radware

Leitfaden

Lösungen für Personal- und Kompetenzmangel im Applikationsschutz

Fast alle Unternehmen weltweit leiden derzeit unter den Auswirkungen von Personal- und Kompetenzmangel auf ihre Cybersicherheit. Dies ist vor allem beim Applikationsschutz ein echtes Problem. Obwohl es auch in den nächsten Jahren schwierig bleiben wird, Fachleute für Cybersicherheit zu finden oder zu halten, können Unternehmen ab sofort eine Reihe wichtiger Maßnahmen ergreifen. Damit wirken sie den Folgen dieses Personalmangels entgegen und können ihre Programme für Webapplikationsschutz verbessern.

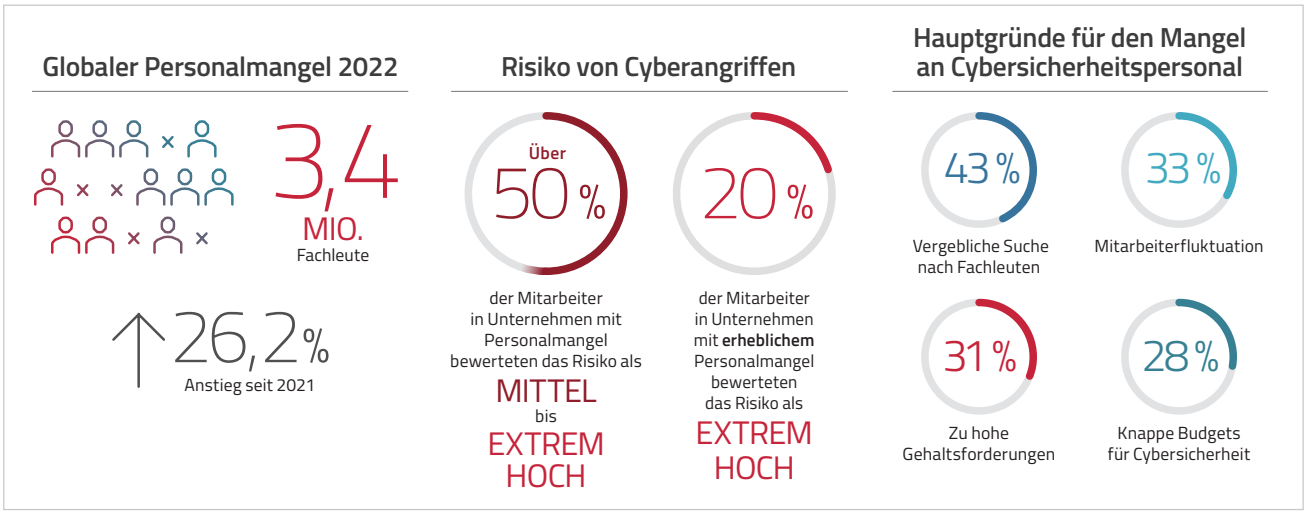
Anpassung an den Personalmangel

Diese Komplexität wird durch enge Budgets und einen Mangel an Sicherheitsfachleuten weltweit noch verstärkt. So wird der Schutz von Applikationen zu einer schweißtreibenden Aufgabe. Wenn Sie versuchen, ein Sicherheitskonzept mit verschiedenen Anbietern zusammenzuschustern, wird das Ganze noch unübersichtlicher. Das Ergebnis sind mangelnde Sicherheit und höhere Kosten. Mit den resultierenden Sicherheitssilos ist das Desaster vorprogrammiert.

Personal- und Kompetenzmangel gehören im Bereich Cybersicherheit seit ein paar Jahren zu den anhaltenden Trends. Laut den Ergebnissen der „ISC2 Cybersecurity Workforce Study 2022“ fehlten in der Cybersicherheit im Jahr 2022 weltweit rund 3,4 Millionen Fachleute. Dies bedeutet einen Anstieg um 26,2 % gegenüber 2021. Somit hält der Mangel an Cybersicherheitsmitarbeitern nicht nur an, sondern verschlimmert sich und beeinträchtigt die Fähigkeit von Unternehmen, Cybersicherheitsvorfälle angemessen zu bekämpfen.

Wie der Bericht bestätigt, sind 70 % aller Unternehmen der Ansicht, dass ihr Cybersicherheitsteam für eine effektive Abwehr nicht mehr ausreicht. Darüber hinaus bewerteten mehr als die Hälfte der Mitarbeiter in Unternehmen, die über zu wenig Cybersicherheitspersonal verfügen, das Risiko eines Cyberangriffs – aufgrund dieses Mangels – als „mittel“ bis „extrem hoch“. In Unternehmen mit „erheblichem“ Personalmangel stuften 20 % der Mitarbeiter das Risiko eines Cyberangriffs als „extrem hoch“ ein.

Zu den Hauptgründen für den Mangel an Cybersicherheitspersonal zählen die vergebliche Suche nach Fachleuten (43 % der Unternehmen), Mitarbeiterfluktuation (33 %), zu hohe Gehaltsforderungen (31 %) und knappe Budgets für Cybersicherheitsprogramme (28 %).



Diese Ergebnisse deuten auf ein häufiges, weitreichendes und dauerhaftes Problem hin: Unternehmen finden nicht genug Mitarbeiter, und falls doch, können sie diese nicht halten.

Deshalb müssen Unternehmen ihre Strategie anpassen und neue Maßnahmen ergreifen, durch die ihre Cybersicherheitsprogramme und -tools weniger von internen Fachleuten abhängig sind.

Webapplikationsschutz wird zu einem eigenen Fachgebiet

Webapplikationsschutz gehört zu den Bereichen, in denen der Mangel an Cybersicherheitspersonal am deutlichsten spürbar ist.

Da Webapplikationen häufig das Herzstück von Geschäftsfunktionen bilden, spielt Applikationsschutz eine immer wichtigere Rolle, um diese Applikationen, ihre Verfügbarkeit und die damit verarbeiteten Kundendaten abzusichern.

Neben der Bedeutung des Applikationsschutzes steigen aber auch sein Umfang und seine Komplexität: Aufgrund der einzigartigen Angriffsarten müssen spezielle Tools und Abwehrmechanismen eingesetzt werden. Folglich entwickelt sich Applikationsschutz zu einem eigenständigen Fachgebiet innerhalb der Cybersicherheit, das sich von anderen Bereichen oder Spezialisierungen unterscheidet.

Diese Entwicklung führt dazu, dass erfolgreiche Programme für Webapplikationsschutz nicht nur spezielle Tools gegen die diversen Angriffsarten erfordern, sondern auch Fachleute für Applikationssicherheit, die dank Fachwissen und Expertise den nötigen Schutz gewährleisten.

Im Folgenden sind die Hauptgründe aufgeführt, aus denen Webapplikationsschutz heute ein eigenes Fachgebiet innerhalb der Cybersicherheit darstellt. Außerdem werden die Kompetenzen erläutert, die Fachleute für Applikationssicherheit mitbringen müssen, um für Schutz auf höchstem Niveau zu sorgen.

Grund 1: Breitere Fachkenntnisse

Eine der größten Herausforderungen beim Webapplikationsschutz lautet, dass Sicherheit kein eigenständiger Aspekt ist. Vielmehr bildet sie ein übergreifendes Thema, das sich durch mehrere Cybersicherheits- und Computingbereiche zieht. Wer Applikationssicherheit verstehen möchte, muss sich mit Applikationen auskennen. Das setzt wiederum detailliertes Fachwissen über IT und Computing voraus, z. B. in diesen Bereichen:

- Netzwerke: Wie werden sie konzipiert, erstellt, konfiguriert und geschützt.
- Applikationsentwicklung: Wie werden Applikationen entwickelt, wie sieht ihre Architektur aus, mit welchen Technologien werden sie erstellt, was beinhaltet der Entwicklungsprozess, wer ist daran beteiligt und wie werden sie bereitgestellt.
- Applikationsfunktionen: Welche Geschäftsfunktion erfüllt die Applikation, welche Hauptfunktionen weist sie auf und wie interagieren Benutzer damit.
- Cloud-Computing: Da die meisten Webapplikationen heute in der Cloud bereitgestellt werden, ist Wissen über Public Clouds, private Clouds und hybride Clouds unabdingbar.
- Kubernetes und Microservices: Wie funktionieren Microservices (und insbesondere Kubernetes), wie werden sie verwaltet, wie sieht der Bereitstellungslebenszyklus aus und worin unterscheiden sie sich vom herkömmlichen Applikationsdesign.

Angesichts dieser Liste ist es kein Wunder, dass Fachleute, die all dieses Wissen besitzen, nur schwer zu finden sind.

Grund 2: Eine größere, komplexere Bedrohungslandschaft

Neben dem Verständnis für die Entwicklung und Implementierung von Applikationen müssen Experten für Applikationssicherheit auch wissen, welchen Bedrohungen moderne Applikationen ausgesetzt sind. Das heißt, sie müssen sich mit Angriffen auf Applikationen, den Angriffsvektoren und neuen Bedrohungen genauestens auskennen.

Dazu zählen Webapplikationsangriffe, Bot-Angriffe, API-Angriffe und -Schwachstellen, DDoS-Angriffe auf Applikationsebene (L7) und – immer häufiger – Supply-Chain- und clientseitige Angriffe.

Für alle diese Vektoren muss bekannt sein, wie sie geplant und ausgeführt werden, wie sie sich von anderen Angriffsvektoren unterscheiden und welche potenziellen Auswirkungen auf die Applikationssicherheit entstehen.

Grund 3: Größere Auswahl von Tools

Nicht nur die Liste der Applikationsbedrohungen wächst ständig an, sondern auch die Liste der für Abwehrmaßnahmen verfügbaren – und notwendigen – Tools. Diese Sicherheitstools und -mechanismen müssen Fachleute für Applikationssicherheit aus dem Effeff beherrschen.

Moderner Applikationsschutz umfasst über Web Application Firewalls (WAF) hinaus auch Bot-Schutz, DDoS-Schutz auf Applikationsebene (L7), API-Sicherheit, clientseitigen Schutz und vieles mehr. Experten für Applikationssicherheit müssen diese Tools kennen und wissen, wie sie funktionieren, was sie abdecken (oder nicht) und wie sich all diese Tools in einem umfassenden Schutzschild für moderne Applikationen kombinieren lassen.

Da Applikationen eine Kernfunktion der Geschäftsabläufe erfüllen, genügt es nicht, dass Fachleute diese Tools bereitstellen und Sicherheitsrichtlinien implementieren können. Sie müssen die Tools auch an die Verhaltensmuster legitimer Applikationsbenutzer anpassen können, Fehlalarme verhindern und Protokolle oder Analysen auswerten, um potenzielle Sicherheitslücken zu erkennen.

Grund 4: Auswirkungen im gesamten Unternehmen

Da Applikationen für die Geschäftsabläufe so bedeutsam sind, müssen Experten für Applikationsschutz zudem verstehen, wie sich die Applikationssicherheit auf das gesamte Unternehmen auswirkt – und auf den Gewinn.

Obwohl die kritische Rolle von Applikationsschutz unumstritten ist, steht Sicherheit immer wieder im Konflikt mit Agilität. Viele Geschäftsabteilungen möchten so agil und flexibel wie möglich agieren, ohne Einschränkungen zu unterliegen. Sicherheit geht jedoch von Natur aus mit Einschränkungen einher, um bösartige Aktivitäten abzufangen. Somit kann die unverzichtbare Sicherheit, die durch Webapplikationsschutz geschaffen wird, auch zum Hindernis oder Spielverderber bestimmter Geschäftsabteilungen werden, darunter DevOps, Marketing, Cloud-Betrieb usw.

Die Kunst besteht darin, einen erstklassigen Applikationsschutz einzurichten, aber dabei möglichst reibungslose Abläufe zu behalten und keine betrieblichen oder technischen Probleme zu verursachen, die den Gewinn des Unternehmens schmälern können.

Aus diesem Grund benötigen Fachleute für Webapplikationssicherheit einen gewissen Geschäftssinn und ein Bewusstsein dafür, wie sich Applikationsschutz auf die geschäftlichen und technologischen Prozesse auswirkt. Sie müssen in der Lage sein, Konflikte zu minimieren und gleichzeitig ein hohes Schutzniveau für Webapplikationen aufrechtzuerhalten.

Lösungen für Personal- und Kompetenzmangel im Applikationsschutz

Unternehmen können im Wesentlichen drei Maßnahmen ergreifen, um die Abhängigkeit von internen Cybersicherheitsfachleuten – und deren Arbeitslast – zu senken: Konsolidierung, Automatisierung und komplett verwaltete Sicherheitsservices.

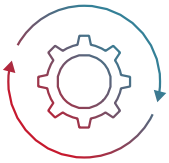
Maßnahme 1: Konsolidierung

Die erste Maßnahme gegen Personalmangel in der Cybersicherheit lautet Konsolidierung von Sicherheitstools. Die Rechnung ist ganz einfach: Je weniger Tools verwaltet und gepflegt werden müssen, desto weniger Zeit und Aufwand entsteht für den Wechsel zwischen Systemen und Management-Konsolen – und desto mehr sinkt die Arbeitslast des Cybersicherheitspersonals.

Einzelne Tools und Abwehrmechanismen, die einen unsystematischen Flickenteppich bilden, sollten in einem „One-Stop-Shop“ mit Best-of-Suite-Lösungen konsolidiert werden. So werden eine Vielzahl von Angriffen und Bedrohungsvektoren mit einem einzigen Tool abgedeckt – und mit einem einzigen Management- und Reporting-Dashboard.

Auf diese Weise können Sicherheitsteams dasselbe Schutzniveau beibehalten, beschleunigen aber die Prozesse durch zentralisiertes Management und Reporting. Außerdem verbringen sie weniger Zeit mit dem Umschalten zwischen Systemen und der Integration separater Produkte.

Achten Sie jedoch darauf, dass die Konsolidierung nicht auf Kosten der Sicherheit geht. Wählen Sie daher ein Best-of-Suite-Tool, das auch in puncto Sicherheit rundum überzeugt, um Ihren Cyberschutz zu maximieren.



Maßnahme 2: Automatisierung

Die nächste Maßnahme zur Entlastung der Cybersicherheitsmitarbeiter besteht in der Automatisierung möglichst vieler Prozesse, um mühsame manuelle Konfiguration zu vermeiden.

Im Bereich Cybersicherheit lassen sich zwei Arten von Automatisierung unterscheiden:

- **Automatisierte Sicherheit** – Automatisierung der eigentlichen Cyberabwehrmaßnahmen, wie Richtlinienkonfiguration, Regelkonfiguration, Signaturerstellung usw.
- **Automatisierte Bereitstellung** – Automatisierung der Implementierung von Cybersicherheitsmechanismen, ohne dass geschäftliche oder technische Prozesse unterbrochen werden.

Da Angriffe immer umfangreicher und raffinierter werden, spielt automatisierte Sicherheit für den kontinuierlichen Schutz vor Angriffen eine wesentliche Rolle. Jede Sicherheitsvorkehrung, die auf manuellen Prozessen basiert, kann durch wechselnde Angriffsmuster und neuartige Zero-Day-Angriffe überlistet werden, für die es derzeit keine Schutzsignaturen gibt.

Dieses Problem wird durch Personalmangel noch verschärft, weil nicht genügend Fachleute zur Verfügung stehen, um im Angriffsfall schnell zu reagieren und die nötigen Aktivitäten durchzuführen.

Wenn Unternehmen diese beiden Arten von Sicherheitsautomatisierung kombinieren, können sie die Arbeitslast von Cybersicherheitsteams senken (z. B. Erstellen neuer Regeln, Definieren von Sicherheitsrichtlinien usw.) und gleichzeitig die allgemeine Auswirkung von Cybersicherheitsmaßnahmen im Unternehmen reduzieren. Letzteres bedeutet, dass weniger Folgen und Unterbrechungen für andere Abteilungen wie DevOps, IT, Operations oder Marketing entstehen.

Maßnahme 3: Komplett verwaltete Sicherheitsservices

Als dritte Maßnahme empfiehlt sich schließlich das Outsourcing von Cybersicherheitsfunktionen an Experten und komplett verwaltete Sicherheitsservices, die Ihnen diese schwierige Aufgabe abnehmen.

Der Begriff „Cybersicherheit“ deckt einen weitläufigen Bereich ab, der aus zahlreichen spezialisierten Teilbereichen besteht. Ein paar Beispiele dafür sind Netzwerksicherheit (Firewalls, VPNs, sichere Web-Gateways usw.), Applikationsschutz (WAF, Bot-Schutz, DDoS-Schutz und vieles mehr), Endgerätesicherheit (Virenschutz, EDR usw.), E-Mail-Sicherheit, Public-Cloud-Sicherheit (z. B. Workload-Schutz, CSPM und IAM-Sicherheit).

Jeder dieser Teilbereiche unterscheidet sich in Bezug auf Schutzumfang, Angriffsvektoren, Angriffsflächen und Tools. Und mit zunehmender Komplexität der Bedrohungslandschaft werden diese Teilbereiche immer spezialisierter und sind stärker voneinander abgegrenzt.

Folglich ist es nahezu unmöglich, Cybersicherheitsexperten zu finden, die mit ihrem Wissen alle Teilbereiche abdecken und alle nötigen Abwehrtools beherrschen. Das bedeutet, selbst wenn Ihr Unternehmen genügend Mitarbeiter gefunden hat, reichen deren Kenntnisse oft nicht aus, um alle Anforderungen zu erfüllen.

Daher macht es Sinn, komplett verwaltete Sicherheitsservices in Anspruch zu nehmen und bestimmte Sicherheitsfunktionen an Expertenteams auszulagern, die diese Aufgaben tagtäglich wahrnehmen.

Stellen Sie jedoch sicher, dass Anbieter dieser Sicherheitsservices in ihrer Branche oder auf ihrem Spezialgebiet einen guten Ruf haben und über ausreichend Personal mit der richtigen Qualifikation verfügen. Mit dieser Strategie lässt sich die Arbeitslast interner Cybersicherheitsteams erheblich senken, während der Schutz sogar noch verstärkt wird.

Radware-Lösungen gegen Personalmangel im Applikationsschutz

Als führender Anbieter von Webapplikationsschutz hilft Radware den Unternehmen mit einer umfassenden Reihe von Maßnahmen, ihre Sicherheitsvorkehrungen für Webapplikationen zu optimieren und zu vereinfachen, damit sie weniger manuell konfigurieren müssen. So fallen fehlende Mitarbeiter und Kompetenzen für Cybersicherheit weniger ins Gewicht.

Maßnahme 1: Automatisierung:

Weil Cyberkriminelle und ihre Angriffe immer raffinierter werden, können sich Unternehmen nicht mehr auf Sicherheitsvorkehrungen mit manueller Konfiguration verlassen. Angreifer haben gelernt, ihre Angriffsvektoren ständig zu wechseln, um die Cyberabwehr zu umgehen. So sind sie in der Lage, alle Arten von manuellen Konfigurationen, Regeln oder Richtlinien im Nu zu überwinden – denn diese können mit den ständig neuen Angriffsmerkmalen nicht Schritt halten.

Hinzu kommt, dass sich Applikationen ständig verändern, und auch die Verhaltensmuster der Benutzer wandeln sich im Laufe der Zeit. Deshalb müssen Sicherheitsregeln und -richtlinien kontinuierlich angepasst werden, um legitimen Benutzertraffic durchzulassen und bösartige Anfragen zu blockieren.

Die Applikationsschutzlösungen von Radware bieten eine Reihe hilfreicher Automatisierungsfunktionen, um die Sicherheit zu erhöhen und Fehlalarme zu reduzieren:

- **Automatisches Lernen in Bezug auf Traffic:** Die Applikationsschutzlösungen von Radware basieren auf einem positiven Sicherheitsmodell, sodass nur legitime Benutzeranfragen akzeptiert werden. Traffic, der nicht dem Verhalten legitimer Benutzer entspricht, wird hingegen blockiert. Dieses Konzept beruht auf automatisierten Lernfunktionen für Traffic, die das Verhalten legitimer Benutzer erlernen und eine Baseline für legitimes Benutzerverhalten erstellen. Anschließend wird alles blockiert, was nicht in diese Verhaltensmuster passt.
- **Automatische Richtlinienoptimierung:** Zunächst generiert Radware maßgeschneiderte Sicherheitsrichtlinien für die Verhaltensmuster der Kunden. Anschließend beginnt eine kontinuierliche Richtlinienoptimierung mithilfe von Machine-Learning-Algorithmen. Dabei werden die laufenden Sicherheitsprotokolle ausgewertet und automatisch Richtlinienverbesserungen vorgeschlagen, um einen präziseren Schutz zu erreichen – ohne dass den Sicherheitsteams mehr Aufwand entsteht.
- **Automatisierte Korrektur von Fehlalarmen:** Damit legitime Benutzeraktivitäten nicht beeinträchtigt werden, scannt die Radware-WAF-Engine automatisch auf potenzielle Fehlalarme und meldet diese, damit Sicherheitsadministratoren ggf. grünes Licht geben können.

Maßnahme 2: Umfassender, zentralisierter Applikationsschutz

Eine weitere wichtige Maßnahme für Personalmangel besteht im Vermeiden unnötiger Verwaltungsprobleme bei Sicherheitstools. Dazu werden mehrere verteilte Lösungen in einer einzigen, einheitlichen Best-of-Suite-Plattform kombiniert, die alle Anforderungen erfüllt.

Die Cloud-Sicherheitsplattform von Radware bietet einen umfassenden One-Stop-Shop für Webapplikationsschutz, der alle gängigen Bedrohungsvektoren und Angriffsflächen abdeckt:

- **Web Application Firewall** – für den Schutz vor Webangriffen wie SQL-Injections, Cross-Site-Scripting (XSS), Server-Side Request Forgery (SSRF) und anderen OWASP-Top-10-Bedrohungen (und viele mehr).
- **Bot-Manager** – zur Unterscheidung zwischen menschlichem und nicht-menschlichem Traffic und zwischen guten Bots (z. B. Suchmaschinen-Crawler) und schädlichen Bots (Web-Scraper, DDoS-Botnets usw.).
- **API-Schutz** – mit integrierter, vollautomatisierter API-Erkennung, um alle nicht dokumentierten APIs oder API-Aufrufe zu ermitteln und den Schutz aller APIs des Unternehmens durchzusetzen.
- **DDoS-Schutz** – für verhaltensbasierten Schutz vor DDoS-Angriffen sowohl auf der Netzwerkebene (L3/4) als auch auf der Applikationsebene (L7).
- **Clientseitiger Schutz** – für den Schutz von Client-Endgeräten vor Supply-Chain-Angriffen wie Formjacking (Magecart) oder DOM-XSS-Angriffen.

Darüber hinaus bietet die Radware-Plattform eine zentralisierte Managementkonsole mit einheitlichen Dashboards, Reporting und Verwaltung für alle diese Funktionen.

Maßnahme 3: Nahtlose Integration

In modernen Umgebungen bildet Applikationsschutz keine eigenständige Disziplin mehr, sondern ist untrennbar mit Applikationsentwicklung, -implementierung und -bereitstellung, DevOps und sogar Marketing und Social Media verbunden. Deshalb ist nahtlose Integration für Applikationssicherheit so wichtig: Webapplikationsschutz darf andere Bereiche in der heutigen Zeit nicht beeinträchtigen.

Radware ermöglicht mit seiner SecurePath-Architektur eine einzigartige, perfekte Integration. Im Gegensatz zu traditionellen Inline-Mechanismen für Applikationsschutz verfügt Radware SecurePath über eine Out-of-Band-Architektur für nahtlosen Applikationsschutz, der keine Änderungen der bestehenden Architektur oder Prozesse erfordert.

Herkömmliche Applikationsschutzlösungen werden inline eingesetzt, entweder als Appliance (für lokale Bereitstellung) oder über DNS-Weiterleitung (für Cloud-basierte Bereitstellung). Dieser Ansatz erlaubt die Inspektion des gesamten Traffics, unterbricht aber auch vorhandene Bereitstellungsverfahren und verursacht zusätzliche Hops und Latenzzeiten bei Cloud-Bereitstellungen. Dieses Problem tritt insbesondere bei Multi-Clouds und hybriden Clouds auf. Die bisherigen Out-of-Path-Bereitstellungsoptionen waren in der Regel auf reine Alarm-Tools beschränkt.

Die Radware SecurePath-Architektur hingegen sorgt mit einem API-basierten Out-of-Path-Modell für umfassenden Schutz ab dem ersten Paket. Durch die Integration mit dem Applikationsserver wird bei jeder eingehenden Anfrage ein API-Aufruf mit den Details der Anfrage an den nächstgelegenen Radware-PoP gesendet. Dort wird eine Analyse auf verdächtige Aktivitäten vorgenommen, um bösartige Anfragen zu blockieren. Dies ermöglicht umfassenden Schutz ohne jegliche Änderungen am Datenpfad, ohne zusätzliche Traffic-Hops oder Latenzzeit und sogar ohne Anforderung des SSL/TLS-Zertifikats der Applikation.

Maßnahme 4: Verwaltete Sicherheitsservices

Abschließend stellt Radware verwaltete Sicherheitsservices bereit, die Unternehmen helfen, den Mangel an Cybersicherheitspersonal abzufangen. An vorderster Front steht dabei das Emergency Response Team (ERT).

Da sich Applikationsschutz zunehmend zu einem eigenen Fachgebiet entwickelt, finden viele Unternehmen nicht mehr genügend Fachleute mit der nötigen Qualifikation, Kompetenz und Erfahrung, um Angriffe auf Webapplikationen zu erkennen und abzuwehren.

Bei den Cloud-Applikationsschutzservices von Radware handelt es sich um einen verwalteten Service. Das Radware SOC und die Supportmitarbeiter unterstützen Kunden beim Onboarding, bei der Konfiguration und laufenden Überwachung, durch 24/7-Support und Schutz im Angriffsfall.

Dieses Konzept verhilft Unternehmen einerseits zu einem besseren Webapplikation-sschutz mithilfe erfahrener Experten, die sich tagtäglich mit Applikationssicherheit befassen. Andererseits entlasten die Unternehmen ihre internen Mitarbeiter, sodass sich diese wieder ihren Hauptaufgaben widmen können.

Niedrigere TCO durch Lösungen für Personalmangel

Angesichts der angespannten Wirtschaftslage versuchen viele Unternehmen derzeit, Kosten zu sparen und die Gesamtbetriebskosten (Total Cost of Ownership, TCO) für ihre Cybersicherheitstools zu senken. Zahlreiche Unternehmen erkennen jedoch nicht, dass sie mit den in diesem Dokument beschriebenen Maßnahmen nicht nur ihre Sicherheit erhöhen, sondern auch noch Kosten sparen.

Zu den wichtigsten Maßnahmen für niedrigere TCO zählen:

Konsolidierung von Lösungen und Anbietern

Reduzieren Sie die Anzahl der Anbieter und konsolidieren Sie Ihre Tools, um mit weniger Lösungen mehr Anforderungen abzudecken.

Automatisierung ressourcenintensiver Prozesse

Verbessern Sie die Schutzqualität, beschleunigen Sie Prozesse und senken Sie den Anteil der manuellen Aufgaben.

Integrierte, zentralisierte Verwaltung und Transparenz

Verlieren Sie weniger Zeit mit dem Wechsel zwischen Tools und Dashboards, indem Sie eine einzige, zentralisierte Managementkonsole für transparente Verwaltung nutzen.

Nutzung komplett verwalteter Sicherheitsservices

Entlasten Sie Ihre Mitarbeiter für Webapplikationsschutz, erhöhen Sie die Sicherheit und sparen Sie dabei Ressourcen ein.

Zusammenfassung

Aufgrund der langfristigen Auswirkungen der COVID-19-Pandemie, der zunehmenden Bedrohungen und der wachsenden Komplexität von Angriffen sehen sich viele Unternehmen mit einem anhaltenden Fachkräftemangel konfrontiert. Dies gilt insbesondere für den Webapplikationsschutz, der sich zunehmend zu einem eigenen Fachgebiet innerhalb der Cybersicherheit entwickelt.

Um diesen Mangel auszugleichen, müssen verschiedene Maßnahmen wie Konsolidierung, Automatisierung und von Experten verwaltete Sicherheitsservices kombiniert werden.

Als führender Anbieter von Webapplikationsschutz stellt Radware eine umfassende Palette von Maßnahmen bereit, mit denen Unternehmen ihre Sicherheitsvorkehrungen für Webapplikationen optimieren und vereinfachen können. Dadurch sind Unternehmen weniger auf manuelle Konfigurationen angewiesen und kompensieren den Mangel an qualifiziertem Cybersicherheitspersonal.

© 2024 Radware Ltd. Alle Rechte vorbehalten. In diesem Dokument genannte Produkte und Lösungen von Radware sind durch Marken, Patente und Patentanmeldungen von Radware in den USA und anderen Ländern geschützt. Weitere Informationen finden Sie hier: https://www.radware.com/LegalNotice/. Alle übrigen Marken und Namen sind Eigentum der jeweiligen Inhaber.