radware

Leitfaden

CISO-Leitfaden für Sicherheit im Zeitalter der KI

Inhalt

Einleitung

Die Cybersicherheit hat sich in den letzten Jahren zunächst schnell und dann rasant weiterentwickelt. Zu alten Problemen wie strengen Vorschriften und Personalmangel haben sich neue Herausforderungen gesellt, darunter automatisierte und KI-gestützte Angriffe. Damit ist die Aufgabe des CISO, die Sicherheit und Effizienz im Unternehmen zu wahren, noch anspruchsvoller geworden. Und die Fragen lassen sich noch schwieriger beantworten. Wie zum Beispiel: Können sich die Abwehrmaßnahmen genauso schnell weiterentwickeln wie die Bedrohungen? Wie kann man mit weniger Sicherheitspersonal mehr Vorschriften einhalten und Schwachstellen beheben? Wie bleibe ich immer einen Schritt voraus, um Sicherheit zu gewährleisten? Genau das erfahren Sie in diesem Leitfaden. Neben den größten Hindernissen der Cybersicherheit, mit denen CISOs heutzutage konfrontiert sind, werden auch die fehlenden Elemente erläutert, die für ein sichereres Arbeitsumfeld erforderlich sind. Außerdem wird gezeigt, wie Radware® EPIC-AI™ mithilfe KI-gestützter Algorithmen und generativer KI-Funktionen für einen plattformübergreifenden Echtzeit-Schutz sorgt – präzise und ohne manuelles Eingreifen. Für CISOs und ihre Teams bedeutet das: schnellere Problemlösung, geringere Kosten und mehr Sicherheit für Applikationen und Infrastruktur.

Teil I. Vier Herausforderungen bei der Aufrechterhaltung von Applikationssicherheit

CISOs müssen eine lange Liste vielfältiger Verantwortlichkeiten wahrnehmen, die von Risikobewertung und schnellen Maßnahmen bis hin zu Kommunikationsaufgaben und der Zuweisung von Ressourcen reicht. Doch welche Herausforderungen rauben ihnen den Schlaf?

Herausforderung 1: Der Wandel der Bedrohungslandschaft

Daten aus dem Cloud-Netzwerk von Radware zeigen signifikante Veränderungen in der modernen Bedrohungslandschaft, einschließlich einer Verlagerung auf die Applikationsebene. Der Umfang, die Häufigkeit und Komplexität dieser Angriffe nehmen über alle Angriffsvektoren hinweg weiter zu. Das durchschnittliche DDoS-Angriffsvolumen stieg 2024 um 127 % (Jahresvergleich), Bot-Angriffe nahmen in H1 2024 um 61 % zu (Jahresvergleich), und die abgewehrten Web-DDoS-Angriffe stiegen von H2 2023 bis H1 2024 um 265 %.

Die Veränderungen in der Cybersicherheit sind auf vier Hauptfaktoren zurückzuführen:

Neue Beweggründe von Hacktivisten

Ein Blick auf die aktivsten Hacker-Aktivistengruppen (Hacktivisten) der letzten Jahre zeigt, dass drei Arten von Angriffsmotiven auf dem Vormarsch sind:

Politisch motivierte Angriffe – Gruppen wie NoName, Killnet, Anonymous Russia und Passion Group haben ihre Aktivitäten nach dem russischen Einmarsch in die Ukraine intensiviert. Seitdem hat dieser Trend auch auf andere Ereignisse übergegriffen, bei denen sich Alltagsleben und Politik überschneiden – vom Eurovision Song Contest bis hin zu den Olympischen Sommerspielen. Alle globalen Zusammenkünfte, die in einem gewissen politischen Kontext stehen, sind für verschiedene Hacktivistengruppen attraktiv, die Organisationen aus den beteiligten Ländern angreifen wollen. So löste beispielsweise der Besuch des ukrainischen Präsidenten Wolodymyr Selenskyj in Kanada im vergangenen Jahr eine Reihe von Angriffen auf kanadische Websites aus. Die Websites des kanadischen Parlaments, des Premierministers, von Banken, Verkehrsbetrieben, dem Flughafen usw. waren im Vorfeld und während des Besuchs tagelang nicht erreichbar. Ähnliche Angriffe auf Websites der französischen Regierung erfolgten, nachdem Frankreich die Lieferung von Raketenabwehrsystemen an die Ukraine angekündigt hatte und damit die Aufmerksamkeit von NoName erregte, einer wichtigen pro-russischen Hacktivistengruppe.

Religiös motivierte Angriffe – Diese Art von Angriffen wird häufig verzeichnet, wenn pro-islamische Hacktivistengruppen ein Land oder eine Organisation ins Visier nehmen, die ihrer Meinung nach den muslimischen Glauben beleidigt oder geschädigt hat. Sie haben vielleicht mitbekommen, dass Gruppen wie Anonymous Sudan, Mysterious Team Bangladesh, Dragon Force Malaysia und andere in den letzten Jahren während verschiedener Konflikte aktiver wurden. Aber man muss keine große Organisation oder Marke sein, die sich lautstark für religiöse Überzeugungen einsetzt, um den Zorn dieser Angreifer auf sich zu ziehen. Im November 2023 wurde Cloudflare angegriffen, das OpenAI schützen wollte, worin pro-palästinensische Hacktivisten eine Verbindung zur pro-israelischen Bewegung sahen. Während der australischen Fashion Week kam es im ganzen Land zu einer merklichen Angriffswelle wegen eines Kleides, das einen arabischen Vers aus dem Koran trug.

Finanziell motivierte Hacktivisten – Andere Hacktivistengruppen sind stärker formalisiert und finanziell motiviert. Sie bieten Angriffstools für DDoS, Kontoübernahme (Account Takeover, ATO) oder Krypto-Ceiling-Services. Diese Gruppen werben in ihren Social-Media-Kanälen für ihre Fähigkeiten, damit die Zielgruppe ihre DDoS-for-hire- und Botnet-for-hire-Tools kauft und nutzt, um ihre eigenen Ziele anzugreifen. Das „Infrashutdown"-Tool von Anonymous Sudan kann problemlos online erworben werden.

Weiterentwicklung der Angriffstools

Neuartige Angriffsmethoden der Hacktivisten haben ebenfalls zum Wandel der Bedrohungslandschaft beigetragen. Dabei haben nicht nur der Umfang und die Geschwindigkeit der Angriffe zugenommen. Sie sind automatisierter und raffinierter als je zuvor und verwenden oft mehrere Zufallsmethoden, um herkömmliche Abwehrmaßnahmen zu umgehen. Außerdem werden verschiedene Angriffsvektoren in einzelnen Tools kombiniert, um eine umfassende Angriffsplattform zu schaffen. Und Sie müssen nicht einmal ins Darknet gehen, um beispielsweise das bekannte MHDDoS-Angriffstool zu suchen. Es ist ganz öffentlich auf GitHub verfügbar. Dieses Tool kombiniert 56 verschiedene Angriffsmethoden, darunter DDoS-Angriffsvektoren (HTTP/S GET, POST Floods), Bot-Angriffsvektoren (umgehen CAPTCHAs und geben sich als Google-Suchmaschinen-Crawler aus, um wie ein legitimer Bot zu erscheinen), Angriffsvektoren für Webapplikationen (PHP-, Apache-, WordPress-Schwachstellen) und integrierte Funktionen zur Umgehung gängiger Abwehrmaßnahmen (Cloudflare, Google Shield).

Diese Art von Multi-Vektor-Angriffstool zeigt, dass moderne Angreifer und ihre Tools nicht zwischen WAF, DDoS-Schutz, Bot-Schutz usw. unterscheiden. Im Gegensatz zu den Angreifern unterscheiden Unternehmen aber sehr wohl zwischen diesen Schutzbereichen und verfügen in der Regel über separate Teams und Budgets für jeden davon. Deshalb müssen Unternehmen umdenken und von Silo-Schutzmaßnahmen auf eine integrierte Plattform übergehen, die vor einer Vielzahl von Bedrohungen schützt und diese All-in-one-Angriffstools effektiv ausschalten kann.

Wachsende Zahl von Angreifern

Dass die Hacker-Community in letzter Zeit stark gewachsen ist, hat vor allem zwei Gründe:

Gamer tragen zum Wachstum der Angreifer-Community bei – Erstens beobachten wir die Umwandlung von normalen Gamern in Angreifer. Bei vier von fünf Angreifern, die an ATO- und DDoS-Angriffen beteiligt sind, handelt es sich um Gamer. Seit der COVID-Pandemie ist die Gaming-Community um 700 Millionen neue Mitglieder angewachsen. Wenn auch nur ein Bruchteil davon zu Angriffen übergeht, wäre das eine enorme Ausweitung dieser Gruppe.

Hacker bauen ihre Reichweite durch Online-Netzwerke aus – Hacker skalieren ihre Angriffe durch soziale Einflussnahme. Sie posten in ihren sozialen Medien und nutzen Marktplätze und Hacking Malls in diesen Netzwerken. Über diese sozialen Netzwerke können Hacker ihre Anhängerschaft erweitern und mehr Menschen zur Teilnahme an Angriffen bewegen.

KI-gestützte Angriffsrevolution

Künstliche Intelligenz scheint unser Leben jeden Tag mehr zu bestimmen – und der Kampf um Cybersicherheit ist dabei keine Ausnahme. Zu den wichtigsten Entwicklungen, die zum Wandel der heutigen Bedrohungslandschaft beitragen, gehört der zunehmende Einsatz von KI bei Cyberangriffen. Und das funktioniert wie folgt:

KI-Automatisierung – Hacker automatisieren ihre Angriffe mithilfe von KI, genau wie Entwickler, die von ChatGPT oder anderen Tools für generative künstliche Intelligenz (GenAI) profitieren, um Code schneller und besser zu erstellen. Hacker wenden dasselbe Prinzip auf Cyberangriffe an, indem sie spezielle GenAI-Tools wie WolfGPT, XXXGPT und andere entwickeln, um Code für Malware, Botnets, Cryptoware, DDoS-Tools, ATO-Tools usw. zu erstellen.

KI im Tool selbst – KI wird immer häufiger direkt in die Angriffstools integriert, um raffiniertere Angriffe zu ermöglichen und herkömmliche Abwehrmechanismen wie CAPTCHAs zu überwinden. Im Mai 2024 veröffentlichte ein bekanntes DDoS-Tool namens stresser.cat eine Bildschirmaufzeichnung, um die CAPTCHA-Lösungsfähigkeiten des Tools zu demonstrieren. Die Genauigkeit des Tools beträgt derzeit bis zu 77 %, wird aber in künftigen Versionen zweifelsohne steigen.

KI für Zero-Days – Aktuelle Studien haben gezeigt, wie Hacker jetzt autonome Angriffe aus Zero-Day-Schwachstellen ableiten können. Sie nutzen allgemeine Schwachstellen und Exploits (CVEs), die veröffentlicht wurden, und verwandeln sie automatisch in Angriffe. Als Forscher der University of Illinois Urbana-Champaign (UIUC) einen Test durchführten, bei dem ChatGPT 4 einen Datensatz mit 15 realen Schwachstellen erhielt, schnitt das Tool deutlich besser ab als andere Modelle und Tools. Es konnte 87 % dieser Schwachstellen ausnutzen, wobei die Leistung noch ausbaufähig ist.

Wie können Sie im Zeitalter der automatisierten und KI-gestützten Cyberbedrohungen überleben? Bekämpfen Sie KI mit KI. Im Kampf gegen Angriffstools, die durch KI- und GenAI-Funktionen verstärkt werden, kann KI-basierte Abwehr einem Unternehmen zu mehr Sicherheit verhelfen. Wählen Sie dabei intelligente Lösungen, die KI und Machine-Learning-Algorithmen nutzen, um den neuesten Bedrohungen einen Schritt voraus zu sein – so bleibt Ihr Unternehmen geschützt.

Herausforderung 2: Neue gesetzliche Anforderungen

Neue gesetzliche Anforderungen an Prozesse und Sicherheitstools machen CISOs, Sicherheitsmanagern und obersten Führungskräften ebenfalls das Leben schwer.

PCI DSS 4.0 – Der Payment Card Industry Digital Security Standard (PCI DSS) 4.0 aktualisiert die Anforderungen für alle Unternehmen, die Finanztransaktionen verarbeiten, ermöglichen oder unterstützen. Ab März 2025 werden mit dem jüngsten PCI DSS-Standard neue Anforderungen für WAF, positive Sicherheitsmodelle, API-Schutz und clientseitige Sicherheit hinzugefügt. Diese Aspekte waren in den Anforderungen früherer Versionen noch nicht enthalten.

NIS2 – Mit der Richtlinie über Netz- und Informationssicherheit (NIS) 2 werden die Cybersicherheitsstandards, die bereits für wesentliche Dienstleistungen in der Europäischen Union gelten, erweitert. Durch die Aktualisierung werden Sanktionen für Verstöße gegen die Risikomanagement- und Berichtspflichten eingeführt.
Die neueste Richtlinie der Europäischen Union erfordert die Aufrechterhaltung der Applikationsverfügbarkeit, z. B. durch DDoS-Schutzlösungen, um vollständig konform und geschützt zu sein.

DORA – Der Digital Operational Resiliency Act (DORA) schafft Regeln für Finanzinstitute, um Schutz, Erkennung, Abwehr, Wiederherstellung und Reparatur für Informations- und Kommunikationstechnologien sicherzustellen.

DSGVO – Die Datenschutz-Grundverordnung (DSGVO) enthält Vorschriften für Unternehmen an jedem Ort, die Daten von Personen in der Europäischen Union erheben oder verarbeiten. Die DSGVO sieht Geldstrafen für alle vor, die gegen Datenschutz- und Sicherheitsvorschriften verstoßen.

HIPAA – Der Health Insurance Portability and Accountability Act (HIPAA) schützt Patientenakten und andere Gesundheitsdaten, die sich individuell zuordnen lassen. Das Gesetz erfordert Schutzmaßnahmen, erlässt Beschränkungen und legt Rechte fest, die Personen in Bezug auf ihre geschützten Daten ausüben können.

Transparenzgesetze – In den USA dürfen Unternehmen Angriffe nicht länger geheim halten. Die Wertpapier- und Börsenaufsichtsbehörde (SEC) schreibt vor, dass sie jeden für ihre Geschäftstätigkeit wesentlichen Cybersicherheitsvorfall innerhalb von vier Werktagen bekannt geben. Unternehmen müssen öffentlich mit ihren Kunden über Sicherheitsverletzungen kommunizieren, und sie sollten Cybersicherheitsvorfälle idealerweise ganz vermeiden.

CISOs können nicht länger nach Einzellösungen suchen. Sie benötigen eine integrierte Plattform, um die vollständige Einhaltung dieser neuen und strengeren Auflagen zu gewährleisten.

Herausforderung 3: Zunahme der hybriden Cloud-Bereitstellungen

Der Anstieg der hybriden Cloud-Bereitstellungen bedeutet für CISOs ebenfalls eine Herausforderung. Immer mehr Unternehmen verfügen über hybride Multi-Cloud-Umgebungen, in denen sie mehrere öffentliche und private Cloud-Dienste nutzen und gleichzeitig ihr Rechenzentrum vor Ort betreiben.

Laut dem Radware-Bericht Applikationssicherheit in einer Multi-Cloud-Welt 2023 nutzen 55 % der Unternehmen mittlerweile drei oder mehr Umgebungen – und 73 % der Unternehmen behalten weiterhin ihre Hardware-Rechenzentren vor Ort. Folglich müssen sie ihr eigenes Rechenzentrum verwalten, mit mehreren Cloud-Anbietern verhandeln und einen konsistenten Schutz über all diese Umgebungen hinweg gewährleisten.

Herausforderung 4: Personal- und Kompetenzmangel bei der Cybersicherheit

Die vierte Herausforderung, vor der CISOs im heutigen Cybersicherheitsumfeld stehen, beeinträchtigt fast alle Aspekte und die Qualität der Arbeit. Es handelt sich um den akuten Mangel an erfahrenen, qualifizierten Cybersicherheitsexperten. Laut einer ISC-Studie über Cybersicherheitspersonal aus dem Jahr 2024 leiden 67 % der Unternehmen unter dem Mangel an Sicherheitsfachleuten oder -kompetenzen, und weltweit gibt es fast 4 Millionen offene Stellen im Cybersicherheitsbereich. Infolgedessen geben 45 % der Unternehmen an, dass sie keine qualifizierten Mitarbeiter finden können. Dieser Mangel belastet die Sicherheitsteams so stark, dass sie nur bedingt in der Lage sind, Bedrohungen zu überwachen und zeitnah darauf zu reagieren. Wie können CISOs dieses Problem lösen? Sie müssen nach mehr automatisierten Schutzmaßnahmen suchen, die weniger von Personal abhängig sind. Gleichzeitig benötigen sie spezialisierte Managed Services, die als Sicherheitsbasis dienen und von Experten betreut werden.

Teil II. Wie können Sie sich dauerhaft schützen?

Wer im Zeitalter der KI-gestützten Angriffe sein Unternehmen schützen möchte, muss den Tools, die größere, schnellere und komplexere Angriffe ermöglichen, immer einen Schritt voraus bleiben. Sie haben bereits erfahren, was die vier wichtigsten Herausforderungen sind. Nun geht es um die Schlüsselaspekte, die CISOs berücksichtigen müssen, wenn sie nach einer moderneren Sicherheitslösung suchen.

4 Voraussetzungen für Cybersicherheit in der KI-Welt

Intelligente Sicherheit – Ohne Unterstützung werden Sie sich schwertun, mit der Geschwindigkeit und Rechenleistung künstlicher Intelligenz mitzuhalten. Bekämpfen Sie KI-basierte Bedrohungen mit KI-basiertem Schutz, indem Sie intelligente Sicherheitslösungen mit KI-gestützten Algorithmen einsetzen.

Integrierte Plattform – Erfüllen Sie die neuesten Standards und gesetzlichen Anforderungen und bekämpfen Sie All-in-one-Angriffstools, die mehrere Angriffsmethoden kombinieren, anstatt sich nur auf DDoS-Schutz, WAF oder eine bestimmte Art von Sicherheit zu fokussieren. Eine integrierte Plattform, die ein breites Spektrum von Bedrohungen abdeckt, bietet Ihnen den besten Schutz vor diesen Tools.

Konsistenter Schutz – Moderne Bedrohungen folgen Ihnen, wohin Sie auch gehen. Schützen Sie daher alle Ihre Umgebungen – vor Ort, öffentlich, privat oder hybrid – und alle Zugangspunkte zu Ihren Applikationen.

Erstklassige Abwehr – Angesichts des massiven Personalmangels in der Cybersicherheit und der komplexen, ständig neuen Angriffskampagnen sollten Sie sich von Sicherheitsexperten unterstützen lassen, die rund um die Uhr bereitstehen.

Nur mit einer Lösung, die diese vier Aspekte kombiniert, können Sie die durchschnittliche Problemlösungszeit (MTTR) senken, Kosten sparen und Ihre Marke schützen. Genau das bietet Ihnen Radware.

So bleiben Sie im Zeitalter der KI sicher

360° Applikationsschutz mit der Radware Cloud-Sicherheitsplattform

Radware bietet 360-Grad-Schutz für Ihre Applikationen und Infrastruktur dank einer integrierten Plattform. Diese vereint intelligente Sicherheit und erstklassige Abwehr und wendet sie konsistent in allen Ihren Umgebungen an. Dabei profitieren alle Schutzbereiche von EPIC-AI, unserer KI-gestützten Intelligenz.

5 Fakten über unseren umfassenden, KI-gestützten Schutz

- Schützt alle Ihre mobilen Apps, Webapplikationen und APIs in allen Umgebungen: öffentliche Clouds, private Cloud-Rechenzentren, Microservices usw.
- Wehrt eine breite Palette von Bedrohungen ab, darunter Webangriffe, API-Missbrauch, bösartige Bots, KI-basierte Angriffe, DDoS-Angriffe usw.
- Bekämpft diese externen Bedrohungen mit einer integrierten Plattform, die Echtzeit-Schutz-Engines wie WAF, API-Schutz, Bot-Manager, DDoS- und Web-DDoS-Schutz, clientseitigen Schutz und Schutz vor Kontoübernahme (ATO) umfasst.
- Bietet vollständige Transparenz und Kontrolle über Ihr Netzwerk und den Schutz Ihrer Applikationen mithilfe unserer Cloud-Sicherheitsplattform, die über ein zentrales Portal verwaltet wird.
- Nutzt die KI-gestützten Machine-Learning-Algorithmen von EPIC-AI, um es mit der Raffinesse und Komplexität moderner Angriffe aufzunehmen.

Teil III. Die Cloud-Sicherheitsplattform von Radware, gestützt von EPIC-AI

Was genau ist EPIC-AI und wie unterstützt diese Technologie den 360-Grad-Cloud-Applikationsschutz von Radware?

Radware EPIC-AI

Radware bietet KI-gestützte Intelligenz und GenAI-Funktionen in seiner Cloud-Sicherheitsplattform, um Applikationen zu schützen, die durchschnittliche Problemlösungszeit (MTTR) zu reduzieren und Kosten zu sparen. EPIC-AI arbeitet plattformübergreifend, um einen präzisen Echtzeit-Schutz ohne manuelles Eingreifen zu gewährleisten.

Mithilfe von EPIC-AI stellt Radware eine mehrstufige, integrierte Cloud-Sicherheitsplattform mit folgenden Merkmalen bereit:

Integration über mehrere Durchsetzungspunkte hinweg

Radware-Lösungen können über verschiedene Durchsetzungspunkte hinweg integriert werden, einschließlich unserer eigenen Produkte (Alteon und DefensePro X) und Cloud-Services sowie Services von Drittanbietern (NGINX, Envoy oder Public Clouds wie AWS, Google Cloud usw.). Durch die Integration dieser Durchsetzungspunkte können Sicherheitsrichtlinien, Signaturen und Regeln einheitlich angewendet werden, unabhängig davon, wo sich die Applikation befindet. Diese auf dem Markt einzigartige Integration bietet Kunden den konsistenten Schutz, den sie für ihre On-Premise-, privaten und öffentlichen Cloud-Umgebungen benötigen.

Echtzeit-Schutz-Engines für Clouds

Die Radware-Engines für den Echtzeit-Schutz von Clouds umfassen WAF, Bot-Management, DDoS-Schutz, Web-DDoS-Schutz, API-Schutz, Schutz vor Kontenübernahme (ATO) und clientseitigen Schutz. Jedes dieser Module bietet Nutzern eine erstklassige Lösung, die auf KI und Machine-Learning-Algorithmen zurückgreift, um bösartige Aktivitäten automatisch und präzise zu erkennen und abzuwehren – einschließlich Web-DDoS-Tsunami-Angriffen, KI-gesteuerten menschenähnlichen Bots und API-Business-Logic-Angriffen.

Plattformübergreifende Struktur

Auf dieser Ebene werden unsere Echtzeit-Schutz-Engines zu einer integrierten, ganzheitlichen Plattformlösung verbunden. Diese nutzt KI-gestützte Quellblockier-Algorithmen, Bedrohungsinformationen und datengesteuerte Feeds, um bösartige Quellen präventiv auszuschalten, bevor sie Schaden anrichten. Modellübergreifende KI-basierte Korrelation und KI-gestützte Richtlinienabstimmung und Empfehlungen helfen den Schutz-Engines, Angriffe präzise zu erkennen und Fehlalarme oder übersehene Bedrohungen zu minimieren. Radware-Kunden können alle Schutz-Engines im Blick behalten und bösartige Quellen blockieren, noch bevor diese den Zugriff auf andere Applikationen versuchen.

SOC Management Core

SOC Management Core von Radware sorgt dafür, dass rund um die Uhr KI-gestützte Managed Services und automatisierte Sicherheitsverwaltung und -abläufe verfügbar sind. AI SOC Xpert von Radware bietet eine automatisierte und sofortige Reaktion auf Vorfälle und beschleunigt die Ursachenanalyse, wodurch die MTTR um bis zu 95 % sinkt. Mit den KI-gestützten Funktionen dieses Services kann das Emergency Response Team (ERT) von Radware bessere und stärker automatisierte Managed Services bereitstellen. Außerdem hilft er Unternehmen mit eigenem SOC, Vorfälle schneller und gezielter zu beheben. Der Service ermöglicht eine automatisierte und sofortige Reaktion auf Bedrohungen, beschleunigt die Ursachenanalyse und bietet Abwehrhilfe und Empfehlungen – und ergreift sogar Maßnahmen, um den Vorfall automatisch für Sie zu beheben. Dadurch wird die MTTR von Stunden auf Minuten reduziert, d. h. um bis zu 95 % pro Vorfall!

Darüber hinaus bietet Radware Compliance-Funktionen, erweiterte Analysen und Integrationen mit Drittanbietern, um eine nahtlose und umfassende Erfahrung zu schaffen. All dies wird über ein zentrales, integriertes Portal verwaltet.

Fallstudie: KI unterstützt Radware beim präzisen Schutz vor Web-DDoS-Tsunamis

Die Ausgangslage

Die Fähigkeit von Radware, evasive Angriffe mit KI-gestütztem Web-DDoS-Schutz abzuwehren, wurde kürzlich bei einer EMEA-Bank unter Beweis gestellt. Die Bank, die von einer Welle von DDoS-Angriffen aus dem Internet betroffen war, hätte im Falle eines erfolgreichen Angriffs mit finanziellen Schäden, Imageverlust und Ausfallzeiten rechnen müssen.

Die Herausforderung

Diese Angriffe hätten sich mit einer gewöhnlichen DDoS-Sicherheitslösung nur schwer abwehren lassen. Die Zahl der Anfragen pro Sekunde (RPS) stieg auf 14,6 Millionen. Dies entspricht dem Versuch von 14 Millionen Menschen, über die gesamte Angriffsdauer jede Sekunde ihr Bankkonto auf dieser Website aufzurufen. Der Angriff hielt tagelang an und erfolgte in mehreren Wellen. Einige davon dauerten bis zu 20 Stunden – für einen einzigen Angriff!

Die Lösung

Radware konnte diese Angriffe innerhalb von Sekunden automatisch abwehren. Durch automatische Signaturerstellung in Echtzeit wurden alle Bedrohungen blockiert, bevor sie sich auf die Bank oder ihre Endnutzer auswirken konnten. Eine der Echtzeit-Signaturen enthielt mehr als 27 Parameter, um genau zu steuern, was blockiert werden sollte oder nicht. Auf diese Weise wurde bösartiger Datenverkehr abgehalten und legitimer Datenverkehr durchgelassen. All dies geschah automatisch, ohne Eingreifen der Bank – und ohne Auswirkungen auf ihre Kunden.

Der Schutz dieser EMEA-Bank durch Radware verdeutlicht CISOs, wie sie KI mit KI bekämpfen können: durch den Einsatz von KI-basierten Algorithmen zur Signaturerstellung in Echtzeit, innerhalb weniger Sekunden.

Zusammenfassung

Radware EPIC-AI in der Praxis: Schutz genau dort, wo er am wichtigsten ist

Weil sich die moderne Cyberbedrohungslandschaft rasant weiterentwickelt, müssen CISOs erhebliche Herausforderungen bewältigen, um am Arbeitsplatz mehr Sicherheit zu schaffen. Sie sehen sich mit einer dynamischen Bedrohungslandschaft konfrontiert, die von motivierten Hacktivisten, neuartigen Angriffstools und automatisierten, KI-gestützten Angriffen geprägt ist. Dazu gesellen sich bekannte Probleme, wie z. B. die Einhaltung strenger Cybersicherheitsvorschriften und die Zunahme der hybriden Cloud-Bereitstellungen. Erschwerend kommt hinzu, dass in der Cybersicherheit derzeit ein Personal- und Kompetenzmangel herrscht.

Radware nutzt künstliche Intelligenz, um Unternehmen bei diesen Herausforderungen unter die Arme zu greifen. KI-gestützte Bedrohungen werden mit Sicherheitslösungen neutralisiert, die auf EPIC-AI basieren. Dies bedeutet, dass KI-gestützte Algorithmen und generative KI eingesetzt werden, um plattformübergreifend für präzisen Echtzeit-Schutz zu sorgen. So erhalten Kunden eine integrierte Plattform, die einen konsistenten Schutz für alle Applikationen und Umgebungen gewährleistet. Darüber hinaus sind intelligente, KI-gestützte Schutz-Engines zur präzisen Erkennung und Abwehr in Echtzeit verfügbar – und die Lösung ermöglicht eine automatisierte, KI-gestützte Reaktion ohne manuelles Eingreifen, für eine kürzere durchschnittliche Problemlösungszeit (MTTR). Verbessern Sie Ihre Sicherheit im Zeitalter der KI und senken Sie gleichzeitig Ihre Gemeinkosten und den Personalbedarf. Bekämpfen Sie KI mit KI – unterstützt von Radware.

RWI 402 | 22.1.2025