Akamai

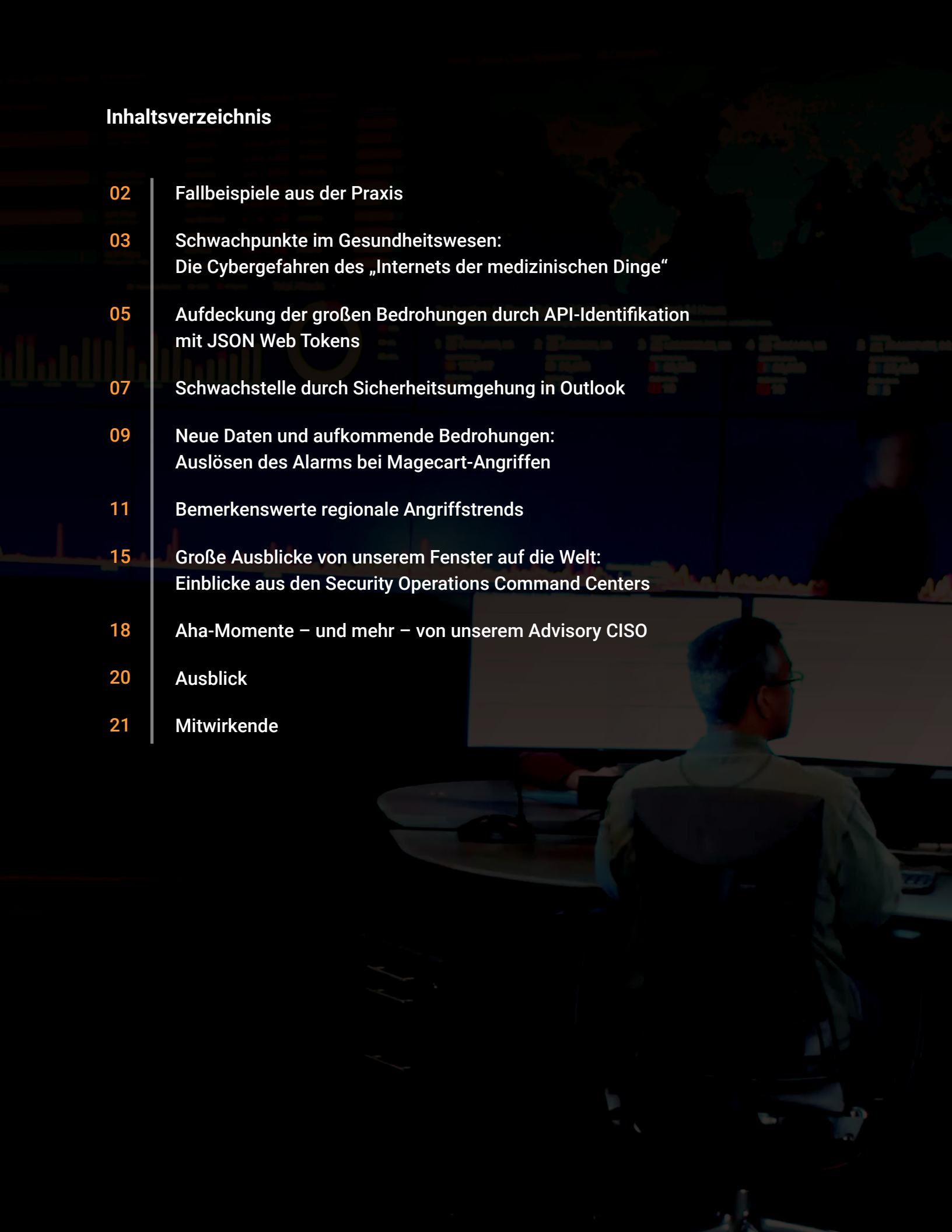
State of the Internet

Band 9 | Ausgabe 6

Ein Jahresrückblick:

Ein Blick auf die Cybertrends von 2023 und die Zukunft

Inhaltsverzeichnis



Fallbeispiele aus der Praxis

Bei diesem „State of the Internet“-Sicherheitsbericht (SOTI) handelt es sich nicht um eine typische Jahresabschlussbilanz, in der wir uns mit jedem Bericht des Jahres befassen. Stattdessen konzentrieren wir uns auf dieses zentrale Thema: Was ist Ihre Lieblingsgeschichte des Jahres zum Thema Sicherheitsfragen? Wir haben die Autoren und einen Datenwissenschaftler der Security Intelligence Group (SIG) von Akamai gebeten, eine Jahresabschlussbewertung einer beliebigen Geschichte durchzuführen, über die wir in den letzten 10 Monaten berichtet haben. Es war sicher eine echte Herausforderung, nur eine der vielen interessanten Geschichten und neuen Entdeckungen aus dem auszuwählen, was wir in unserem Blog zur Sicherheitsforschung und in den SOTI-Berichten für 2023 behandelt haben. Außerdem haben wir unseren Advisory CISO und einen Vice President unserer Security Operations Command Centers (SOCCs) gebeten, sich über die Angriffstrends in diesem Jahr zu informieren, und was davon wir mit ins Jahr 2024 nehmen können.

In diesem Jahr ist in der Welt der Sicherheit und im Rahmen der Sicherheitsforschung bei Akamai viel passiert. Die Forschungsbeiträge unserer Sicherheitsexperten sind ohne Zweifel von unschätzbarem Wert für die Community. Über unseren dedizierten Hub können Sicherheitsexperten problemlos auf vertrauenswürdige Ressourcen zugreifen, die Einblicke, Strategien zur Abwehr und Angriffstrends enthalten, die sie beim Schutz ihrer Unternehmen unterstützen können. Zur Emulation von Angriffen können sie zusätzlich auf kostenlose Tools zugreifen, wie unser RPC-Toolkit sowie unsere kostenlose Open-Source-Plattform Infection Monkey. Der Infection Monkey verhält sich wie Malware und propagiert und „verschlüsselt“ Dateien, auf die er zugreifen kann, indem er die Bits umdreht. So erhält der Anwender einen realistischen Überblick darüber, wie sich ein Angreifer in dieser Umgebung bewegen kann (oder nicht). Die Geschwindigkeit, mit der sich Bedrohungen entwickeln, macht kontinuierliche Tests erforderlich. Sicherheitsexperten müssen wissen, wo ihr Netzwerk heute steht, nicht nur, wo es während des letzten Penetrationstests stand.

Wenn ein Wort erfassen könnte, wie die Landschaft 2023 aussah, wäre dieses Wort *Pivot*. Angreifer verlagerten ihre Taktik, um Sicherheitsmaßnahmen zu umgehen, und suchten nach neuartigen Angriffsflächen und unerschlossenen Zielen, um bei Unternehmen aller Größen und Branchen Schaden anzurichten. Das Gleiche gilt für Abwehrspezialisten, die sich ständig neu kalibrieren und neue Wege zur Abwehr von Angriffen und zum besseren Schutz von Unternehmen erlernen müssen. Wir suchen Lösungen, Forschung und Tools mit diesem Ziel: Bereitstellung umsetzbarer Erkenntnisse und Strategien zur Risikominderung für Sicherheitsexperten, die dieselben Sicherheitsbedrohungen bekämpfen wie wir.

Viel Spaß beim Lesen!

Beliebte Geschichten zum Thema Sicherheit

Angriffstrends 2023

Ausblick auf 2024

Schwachpunkte im Gesundheitswesen: Die Cybergefahren des „Internets der medizinischen Dinge“

Mein Name ist Badette Tribbey, ich bin eine der Verfasserinnen hinter den SOTI-Berichten, und ich arbeite mit Sicherheitsexperten und Datenwissenschaftlern zusammen, um die technischen Erkenntnisse und Daten in aussagekräftige Erkenntnisse zu verwandeln. Ich hasse Mathematik, aber ich liebe es, wie Zahlen überzeugende Angriffstrends aufzeigen können.

Eines der wichtigsten Themen, die wir in diesem Jahr behandelt haben, betrifft uns wirklich alle – die erhöhten Risiken des Internets der medizinischen Dinge (IoMT). Sowohl im Bericht Ausnutzung von Sicherheitslücken als auch in Ransomware auf dem Vormarsch haben wir die Risikolandschaft von Gesundheitswesen und Life Sciences näher betrachtet und untersucht, was diese Branchen anfällig für Angriffe macht. Eines der Dinge, die mich am meisten beeindruckt hat, ist, wie IoMT-Anlagen wie MRT-Geräte, Insulinpumpen und Wearables, obwohl sie für Patienten sehr nützlich sind, die Risiken von Gesundheitsdienstleistern erheblich erhöht haben. Diese Unternehmen standen bereits vor Herausforderungen, ihre Netzwerke zu schützen, da das gesamte Gesundheitswesen komplex ist, veraltete Technologien gefährdet sind und es in IT- und Cybersicherheitsteams an Personal fehlt. Darüber hinaus kann das zeitnahe Patching in dieser Umgebung eine Herkulesaufgabe sein, da Updates von verschiedenen Anbietern für mehrere Systeme oder Anwendungen bereitgestellt werden, was die Nachverfolgung schwierig macht.

Nicht gepatchte IoMT-Geräte gehören zu den anfälligsten Assets über alle Branchen hinweg und können schädlichere Bedrohungen wie Ransomware einschleppen. Durch das stetige Wachstum des IoMT – und damit auch der APIs – werden auch die Schwachstellen zahlreicher. Diese können zur Eintrittsstelle für Angreifer oder ausgenutzt werden und zu Datenlecks führen (Abbildung 1). Ein gemeinsamer Bericht von Cynerio und dem Ponemon Institute über eine Studie, die in mehreren Krankenhäusern und Gesundheitssystemen in den USA durchgeführt wurde, zeigte, dass mehr als die Hälfte der Cyberangriffe aufgrund von Sicherheitslücken in IoMT-Geräten aufgetreten sind.

> “Zeitnahes Patching [im Gesundheitswesen] kann eine Herkulesaufgabe sein, da Updates von verschiedenen Anbietern für mehrere Systeme oder Anwendungen bereitgestellt werden, was die Nachverfolgung schwierig macht.
>
> **– Badette Tribbey, Senior Technical Writer, Akamai**

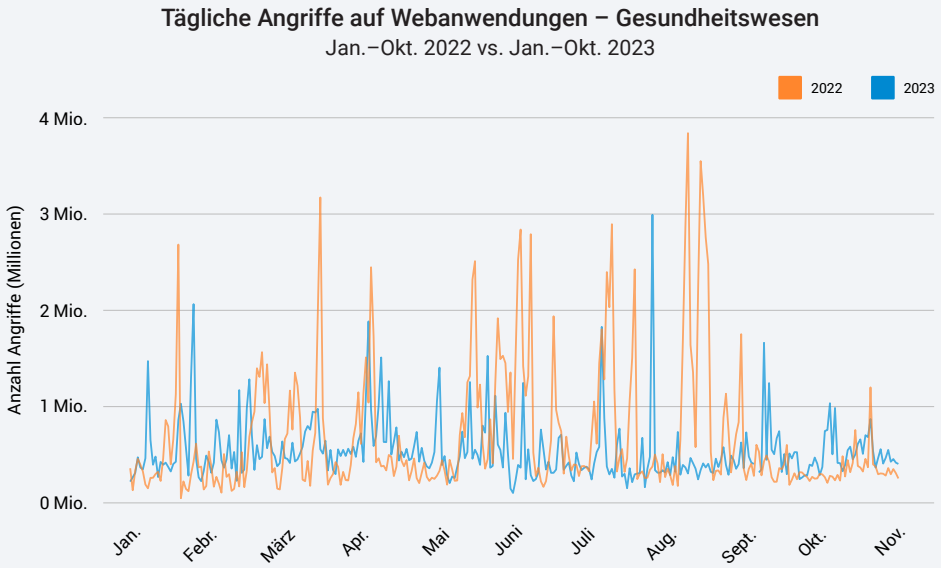


Abb. 1: Angriffe auf Webanwendungen und APIs im Gesundheitswesen und der pharmazeutischen Industrie weisen – mit sporadischen Spitzen zwischen 2022 und 2023 – eine stetige Aktivität auf. Obwohl die Zahl der Angriffe in den letzten Jahren um 21 % zurückging, ist die durchschnittliche Anzahl der Angriffe pro Tag im Jahr 2023 höher als 2022.

Wie geht es weiter im Gesundheitswesen?

Während die Gesundheitsbranche ihr IoMT ausbaut, werden APIs auch weiterhin eine entscheidende Rolle bei der Zugänglichkeit medizinischer Dienste spielen (z. B. Telemedizin und Fernüberwachung von Patienten), was zu besseren klinischen und finanziellen Ergebnissen führen wird. Da Krankenakten und Patientendaten im Darknet einen hohen Wert haben, werden sich die Angriffe auf das Gesundheitswesen wohl auch nicht verringern.

Wenden wir also nun unseren Blick ab von der Vergangenheit und der Zukunft zu, dann wird klar, dass Angreifer den Umfang und die Komplexität ihrer Angriffe weiterhin innovieren und vergrößern werden. Wir werden wahrscheinlich einen anhaltenden Trend zu mehr technischen Angriffen beobachten, die Zero-Day-Schwachstellen ausnutzen. Darüber hinaus ändert sich die regulatorische Landschaft (einschließlich des Protecting and Transforming Cyber Health Care [PATCH] Act von 2022). Daher müssen wir sicherstellen, dass unsere Lösungen dazu beitragen können, ein hohes Volumen an bevorstehenden Gesetzen zu Datenschutz, Reporting, Zahlung, Datensouveränität und Resilienz einzuhalten. Und schließlich erwarten wir, dass die CISOs, die Budgets auf weniger Anbieter verlagern und Lösungen einsetzen, die die Verweildauer für Hacker minimieren, mehr Unterbrechungen bei Angriffen erwarten können.

Aufdeckung der großen Bedrohungen durch API-Identifikation mit JSON Web Tokens

Mein Name ist Lance Rhodes und bin seit März 2023 gerne als Cybersecurity Writer im SIG-Team von Akamai tätig! Ein Großteil meiner Arbeit dient als Bindeglied zwischen unseren Berichten und Blogs, da ich sowohl an den Veröffentlichungs- als auch an den Schreibaspekten für die Blogbeiträge und die sektionale Forschung gearbeitet und zusätzlich Inhalte sowie Marketingmaterialien für die SOTI-Berichte verfasst habe. All dies wird gebündelt in der Zusammenarbeit mit dem Team bei unserem monatlichen internen und externen Newslettern und Einreichungen für die Sicherheitskonferenz.

Ich muss sagen, dass einer der aufregenderen Blogbeiträge, an denen ich in diesem Jahr gearbeitet habe, der Beitrag zu JSON Web Tokens (JWT) war. Dieser Beitrag hatte eine direkte Verbindung zum SOTI-Bericht zu Anwendungen und APIs (Ausnutzung von Sicherheitslücken), da er sich mit der unterbrochenen Authentifizierung in JWTs, eine der Standardmethoden zur Identifizierung von APIs, beschäftigte. Es hat also Spaß gemacht, ein tieferes Verständnis von JWTs zu erhalten.

Nachdem ich Anfang des Jahres am SOTI-Bericht zu Anwendungen und APIs gearbeitet hatte, begann ich mit Nitzan Namer, am JWT-Beitrag zu arbeiten, der sich auf JWT als Angriffsvektor für fehlerhafte Nutzerauthentifizierung konzentrierte, ein Open Web Application Security Project (OWASP) API Security Top 10. Im SOTI-Bericht ist dem ein ganzer Abschnitt gewidmet, aber für den Blogbeitrag tauchten wir noch tiefer in die JWT-Struktur ein. Wir untersuchten, welche Best Practices man nutzen kann, um sich gegen die größten Bedrohungen zu schützen, einschließlich Berechtigungseskalation, Datenlecks und Kontoübernahmen.

Ich erinnere mich, wie ich mit Nitzan darüber sprach, wie wir hofften, dass der Beitrag als fortlaufende Ressource für Sicherheitsforscher, technische Experten sowie JWT-Nutzer und -Administratoren genutzt werden würde. Der Beitrag erfüllt diese Hoffnung durch seinen strukturellen Stil – die JWT-Grundlagen werden zuerst aufgelistet, gefolgt von sechs Fallszenarien, die einige häufige Bedrohungen veranschaulichen und Best Practices für jedes einzelne nennen. Die Grundlagen enthalten Informationen darüber, wie JWTs APIs sichern, indem Token ausgegeben werden, die Informationen enthalten, die als JSON-Objekte freigegeben werden sollen. Jedes Token ist codiert – aber nicht verschlüsselt – und besteht aus einem Header, einer Payload und einer Verifizierungssignatur (die autorisiert, dass die Daten seit der Erstellung des Tokens durch den Server nicht geändert wurden).

> Im Blogbeitrag tauchten wir noch tiefer in die JWT-Struktur ein. Wir untersuchten, welche Best Practices man nutzen kann, um sich gegen die größten Bedrohungen zu schützen, einschließlich Berechtigungseskalation, Datenlecks und Kontoübernahmen.
>
> **– Lance Rhodes, Cybersecurity Writer, Akamai**

Die sechs Szenarien sind:

1. Zulassen, dass der Server ein Token ohne Validierung verwendet
2. Verwendung desselben privaten Schlüssels für verschiedene Anwendungen
3. Verwendung eines schwachen Signieralgorithmus
4. Die Wahl eines privaten Schlüssels, der kurz ist und/oder eine geringe Entropie aufweist
5. Sensible Daten in der Payload eines JWT
6. Verwechslung von Schlüsseln

JWTs sind eines der gängigsten Verifikationsformate. Angemessene Sicherheitsmaßnahmen sind von entscheidender Bedeutung, da das Format eine breite Angriffsfläche bietet, die viel Raum für Fehler lässt. Obwohl diese Szenarien einige der häufigsten Bedrohungen für JWTs zeigen, gibt es noch viel mehr, und Angriffstechniken entwickeln sich kontinuierlich weiter.

JWTs werden weder verschlüsselt noch mit Blick auf die Sicherheit implementiert

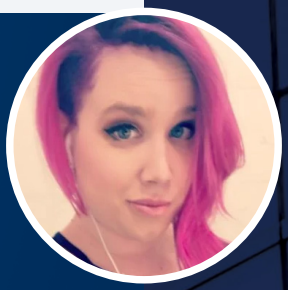
Eine meiner wichtigsten Erkenntnisse aus dem Blogbeitrag ist, dass JWTs weder verschlüsselt noch mit Blick auf Sicherheit implementiert werden. Es ist schwer zu glauben, dass solch ein beliebtes Authentifizierungstoken so anfällig sein kann. Ein Teil der Attraktivität von JWTs besteht darin, dass sie die Verwendung vieler Webanwendungen und APIs ermöglichen, ohne sich häufig anmelden zu müssen. Sowohl der SOTI-Bericht als auch der JWT-Blogbeitrag analysierten die JWT-Algorithmen im Akamai-Traffic und stellten fest, dass symmetrische Algorithmen die häufigsten sind, obwohl sie theoretisch weniger sicher und nicht so schützend sind wie asymmetrische Algorithmen. Beide Publikationen zeigen beispielsweise, dass 54 % der Kunden von Akamai den symmetrischen HS256-Algorithmus verwenden.

Es ist wahrscheinlich, dass symmetrische Algorithmen häufiger gewählt werden, weil der Nutzer nur einen Schlüssel benötigt und asymmetrische Algorithmen eine höhere Anzahl an Rechenressourcen erfordern. JSON Web Encryption, die verschlüsselte Version von JWT, wird ebenfalls nicht häufig verwendet. Die meisten Unternehmen entscheiden sich für JWT, um Rechenressourcen zu verringern.

Das Ergebnis: Nutzerfreundlichkeit, Kosten und Geschwindigkeit werden oft vor Sicherheit priorisiert. Dies ist eine wertvolle Erinnerung an die Bedeutung unserer Arbeit als Sicherheitsforscher und -autoren. Gute Sicherheitsforschung und -verfahren sind erforderlich, um ein ausgewogenes Verhältnis zwischen Effizienz und Sicherheit zu ermöglichen.

> Es ist schwer zu glauben, dass solch ein beliebtes Authentifizierungstoken so anfällig sein kann.
>
> – Lance Rhodes, Cybersecurity Writer, Akamai

Schwachstelle durch Sicherheitsumgehung in Outlook



Hallo, ich hoffe, Sie hatten einen guten Tag! Mein Name ist Tricia Howard, und ich arbeite für die SIG-Blogseite. Ich lebe in der Welt der technischen Beiträge und arbeite (unter anderem) mit unseren Forschern, unserem Team für Unternehmenskommunikation und unserer Rechtsabteilung zusammen, um die Beiträge zeitnah und effektiv herauszubringen. Das Beste an meinem Job ist, dass ich im Namen unserer Forscher prahlen darf, weil sie wirklich coole Sachen machen!

Von all den Dingen, über die ich dieses Jahr schreiben durfte, ist das vielleicht das schwierigste. Wie soll ich unter all den unglaublich coolen Dingen, die unser Team in den letzten 12 Monaten getan hat, einen Favoriten auswählen? Aber da ich etwas auswählen muss, entscheide ich mich für Ben Barneas Arbeit zur berühmt-berüchtigten Schwachstelle durch Sicherheitsumgehung in Outlook. Ben ist einer der brillantesten Forscher, die ich kenne. Er hat es geschafft, einen ganzen Patch zu Fall zu bringen – mit nur einem Schrägstrich. Klar, das klingt absurd oder sogar unmöglich, aber es war möglich, und er hat es geschafft.

Die ursprüngliche Schwachstelle ermöglichte einem nicht autorisierten Angreifer, eine Outlook-Einladung mit einem individuellen Benachrichtigungston zu senden. Dieser Ton wurde vom Angreifer als Pfad festgelegt, über den eine Verbindung zum Server des Angreifers erzwungen und NTLM-Anmeldedaten bereitgestellt wurden. Das ist ein echtes Problem, denn dadurch kann der Angreifer die Anmeldedaten knacken oder einen Relay-Angriff ausführen. All das kann wiederum zu einer Berechtigungseskalation führen – und wir alle wissen, was dann passiert. Das Schlimmste daran ist, dass bei dieser Schwachstelle keine Interaktion mit dem Nutzer erforderlich war, also „Null-Klick“. Hinter derartigen Aktionen steckt häufig viel Macht, und deswegen sind sie so gefährlich. Insbesondere wenn man erfährt, dass diese Aktion von Russland aus durchgeführt wurde, und gezielt gegen mehrere europäische Regierungsbehörden gerichtet war.

Der Patch wurde im März veröffentlicht. Durch ihn konnte *PidLidReminderFileParameter* nicht mehr verwendet werden, das es dem Angreifer ermöglicht hatte, den individuellen Pfad anzugeben (d. h. eine Verbindung zum Server des Angreifers herzustellen). Der Patch verwendete stattdessen die Funktion *MapURLtoZone*, die überprüft, ob der Pfad sich auf eine Internet-URL bezieht. Wenn dies der Fall ist, wird der standardmäßige Benachrichtigungston anstelle des individuellen Tons abgespielt. In der Theorie setzt das die Möglichkeit für einen Remote-Angreifer außer Kraft, diese Schwachstelle auszunutzen. Denn schließlich muss eine Internet-URL aufgerufen werden, um eine Verbindung zwischen dem Angreifer und dem Angriffsziel herzustellen.

> “Für Verteidiger gibt es ohnehin genug zu tun, auch ohne dass sich diese um Null-Klick-Berechtigungseskalationen Gedanken machen müssen.
>
> **– Tricia Howard,**
> **Senior Technical Writer,**
> **Akamai**

Der Patch wird ausgebremst

Hier wird es erst richtig interessant und – wie ich finde – auch ein wenig lustig. Wie jeder große Forscher wollte Ben überprüfen, ob die Schwachstelle wirklich nicht mehr ausgenutzt werden kann. Dies ist eine stark heruntergebrochene Art und Weise, dies auszudrücken, aber es gibt im Wesentlichen zwei Optionen für *MapURLtoZone*: Zulassen oder verweigern. Wird eine Verbindung zum Internet hergestellt oder nicht? Größtenteils konnte der Patch wie geplant verwendet werden. Denn auch wenn es nach einem lokalen Pfad aussah, erkannte *MapURLtoZone*, dass von diesem Pfad ein Verbindungsversuch zu einer Internet-URL ausgeführt wurde.

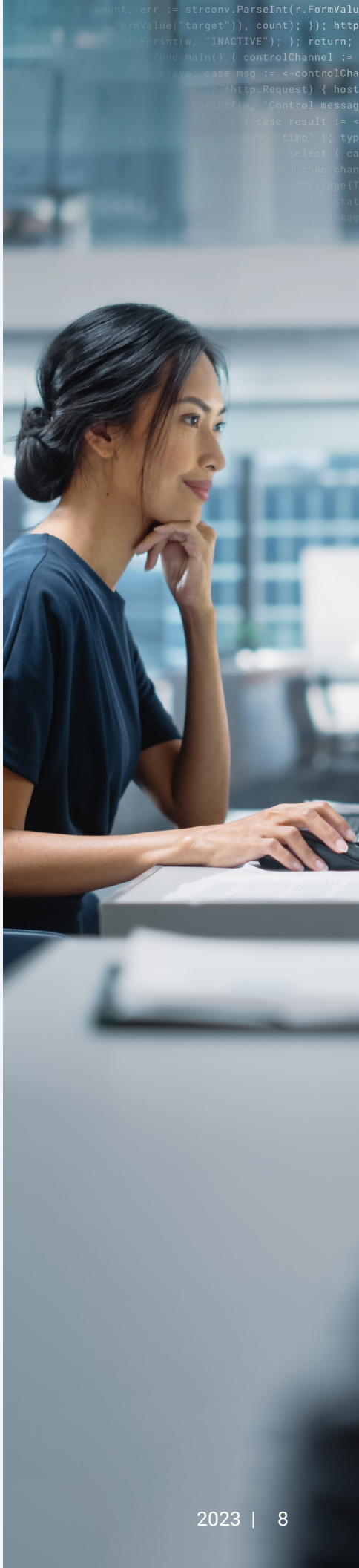
Ben entschied sich, mit dem Pfadnamen herumzuspielen, indem er am Ende „/“ Ende hinzufügte. Wenn man etwas bereitstellt, das *MapURLtoZone* nicht erwartet hat, muss es trotzdem entscheiden, ob die Aktion „Zulassen“ oder „Verweigern“ ausgeführt werden soll. Der zusätzliche Schrägstrich wurde nicht erkannt, was wiederum eine 0 zurückgab, die die Funktion als lokal und vertrauenswürdig las. Danach konnte die Schwachstelle genau wie geplant ausgelöst werden, indem *CreateFile* für den nutzerdefinierten Pfad verwendet wurde.

Das war alles! Ein kleiner Schrägstrich wurde hinzugefügt, und ein vollständiger Patch für eine **kritische** Schwachstelle war plötzlich keine effektive Lösung mehr. In die Entwicklung dieses Patches haben wahrscheinlich viele Cybersicherheitsexperten jede Menge Zeit und Kraft investiert, um die Schwachstelle zu beseitigen – nur um dann von einem einzigen Schrägstrich völlig zurückgeworfen zu werden.

Die Ausgeklügeltheit des ursprünglichen Angriffs ist wirklich unvorstellbar, wenn man es genau betrachtet. Die Schachzüge des Angreifers können mit denen von Magnus Carlsen mithalten. Wenn man bedenkt, dass nur ein Schrägstrich erforderlich war, um einen ganzen Patch nutzlos zu machen, wird deutlich, dass die Angreifer selbst wohl auch irgendwann auf diese Umgehung gekommen wären. Umso besser, dass es Ben war, der diese Sicherheitslücke aufdeckte, indem er mit üblichen Denkmustern brach.

Aus diesem Grund sind Forscher, die diese Fehler finden, wirklich die Lebensader der Cybersicherheits-Community. Für Verteidiger gibt es ohnehin genug zu tun, auch ohne dass sich diese um Null-Klick-Berechtigungseskalationen Gedanken machen müssen. Sicherheitsforscher leisten einen echten Beitrag, vor allem, da wir in unserem täglichen Leben immer mehr von Technologie und dem Internet abhängig werden.

Ich bin so stolz, Teil dieses unglaublichen Teams zu sein und mit einigen der brillantesten Köpfe auf diesem Planeten zusammenzuarbeiten. An alle, die unsere Blogs, Tweets und SOTIs gelesen haben: Vielen Dank. Und an die Forscher, sowohl innerhalb als auch außerhalb von Akamai SIG: Danke für eure Arbeit und eure Ergebnisse. Ich bin schon gespannt, was das nächste Jahr für uns bereithält!



Neue Daten und aufkommende Bedrohungen: Auslösen des Alarms bei Magecart-Angriffen

Mein Name ist Chelsea Tuttle, und ich arbeite seit fast acht Jahren bei Akamai. Als Datenwissenschaftlerin, die in den letzten vier Jahren für die im SOTI dargestellten Daten verantwortlich ist, verbringe ich den Großteil meiner Zeit mit der Reinigung, Untersuchung, Analyse und Visualisierung unserer Daten. Wenn ich nicht auf Daten starre, arbeite ich eng mit den SOTI-Autoren zusammen, um die Geschichten zu vermitteln, die unsere Daten uns erzählen. Aufgrund der Komplexität von Big Data und der Vorteile von Berichten zu Verlaufsdaten fügen wir nicht oft einen neuen Datensatz hinzu, aber dieses Jahr haben wir es geschafft! Wenn ich auf 2023 zurückblicke, fallen mir die Geschichten, die wir zu diesem neuen Datensatz veröffentlicht haben, als einige meiner Favoriten ein, weil mir die Lernkurve, die wir bei diesem Unterfangen durchlaufen haben, sehr gut gefallen hat.

In unserer Welt konzentrieren wir uns allzu oft darauf, die Anzahl der Angriffsversuche in unserem Netzwerk zu melden, und verpassen wichtige Gelegenheiten, Daten zu melden, die für die Absicherung potenzieller Schwachstellen und die Verhinderung von Angriffen relevant sind. Ein Datensatz, den wir in diesem Jahr unseren SOTI-Berichten hinzugefügt haben, zeichnet sich dadurch aus, dass er eine potenzielle Schwachstelle hervorhebt, anstatt sich auf das Ausmaß der Angriffe zu konzentrieren. Dieser Datensatz basiert auf Beobachtungen von Akamai Client-Side Protection & Compliance, die täglich mit ihren Adleraugen Milliarden von Webseitenskripten durchkämmen. Einer der Bereiche, in denen potenzielle Schwachstellen bestehen, ist die Anzahl der Erst- und Drittanbieterskripte, die auf Websites verwendet werden. Auch wenn die Verwendung eines Erstanbieterskripts keine Sicherheit garantiert und die Verwendung eines Drittanbieterskripts nicht zwangsweise eine Sicherheitslücke darstellt – je mehr Vertrauen in eine weitere Partei gelegt wird, wie z. B. durch ein Webseitenskript von einem Drittanbieter, desto mehr Risiken werden dem Sicherheitsprofil hinzugefügt. Akamai arbeitet daran, die Lücke zwischen Nutzerfreundlichkeit und Sicherheit zu schließen, die durch den zunehmenden Einsatz von Drittanbieterskripten in allen Branchen entstanden ist.

> Akamai arbeitet daran, die Lücke zwischen Nutzerfreundlichkeit und Sicherheit zu schließen, die durch den zunehmenden Einsatz von Drittanbieterskripten in allen Branchen entstanden ist.
>
> **– Chelsea Tuttle, Senior Data Scientist, Akamai**

Wie bereits in unserem SOTI-Bericht Eine Analyse der Bedrohungstrends im Handelssektor vom Juni 2023 erwähnt, waren ein Schwerpunkt für die diesjährige Studie von Akamai die jüngsten Web-Skimming-Angriffe im Magecart-Stil. Insbesondere wurde beobachtet, wie Magecart-Angriffe den digitalen Handelssektor weiterhin durchdringen. Bei dieser Art von Angriff wird versucht, vertrauliche Nutzeranmeldedaten wie Kreditkarteninformationen aus dem Warenkorb einer digitalen Handelswebsite zu stehlen, indem schädlicher JavaScript-Code injiziert wird. Diese Art von Angriffen ist für Gegner in der Regel leicht, birgt jedoch große Risiken für die Verbraucher – und sie sind immer schwieriger zu erkennen. Diese

Magecart- oder auch Web-Skimming-Angriffe werden vom Websitenutzer oder -besitzer häufig nicht bemerkt, und Angreifer wählen oft digitale Handelswebsites, die anfällige oder veraltete Software verwenden.

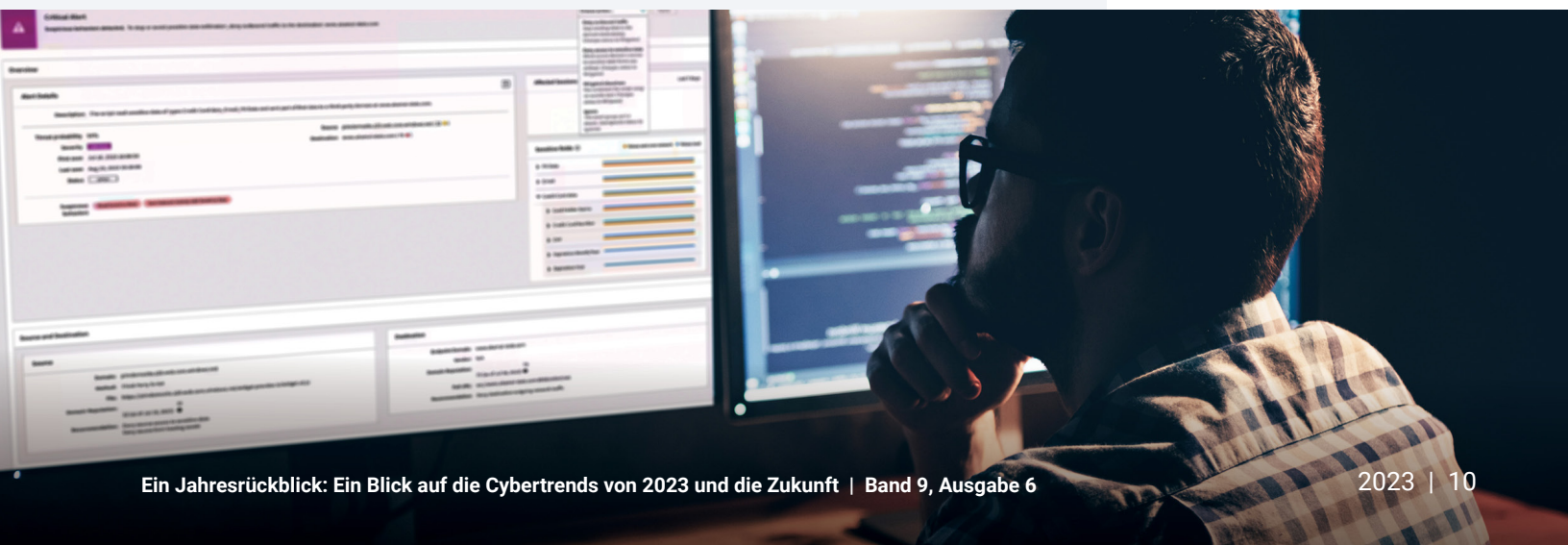
Die jüngsten Magecart-Varianten

Eine Reihe von Magecart-Varianten sind in den neuesten Magecart-Kampagnen zu sehen, die von Akamai-Forschern untersucht wurden. Unser SOTI-Bericht vom Juni 2023 konzentrierte sich auf die clientseitigen Magecart-Angriffe und wies auf ausgenutzte Schwachstellen in Drittanbieterskripten aus Open-Source-Bibliotheken hin, die zu Angriffen in der Lieferkette führen könnten. Kurz nach der Veröffentlichung des SOTI-Berichts veröffentlichten wir einen Blogbeitrag darüber, wie Forscher von Akamai eine neue Kampagne im Magecart-Stil entdeckten, bei der legitime Websites missbraucht wurden, um andere anzugreifen. In dieser Kampagne gab es im Wesentlichen zwei Gruppen von attackierten Websites: legitime Websites, die für das Hosting kompromittiert wurden, um als von Angreifern kontrollierte Server zu fungieren, und anfällige Handelsseiten, die mit clientseitigem Web-Skimming angegriffen wurden. Im August wurde ein zweiter Blogbeitrag veröffentlicht, in dem beschrieben wird, wie Akamai-Forscher eine neue Magento-Kampagne mit einer versteckten serverseitigen Template Injection entdeckten, die digitale Handelswebsites ausnutzte, um Informationen zum finanziellen Status des Angriffsziels herauszufinden.

Der neueste Magecart-Blogbeitrag von Akamai SIG enthüllt eine neue Verschleierungstechnik, bei der Angreifer die standardmäßige Fehlerseite 404 der Website manipulieren, um schädlichen Code zu verbergen. Forscher von Akamai haben herausgefunden, dass diese neue Kampagne aus zwei zusätzlichen, fortschrittlichen Verschleierungstechniken besteht. Sie präsentieren die sich entwickelnden Taktiken, mit denen Angreifer die Angriffskette verlängern und eine Erkennung verhindern.

Das Jahr 2023 neigt sich dem Ende zu, und ich blicke zurück auf alle Forschungs- und Reporting-Möglichkeiten, die wir dank neuer Daten und aufkommender Bedrohungen hatten. Ich freue mich bereits auf die neuen Daten und die Lernmöglichkeiten, die das Jahr 2024 für uns bereithält.

Forscher von Akamai entdeckten eine neue Kampagne von Magecart-Angriffen, bei der seriöse Websites für den Angriff Dritter missbraucht wurden



Bemerkenswerte regionale Angriffstrends

Mein Name ist Charlotte Pelliccia. Ich stieß 2023 zum SOTI-Team, um die Geschichten aus dem asiatisch-pazifischen Raum und Japan (APJ) sowie den Regionen Europa, Naher Osten und Afrika (EMEA) ans Licht zu bringen. Unsere APJ- und EMEA-Snapshots sind Begleitstücke zu unseren globalen SOTI-Berichten. Hier werde ich einige der wichtigsten Angriffstrends, die wir im Jahr 2023 behandelt haben, erneut aufgreifen und Daten aus Snapshots aktualisieren, die Anfang des Jahres veröffentlicht wurden.

Angriffe auf Webanwendungen und APIs – eine Geschichte aus zwei vertikalen Märkten

Wie bereits in unseren jüngsten SOTI-Berichten zu Finanzdienstleistungen und Handel beschrieben, sind Finanzdienstleister nach wie vor oberstes Ziel bei Angriffen auf Webanwendungen und APIs in APJ, gefolgt vom Handel. Seit unserem Bericht vom Juni 2023 haben sich die Angriffe auf Finanzdienstleistungen auf mehr als 4,5 Milliarden erhöht (ein Anstieg um 22 % von zuvor 3,7 Milliarden). Und seit unserem Bericht vom März 2023 sind die Angriffe auf den Handel von 1,2 Milliarden auf 1,9 Milliarden gestiegen, was einem Anstieg von 58 % entspricht. Die Aufteilungen zwischen subvertikalen Märkten bleiben relativ konsistent (Abbildung 2).

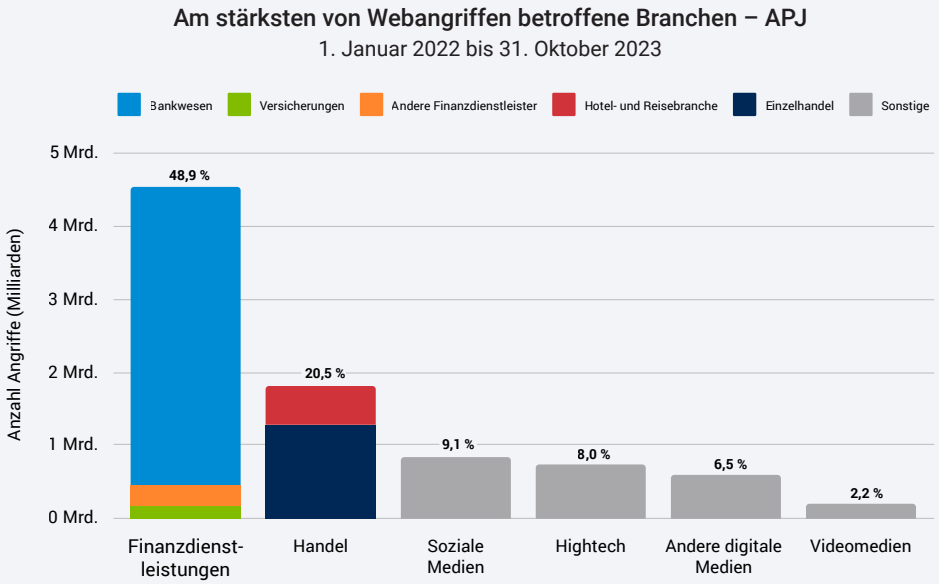


Abb. 2: Vertikale Webangriffe in APJ bis Oktober 2023

> Einblicke in regionale Angriffstrends ist entscheidend, damit Unternehmen ihre Risiken besser verstehen und ihre Tools und Best Practices optimieren können.
>
> **– Charlotte Pelliccia, Cybersecurity Writer, Akamai**

In der EMEA-Region ist der Handel nach wie vor die am stärksten von Angriffen auf Webanwendungen und APIs betroffene Branche. Seit unserem Bericht vom März 2023 stiegen die Angriffe mittlerweile auf über 6,5 Milliarden (ein Anstieg von 41 % von zuvor 4,6 Milliarden). Obwohl das verarbeitende Gewerbe von der vierten an die dritte Stelle gerückt ist und damit die Finanzdienstleistungen verdrängt hat, sind die Angriffe auf Finanzdienstleister seit unserem Bericht vom Juni 2023 um 70 % gestiegen und erreichen nun 1,7 Milliarden gegenüber zuvor 1 Milliarde. Auch hier ist die Aufteilung zwischen den subvertikalen Märkten relativ konstant geblieben (Abbildung 3).

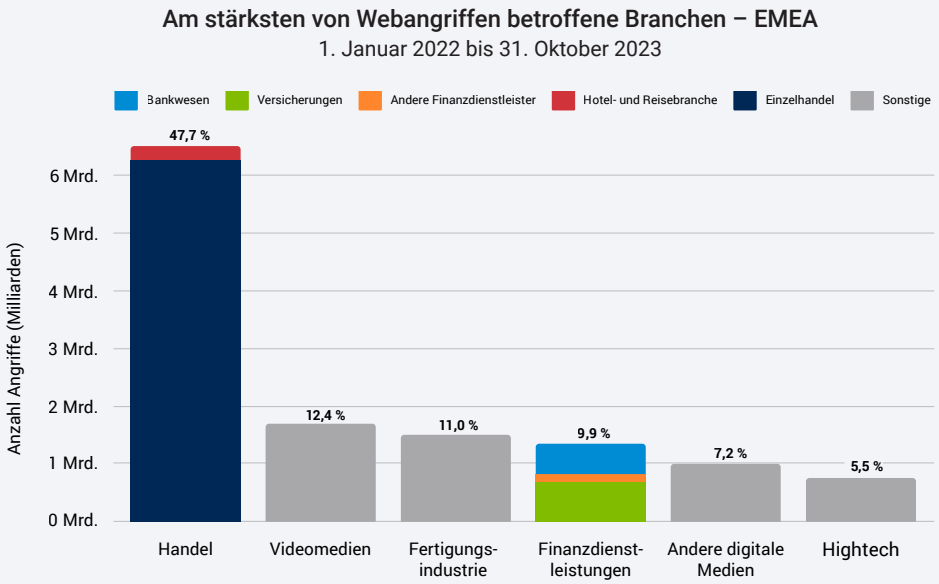


Abb. 3: Vertikale Webangriffe in EMEA bis Oktober 2023

Schädliche Bots sind eine Waffe der Wahl

Wie wir in früheren Berichten gesehen haben, steht APJ bei schädlichen Bot-Aktivitäten an zweiter Stelle nach Nordamerika. Die drei wichtigsten vertikalen Angriffsbereiche von Januar 2022 bis Oktober 2023 in APJ sind Handel (27,4 %), Videomedien (15,0 %) und Finanzdienstleistungen (14,3 %). In der EMEA-Region zielte die Hälfte (50,1 %) aller schädlichen Bot-Aktivitäten auf den Handel ab, gefolgt von anderen digitalen Medien mit 15,3 % und Videomedien mit 12,2 % (Abbildung 4).

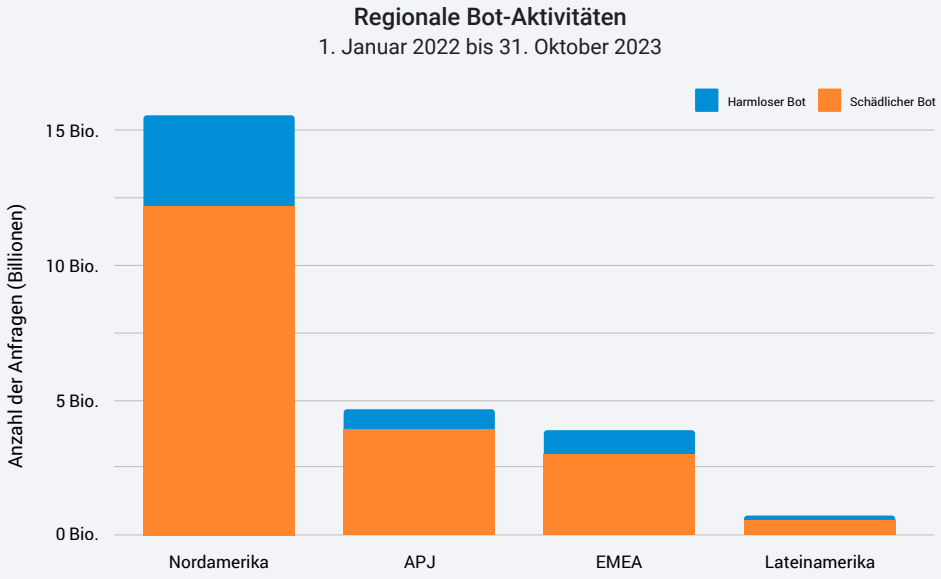


Abb. 4: Die Verwendung schädlicher Bots ist in allen Regionen weit verbreitet und übertrifft die Verwendung gutartiger Bots bei Weitem

Im folgenden Essay erfahren Sie, wie sich Bot- und DDoS-Angriffe verändern.

EMEA im Fadenkreuz der regionalen Verschiebung bei DDoS-Angriffen

In unserem Bericht von 2023 wurde deutlich, dass die Bedrohungsakteure EMEA im Visier haben, was zum Teil auf das aktuelle geopolitische Klima zurückzuführen ist. Ein Paradebeispiel: Die Anzahl der DDoS-Angriffe (Distributed Denial of Service) gegen die Finanzdienstleistungs-, Glücksspiel- und Fertigungsbranchen in EMEA überstieg die Zahl in allen anderen Regionen zusammen (Abbildung 5).

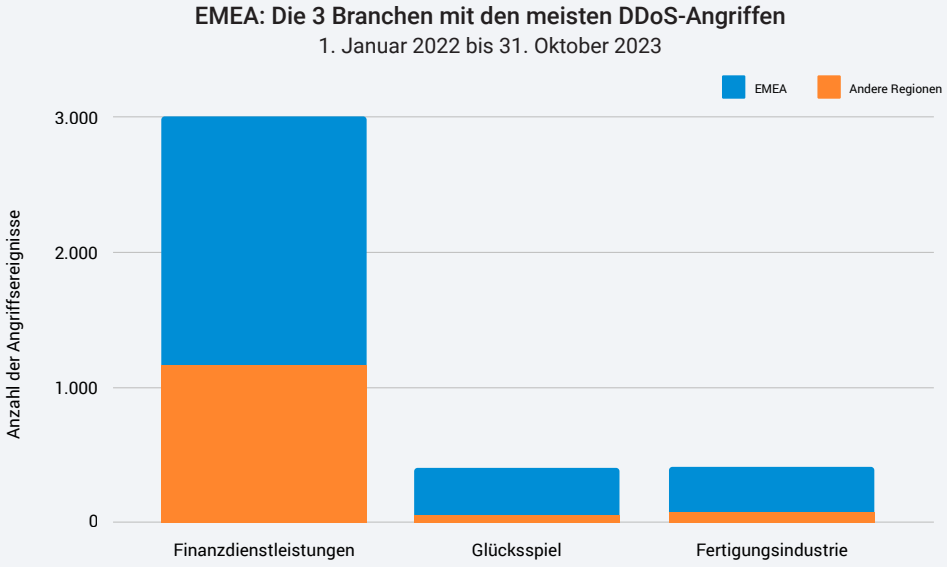


Abb. 5: In EMEA fanden mehr DDoS-Angriffsereignisse als in allen anderen Regionen zusammen statt

Ausblick

Solange Bedrohungsakteure mit Web-, Bot- und DDoS-Angriffen erfolgreich sind, kann man davon ausgehen, dass diese die Waffen der Wahl bleiben. Tatsächlich entwickeln sich diese drei Vektoren stetig weiter und werden immer stärker. Zero-Day-Exploits von Webanwendungen werden mit Ransomware-Techniken (von Ransomware-Gruppen wie CL0P) verwoben und umfassen DDoS-Angriffe, um eine dreifaches Erpressungsszenario zu schaffen. Web-Scalping über Bots ist für fast jede größere Fluggesellschaft oder jeden Ticketverkauf zur neuen Normalität geworden. Und API-Angriffe auf die Geschäftslogik der API werden immer häufiger.

Als Reaktion darauf nehmen die Aufsichts- und Meldepflichten weltweit und branchenübergreifend zu, da keine Region oder Branche vor Angriffen geschützt ist. Ziel ist es, die Cybersicherheitsgesetze mit der sich entwickelnden Bedrohungslandschaft auf dem neuesten Stand zu halten. Unternehmen müssen wachsam bleiben, um die Reporting-Pflichten zu erfüllen, und darauf vorbereitet sein, Risiken durch eine mehrschichtige Verteidigung zu mindern.

Große Ausblicke von unserem Fenster auf die Welt: Einblicke aus den Security Operations Command Centers

Mein Name ist Roger Barranco, Vice President of Global Security Operations. Ich arbeite seit fast 12 Jahren bei Akamai und bin im Unternehmen für die Managed Security Operations verantwortlich, die von sechs SOCCs rund um den Globus betreut und von einem fantastischen Team unterstützt werden. Ich habe meine Karriere im Bereich Cybersicherheit begonnen. Zu diesem Feld fühlte ich mich hingezogen, weil es sich um einen interessanten, sich ständig verändernden Markt handelt – 2023 ist ein gutes Beispiel dafür.

Das SOCC von Akamai war noch nie so beschäftigt – bis Ende 2023 werden wir etwa 30 % mehr sicherheitsrelevante Tickets als im letzten Jahr abwickeln. Hier sind die wichtigsten Erkenntnisse, die wir aus der Zusammenarbeit mit unseren Managed Security Service-Kunden gewonnen haben und die Unternehmen für 2024 im Auge behalten sollten.

DDoS-Angriffe verändern sich

Obwohl die Zahl der angegriffenen Kunden seit jeher jährlich ansteigt, hat sich die Art der Angriffe verändert. Zuerst haben sich Typ und Umfang der angegriffenen Kundeneigenschaften geändert. Statt 10 Angriffe auf dieselben oder ähnliche Endpunkte sehen wir jetzt 100 Angriffe, die alle auf verschiedene IPs im Netzwerkbereich des Kunden gerichtet sind. Diese Angriffe zielen nicht nur auf Layer 3, sondern gleichzeitig auch auf Layer 7 ab. Außerdem haben die Angriffe auf DNS drastisch zugenommen. Dabei handelt es sich hauptsächlich um gültige Abfrageangriffe, die die DNS-Infrastruktur des Kunden leicht überfordern können. Nur wenige Megabit unerwünschter DNS-Traffic können ein Unternehmen erheblich belasten. Wir beginnen auch, ein Wiederaufleben der Aktivitäten an der Mirai-Front zu beobachten, das bekannt wurde, weil es die Macht des Internets der Dinge nutzte, um heftige Störungen zu verursachen.

In der heutigen Bedrohungslandschaft reicht es nicht aus, leistungsstarke Geräte auf den Markt zu bringen, um mit Angriffen Schritt zu halten. Unternehmen benötigen einen zuverlässigen Sicherheitsservice auf Cloud-Ebene, um diese Workload zu bewältigen, den Status zu erhalten und gleichzeitig einzigartige Schutzmaßnahmen für jeden dieser Endpunkte zu implementieren. Hier zeichnet sich Akamai sowohl aus der Plattform- als auch aus der Serviceperspektive aus. Wir können mehrere Sicherheitsebenen anwenden, um das gesamte Spektrum von Cyberangriffen abzuwehren. Und unsere praktischen Experten untersuchen die Nuancen und Trends für alle Kunden, um sie auf eine ganz spezifische Weise zu überwachen und abzuschwächen, die die Bedrohung abwehrt, aber den erwarteten, sauberen Traffic ermöglicht.

> “Das SOCC von Akamai war noch nie so beschäftigt – bis Ende 2023 werden wir etwa 30 % mehr sicherheitsrelevante Tickets als im letzten Jahr abwickeln.
>
> – Roger Barranco, Vice President of Global Security Operations, Akamai

Der Kampf gegen Bots kann brutal sein

Der Missbrauch von Anmeldedaten ist schwer einzudämmen, da es schwierig ist, unerwünschten Traffic von gewünschtem Traffic zu unterscheiden. Kunden haben zudem ziemlich einzigartige Backend-Systeme, die möglicherweise sehr unterschiedliche Abhilfemaßnahmen erfordern. Darüber hinaus gehören Angreifer, die den Missbrauch von Anmeldedaten ausführen, zu den qualifiziertesten und skrupellosesten, da erfolgreicher Missbrauch von Anmeldedaten die einfachste Möglichkeit ist, Gewinne zu erzielen. Aufgrund der gefährlichen und kostspieligen Art dieser Bot-Angriffe ist es wichtig, eine Lösung zum Schutz vor Missbrauch von Anmeldedaten zu haben, insbesondere in der Finanzdienstleistungs- und Handelsbranche, in der die Nutzung schädlicher Bots weiter zunimmt.

EMEA bleibt im Visier der Angreifer

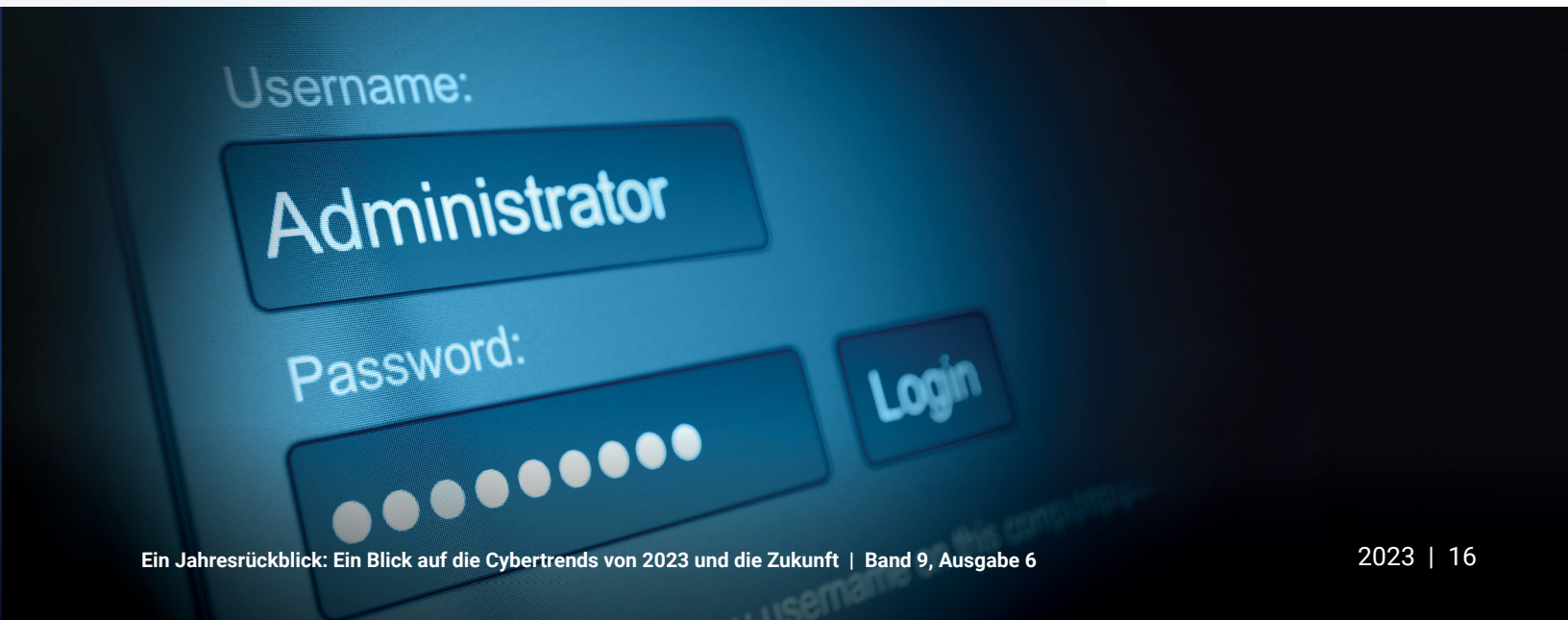
Seit der Ukraine-Krise hat EMEA (insbesondere Europa) die USA als die wichtigste Region für Cyberangriffe in einer Reihe verschiedener Branchen und Kategorien von Angriffsarten, insbesondere DDoS, verdrängt. Dieser Wandel unterstreicht die Tatsache, dass viele Aggressoren Nationalstaaten oder Sympathisanten von Nationalstaaten sind und ihr Fokus auf Europa nicht nachlässt.

Die Raffinesse der Angreifer steigt

Vorbei sind die Zeiten, in denen Skript-Kiddies die größte Bedrohung darstellten, die herkömmliche Tools nutzten, um einen Angriff zu starten, oder ein DDoS-Botnet für 10 US-Dollar pro Stunde mieteten, um einen Konkurrenten bei einem Videospiel zu besiegen. Heute sind Angreifer trickreicher, und sie scheinen sich auf bestimmte Ziele im Detail zu konzentrieren, ihre Strategie zu planen, Aufklärungsarbeit manchmal ein Jahr im Voraus durchzuführen und Angriffe zu entwickeln, um wahrgenommene mögliche Schwächen auszunutzen. Als Ergebnis der von den Aggressoren eingeleiteten Grundarbeit dauern Angriffe aktuell oft länger als in den letzten Jahren, in denen sie häufig nur wenige Minuten dauerten.

> Als Ergebnis der von den Aggressoren eingeleiteten Grundarbeit dauern Angriffe aktuell oft länger als in den letzten Jahren, in denen sie häufig nur wenige Minuten dauerten.

– Roger Barranco,
Vice President of
Global Security Operations,
Akamai



Best Practices für die Abstimmung von Cyber- und Betriebsabläufen

Trotz dieser Herausforderungen können Kunden die Effektivität ihrer Bemühungen um ihren eigenen Schutz erhöhen, indem sie zwei Best Practices für die Abstimmung von Cybersicherheit und Betrieb befolgen, die es Akamai ermöglichen, als Erweiterung des Cyberteams zu fungieren. Zuerst sollte aktiv eine Partnerschaft mit dem SOCC außerhalb einer Bedrohungslage entstehen, damit die Abwehr nicht erst bei einem Angriff eingesetzt wird. Auf diese Weise können Angriffe vorab abgewehrt werden, ohne Auswirkungen auf die Produktion zu haben. Kunden erhalten einen Follow-up-Bericht mit detaillierten Angaben zu den abgewehrten Angriffen.

Zweitens sollten sie proaktiv an betrieblichen Bereitschaftsplänen und Backup-Plänen arbeiten. Sie sollten zum Beispiel sicherstellen, dass sie wissen, wie sie während der Tests ein Route-on oder Route-off für verschiedene Plattformen durchführen. Ein fünfminütiger Angriff kann einen Kunden aufgrund betrieblicher Probleme eine Stunde lang schädigen. Daher ist es genauso wichtig, auf ein reines Cyberproblem vorbereitet zu sein.

Dieses Jahr hat deutlich gemacht, wie sich die Cybersicherheit ständig verändert. Wir gehen davon aus, dass sich dieser Trend fortsetzen wird. Die gute Nachricht ist, dass Kunden durch die Anwendung dieser Erkenntnisse im Jahr 2024 einen Schritt voraus sein werden und sich selbst schützen können.

Aha-Momente – und mehr – von unserem Advisory CISO

Mein Name ist Steve Winterfeld. Ich bin der Advisory CISO von Akamai. Vor meiner Tätigkeit bei Akamai war ich CISO bei der Nordstrom Bank und Director of Incident Response and Threat Intelligence bei Charles Schwab. Meine Rolle ist, dafür zu sorgen, dass unsere Partner ihre Kunden erfolgreich schützen können. Außerdem bestimme ich, worauf wir als Unternehmen unsere Anstrengungen richten sollten.

In diesem Jahr gab es einige Trends, die mich überraschten, und einige wurden durch Daten bestätigt, die zur Aktualisierung unserer Strategie verwendet werden können. Meine Top-neun-Geschichten dieses Jahr beinhalteten einige Aha-Momente, einige erwartete Nachrichten und einige Dinge, die sich wohl nie ändern.

Aha-Momente

- Insgesamt 10 bis 16 % der Unternehmen haben mindestens einmal pro Quartal Command and Control-Traffic (CnC) in ihrem Netzwerk festgestellt. Darüber hinaus erreichten 26 % der infizierten Geräte Domains, die mit einem anfänglichen Access Broker in Verbindung standen.
- Bei der Bedrohungslandschaft mit Ransomware war in den letzten sechs Monaten ein besorgniserregender Wandel bei den Angriffstechniken mit dem rasanten Missbrauch von Zero-Day- und One-Day-Schwachstellen zu sehen.
- Akamai hat herausgefunden, dass für Unternehmen, die zu Opfern von mehreren Ransomware-Gruppen wurden, in den drei Monaten nach dem ersten Angriff eine sechsmal höhere Wahrscheinlichkeit besteht, erneut angegriffen zu werden.

Erwartete Neuigkeiten

- API-Angriffe auf die Geschäftslogik der API sind schwer zu erkennen und abzuwehren. Daher ist es schwierig, sie in individuellen Anfragen zu bestimmen.
- Unternehmen müssen die Einhaltung der neuen PCI DSS v4.0-Anforderungen (Payment Card Industry Data Security Standard) und des Digital Operational Resilience Act (DORA) sicherstellen.

> Diese Einblicke sind großartige Richtlinien, die Ihnen helfen, Ihr Sicherheitsprogramm für den Ernstfall zu rüsten, und herauszufinden, wo Sie redundante Tools oder Lücken haben.
>
> **– Steve Winterfeld, Advisory CISO, Akamai**

Dinge, die sich wohl nie ändern

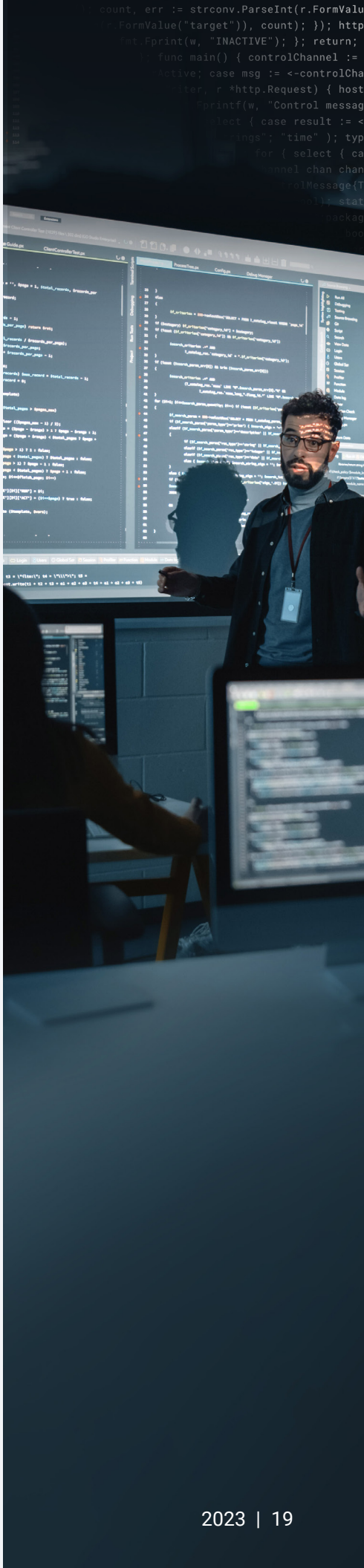
- Die Anzahl der Bots und API-Angriffe nimmt weiter zu, und es werden momentan neue Rekorde für DDoS-Angriffe gesetzt.
- Die am meisten angegriffenen Branchen sind in der Regel Finanzdienstleistungen, Hightech und Handel.
- Local File Inclusion (LFI) ist die am häufigsten genutzte Angriffstechnik.
- Die Region mit den meisten DDoS-Angriffen hat sich zunehmend von Nordamerika nach Europa verlagert.

Eine entscheidende Erkenntnis, die mich erstaunte, waren die validierten Indicators of Compromise aus der CnC-Kommunikation. Besonders beunruhigend war die hohe Häufigkeit der Ersterkennung, nachdem Malware bereits erfolgreich Systeme kompromittiert und die Kommunikation aufgebaut hatte. Dies unterstreicht das kritische Gleichgewicht zwischen vorbeugenden Maßnahmen und rascher Erkennung, um die Auswirkungen zu minimieren.

Die Geschichte, die mich am meisten überraschte, war der Wandel von Angriffen auf Menschen über Social Engineering hin zu Zero-Day-Angriffen. In den letzten Jahren hatte ich das Gefühl, dass unsere technischen Abwehrmaßnahmen stärker wurden und dass ich die Mitarbeiter durch Schulungen und Überwachung stärken musste. Aber nach der diesjährigen Umstellung auf Zero-Day-Angriffe muss ich mir genau überlegen, wo ich im nächsten Jahr Ressourcen einsetze.

Die Angriffe, die am unfairsten erscheinen, passieren, während Ihr Unternehmen bereits mit einem Ransomware-Angriff zu tun hat oder sich von diesem erholt. Es ist leicht, sich auf die Krise zu konzentrieren und Ressourcen aus der laufenden defensiven Überwachung zu ziehen. Diese Forschung war eine machtvolle Erinnerung, dass Sie es sich NICHT leisten können, Ihre Verteidigung zu vernachlässigen!

Diese Einblicke sind großartige Richtlinien, die Ihnen helfen, Ihr Sicherheitsprogramm für den Ernstfall zu rüsten, und herauszufinden, wo Sie redundante Tools oder Lücken haben. Sie können Übungen vorantreiben, Playbooks oder Prozesse zu aktualisieren, Penetrationstestpläne zu verbessern und Risikoportfolioprüfungen zu unterstützen. Cybersicherheit ist ein Teamsport, daher sind diese Erkenntnisse auch nützlich, um Gespräche mit internen Partnern (z. B. Ihren Rechts- oder IT-Teams) und Anbietern anzuregen. Wie immer sind Referenzen/Tools wie das National Institute of Standards and Technology (NIST), die MITRE ATT&CK-Wissensdatenbank und die OWASP Top 10 großartige Ressourcen.



Ausblick

Es ist unmöglich, die Zukunft vorherzusagen, aber wir können davon ausgehen, dass DDoS- und API-Angriffe 2024 dominieren werden. Die fortgesetzten Bemühungen, größere Botnet-Armeen aufzubauen und neue Techniken zu entwickeln, werden zusammen mit dem Einfluss der Nationalstaaten dazu führen, dass DDoS zunimmt. Dieser Faktor wird zusammen mit der Entwicklung der Ransomware die Entstehung von Rechtsvorschriften und Resilienz sein.

Die Transformation ist in den meisten Branchen nach wie vor die treibende Kraft für die Implementierung von APIs. Dieses schnelle Wachstum führt unbeabsichtigt zu größeren Angriffsflächen und mehr Schwachstellen, Shadow-APIs, Zombie-APIs und API-Missbrauch. Wir erwarten ein deutliches Wachstum bei Angriffen auf Webanwendungen und APIs. Dies wird sowohl durch Standardangriffe wie LFI als auch durch neue Techniken wie Server-Side Request Forgery (SSRF) und Server-Side Template Injections (SSTI) verursacht, die Tools erfordern, die laterale Bewegungen erkennen und Auswirkungen abmildern können.

Abgesehen von einigen branchen- und regionsspezifischen Trends erwarten wir schließlich einen allgemeinen Mangel an qualifizierten Cybersicherheitsexperten. Die Bereiche maschinelles Lernen und künstliche Intelligenz für Large Language Models (LLMs) werden etwas entlastet, aber insgesamt wird es äußerst schwierig sein, die benötigten Talente zu finden und zu halten. Dies führt zu Partnerschaften mit Anbietern für On-Demand-Mitarbeiter oder Managed Services bei nicht wesentlichen Funktionen.

Was das Akamai SIG anbelangt, so werden wir weiterhin Alarm schlagen, wenn es um weit verbreitete Bedrohungen und sich abzeichnende Sicherheitsrisiken geht. Wir werden über unsere Plattformen und Kanäle mit der Sicherheits-Community zusammenarbeiten, um die Bemühungen um Bedrohungsinformationen zu unterstützen. Außerdem feiern wir im Jahr 2024 den 10. Jahrestag unserer SOTI-Berichte! Wir freuen uns darauf, unsere Berichte weiter zu verbessern, indem wir neue Datensätze, visuelle Hilfsmittel und wichtige Erkenntnisse einführen, die Sicherheitsexperten bei ihrem Bestreben unterstützen, ihre Unternehmen zu schützen.

Wir freuen uns darauf, im nächsten Jahr weitere Erkenntnisse aus der Forschung weiterzugeben. Achten Sie in der Zwischenzeit auf Ihre Sicherheit!

Mitwirkende

Redaktion und Text

Roger Barranco
Tricia Howard
Charlotte Pelliccia
Lance Rhodes
Badette Tribbey
Chelsea Tuttle
Steve Winterfeld

Prüfung und Fachleute

Kimberly Gomez
Reuben Koh
Emily Lyons
Richard Meeus
Carley Thornell

Datenanalyse

Chelsea Tuttle

Marketing und Veröffentlichung

Georgina Morales Hampe
Emily Spinks

Weitere „State of the Internet“-Sicherheitsberichte

Lesen Sie vorherige Ausgaben und informieren Sie sich über bevorstehende Veröffentlichungen der renommierten „State of the Internet“-Sicherheitsberichte von Akamai. **akamai.com/soti**

Weitere Informationen zur Bedrohungsforschung von Akamai

Halten Sie sich unter diesem Link zu neuesten Threat-Intelligence-Analysen, Sicherheitsberichten und Cybersicherheitsforschung auf dem Laufenden: **akamai.com/security-research**

Greifen Sie auf Daten aus diesem Bericht zu

Sehen Sie sich die hochauflösenden Versionen der Diagramme und Grafiken an, auf die in diesem Bericht verwiesen wird. Diese Bilder können kostenlos verwendet und referenziert werden, vorausgesetzt, Akamai wird ordnungsgemäß als Quelle genannt und das Akamai-Logo wird beibehalten.
akamai.com/sotidata

Weitere Informationen zu Akamai-Lösungen

Weitere Informationen zu Akamai-Lösungen zur Bedrohungsabwehr finden Sie auf unserer Seite zu **Sicherheitslösungen**.