Akamai

E-BOOK

Das Überwinden von Bereitstellungshindernissen zum Schutz von Systemen in der Energie-, Öl- und Gasindustrie

Bericht zum allgemeinen Zustand der Segmentierung

Inhaltsverzeichnis

Einführung

IT- und OT-Sicherheitsabteilungen stehen schon immer vor erheblichen Herausforderungen. Doch im Energie-, Öl- und Gassektor sowie im Versorgungssektor im Allgemeinen ist der Druck noch stärker, da Versorgungsunternehmen für die Bevölkerung kritisch sind. Häufig verschärfen regionale Konflikte, politischer Druck und ideologische Auseinandersetzungen die Schwierigkeiten und die Gefahren, mit denen diese Branche konfrontiert ist. Da Angreifer jedoch immer raffinierter werden und Techniken kombinieren, um größere und häufigere Bedrohungen zu schaffen, stehen die Sicherheitsteams von Energieunternehmen unter einem nie dagewesenen Druck. Ohne online verbundene Systeme – oder Systeme, die mit ihren privaten OT-Netzwerken verbunden sind – wird der Betrieb für Energieunternehmen unmöglich, und ein einziger erfolgreicher Angriff kann zu erheblichen Schäden an Reputation und finanzieller Performance des Unternehmens führen.

Die Ergebnisse dieses Berichts deuten darauf hin, dass die Auswirkungen dieser Angriffe zunehmen. Und damit steigt auch die Belastung für Sicherheitsverantwortliche, geeignete Lösungen auszuwählen, die die Sicherheit der gesamten Umgebung gewährleisten und gleichzeitig die Performance erhalten.

Im Gegensatz dazu formulieren Regulierungsbehörden und Regierungen weltweit derzeit Sicherheitsrichtlinien und -vorschriften, um auf die erhebliche Zunahme der Cyberbedrohungen in diesem Sektor und auf die kritische Natur der von ihm angebotenen Dienste zu reagieren. Energieunternehmen sind verpflichtet, sich an regulatorische Standards zu halten und die Aufrechterhaltung und Sicherheit ihrer Dienstleistungen zu gewährleisten.

Die Befragten in Energieunternehmen (aus allen Regionen, einschließlich USA, LATAM, EMEA und APAC) sind sich mit überwältigender Mehrheit einig, dass Segmentierung Assets effektiv schützt.
Der Fortschritt bei ihrer Umsetzung für kritische Geschäftsanwendungen und Assets ist unter den Teilnehmern jedoch geringer als erwartet. Das Haupthindernis für Energieunternehmen sind zunehmende Performanceengpässe. Das deutet darauf hin, dass Teams möglicherweise zögern, ein Projekt zu starten, bei dem sie sich nicht absolut sicher sind, dass es nicht die Performance beeinträchtigen wird. Hierbei ist zu bedenken, dass angesichts der Kritikalität der Dienstleistungen, die diese Organisationen für die Öffentlichkeit erbringen, Unterbrechungen der Lösungen zu Schäden bei Kunden führen oder die Sicherheit des Wartungspersonals gefährden können.

Umgekehrt wird erwartet, dass der Energiesektor der Segmentierung einen größeren Stellenwert einräumt als die meisten anderen Branchen, was darauf hindeutet, dass ihr Wert zweifellos anerkannt wird.

Segmentierung hat sich insgesamt langsam entwickelt, aber diejenigen, die durchgehalten haben, haben ihr Risiko enorm reduziert

Segmentierung ist gut. Mikrosegmentierung ist besser.

Segmentierung ist ein Architekturansatz, bei dem ein Netzwerk in kleinere Segmente unterteilt wird, um Performance und Sicherheit zu verbessern.

Die Mikrosegmentierung ist eine Sicherheitstechnik, mit der Sie ein Netzwerk bis hin zur individuellen Workload-Ebene logisch in verschiedene Sicherheitssegmente unterteilen können. Sicherheitskontrollen und Servicebereitstellung können dann für jedes einzelne Segment definiert werden. Dieser präzise Sicherheitsansatz ermöglicht eine genauere Kontrolle über den Zugriff und den Schutz vertraulicher Daten. Durch die Implementierung von Mikrosegmentierung können Unternehmen die Auswirkungen einer Sicherheitsverletzung begrenzen und ihr Netzwerk besser vor hoch entwickelten Cyberbedrohungen schützen. Insgesamt bietet die Kombination aus Segmentierung und Mikrosegmentierung eine umfassende Sicherheitsstrategie, die für den Schutz kritischer Assets in der komplexen und dynamischen Bedrohungslandschaft von heute unerlässlich ist.

Ransomware-Angriffe und ihre Auswirkungen nehmen weiter zu

Die Zahl der (erfolgreichen und erfolglosen) Ransomware-Angriffe in Energieunternehmen ist in den letzten zwei Jahren deutlich gestiegen: von durchschnittlich 37 im Jahr 2021 auf 62 im Jahr 2023. Und es gibt keinen Grund zu der Annahme, dass sich dieses Wachstum kurzfristig nicht fortsetzen wird. Die Folgen können sich nachteilig auf die Bevölkerung und die Wirtschaft auswirken, z. B. durch Stromausfälle oder Schäden an der Infrastruktur, die zum Verlust der Glaubwürdigkeit des Unternehmens, zum Diebstahl von geschäftlichen und persönlichen Daten oder sogar zur Gefährdung von Menschenleben führen können. Angesichts der zunehmenden Häufigkeit und Schwere von Ransomware-Angriffen ist es für Energieunternehmen von entscheidender Bedeutung, ihre Systeme und Daten zu schützen. Andernfalls ist nicht nur das Unternehmen selbst gefährdet, sondern auch die Sicherheit von Personen und Gemeinden, die auf diese Dienste angewiesen sind. Da Ransomware-Angriffe immer raffinierter werden, ist es für Unternehmen unerlässlich, wachsam zu bleiben und proaktive Verteidigungsstrategien zu entwickeln, um den potenziellen Schaden und die Unterbrechung durch diese bösartigen Bedrohungen zu minimieren.

Durchschnittliche Anzahl der Ransomware-Angriffe in den letzten 12 Monaten nach Sektor

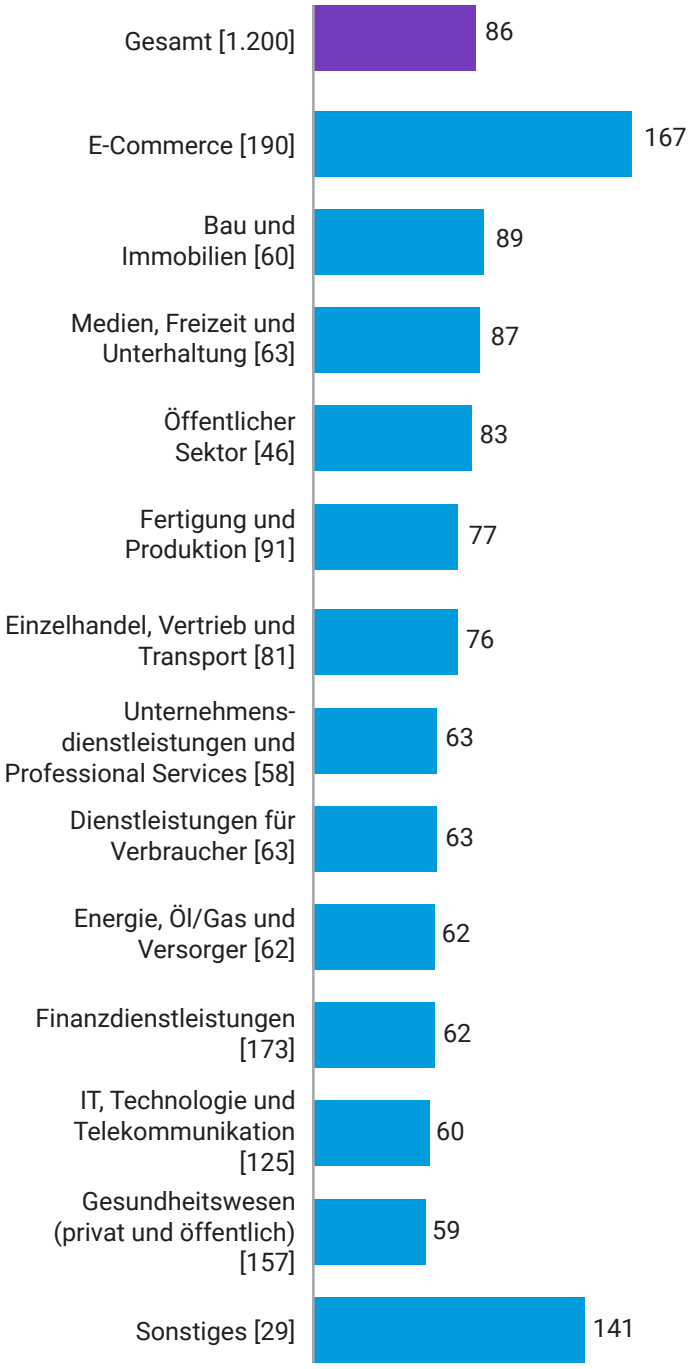

Abb. 1: Wie oft wurde Ihre Organisation in den letzten 12 Monaten von Ransomware angegriffen (unabhängig davon, ob die Angriffe erfolgreich waren oder nicht)? Das Diagramm zeigt die durchschnittliche Anzahl von Angriffen in den letzten 12 Monaten, aufgeschlüsselt nach Sektor.

Ein Grund für diese relativ geringe Anzahl von Angriffen ist, dass das wichtigste Asset eines Energieunternehmens eher physisch (Öl, Gas usw.) als digital (Finanz- oder Kundendaten) ist. Sie sind auch nicht als einfache Ziele bekannt, wie es bei einigen anderen Unternehmen mit relativ wenigen Vorschriften der Fall ist, wie z. B. bei Medien oder Einzelhandel. Das heißt, dass Angriffe in diesem Sektor eher auf politische Ziele als auf finanzielle Ziele ausgerichtet sein können. Und das wird durch die Tatsache unterstützt, dass branchenübergreifend nur 5 % der Befragten angeben, dass ihr Unternehmen nie einen Cyberangriff erlebt hat, während es im Energiesektor 24 % sind.

Ransomware-Angriffe im Energiesektor traten 2023 häufiger auf als 2021, aber die Schwere ihrer Auswirkungen ist unterschiedlich (Abbildung 2). Unsere Befragten gaben einen deutlichen Anstieg der Datenverluste an, aber einen Rückgang bei allen anderen Problemen. Dieser allgemeine Trend kann auf das wachsende Bewusstsein für den Wert von Daten zurückzuführen sein (die daher von Hackern als Ziel bevorzugt werden), aber auch auf Verbesserungen der Vorgehensweise im Energiesektor. Die Zahl der Energieunternehmen, die ihre Cybersicherheitsstrategien oder -richtlinien mindestens wöchentlich aktualisieren, stieg von nur 2 % im Jahr 2021 auf 23 % im Jahr 2023. Angesichts globaler Ereignisse (vor allem im Zusammenhang mit Konflikten oder Klimawandel), die die Länder dazu veranlassen, ihre Energiesicherheit genauer unter die Lupe zu nehmen, ist es keine Überraschung, dass Energieunternehmen ihre Cybersicherheitsstrategien stärker in den Mittelpunkt rücken.

Auswirkungen von Ransomware/ Cyberangriffen im Energiesektor

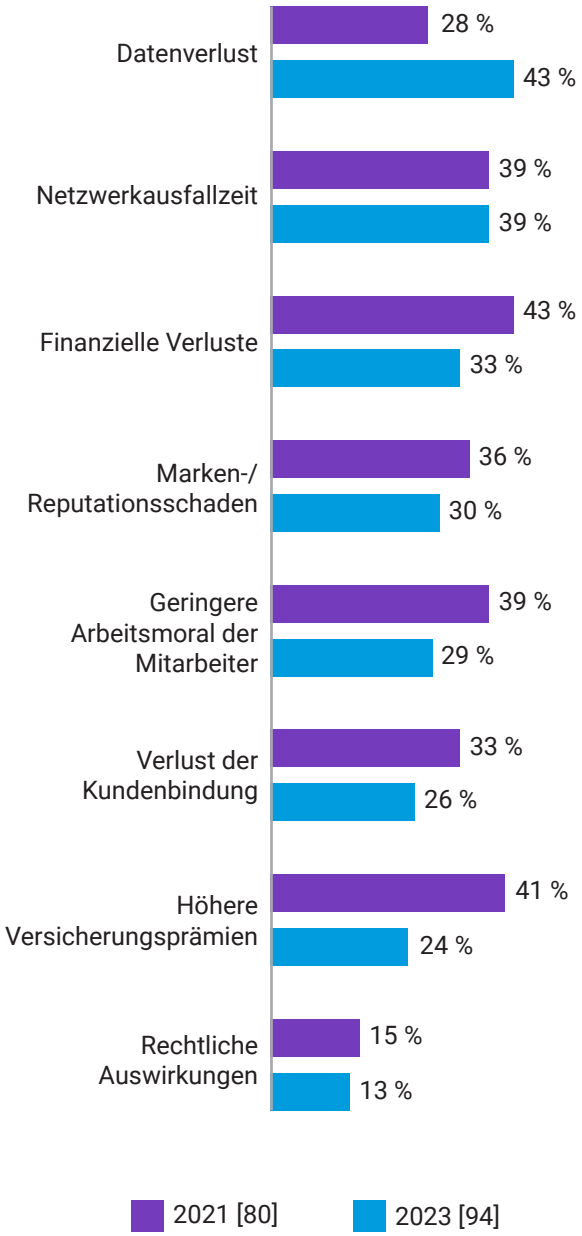

Abb. 2: Welche der folgenden Auswirkungen hatte es für Ihr Unternehmen, wenn es in der Vergangenheit Ransomware oder einen anderen Cyberangriff erkannt hat? Das Diagramm zeigt die Basisgrößen nach Jahr, nicht alle Antwortoptionen werden angezeigt; aufgeschlüsselt nach historischen Daten, nur Daten des Energiesektors.

Segmentierung ist allgemein als wichtiger Teil von Zero Trust anerkannt

Die Befragten aus dem Energiesektor sind sich einig, dass Segmentierung wichtig ist, um die Sicherheit des Unternehmens zu gewährleisten, insbesondere bei der Abwehr von Malware: 66 % (einer der höchsten Werte aller Sektoren) geben an, dass dies äußerst wichtig ist, und 95 % glauben, dass es entscheidend ist, um schädliche Angriffe abzuwehren.

Segmentierung trägt ebenfalls wesentlich zu einem Zero-Trust-Framework bei und die gute Nachricht für Energieunternehmen ist, dass in diesem Bereich bereits Fortschritte erzielt wurden. Alle (100 %) sind dabei, ein Zero-Trust-Sicherheitsframework zu implementieren, oder haben bereits ein solches Framework implementiert. Allerdings haben nur 46 % der befragten Unternehmen das Zero-Trust-Framework vollständig definiert und abgeschlossen. Dies ist daher ein Bereich, in dem Segmentierung Energieunternehmen auf ihrem Weg zu Zero Trust unterstützen kann. Dies ist das Ergebnis der Umfrage hinsichtlich der IT-Umgebungen von Unternehmen – in der OT-Umgebung kann es aufgrund der verwendeten Technologien anders aussehen.

Die Mehrheit der befragten Unternehmen im Energiesektor möchte noch weiter gehen und eine Mikrosegmentierung implementieren, die Anwendungs-Workloads auf präziserer Ebene schützt: 88 % geben an, Mikrosegmentierung habe mindestens eine hohe Priorität, und 47 % nennen sie als ihre oberste Priorität. In allen Sektoren geben nur 34 % der Befragten an, dass Mikrosegmentierung oberste Priorität hat. Das zeigt, dass Organisationen des Energiesektors im Durchschnitt stärker darauf drängen, dass dieser Ansatz so schnell wie möglich eingeführt wird. Darüber hinaus geben fast alle (98 %) IT- und Sicherheitsentscheider in diesem Sektor an, dass Mikrosegmentierung zumindest von einer Minderheit in ihrer Branche angenommen wurde, was unterstreicht, dass es sich um eine Lösung handelt, die weithin bekannt ist.

Implementierungen gehen langsam voran, doch Beharrlichkeit zahlt sich aus

Die harte Realität: Zwar gibt es eine breite Zustimmung für die These, dass Segmentierung der Schlüssel zur Abwehr von Angriffen ist. Doch die Wahrheit ist, dass die Implementierung von Segmentierungen langsamer vorankommt als erwartet. Nur 38 % der Unternehmen im Energiesektor haben 2023 mehr als zwei kritische Geschäftsbereiche segmentiert (gegenüber 30 % im Jahr 2021), und 33 % haben vor zwei oder mehr Jahren das letzte Netzwerksegmentierungsprojekt gestartet, was darauf hindeutet, dass die Bemühungen zum Stillstand gekommen sind.

Langsame Implementierungen lassen sich am deutlichsten durch die größten Hindernisse erklären, mit denen die Befragten konfrontiert sind: erhöhte Leistungsengpässe (49 %), Compliance-Anforderungen (43 %) und unternehmenseigene Geräte (41 %, Abbildung 3).

Hindernisse bei der Segmentierung des Netzwerks im Energiesektor

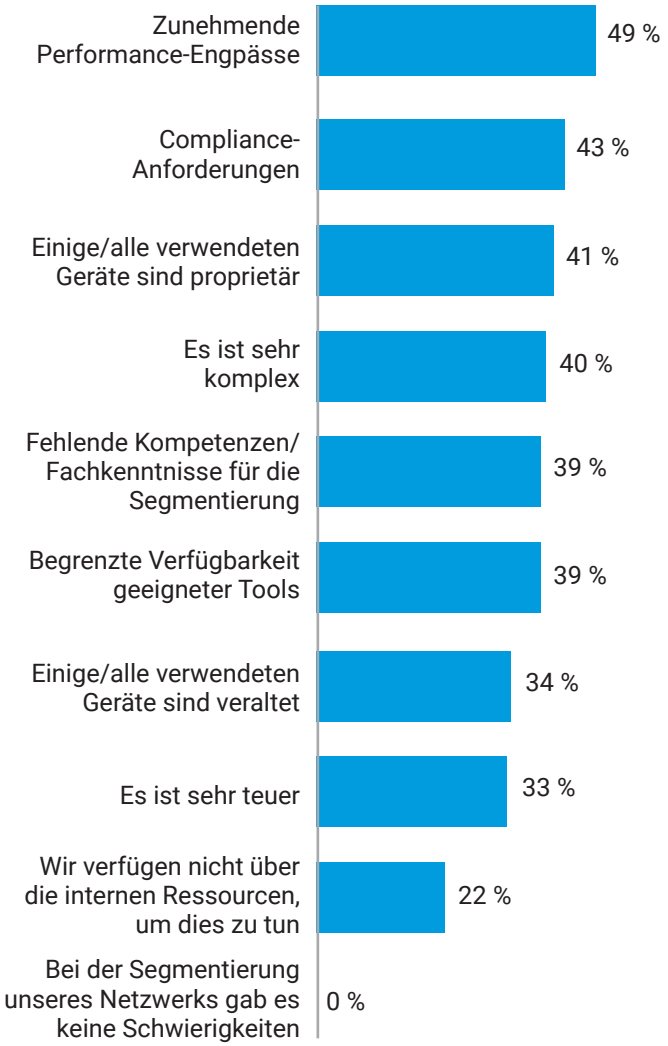

Abb. 3: Mit welchen Problemen war Ihr Unternehmen bei der Segmentierung des Netzwerks konfrontiert, bzw. mit welchen Problemen rechnen Sie? Das Diagramm zeigt die Basisgröße von 94; die Frage wurde nur denjenigen angezeigt, die ihr Netzwerk zu einem bestimmten Zeitpunkt segmentiert haben; nicht alle Antwortoptionen werden angezeigt, nur Daten des Energiesektors.

Ermutigend für den Energiesektor ist jedoch die Tatsache, dass 42 % der Befragten angaben, dass ihr Netzwerksegmentierungsprojekt auf eine Empfehlung der Unternehmensleitung/des Vorstands zurückging. Dies ist der höchste Wert aller Sektoren (der Gesamtdurchschnitt liegt bei 28 %) und zeigt, dass die Segmentierung in diesem Sektor eindeutig als wichtig angesehen wird.

Wie eine softwarebasierte Mikrosegmentierungslösung Herausforderungen meistert

Mikrosegmentierung ermöglicht nicht nur eine fortschrittlichere, detailliertere Segmentierung, sondern erleichtert auch die Implementierung.

Softwarebasierte Lösungen wie Akamai Guardicore Segmentation können schnell implementiert werden, ohne dass physische Änderungen am Netzwerk vorgenommen werden müssen. Sie müssen Ihren neuen Segmenten keine neuen IP-Adressen zuweisen oder sich Gedanken darüber machen, wo sich Ihre physischen Server und Geräte befinden könnten. Dies macht die Bereitstellung der Lösung wesentlich schneller und einfacher als infrastrukturbasierte Ansätze wie Firewalls und VLANs. Und da die Lösung einen eigenen proprietären Treiber für die Durchsetzung von Richtlinien verwendet, funktioniert sie nahtlos über alle Rechner und Betriebssysteme hinweg: von Bare-Metal-Servern bis hin zu Multicloud-Bereitstellungen, von Legacy-Technologien wie Windows Server 2003 bis hin zu den neuesten IoT/OT-Geräten und containerisierten Technologien. Das bedeutet, dass Sie nur eine Lösung mit einer einzigen Oberfläche verwalten müssen, um die von verschiedenen Betriebssystemen und Geräten in Ihrer gesamten Umgebung hergestellten Verbindungen anzuzeigen und zu verwalten – unabhängig von deren physischem Standort.

Es ist wichtig zu beachten, dass die Akamai Guardicore-Segmentierungslösung auch in OT-Umgebungen eingesetzt werden kann, sodass die Mikrosegmentierung auf private Kontrollnetzwerke, ältere Betriebssysteme und agentenlose IoT-Geräte angewendet werden kann.

Wie sie die Bereitstellung erleichtert

Die Mikrosegmentierung erzeugt zunächst eine interaktive Darstellung aller Verbindungen in Ihrer Umgebung, was eine wichtige Komponente zur Überwindung der wichtigsten Hindernisse für die Implementierung ist. Darüber hinaus hat Akamai in die Lösung Optionen zur aktiven Behebung von Performance-Engpässen und zum Umgang mit Compliance-Anforderungen integriert.

Performance-Engpässe entstehen nicht notwendigerweise infolge technischer Belastungen eines Systems, die durch eine Segmentierungslösung verursacht werden. Vielmehr können sie aus Personalengpässen resultieren, die auftreten, wenn Geschäftsbereiche manuell segmentiert und Probleme in diesen Bereichen dann manuell behoben werden müssen. Bei Akamai arbeiten wir daran, dieses Problem – und das Problem fehlender Expertise als größtes Hindernis für die Implementierung – zu lösen, indem wir die Notwenigkeit einer manuellen Segmentierung reduzieren und technischen Support sowie Professional Services auf höchstem Niveau anbieten. Unsere Segmentierungsexperten arbeiten während des gesamten Implementierungsprozesses mit Ihnen zusammen, um sicherzustellen, dass Sie die Segmentierungsziele in Ihrer speziellen IT- oder OT-Umgebung erreichen.

Unterstützung bei der Implementierung bietet auch die Lösung selbst: Die auf KI basierenden Richtlinienempfehlungen und vorkonfigurierten Richtlinienvorlagen für häufige Anwendungsfälle sparen Zeit und Klicks, vereinfachen den Workflow, verkürzen die Gesamtzeit bis zur Richtlinieneinführung und verhindern Fehlkonfigurationen aufgrund menschlicher Fehler. Für einen unserer Kunden konnten wir mit einem einzigen Techniker ein Projekt zur präzisen Segmentierung, für das eine Dauer von zwei Jahren und Gesamtkosten von einer Million US-Dollar veranschlagt waren, in nur sechs Wochen durchführen. Dadurch konnten die Gesamtkosten des Projekts um 85 % gesenkt werden. Das Beispiel macht deutlich, dass präzise Segmentierung schnell und einfach und ohne Belastung durch Engpässe implementiert werden kann.

So vereinfacht Mikrosegmentierung die Compliance

Viele unserer Kunden verwenden unsere Lösung, um die Einhaltung verschiedener nationaler und internationaler Compliance-Auflagen wie PCI-DSS, SWIFT, Sarbanes-Oxley, HIPAA, DSGVO oder LGPD zu gewährleisten und nachzuweisen. Diese Compliance-Auflagen verlangen in der Regel, dass die betreffenden Daten von anderen Systemen in Ihrer Umgebung getrennt werden. Während es kostspielig sein kann, dies mithilfe von Firewalls und VLANs zu erreichen, können Sie mit unserer softwarebasierten Lösung Segmente speziell für die bereichsinternen Daten erstellen. Außerdem können Sie durch Kommunikationsregeln steuern, was auf diese Daten zugreifen kann und was nicht. Mithilfe unserer visuellen Karte, die Ansichten nahezu in Echtzeit sowie Verlaufsansichten bietet, können Sie die Einhaltung dieser Auflagen nachweisen, indem Sie physisch aufzeigen, dass nur autorisierte Nutzer und Computer auf die betreffenden Daten zugreifen.

Mit der richtigen Lösung und dem richtigen Support verbessern Sie Ihre Sicherheitslage nachhaltig

Die Implementierung einer Segmentierung kann sehr schwierig sein. Doch dieser Bericht zeigt: Wer es schafft, sie effektiv umzusetzen, senkt sein Cyberrisiko erheblich. Eine ordnungsgemäße Segmentierung begrenzt die laterale Netzwerkbewegung von Bedrohungen und ermöglicht Ihnen, bei einem akuten Angriff schneller zu reagieren. Im Falle eines Verstoßes sind die Wiederherstellungsbemühungen sicher und kosten weniger Zeit, da sich die Auswirkungen nur auf das betroffene Segment beschränken sollten.

Wenn Sie sich für eine Lösung entscheiden, die die häufigsten Herausforderungen bei der Implementierung einer Segmentierung bewältigen soll, und wenn Sie dabei mit den zur Verfügung gestellten Experten zusammenarbeiten, sind Sie optimal aufgestellt, um Ihre Sicherheitslage grundlegend zu verbessern. Und je mehr Geschäftsbereiche Sie segmentieren, desto größere Fortschritte erzielen Sie auch für Ihre Zero-Trust-Architektur, denn Sie reduzieren Ihr gegenwärtiges Risiko und errichten eine erste Verteidigungslinie gegen künftige Bedrohungen.

Fazit

Segmentierung und Mikrosegmentierung sind im Energiesektor wichtiger als in vielen anderen Sektoren: IT-, IT-Sicherheits- und OT-Entscheidungsträger in Unternehmen des Energiesektors (66 %) geben mit größerer Wahrscheinlichkeit an, dass die Netzwerksegmentierung für die Sicherheit ihres Unternehmens äußerst wichtig ist, als Entscheider im Bereich der Verbraucherdienste (36 %), jedoch mit geringerer Wahrscheinlichkeit als Entscheider in IT und Technologie (73 %).

Im Energiesektor ist die Wahrscheinlichkeit, dass Mikrosegmentierung oberste Priorität hat, deutlich höher (47 %) als bei Verbraucherdiensten (12 %) und nur geringfügig niedriger als im öffentlichen Sektor (48 %).

Die Befragten aus dem Energiesektor gehören zu denjenigen, die am seltensten überhaupt nicht segmentiert haben: Es ist unwahrscheinlich, dass Befragte aus dem Energiesektor angeben, keine geschäftskritischen Anlagen segmentiert zu haben (4 %), obwohl dies immer noch wahrscheinlicher ist als in Baugewerbe, Verbraucherdiensten und Medien (alle 0 %), aber weniger wahrscheinlich als im öffentlichen Sektor (15 %).

Unternehmen im Energiesektor gehören zu denjenigen, die am ehesten Fortschritte bei der Segmentierung gemacht haben: In der Energiebranche ist die Wahrscheinlichkeit, dass mehr als zwei geschäftskritische Anlagen segmentiert wurden, nur geringfügig geringer (38 %) als im Einzelhandel (43 %) und weitaus größer als im Bereich der Verbraucherdienstleistungen (3 %).

Die Umfrageteilnehmer

Für die vollständige Studie haben wir 1.200 Entscheidungsträger im Bereich IT und Sicherheit in 10 Ländern befragt, um die Fortschritte zu messen, die Unternehmen bei der Sicherung ihrer Umgebungen erzielt haben. Dabei wurde der Schwerpunkt auf die Rolle der Segmentierung gelegt.

Es wurden Fragen zu IT-Sicherheitsansätzen, zu Segmentierungsstrategien und zu den Bedrohungen gestellt, denen die Unternehmen 2023 ausgesetzt waren. Diese Ergebnisse geben uns Einblicke in die Veränderung der Sicherheitsstrategien seit 2021 und in die Bereiche, in denen noch Fortschritte erzielt werden müssen.

Die Umfrage berücksichtigte Unternehmen aus den USA, Indien, Mexiko, Brasilien, dem Vereinigten Königreich, Frankreich, Deutschland, China, Japan und Australien. Die befragten Personen arbeiteten für Unternehmen mit mehr als 1.000 Mitarbeitern und repräsentierten unterschiedliche Branchen und Sektoren.

Hinweis: Diese Stichprobe unterschied sich geringfügig von der des Jahres 2021. Stichprobengröße: 2023: 1.200 ausgefüllte Umfragen, 2021: 1.000 ausgefüllte Umfragen. 2023 wurden auch Teilnehmer aus Australien, Japan und China befragt. Die Sektoren unterschieden sich leicht von 2021.

Für die Zwecke dieses Berichts haben wir die Antworten von 94 (2023) bzw. 80 (2021) befragten Unternehmen aus dem Energiesektor ausgewertet.

Weitere Informationen zu Akamai Guardicore Segmentation

Akamai unterstützt und schützt das digitale Leben. Führende Unternehmen weltweit setzen bei der Erstellung, Bereitstellung und beim Schutz ihrer digitalen Erlebnisse auf Akamai. So unterstützen wir täglich Milliarden von Menschen in ihrem Alltag, bei der Arbeit und in ihrer Freizeit. 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 Lösungen von Akamai erfahren? Dann besuchen Sie uns unter akamai.com und akamai.com/blog, oder folgen Sie Akamai Technologies auf X (ehemals Twitter) und LinkedIn. Veröffentlicht: 05/24.

Vanson Bourne ist ein unabhängiger Spezialist für Marktforschung im Technologiesektor. Das Unternehmen hat sich mit robusten und glaubwürdigen forschungsbasierten Analysen einen hervorragenden Ruf erworben. Die Analysen gründen auf strengen Forschungsprinzipien und der Fähigkeit, die Meinung von Entscheidungsträgern in technischen und geschäftlichen Funktionen, in allen Geschäftsbereichen und in allen wichtigen Märkten einzuholen. Weitere Informationen finden Sie unter www.vansonbourne.com.