WHITEPAPER

Durchbrechen der Ransomware-Kill-Chain mit der Akamai Enterprise Security Suite

Inhaltsverzeichnis

Einführung

Bekämpfen Sie Ransomware in verschiedenen Phasen der Kill Chain mit den Enterprise Security Solutions von Akamai

Eine der größten Sicherheitsbedrohungen, mit denen Unternehmen heute konfrontiert sind, ist Ransomware: eine Form von Malware, die wichtige Dateien auf einem Gerät verschlüsselt und unbrauchbar macht. Die Malware-Betreiber fordern dann ein Lösegeld für einen Entschlüsselungscode oder eine Software, mit der die Dateien auf ihre ursprünglichen Daten zurückgesetzt werden können. In den letzten Jahren haben kriminelle Ransomware-Banden ihre Taktik weiterentwickelt und damit begonnen, Daten ihrer Opfer zu extrahieren, um ein zusätzliches Druckmittel zu erhalten. Sie drohen dann damit, die Daten öffentlich zu verbreiten oder im Dark Web zu verkaufen.

Um sich gegen diese Art von Angriff verteidigen zu können, müssen die Verteidiger verstehen, wie Ransomware-Gruppen vorgehen. Dieses Whitepaper wird Ihnen dabei helfen.

Die Kill Chain von Ransomware verstehen

Ransomware-Angriffe sind komplex, und der Einbruch in das System ist erst der Anfang. Um den Schaden zu maximieren, müssen die Angreifer noch ihre schädliche Payload im Netzwerk verteilen. Dann können sie mit der Verschlüsselung beginnen. Wenn nur ein einzelner Rechner verschlüsselt wird, ist das Druckmittel nicht stark genug, um Lösegeld zu verlangen. Damit der Ransomware-Angriff erfolgreich ist, muss der Angreifer verschiedene Schritte ausführen. So muss er Netzwerkressourcen ermitteln, sich lateral im Netzwerk bewegen usw. Diese Schritte werden oft als die Kill Chain von Ransomware bezeichnet.

Jeder Schritt in dieser Kette eröffnet viele Chancen zur Erkennung und Abwehr. Mit der Akamai Enterprise Security Suite können Sie Ihr Netzwerk rechtzeitig vorbereiten und Ihre Angriffsfläche reduzieren. So lassen sich mögliche Schäden durch Ransomware minimieren und eindämmen, bevor Sie überhaupt wissen, dass Sie betroffen sind. In diesem Whitepaper erfahren Sie, wie Sie Akamai Guardicore Segmentation, Enterprise Application Access und Secure Internet Access nutzen können, um Ransomware-Aktivitäten in den verschiedenen Stadien der Kill Chain zu erkennen und zu blockieren:

Erstzugang

Die erste Phase des Angriffs, in der Angreifer von außen in das interne Netzwerk eindringen

Erkundung

Methoden, die Angreifer verwenden, um wichtige Assets innerhalb des Netzwerks zu identifizieren

Laterale Bewegung

Die Phase, in der sich Angreifer im Netzwerk ausbreiten und weitere Assets infizieren

Command and Control

Die verschiedenen Arten, wie Angreifer einen Kommunikationskanal ins Netzwerk unterhalten, um Informationen und Befehle an kompromittierte Assets zu senden

Extraktion

Methoden, die von Angreifern verwendet werden, um gestohlene vertrauliche Daten unbemerkt zu extrahieren

Erstzugang

Jedes Unternehmen verfügt über zahlreiche Schnittstellen zum Internet. Angreifer missbrauchen diese Schnittstellen, um Zugriff auf das Netzwerk zu erhalten. Mit Akamai können Sie die Schnittstellen lückenlos schützen und Angreifer von Ihrem Netzwerk fernhalten.

Server mit Internetzugriff schützen

> Nutzen Sie die Funktionen von Secure Internet Access für eine Payload-Analyse, um Server mit Internetzugriff zu schützen

Am häufigsten erlangen Angreifer laut Kaspersky Lab einen ersten Zugang zum System, indem sie Schwachstellen von Anwendungen mit Internetzugang attackieren. Oft nutzen sie dabei One-Day-Sicherheitslücken auf nicht gepatchten Systemen aus. Schwachstellen wie Log4Shell (CVE-2021-44228) und ProxyLogon (CVE-2021-26855) werden da draußen heute noch ausgenutzt, um Netzwerke zu infiltrieren und Ransomware zu verbreiten.

Enterprise Threat Protector kann so konfiguriert werden, dass der gesamte eingehende Webtraffic zu Ihren internetbasierten Servern überwacht wird. Dieser Traffic wird analysiert, und schädliche oder ungewöhnliche Aktivitäten können identifiziert und blockiert werden.

Phishing-URLs blockieren

> Verwenden Sie die URL-Prüffunktionen von Enterprise Threat Protector, um Phishing-Versuche zu erkennen und zu blockieren

Phishing ist eine sehr häufig angewandte Methode, in Netzwerke einzudringen. Angreifer senden häufig E-Mails mit Links zu schädlichen Anhängen oder gefälschten Anmeldeseiten, die dazu dienen, Anmeldedaten zu stehlen. Mit dem Enterprise Threat Protector Client auf Ihren Endgeräten können Sie jede der URLs, auf die Ihre Nutzer klicken, in Echtzeit scannen, schädliche oder anomale Links identifizieren und blockieren.

VPN-Angriffsfläche verringern

Verwenden Sie Enterprise Application Access, um einen sicheren, anwendungsspezifischen VPN-Zugriff zu ermöglichen und die Angriffsfläche für Attacken von außen zu reduzieren

In der heutigen hybriden Arbeitsumgebung, die oft Remotearbeit einschließt, können Nutzer sich immer häufiger über ein VPN im Unternehmensnetzwerk anmelden. Angreifer haben sich darauf eingestellt und nutzen diese Möglichkeit, um Zugriff auf das interne Netzwerk zu erlangen. Die Kriminellen attackieren häufig die PCs von Mitarbeitern und nutzen deren VPN-Anmeldedaten, um auf das interne Netzwerk zuzugreifen. Manchmal nehmen die Angreifer auch anfällige Server ins Visier, um Anmeldedaten abzugreifen. Im November 2022 nutzten Angreifer eine Sicherheitslücke bei Fortinet VPN-Servern aus, um einen ersten Zugang ins System zu erlangen. Anschließend verbreiteten sie Ransomware im gesamten Netzwerk.

Mit Enterprise Application Access können Sie dieses Risiko erheblich reduzieren, indem Sie einen anwendungsspezifischen, rollenbasierten Zugriff auf Ihr Netzwerk zulassen. Anders als bei herkömmlichen VPNs erhalten Nutzer nicht den vollen Zugriff auf das gesamte Netzwerk, sondern nur begrenzten Zugriff auf bestimmte Anwendungen. Selbst wenn ein Angreifer die Anmeldedaten des Nutzers missbrauchen und den MFA-Schutz umgehen sollte, erhält er trotzdem keinen Zugriff auf das Netzwerk, sondern nur auf eine begrenzte Anzahl von Anwendungen.

Command and Control

C2-Server (Command and Control) blockieren

Verwenden Sie Akamai Secure Internet Access, um bekannte Command-and-Control-Server der Malware zu blockieren

Malware im Allgemeinen und Ransomware im Besonderen erfordern die Kommunikation mit externen C2-Servern, um Befehle zu senden und Informationen von infizierten Assets abzurufen. Durch die Analyse der umfangreichen Kommunikationsdaten von Akamai sind wir in der Lage, Ransomware- und Malware-C2-Domains zu überwachen und neue und sich weiterentwickelnde Kampagnen zu verfolgen. Mit dem Enterprise Threat Protector Client können wir Ihre gesamte DNS-Kommunikation in Echtzeit überwachen und die Kommunikation mit schädlichen Domains blockieren. So lässt sich verhindern, dass die Malware erfolgreich ausgeführt wird.

Erkundung

Sobald Angreifer in das Netzwerk eingedrungen sind, versuchen sie, weitere Assets zu identifizieren, um die Netzwerkstruktur zu verstehen und sich dann lateral im Netzwerk zu bewegen. Dies führt häufig zu interner Kommunikation, die von Akamai Guardicore Segmentation erkannt werden kann.

Netzwerk-Scans identifizieren

> Verwenden Sie Akamai Guardicore Segmentation-Detektoren, um verdächtige Netzwerk-Scans zu identifizieren

Eine der häufigsten Methoden, die Angreifer für die Netzwerkerkundung verwenden, sind Port-Scans zur Identifizierung von Netzwerkdiensten. Viele Ransomware-Gruppen setzen Open-Source-Netzwerkscanner ein. Ein aktueller CISA-Bericht zur Ransomware LockBit 3.0 zeigt, dass die Gruppe den „SoftPerfect Network Scanner“ verwendet, um Port-Scans durchzuführen. Ein weiteres Beispiel ist die Ransomware-Gruppe Nokoyawa, die Netzwerke nach SQL-Servern scannt, um Zugriff auf dort liegende sensible Daten zu erhalten.

Akamai Guardicore Segmentation überwacht die gesamte Kommunikation in Ihrem Netzwerk und verfügt über integrierte Detektoren, die solche Scans erkennen und Sie benachrichtigen. So können Sie die Verbreitung der Malware stoppen, bevor sie beginnt.

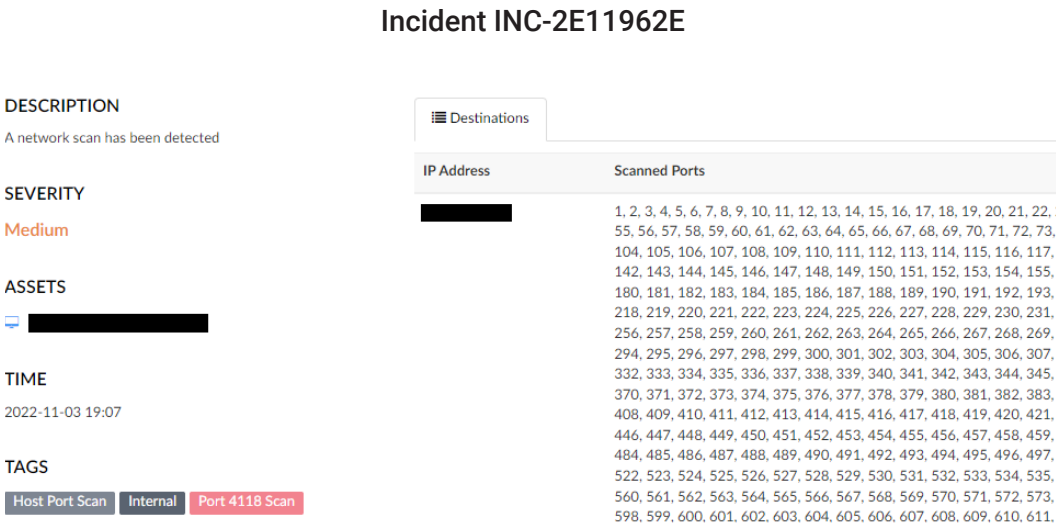
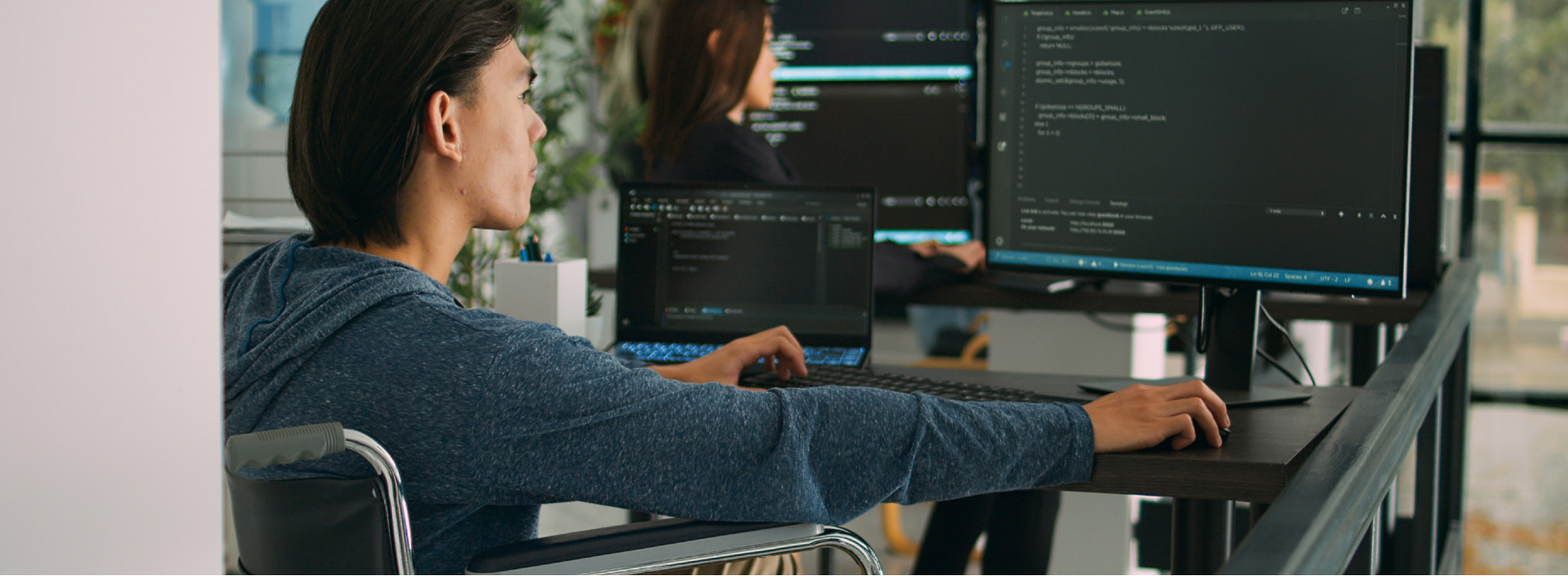


Abb. 1: Netzwerk-Scan-Vorfälle in Akamai Guardicore Segmentation



Täuschungsstrategie gegen Erkundung

Verwenden Sie Akamai Guardicore Segmentation, um Erkundungsversuche zu identifizieren

Wenn Angreifer in ein Netzwerk eindringen, haben sie keine Vorkenntnisse über dessen Struktur und die verschiedenen darin vorhandenen Assets. Um diese Wissenslücke zu schließen, müssen sie „im Dunkeln" sondieren und versuchen, ihren Weg manuell zu finden. Mit Akamai Guardicore Segmentation können Sie sich diesen Umstand zunutze machen, indem Sie den Täuschungsservice nutzen. Er lockt Angreifer in Honeypot-Server und überwacht ihre Aktivitäten. Sobald Anomalien erkannt werden, erhalten Sie eine Benachrichtigung.

Ein Angreifer dringt beispielsweise in das Netzwerk ein und versucht, mit einer Brute-Force-Strategie an die SSH-Anmeldedaten eines Linux-Servers zu kommen. Akamai Guardicore Segmentation identifiziert diese Anomalie und leitet den Angreifer an einen dynamisch generierten Honeypot weiter. Sobald sich der Angreifer im Inneren des Honeypot befindet, werden all seine Aktionen protokolliert, und eine Warnung wird erzeugt.

Im Folgenden finden Sie ein Beispiel für eine solche Warnung:

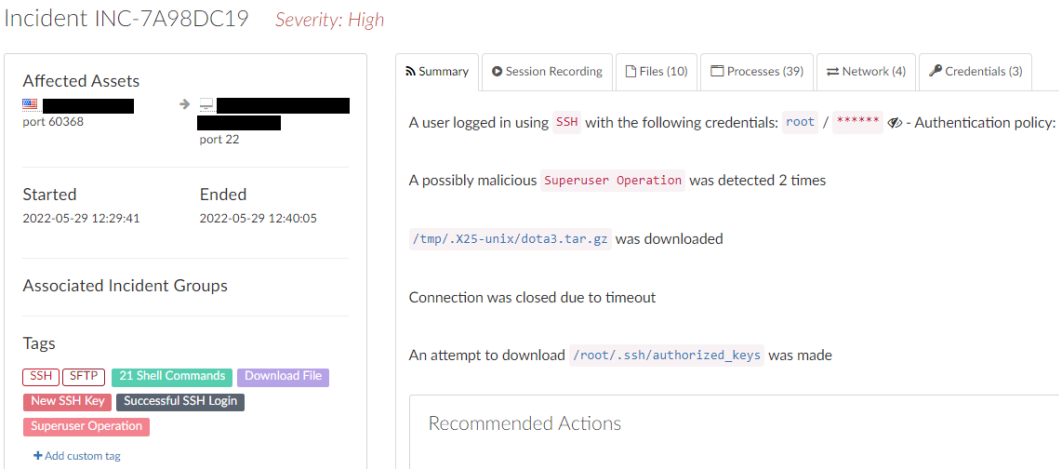


Abb. 2: Täuschungsvorfall in Akamai Guardicore Segmentation

Laterale Netzwerkbewegungen

Nachdem ein Angreifer Zugriff auf das Netzwerk und Kenntnis seiner Topologie erlangt hat, wird er dies nutzen, um sich lateral im Netzwerk zu bewegen. Moderne Ransomware-Gruppen dringen in ein Netzwerk ein und bewegen sich dann lateral, um so viele Assets wie möglich zu infizieren und zu verschlüsseln. Mit den Enterprise-Security-Produkten von Akamai können Sie die Möglichkeiten der lateralen Bewegung einschränken und das Ausmaß des Angriffs minimieren.

Verdächtige Host-Indikatoren identifizieren

> Verwenden Sie das Modul Akamai Guardicore Segmentation Insight, um verdächtige Host-Indikatoren auf verschiedene Weisen zu identifizieren

Angreifer verwenden PowerShell-Tools, um unterschiedliche Ziele zu erreichen. Eines davon ist die laterale Bewegung. PowerShell-Dropper sind sehr verbreitet. Angreifer verwenden sie oft als ersten Code, den sie auf einem kompromittierten Asset ausführen. In letzter Zeit beobachtete Infektionen durch die Ransomware Quantum zeigten genau das: PowerShell-Code, der über WMI (Windows Management Instrumentation) ausgeführt wurde.

Mit dem Insight-Modul von Akamai Guardicore Segmentation können Sie geplante Abfragen ausführen, um das PowerShell-Ereignisprotokoll auf all Ihren Assets zu untersuchen, Assets mit schädlichen Indikatoren zu kennzeichnen und diese in Quarantäne zu stellen.

Abb. 3: Erstellen einer geplanten Insight-Abfrage zur Erkennung schädlicher PowerShell

Doch PowerShell ist nur ein Beispiel. Insight kann genutzt werden, um eine Vielzahl von lateralen Bewegungsindikatoren zu untersuchen. Dazu wird eine der vorhandenen OSQuery-Tabellen verwendet. Zum Beispiel:

- Verwenden Sie die Tabelle File, um Malware-Dateien anhand von Namen oder Hashes zu erkennen
- Verwenden Sie die Tabelle Startup Items, um verdächtige Einträge für Autorun-Eingaben in Ihren Assets zu erkennen
- Verwenden Sie die Tabelle Yara, um Dateien auf Ihren Assets mithilfe von YARA-Regeln zu untersuchen und Malware-Bedrohungen zu erkennen

LAN-Angriffe blockieren

> Verwenden Sie Akamai Guardicore Segmentation, um Angriffe auf lokale Netzwerkprotokolle zu blockieren und zu erkennen

Nachdem Angreifer ein erstes Asset im Netzwerk infiltriert haben, missbrauchen sie Schwachstellen in LAN-Protokollen wie ARP, um weitere Ressourcen zu kompromittieren. Mit einer herkömmlichen Firewall können diese Angriffe leicht unentdeckt bleiben, da sie in Layer 2 ausgeführt werden. Diese Art der Kommunikation erreicht die Firewall nicht.

Der softwarebasierte Ansatz von Akamai Guardicore Segmentation ermöglicht es Ihnen, den gesamten Traffic zu überwachen und zu blockieren, der in ein Asset hineingeht bzw. herauskommt. Das gilt selbst für den lokalen Traffic, der normalerweise die regulierende Firewall nicht erreicht.

Verwaltungsports beschränken

> Verwenden Sie Akamai Guardicore Segmentation, um Richtlinien auf Prozessebene zu erstellen und dadurch die Angriffsfläche für Attacken über sensible Ports zu reduzieren

Sobald sich die Angreifer im Netzwerk befinden, führen sie in der Regel eine Berechtigungseskalation für kompromittierte Assets durch, um Anmeldedaten zu stehlen. Haben die Angreifer die Anmeldedaten, verwenden sie häufig Verwaltungsprotokolle wie RDP, RPC, SMB und WinRM, um auf allen Assets im Netzwerk eine Ransomware-Payload auszuführen. Das vollständige Blockieren dieser Ports ist jedoch oft keine praktikable Option, da Administratoren sie für den regulären Betrieb benötigen.

Mit Akamai Guardicore Segmentation können Sie Richtlinien auf Prozessebene anwenden und bestimmen, welche Prozesse über sensible Verwaltungs-Ports kommunizieren sollen. Sehen wir uns nun einmal WinRM an. Es wird von vielen Verwaltungsprogrammen verwendet, unter anderem von Ansible. Häufig wird es jedoch auch von Angreifern missbraucht, die Tools wie Evil-WinRM verwenden, um laterale Bewegungen im Netzwerk durchzuführen. Mithilfe von Akamai Guardicore Segmentation können wir eine Richtlinie erstellen, die eingehende WinRM-Verbindungen nur von Ansible-Prozessen zulässt und andere Prozesse über denselben Port blockiert:

Section	Source	Destination	Ports/Protocols	Action
Allow	ansible-operator	Windows Any	5985 TCP | UDP	Allow
Block	Any	Windows Any	5985 TCP | UDP	Block

Abb. 4: Beispiel für die Akamai Guardicore Segmentation-Richtlinie zur Einschränkung der WinRM-Kommunikation

Extraktion

In den letzten Jahren haben Angreifer ihre Erpressungstaktiken angepasst und damit begonnen, vertrauliche Dateien ihrer Opfer zu verbreiten und als zusätzliches Druckmittel zu benutzen. Angreifer versuchen, sich im Netzwerkrauschen zu verbergen, während sie die Daten aus dem Unternehmen extrahieren. In dieser Phase können sie jedoch oft noch erkannt und blockiert werden.

Extraktionsdomains blockieren

> Verwenden Sie Akamai Guardicore Segmentation, um den Zugriff auf Services zu beschränken, die für die Datenextraktion missbraucht werden können

Angreifer verwenden häufig öffentliche Tools, um Daten aus dem Netzwerk zu verbreiten. Eine sehr häufige Option sind öffentliche Hosting-Dienste wie MEGA, Dropbox und Google Drive. Die Herausforderung bei der Überwachung dieser Domains besteht darin, dass sie üblicherweise rechtmäßig innerhalb des Netzwerks verwendet werden. Beispielsweise kann der Zugriff auf die MEGA-Domain über einen Browser als legitim angesehen werden. Dagegen würde der Zugriff mithilfe des Dienstprogramms rclone, das von mehreren Angriffsgruppen aktiv für die Datenextraktion genutzt wird, als schädlich eingestuft.

Mit Akamai Guardicore Segmentation können wir das mit solchen Tools verbundene Risiko minimieren, indem wir ihre Domains von allen Endpunkten aus blockieren, die keinen Zugriff auf sie benötigen, und den Zugriff nur über genehmigte Anwendungen wie Browser zulassen.

Mehrschichtige Verteidigung

Um ihr Ziel zu erreichen, müssen Angreifer verschiedene Angriffsphasen durchlaufen. Jede Phase bietet Verteidigern die Möglichkeit, die damit verbundenen schädlichen Aktivitäten zu blockieren und zu erkennen. Mit den verschiedenen Sicherheitsprodukten von Akamai können Verteidiger in jedem Stadium einer Ransomware-Kill-Chain Abwehrmaßnahmen ergreifen, um Angreifer zu stoppen und ungewöhnliches Verhalten zu erkennen.

Weitere Informationen über Akamai Guardicore Segmentation oder eine personalisierte Produktdemo erhalten Sie unter akamai.com/guardicore

Akamai schützt Ihr Kundenerlebnis, Ihre Mitarbeiter, Systeme und Daten und integriert Sicherheit in alle von Ihnen erstellten Inhalte – überall dort, wo Sie sie erstellen und bereitstellen. Dank der Einblicke unserer Plattform in globale Bedrohungen können Sie Ihre Sicherheitsstrategie anpassen und weiterentwickeln, um Zero Trust zu implementieren, Ransomware zu stoppen, Anwendungen und APIs zu schützen oder DDoS-Angriffe abzuwehren. Das gibt Ihnen das nötige Vertrauen, um kontinuierlich Innovationen zu entwickeln, zu expandieren und alles zu transformieren, was möglich ist. Möchten Sie mehr über die Sicherheits-, Computing- und Bereitstellungslösungen von Akamai erfahren? Dann besuchen Sie uns unter akamai.com und akamai.com/blog oder folgen Sie Akamai Technologies auf Twitter und LinkedIn. Veröffentlicht: 09/23.