LogRhythm®
The Security Intelligence Company

Die Evolution von Netzwerk-Monitoring und Netzwerk-Forensik

So reagieren Sie auf komplexe Bedrohungen

LogRhythm
The Security Intelligence Company

Netzwerk-Monitoring und Netzwerk-Forensik müssen mit den Angriffen Schritt halten, die laufend die Perimeterabwehr durchbrechen. Die Bedrohungen entwickeln sich weiter – und deshalb müssen auch die Sicherheitstechnologien voranschreiten.

Cyberkriminalität kostet Unternehmen im Durchschnitt 11,7 Mio. US-Dollar pro Jahr

Die Cyberbedrohungen für Unternehmen werden immer komplexer und folgenreicher. Man braucht nur einen Blick auf die Schlagzeilen des Jahres 2017 zu werfen, um dies bestätigt zu finden.

Der britische National Health Service war eines der bekanntesten Opfer der weltweiten WannaCry Ransomware-Attacke im Mai. Und im Juni schlug die Malware NotPetya zu - die zunächst für eine neue Variante der Ransomware Petya gehalten wurde - und traf unter anderem den Containerschiff-Riesen Maersk und die TNT-Abteilung von FedEx.

Indessen ist die Wirtschaftsauskunftei Equifax erst noch dabei, das gesamte Ausmaß der Schäden durch den Hack abzuschätzen, bei dem im Mai personenbezogene Daten von 143 Millionen US-Kunden gestohlen wurden. Die Aufarbeitung dauert nicht zuletzt deswegen so lange, weil der Angriff erst im Juli entdeckt wurde. Zum Zeitpunkt der Abfassung dieses Leitfadens hatten aufgrund des Vorfalls bereits mehrere leitende Mitarbeiter ihren Posten räumen müssen.

Abgesehen von den Schäden für die betroffenen Marken und deren Ruf sind auch die finanziellen Belastungen durch solche Sicherheitsverletzungen enorm. Wie die „2017 Cost of Cybercrime Study" von Accenture und Ponemon zeigt, kosten Cyberangriffe Unternehmen im Durchschnitt 11,7 Mio. US-Dollar pro Jahr[1].

Und schließlich besteht die Wahrscheinlichkeit, dass im weiteren Verlauf zusätzliche, versteckte Kosten entstehen - durch Betriebsstörungen oder den Verlust von geistigem Eigentum oder anderen strategisch wichtigen Assets.

Unternehmen können es sich nicht leisten, die modernen Cyberbedrohungen auf die leichte Schulter zu nehmen. Und da sich die Angriffe weiterentwickeln, reichen auch die herkömmlichen Ansätze für Netzwerk-Monitoring und -Forensik nicht mehr aus. Wer auf der Stelle tritt, läuft Gefahr, mit der nächsten großen Cyberpanne Schlagzeilen zu machen.

[1] „2017 Cost of Cybercrime Study" von Accenture und Ponemon
https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

+49 89 919292 - 200 | europe@logrhythm.com | www.logrhythm.com

Rechnen Sie mit Kompromittierungen

Angreifer nutzen Methoden wie Spear Phishing und Whaling, um an Zugangsdaten zu kommen und damit in Firmennetze einzudringen. Einmal im Netz, bewegen sie sich seitwärts, um ihre Position zu verstärken und andere Konten mit erweiterten Rechten zu kompromittieren.

Verschärft wird das Problem noch dadurch, dass die Zahl der Wege in die Netzwerke zugenommen hat: Cloud Computing, mobile Geräte und das Internet der Dinge bieten Angreifern potenzielle Einfallstore. Dies erklärt zum Teil, warum in einer aktuellen Umfrage 79 Prozent der teilnehmenden Unternehmen angaben, 2016 Opfer einer Sicherheitsverletzung geworden zu sein[2].

Dass Kriminelle in Ihr Netzwerk eindringen werden, ist das „neue Normal". Deshalb ist es kein realistischer Ansatz mehr, zu viele Ressourcen für den defensiven Perimeterschutz aufzuwenden – die sogenannten „Gates, Guards and Guns" –, anstatt sich genügend auf das zu konzentrieren, was im Inneren des Netzwerks geschieht.

Bis moderne Bedrohungen ans Tageslicht kommen, vergeht meist viel Zeit. 2016 betrug die Durchschnittszeit bis zur Entdeckung einer Kompromittierung in einem Unternehmen 99 Tage[3]. Das ist zwar besser als die 146 Tage, die 2015 verzeichnet wurden, aber immer noch bei Weitem ausreichend, um Schäden anzurichten.

Unternehmen müssen eine Bedrohung identifizieren, bevor sich Auswirkungen zeigen, also so früh im Angriffslebenszyklus wie nur möglich. Dies könnte den Unterschied ausmachen zwischen einer Kompromittierung, die nur wenig Kopfschmerzen bereitet, und einer, die sich zu einer regelrechten Sicherheitspanne ausweitet, in der der Verlust der „Kronjuwelen" das Unternehmen in die Schlagzeilen bringt.

Unternehmen müssen eine Bedrohung identifizieren, bevor sich Auswirkungen zeigen, also so früh im Angriffslebenszyklus wie nur möglich

Die Kill Chain schneller durchbrechen

VPNs und Firewalls bleiben ein Muss für die „Nord-Süd"-Bewegungen von Daten ins und aus dem Netzwerk. Gleichzeitig aber wird es immer wichtiger, die Daten auch effektiv zu überwachen, wenn sie sich in „Ost-West"-Richtung durch ein Netzwerk bewegen.

Entscheidend ist, dass ein Cyberangriff in einer möglichst frühen Phase seines Lebenszyklus – auch „Kill Chain" genannt – gestoppt wird, um den Schaden für das Netzwerk zu minimieren. Die Kill Chain umfasst sechs Stufen: Erkundung, erstes Eindringen, Steuerung, Seitwärtsbewegungen, Zielerreichung und schließlich Exfiltration, Schädigung und Störung.

[2] 2017 Cyberthreat Defense Report
http://www.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/Webroot_Q3_2017_CyberEdge_Cyberthreat_Defense_Report.pdf
[3] Mandiant M-Trends 2017 https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

LogRhythm
The Security Intelligence Company

Je mehr Stufen der Angriff durchlaufen kann, desto größer die Wahrscheinlichkeit, dass das Unternehmen Schaden nimmt. Wird ein Malware-Vorfall in der Phase der Seitwärtsbewegungen entdeckt, kann sich die Malware nicht mehr durchs Netzwerk weiterbewegen und die Daten erreichen, die der Angreifer beschädigen oder stehlen will. Wenn dagegen bereits Daten exfiltriert werden, ist der Schaden mehr oder weniger angerichtet.

Aus diesem Grund sind effektive Monitoring- und Forensikmechanismen absolut unerlässlich. Nur so können die Aktivitäten im Netzwerk aufgedeckt werden, die darauf schließen lassen, dass ein Angriff in einem frühen Stadium der Kill Chain im Gang ist.

Wie sich Monitoring und Forensik weiterentwickeln müssen

Bevor eine Bedrohung entdeckt werden kann, müssen Sie in der Lage sein, Hinweise auf den Angriff in Ihrer IT-Umgebung zu sehen.

Die Aktivitäten, die auf einen Cyberangriff hindeuten – beispielsweise ein dafür typisches Benutzerverhalten –, erzeugen digitale Fingerabdrücke, Audit-Trails und Logdaten sowohl am Netzwerkzugang als auch im Netzwerk selbst. Monitoring- und Forensiktechnologien müssen diese digitalen Fingerabdrücke identifizieren und das Security Operations Center schnellstmöglich alarmieren, bevor die nächste Phase der Kill Chain beginnt.

Monitoring und Forensik dürfen sich nicht mehr darauf beschränken, nach einem Bedrohungsindikator (Indicator of Compromise, IoC) zu suchen, beispielsweise der Signatur einer Malware-Datei. Vielmehr müssen sie sich auf die Tools, Techniken und Prozeduren (TTPs) konzentrieren, die Cyberkriminelle anwenden.

Wenn die Monitoring-Technologien der Signatur einer Malware-Datei hinterherjagen, müssen sie mit jedem auftretenden IoC Schritt halten. Das macht es schwerer, neue Bedrohungen zu entdecken. Wesentlich effektiver ist es, diese Technologien auf TTPs zu fokussieren. So wird beispielsweise aufgezeigt, wenn sich ein Benutzer ungewöhnlich verhält oder massenhaft Dateien verschlüsselt werden – sichere Zeichen dafür, dass etwas nicht stimmt.

Die Threat Lifecycle Management-Plattform von LogRhythm kann Unternehmen zu der breiten und tiefen Übersicht verhelfen, die sie benötigen, damit sich Kompromittierungen nicht zu gravierenden Datenpannen entwickeln. Setzen Sie sich mit LogRhythm in Verbindung, damit Ihre Sicherheitsmitarbeiter die Sichtbarkeit und Transparenz erhalten, die sie heute brauchen.

Über LogRhythm

LogRhythm ist der Pionier für Threat Lifecycle Management™ (TLM) und befähigt Unternehmen auf sechs Kontinenten, gefährliche Cyberbedrohungen schnell zu erkennen, abzuwehren und zu neutralisieren. Die TLM-Plattform von LogRhythm vereint führende Data-Lake-Technologien, künstliche Intelligenz, Sicherheitsanalysen sowie Sicherheitsautomatisierung und -orchestrierung in einer einzigen, durchgängigen Lösung. LogRhythm schafft die Grundlagen für das KI-gestützte Security Operations Center und hilft den Kunden, ihre Cloud-, physischen und virtuellen Infrastrukturen für IT- wie auch OT-Umgebungen zu schützen. LogRhythm hat eine Reihe von Auszeichnungen erhalten, darunter die Einstufung als „Leader" in Gartners SIEM Magic Quadrant.

www.logrhythm.com

+49 89 919292 - 200 | europe@logrhythm.com | www.logrhythm.com