickelt, die eine Vielzahl unterschiedlicher Angriffe ausführen kann. Einige Module stehlen E-Mail-Anmeldeinformationen, andere konzentrieren sich auf Benutzernamen und Passwörter, die im Browser gespeichert sind. Einige besitzen Funktionen für Distributed-Denial-of-Service (DDoS)-Angriffe, während andere Ransomware verteilen. Die Weiterentwicklung der Malware ist eine Möglichkeit für Angreifer, das Umsatzpotenzial zu erhöhen, indem sie den gefährdeten Computer je nach Schwachstelle ausnutzen. Was Emotet wirklich von vielen aktuellen Gefahren unterscheidet, ist einerseits die Reichweite und Modularität sowie andererseits, dass die Akteure dahinter sie offenbar als Vertriebskanal für andere Angriffsgruppen nutzen. Heute ist Emotet eine der erfolgreichsten Bedrohungen überhaupt.

Modulare Bedrohungen erfreuen sich allgemein zunehmender Beliebtheit. Sie bieten Angreifern ein bedarfsgerechtes Menü und geben ihnen die Möglichkeit, ihre Methode an das infizierte Gerät und das beabsichtigte Ziel anzupassen.
Neben Emotet ist auch VPNFilter ein Beispiel für eine modulare Bedrohung. Sie infizierte 2018 mindestens eine halbe Million Geräte in 54 Ländern. Obwohl VPNFilter vermutlich seinen Höhepunkt überschritten hat, werden weiterhin Schwachstellen in IoT-Geräten entdeckt. Es ist fast unvermeidlich, dass in Zukunft weitere Gefahren für das IoT auftreten, die eine stärkere Absicherung der Geräte zwingend erfordern.

Mobile Device Management (MDM) ermöglicht eine wesentlich bessere Kontrolle über mobile Geräte im Netzwerk. Doch Cisco Talos entdeckte 2018, dass es auch ein Eingangstor für gut finanzierte böswillige Akteure öffnet. In einem Fall wurden Geräte in Indien mit Hilfe eines Open-Source-MDM-Systems kompromittiert. Die Angreifer hatten es geschafft, bösartige Profile auf den Geräten zu installieren und Apps zu nutzen, um unter anderem Daten abzufangen, SMS-Nachrichten zu stehlen, Fotos und Kontakte herunterzuladen und den Standort der Geräte zu verfolgen.
Interessanterweise ist der beste Schutz vor einem bösartigen MDM – MDM. Unternehmen sollten sicherstellen, dass ihre Geräte damit die Installation von bösartigen Profilen oder Anwendungen überwachen und verhindern können.

Schließlich wollen einige Bedrohungen nur Schaden anrichten, wie es bei Olympic Destroyer der Fall war. Cisco Talos sah im letzten Jahr eine Reihe von ähnlichen Gefahren, aber keine machte solche Schlagzeilen wie diese Malware, deren einziger Zweck es zu sein schien, die Olympischen Winterspiele zu stören.

Mögliche Schutzmaßnahmen

Ein mehrschichtiger Sicherheitsansatz ist immer empfehlenswert. Die folgende Liste gibt einen Überblick über aktuelle Cybersicherheitstechnologien und wie sie sich im Rahmen einer integrierten Security-Architektur einsetzen lassen.

Fortschrittliche Malware-Erkennungs- und Schutztechnologien (wie Cisco Advanced Malware Protection oder AMP) können unbekannte Dateien verfolgen, bekannte bösartige Dateien blockieren und die Ausführung von Malware auf Endgeräten und Netzwerkgeräten verhindern. Cisco AMP für Endgeräte kann auch dazu beitragen, infizierte Endpunkte zu isolieren, zu untersuchen und zu bereinigen, bei Attacken die selbst die stärkste Verteidigung durchbrechen.

Lösungen für die Netzwerksicherheit wie die Cisco Next-Generation Firewall (NGFW) und das Next-Generation Intrusion Prevention System (NGIPS) können bösartige Dateien erkennen, die über das Internet in ein Netzwerk eindringen wollen oder sich innerhalb eines Netzwerks bewegen. Plattformen für Netzwerktransparenz und Sicherheitsanalysen wie Cisco Stealthwatch können interne Netzwerkanomalien erkennen, die möglicherweise darauf hinweisen, dass Malware die Nutzlast aktiviert. Schließlich kann Segmentierung eine Bewegung von Bedrohungen innerhalb eines Netzwerks verhindern und die Verbreitung eines Angriffs eindämmen.

Web-Scanning an einem Secure Web Gateway (SWG) oder Secure Internet Gateway (SIG) wie Cisco Umbrella kann Nutzer daran hindern, bösartige Domänen, IPs und URLs aufzurufen – unabhängig davon, ob sie sich im Unternehmensnetzwerk befinden oder nicht. Das hält Anwender davon ab, versehentlich Malware den Zugriff auf das Netzwerk zu ermöglichen. Zudem verhindert es eine Verbindung der Malware zu einem Command and Control (C2)-Server.

E-Mail-Sicherheitstechnologien (wie Cisco Email Security), die auf den eigenen Servern oder in der Cloud installiert sind, blockieren bösartige E-Mails. Dies reduziert die Menge an Spam, entfernt gefährliche Mails und überprüft alle Komponenten einer E-Mail (wie Absender, Betreff, Anhänge und eingebettete URLs), um darin versteckte Malware zu finden. Diese Funktionen sind sehr wichtig, da E-Mail weiterhin der wichtigste Vektor für Angriffe ist.