FORTINET

WHITEPAPER

Ein endloser Kreislauf von „Zu wenig, zu spät“

CISOs brauchen eine vollständige Automatisierung für einen proaktiven statt reaktiven Ansatz

Zusammenfassung

Viele CISOs und Security-Teams sind von der Fülle der Aufgaben überwältigt, die die aktuelle Bedrohungslage mit sich bringt. Für proaktive Sicherheitsmaßnahmen bleibt keine Zeit. Stattdessen wird nur noch reagiert und alles daran gesetzt, Sicherheitslücken möglichst ohne Störungen der Betriebsabläufe zu überprüfen und zu schließen. Dabei geraten viele Security-Teams gegenüber Cyber-Kriminellen in den Rückstand, die sich immer besser zu organisieren wissen und zunehmend ausgefeiltere Technologien einsetzen. Ihre Angriffe treffen Unternehmen in voller Härte, wenn die Bedrohungserkennung und -abwehr versagt und immer mehr automatisierte Angriffe so schnell ausgeführt werden, dass manuelle Reaktionen zum Scheitern verurteilt sind.

56 % der Führungskräfte bezeichnen ihre Cyber-Security-Analysten als überfordert.[1]

Vor nicht allzu langer Zeit waren Erkennung und Prävention von Bedrohungen noch klarer definiert. Auch wurde bei Reaktionen und Analysen von Vorfällen taktischer reagiert – und sowohl Security-Teams als auch Hacker agierten mit menschlicher Geschwindigkeit. Angesichts des Anstiegs der Cyber-Kriminalität und des Cyber-Risikos kann der Schutz vor den neuesten Cyber-Bedrohungen jedoch selbst für einen erfahrenen CISO zur Herausforderung werden.

Erschwerend kommt hinzu, dass heutige Unternehmen eine stark dezentrale Infrastruktur schützen müssen, die Dienste in mehreren Public und Private Clouds, Netzwerk-Traffic über das öffentlich zugängliche Internet und Verbindungen einer schnell wachsenden Anzahl von IoT-Geräten (Internet der Dinge) umfasst.[2] Um mit neuen Bedrohungen Schritt zu halten, implementieren viele Cyber-Security-Teams isolierte Einzellösungen – was in einer disaggregierten Security-Architektur nicht nur die Sicherheitskomplexität, sondern auch den manuellen Aufwand bei der Koordinierung von Informationen und Schutzmaßnahmen erhöht. Solche Vorgehensweisen bei der Security führen oft paradoxerweise zu einer zusätzlichen Belastung für das Unternehmen.

Ein derartiger „Flickenteppich“ bei der Sicherheit würde dem CISO und Security-Teams selbst dann große Probleme bereiten, wenn sich die Bedrohungslage gleichbleibend wäre – wovon wir leider meilenweit entfernt sind. Tatsächlich nehmen *Volumen, Geschwindigkeit* und *Raffinesse* von Bedrohungen dramatisch zu, was das Problem exponentiell verschärft. Das Ergebnis: Das CISO-Team bleibt unausweichlich in einer reaktiven Haltung gegenüber der sich weiterentwickelnden Bedrohungslage gefangen – und immer einen Schritt hinter seinen Gegnern zurück.

Steigende Alert- und Angriffszahlen: Security-Teams droht Burnout

Bedrohungsakteure beschäftigen sich intensiv mit der Entwicklung und Durchführung stärker automatisierter Methoden zum Erstellen, Testen und Verbreiten von Malware und anderen Bedrohungen. Dieses aggressive Vorgehen führt häufig dazu, dass sich CISOs und Security-Teams von der schieren Masse der Vorfälle und Warnungen schnell überwältigt fühlen: Laut einer Studie erhält das Security Operations Center (SOC) eines durchschnittlichen Unternehmens täglich über 10 000 Alerts – von denen ein Analyst jedoch realistisch betrachtet nur 20 bis 25 untersuchen kann.[3] Eine weitere Studie zeigt, dass 47 % der Security-Experten nicht glauben, dass ihre Teams angemessene Informationen über Angriffe sammeln, um proaktive Maßnahmen zu ergreifen.[4]

Aber selbst wenn die Informationen vorhanden sind, können Cyber-Security-Teams in vielen Fällen nicht darauf reagieren. Bei einer Umfrage nannten über ein Drittel der Security-Experten die Menge der Sicherheitswarnungen als eine der größten Herausforderungen.[5] Von den Befragten gaben 42 % an, dass ihr Team eine erhebliche Anzahl der Sicherheitswarnungen ignoriert, weil es mit der Masse der Alerts nicht Schritt halten kann.[6]

Wie kommt es zu dieser exponentiellen Zunahme des Volumens? Tatsächlich tragen mehrere Faktoren zu dieser Entwicklung bei: Nie zuvor gab es so viele gezielte und polymorphe Malware, wodurch die Anzahl unbekannter oder Zero-Day-Angriffe erheblich zunimmt. Wie eine Analyse von FortiGuard Labs zeigt, handelt es sich mittlerweile bei bis zu 40 % der an einem beliebigen Tag erkannten Malware um Zero-Day- oder unbekannte Bedrohungen.[7] Arbeitet ein Cyber-Security-Team ohnehin schon an der Belastungsgrenze, kann es auf Zero-Day-Angriffe nur noch reagieren und sich nach Kräften um eine schnelle manuelle Bedrohungsabwehr bemühen – was wiederum langfristig oft zu Problemen führt.

Hinzu kommt Malware-as-a-Service (MaaS), wovon auch Cyber-Kriminelle ohne Programmierkenntnisse profitieren. Malware wird so für breitere kriminelle Kreise verfügbar, was ebenfalls zum Anstieg des Angriffsvolumens beiträgt. Laut einem Threat Landscape Report von Fortinet wurden 2019 im Dark Web mindestens drei Ransomware-Familien und der Emotet-Banking-Trojaner „as a Service“ angeboten.[8]

Ein weiterer Faktor ist die zunehmende Anwendungsentwicklung, die von Prozessen wie DevOps angetrieben wird. Durch den DevOps-Prozess entstehen neue Einstiegspunkte, die ausgenutzt werden können. Auch führt die steigende Zahl der Anwendungen zu mehr potenziellen Schwachstellen. Dazu kommt, dass diese neuen Anwendungen häufig mit unsicheren IoT-Geräten interagieren. Wie eine Analyse zeigt, kommen täglich 1 Million IoT-Geräte zu Unternehmensnetzwerken hinzu – mit der Prognose, dass 25 % aller Angriffe im Verlauf dieses Jahres auf IoT-Geräte abzielen werden.[9] Angesichts einer so breiten Angriffsfläche dürfte auch die Anzahl der Bedrohungen entsprechend steigen.

Ein durchschnittliches SOC erhält über 10 000 Alerts pro Tag.[10]

„Schon bald wird sich mit einer offensiven KI in einem Bruchteil der Zeit und in vielfacher Größenordnung das gleiche Maß an Ausgefeiltheit [bei Angriffen] erreichen lassen.“[16]

Schnellere Angriffe: Notwendigkeit einer automatisierten Abwehr

Früher, als Cyber-Attacken in menschlicher Geschwindigkeit abliefen und Cyber-Kriminelle jeden Angriffsschritt manuell ausführten, bestand noch eine realistische Chance, mit manuellen Prozessen einen Exploit zu erwischen, bevor er größeren Schaden anrichtete.[11] Heutzutage automatisieren Angreifer jedoch viele ihrer Praktiken und arbeiten mit künstlicher Intelligenz (KI), um Angriffe mit Maschinengeschwindigkeit durchzuführen.

Die ersten Automatisierungsansätze von Cyber-Kriminellen umfassten hochgradig wiederholbare Aktionen wie z. B. bei einem DDoS-Angriff (Distributed Denial-of-Service).[12] Mittlerweile setzen Angreifer aber neuere Technologien ein, um die Ausführung von Angriffen aller Art zu beschleunigen. Beispielsweise gibt es Hinweise auf Schwarmtechnologien, um über ein Botnetz schneller in ein System einzudringen.[13] Das IoT-Botnetz „Hide ‘N Seek“, das eine „dezentrale, maßgeschneiderte Peer-to-Peer-Kommunikation zur Implementierung einer Vielzahl bösartiger Routinen“ verwendet, ist so etwas wie ein Prototyp dieses Ansatzes.[14] Auch künstliche Intelligenz (KI) wird zunehmend von Hackern eingesetzt, um mit einem schnelleren Fuzzing neue Schwachstellen in Anwendungen zu entdecken – womit ein bewährtes, legitimes Security-Tool nun zu einer weiteren Angriffsmethode wird.[15]

All dies bestätigt, dass jeder manuelle Schritt bei der Bedrohungserkennung und -abwehr zum Risiko für ein Unternehmen wird. Dazu zählen sowohl Routine-Aufgaben als auch Arbeiten, die Intuition und Analysen erfordern. Bedrohungen, die sich mit Maschinengeschwindigkeit bewegen, lassen sich einfach nicht durch manuelles menschliches Handeln aufhalten.

Komplexere Angriffe: Scrambling gegen ausgefeilte Taktiken

Dass Cyber-Kriminelle ihre Angriffe beschleunigen, ist nur ein Beispiel dafür, wie moderne Technologie für gezieltere, noch effektivere Attacken missbraucht wird. Als Malware noch massenhaft erzeugt und unverändert wiederverwendet oder zur Verschleierung manuell modifiziert wurde, konnte ein signaturbasierter Virenschutz noch viele Bedrohungen stoppen.

Diese Zeiten sind vorbei. Tatsächlich sind 97 % der Viren mittlerweile polymorph und ändern ihren Code automatisch bei jeder Infizierung.[17] Das bedeutet, dass eine vor wenigen Minuten extrahierte Signatur die Ausbreitung eines Virus nicht mehr verhindern kann – ein Beispiel für die zunehmende technologische Ausgefeiltheit, die der aktuellen Bedrohungslage innewohnt.

Es gibt viele weitere Beispiele für die zunehmende Komplexität von Bedrohungen:

- Spear Phishing ist eine Weiterentwicklung des herkömmlichen Phishings durch NLP (Natural Language Processing) und Data Scraping. Cyber-Kriminelle können damit den sozialen und beruflichen Kontext einer Person auswerten und automatisiert glaubwürdig erscheinende E-Mails mit bösartigen Inhalten verschicken, die genau auf den Empfänger abgestimmt sind.[18]
- Ransomware entwickelt sich zu einer Angriffsform, die immer gezielter gegen bestimmte Unternehmen eingesetzt wird. Auch lokale Regierungsstellen zählen in den letzten Monaten zu den bevorzugten Opfern.[19] Mit solchen Angriffen wurden in den vergangenen Monaten und Jahren Bürgerdienste lahmgelegt sowie Lösegeldzahlungen und Sanierungskosten in Millionenhöhe verursacht.[20]
- Wie viele andere Angriffsvektoren ist auch das Cryptojacking jetzt „as a Service“ für Cyber-Kriminelle mit weniger Fachwissen verfügbar. Dabei werden Anwendungen auf den Computern der Opfer installiert, die die Leistung erheblich ausbremsen können. Solche „Dienste“ beinhalten mittlerweile auch neue Funktionen, um Sicherheitslösungen zu deaktivieren und Firewall-Ports zu öffnen.[21]

- Im Dark Web existiert eine Open-Source-Community, die Anti-Analyse- und Verschleierungstechniken entwickelt. Malware kann dann erkennen, wann sie in einer Sandbox oder einer Emulation ausgeführt wird, oder auch Security-Tools auf infizierten Systemen deaktivieren.[22]
- Angreifer können mithilfe künstlicher Intelligenz CAPTCHA-Systeme aushebeln, die überprüfen, ob es sich bei einem Benutzer um einen Menschen und keinen Bot handelt. In 98 % der Fälle konnte bei Tests von Security-Experten das reCAPTCHA-System von Google umgangen werden.[23]

Zum Erreichen ihrer Ziele nutzen Cyber-Kriminelle mittlerweile einige der modernsten Technologien auf dem Markt. Der Emotet-Trojaner ist ein Beispiel für einen Prototyp-Angriff, der auf künstlicher Intelligenz (KI) basiert:[24] Er wird per E-Mail verbreitet – meistens in Form von Rechnungen, die der Empfänger bezahlen soll. Seit kurzem gibt es ein Zusatzmodul, das E-Mail-Threads exfiltriert und es Cyber-Angreifern ermöglicht, sich in eine gerade stattfindende E-Mail-Korrespondenz einzuschalten. Dabei wird vollkommen automatisch ein kontextbezogener Text eingefügt. Angreifer können sich so als vertrauenswürdige Benutzer ausgeben. Das erhöht die Wahrscheinlichkeit, dass ein Empfänger den Anhang öffnet, wodurch Malware auf seinem Computern installiert wird.

Auf die zunehmende Raffinesse von Cyber-Kriminellen reagieren viele CISOs mit einer ständigen Erweiterung des eigenen „Waffenarsenals“ – nur um dann festzustellen, dass der Gegner eine noch komplexere Angriffsmethode entwickelt hat.

Fazit

Die Besorgnis vieler CISOs ist nachvollziehbar – und gerechtfertigt. Das bestätigt auch der Fortinet Threat Landscape Index, den es jetzt seit knapp einem Jahr gibt. Dieser Index, der einen Eindruck von der Größe und dem Umfang der Bedrohungslandschaft vermittelt, zeigt bislang zwei Konstanten auf: eine hohe Volatilität und ein Aufwärtstrend bei den Gesamtbedrohungen.[26]

Eine stetige Zunahme der Anzahl, Schnelligkeit und Komplexität von Angriffen erfordert einen neuen Ansatz bei der Cyber-Sicherheit. Notwendig ist eine umfassende Automatisierung für den gesamten Lebenszyklus einer Bedrohung, um Cyber-Kriminelle frühestmöglich an ihrer Zielsetzung zu erkennen. Selbst Aufgaben, bei denen Entscheidungen getroffen oder Analysen durchgeführt werden müssen, dürfen nicht mehr von der Automatisierung ausgenommen werden. Fakt ist: Manuelle Security-Konzepte können mit der heutigen Bedrohungslage einfach nicht Schritt halten und müssen durch alternative Modelle ergänzt werden.

CISOs stellen fest, dass sie „nicht nur tägliche Aufgaben erledigen, sondern auch ständig über neue Risiken auf dem Laufenden bleiben müssen.“[25]

„Mittels Automatisierung werden neue Angriffsformen und Attacken in einem derartigen Tempo und Umfang entwickelt und ausgeführt, dass praktisch jeder Malware-Stamm als Zero-Day-Angriff und jede Attacke als komplexe persistente Bedrohung betrachtet werden muss.“[27]

[1] „Reinventing Cybersecurity with Artificial Intelligence: A new frontier in digital security“. Capgemini, abgerufen am 27. Januar 2020.

[2] „25% Of Cyberattacks Will Target IoT In 2020“. Retail TouchPoints, abgerufen am 27. Januar 2020.

[3] Barbara Filkins: „An Evaluator’s Guide to NextGen SIEM“. SANS Institute, 6. Dezember 2018.

[4] „Security Teams Overwhelmed by Rising Volume of Attacks“. Dark Reading, 31. Mai 2017.

[5] Jon Oltsik: „Dealing with Overwhelming Volumes of Security Alerts“. ESG, 3. März 2017

[6] Ebd.

[7] Laut internen Daten der FortiGuard Labs.

[8] „Threat Landscape Report Q3 2019“. Fortinet, 2019.

[9] „25% Of Cyberattacks Will Target IoT In 2020“. Retail TouchPoints, abgerufen am 27. Januar 2020.

[10] Barbara Filkins: „An Evaluator’s Guide to NextGen SIEM“. SANS Institute, 6. Dezember 2018.

[11] Meg King und Jacob Rosen: „The Real Challenges of Artificial Intelligence: Automating Cyber Attacks“. The Wilson Center, 28. November 2018.

[12] Ebd.

[13] Derek Manky: „The Evolving Threat Landscape—Swarmbots, Hivenets, Automation in Malware“. CSO, 29. August 2018.

[14] Ebd.

[15] Derek Manky: „Using Fuzzing to Mine for Zero-Days“. Threatpost, 7. Dezember 2018.

[16] William Dixon und Nicole Eagan: „3 ways AI will change the nature of cyber attacks“. World Economic Forum, 19. Juni 2019.

[17] Kevin Williams: „Threat Spotlight: Advanced polymorphic malware“. SmarterMSP.com, 13. Juni 2018.

[18] Meg King und Jacob Rosen: „The Real Challenges of Artificial Intelligence: Automating Cyber Attacks“. The Wilson Center, 28. November 2018.

[19] „Threat Landscape Report Q2 2019“. Fortinet, 2019.

[20] Niraj Chokshi: „Hackers Are Holding Baltimore Hostage: How They Struck and What’s Next“. The New York Times, 22. Mai 2019; Samuel Gibbs: „Ransomware attack on San Francisco public transit gives everyone a free ride“. The Guardian, 28. November 2016.

[21] Jon Bove: „An Approach for Securing Advanced Threats for Your Customers“. Fortinet, 30. Januar 2019.

[22] „Threat Landscape Report Q2 2019“. Fortinet, 2019.

[23] Stephen Helm: „Artificial Intelligence Part 2: Cyber Criminals Get Smart with AI“. Secplicity, 27. August 2018.

[24] Meg King und Jacob Rosen: „The Real Challenges of Artificial Intelligence: Automating Cyber Attacks“. The Wilson Center, 28. November 2018.

[25] Zitat eines Umfrageteilnehmers der Studie: „CISOs und Cyber-Security: Ein Bericht über aktuelle Prioritäten und Herausforderungen“. Fortinet, 26. April 2019.

[26] „Threat Landscape Report Q1 2019“. Fortinet, 2019.

[27] Saumitra Das: „When Every Attack Is a Zero Day“. Dark Reading, 23. April 2019.

FORTINET®

www.fortinet.com/de

Copyright © 2020 Fortinet, Inc. Alle Rechte vorbehalten. Fortinet®, FortiGate®, FortiCare® und FortiGuard® sowie bestimmte andere Marken sind eingetragene Marken von Fortinet, Inc. Bei anderen hier aufgeführten Namen von Fortinet kann es sich ebenfalls um eingetragene und/oder Gewohnheitsmarken von Fortinet handeln. Alle weiteren Produkt- und Unternehmensnamen sind u. U. Marken ihrer jeweiligen Eigentümer. Leistungs- und andere hierin enthaltenen Kennzahlen stammen aus internen Labortests unter idealen Bedingungen. Die tatsächliche Leistung und andere Ergebnisse können davon abweichen. Keine der hierin enthaltenen Angaben stellt eine verbindliche Verpflichtung durch Fortinet dar und Fortinet lehnt alle ausdrücklichen oder implizierten Garantien ab. Ausnahme: Fortinet geht einen verbindlichen, schriftlichen Vertrag mit einem Käufer ein, der vom Leiter der Rechtsabteilung von Fortinet unterzeichnet wird und der eine ausdrückliche Garantie dafür gewährt, dass ein bestimmtes Produkt entsprechend den genau angegebenen Leistungskennzahlen bestimmungsgemäß funktioniert. In diesem Fall sind ausschließlich die in diesem verbindlichen, schriftlichen Vertrag aufgeführten spezifischen Leistungskennzahlen für Fortinet bindend. Jede diesbezügliche Garantie beschränkt sich einzig auf die Leistung unter den gleichen idealen Bedingungen wie bei den internen Labortests von Fortinet. Fortinet lehnt dementsprechend jegliche ausdrücklichen oder implizierten Verpflichtungen, Zusagen und Garantien ab. Fortinet behält sich das Recht vor, diese Veröffentlichung ohne Ankündigung zu ändern, zu bearbeiten, zu übertragen oder anderweitig zu überarbeiten. Es gilt die jeweils aktuellste Fassung der Veröffentlichung.

5. Mai 2020, 9:36 Uhr

595005-0-1-DE