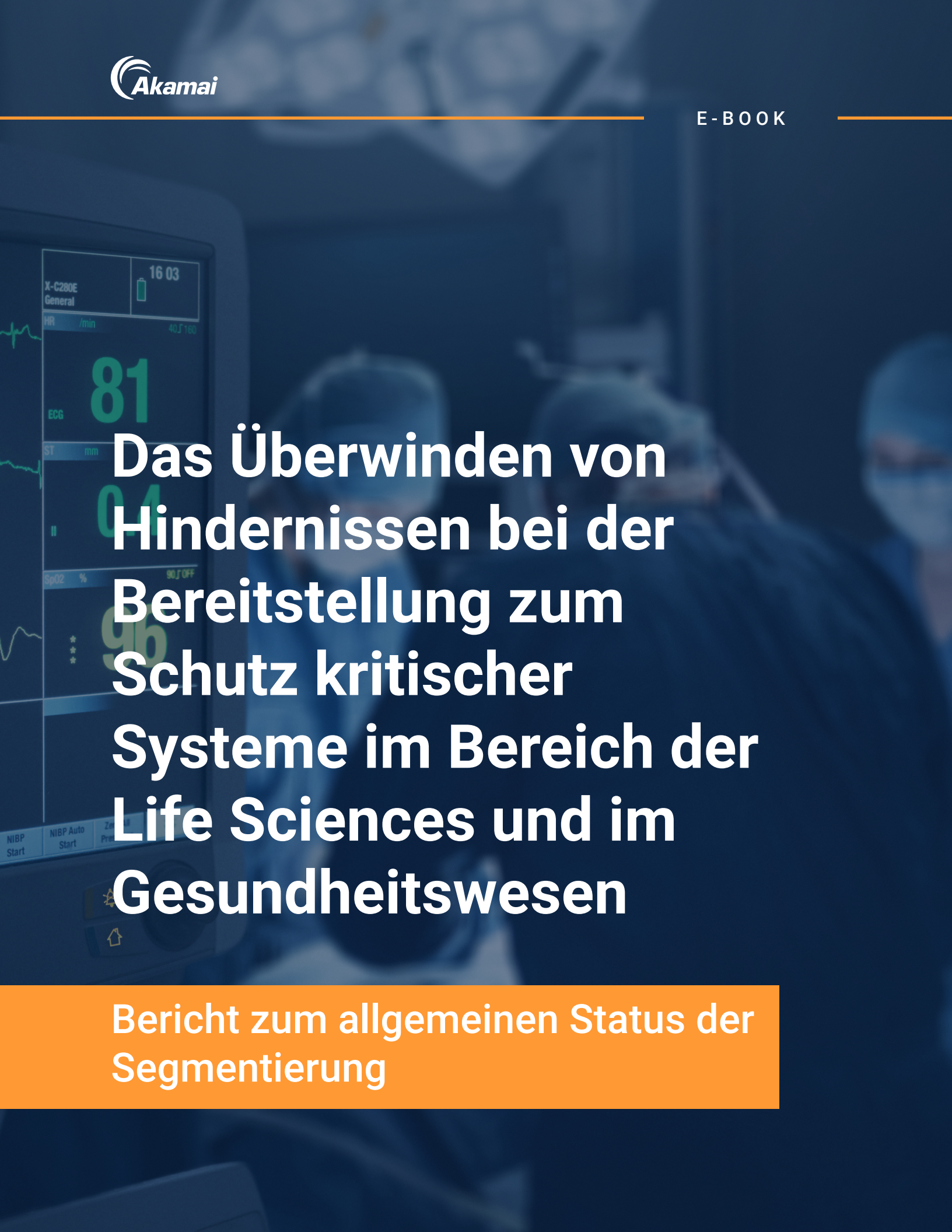
Akamai

E-BOOK



Das Überwinden von Hindernissen bei der Bereitstellung zum Schutz kritischer Systeme im Bereich der Life Sciences und im Gesundheitswesen

Bericht zum allgemeinen Status der Segmentierung

Inhaltsverzeichnis

Einführung — 2

Die Segmentierung hat sich insgesamt langsam entwickelt, doch diejenigen, die durchgehalten haben, haben ihr Risiko enorm reduziert. — 3

Segmentierung ist allgemein als Eckpfeiler von Zero Trust anerkannt. — 5

Implementierungen gehen langsam voran, doch Beharrlichkeit zahlt sich aus — 6

Erkenntnisse aus der Segmentierung von sechs kritischen Geschäftsbereichen — 7

Wie eine softwarebasierte Mikrosegmentierungslösung Herausforderungen meistert — 8

Mit der richtigen Lösung und dem richtigen Support verbessern Sie Ihre Sicherheitslage nachhaltig — 9

Fazit — 10

Die Umfrageteilnehmer — 11

Einführung

Mehr denn je wirkt sich die IT im Gesundheitswesen auf das Backoffice, Vorstandsetagen und Untersuchungszimmer aus. Die Schwere und Häufigkeit von massiven Datenschutzverletzungen steigt stetig an, was erhebliche Auswirkungen auf den Betrieb und den Ruf hat. Da Bedrohungsakteure immer raffiniertere Taktiken anwenden – und in vielen Fällen gemeinsam vorgehen –, sind die Gefahren, denen das Gesundheitssystem ausgesetzt ist, häufiger und ernster. Angesichts der großen Mengen an veralteten Technologien, des finanziellen Werts von Patientendaten und der Herausforderungen im Zusammenhang mit der schnellen Digitalisierung und dem Ausbau des Internet der medizinischen Dinge (IoMT) muss diese dynamische Umgebung ihre Infrastruktur, Organisation, Anwendungen und APIs auf eine Art und Weise schützen, die sich noch vor fünf Jahren niemand hätte vorstellen können.

Wie die Ergebnisse in diesem Bericht zeigen, erhöhen Cyberangriffe den Druck auf Sicherheitsfachleute, die richtigen Lösungen zu finden, deren kontinuierliche Verfügbarkeit eine Frage von Leben oder Tod ist.

Befragte aus Organisationen im Gesundheitswesen und im Bereich Life Sciences in den USA, Lateinamerika, Europa, Afrika, im Nahen Osten und im asiatisch-pazifischen Raum stimmen mit überwältigender Mehrheit der Effektivität der Segmentierung beim Schutz von Assets zu. Die Befragten geben jedoch auch an, dass der Fortschritt bei der Bereitstellung von Segmentierungen für kritische Geschäftsanwendungen und Assets nicht ideal ist. Die Befragten (darunter Gesundheitsdienstleister und Spezialisten für Gesundheitstechnologie sowie andere Organisationen, die sich auf Gesundheitsdienstleistungen oder -produkte spezialisiert haben) geben an, dass das größte Hindernis für Organisationen im Gesundheitswesen und im Bereich Life Sciences der Mangel an Fachwissen bei der Implementierung der Segmentierung war. Die historische Komplexität des Einsatzes herkömmlicher Segmentierungsmethoden – die medizinische Geräte nicht abdecken – wird durch die Tatsache verschärft, dass Teams immer noch mit personellen Engpässen zu kämpfen haben, die bereits vor der COVID-19-Pandemie begannen.

Eine Umfrage der US-amerikanischen Non-Profit Healthcare Information and Management Systems Society (HIMSS) ergab, dass 84 % der US-amerikanischen IT-Fachleute im Gesundheitswesen Schwierigkeiten haben, Mitarbeitende zu gewinnen, und 67 % geben an, dass die Bindung von Mitarbeitenden ein Problem ist. Laut der HIMSS kann die Mehrheit des Personals keine Schulungen zu aktuellen und neuen Bedrohungen vorweisen.

Was genau würden diese aktuellen Schulungen beinhalten? Für jene, die die meisten ihrer kritischen Assets segmentiert hatten, erwies sich die Segmentierung als überaus effektive Abwehrlösung. So konnten die Verantwortlichen Ransomware 11 Stunden schneller abwehren und eindämmen als diejenigen, die nur eine einzelne Ressource segmentiert hatten. Stellen Sie sich vor, welchen Unterschied diese 11 Stunden für Ihr Team, Ihre Patienten und Ihren Ruf machen.

Die Segmentierung hat sich insgesamt langsam entwickelt, doch 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.

Ransomware-Angriffe und ihre Auswirkungen nehmen weiter zu

Daten aus dem Jahr 2021 im Vergleich zu 2023 zeigen, dass die Anzahl der Ransomware-Angriffe (sowohl erfolgreich als auch erfolglos) gegen Organisationen im Gesundheitswesen in einem Zeitraum von 12 Monaten um 162 % gestiegen ist. Die Auswirkungen dieser Angriffe sind vielfältig und reichen von betrieblichen Ausfallzeiten wie Stornierung oder Verschiebung medizinischer Eingriffe über Probleme bei der Medikation aufgrund von mangelndem Zugriff auf Patientenakten, bis hin zur Umleitung von Krankenwagen auf andere Gesundheitseinrichtungen.

Prozentualer Anstieg der Anzahl der Ransomware-Angriffe in den letzten 12 Monaten nach Sektoren (Daten von 2021 gegenüber Daten von 2023)

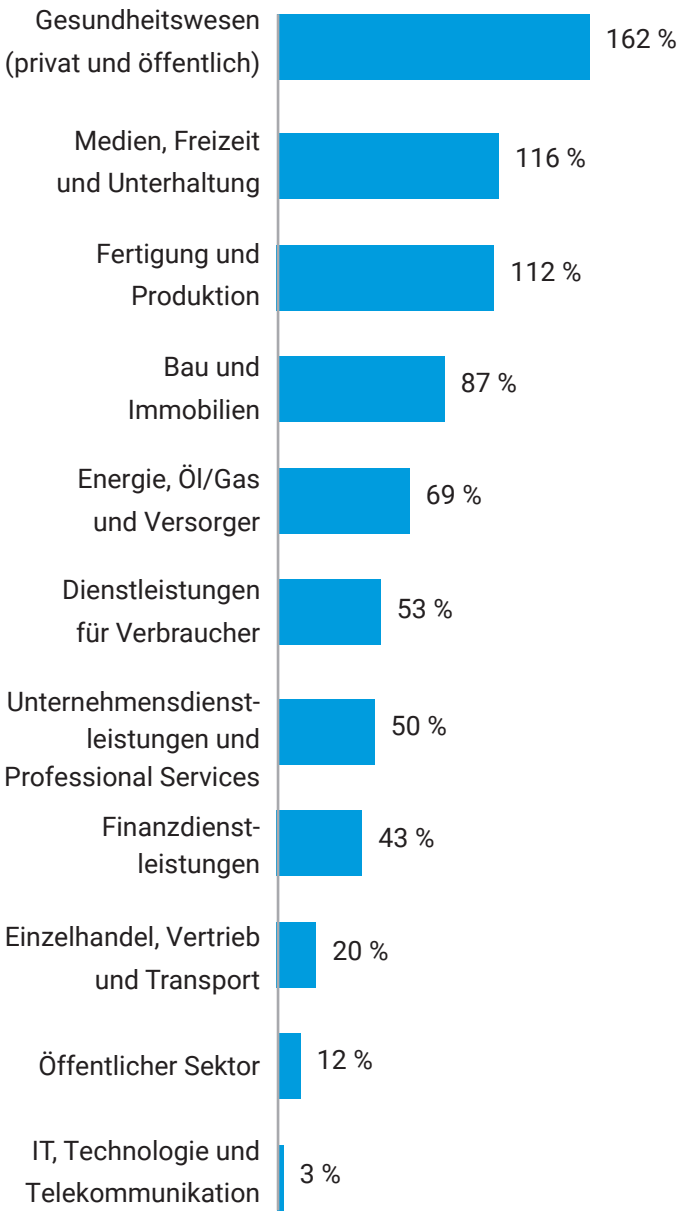


Abb. 1: Wie oft wurde Ihre Organisation in den letzten 12 Monaten von Ransomware angegriffen (unabhängig davon, ob die Angriffe erfolgreich waren oder nicht)? Das Diagramm bezieht sich auf eine Basisgröße von 1.200 Teilnehmern und zeigt nur den durchschnittlichen prozentualen Anstieg der Anzahl der Angriffe in den letzten 12 Monaten, aufgeschlüsselt nach Sektoren.

Im Durchschnitt ist der Anstieg im Gesundheitswesen von allen Branchen am höchsten. Dies könnte ein Hinweis darauf sein, dass Organisationen im Gesundheitswesen – selbst Kinderkrankenhäuser, die ebenfalls zunehmend Opfer von Angriffen werden – immer häufiger kein Tabu mehr für Hacker sind.

Ransomware-Angriffe auf Organisationen im Gesundheitswesen waren im Jahr 2023 nicht nur häufiger als im Jahr 2021, sondern auch schädlicher (Abbildung 2). Die Befragten weisen auf eine Zunahme an Rufschädigung, einen Verlust der Kundentreue und Netzwerkausfälle hin. All diese Faktoren erhöhen den Druck für Sicherheitsteams erheblich.

Dieser Druck hat sich auch auf agile Strategien ausgewirkt. Die Zahl der Organisationen im Gesundheitswesen, die Strategien oder Richtlinien zur Cybersicherheit wöchentlich aktualisieren, ist von 17 % im Jahr 2021 auf 25 % im Jahr 2023 gestiegen. Dies geschah nicht nur als Antwort auf Ransomware, sondern generell in Reaktion auf die ständige Veränderung der Angriffsfläche.

Wenn man dies genauer betrachtet, ist die Wahrscheinlichkeit, dass Organisationen im Gesundheitswesen nach einem Cybersicherheitsangriff finanzielle Verluste erleiden, höher als in anderen Sektoren (43 %, verglichen mit 36 % insgesamt). Organisationen im Gesundheitswesen leiden nach einem Cybersicherheitsangriff zudem eher unter dem Verlust der Patienten-/Mitgliedertreue (48 % im Vergleich zu 33 % insgesamt). Dies zeigt, dass Organisationen im Gesundheitswesen in vielerlei Hinsicht einem größeren Risiko ausgesetzt sind als andere Organisationen.

Auswirkungen von Ransomware/ Cyberangriffen im Gesundheitswesen und im Bereich der Life Sciences

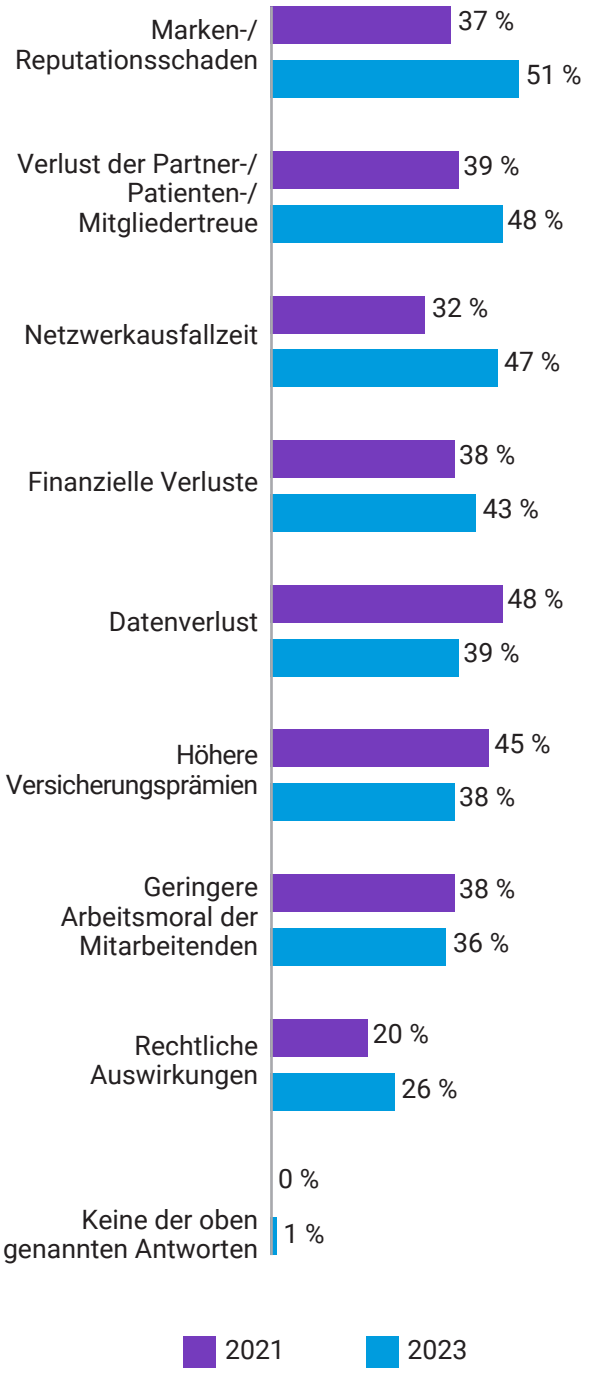


Abb. 2: Welche der folgenden Auswirkungen hatte es für Ihr Unternehmen, wenn es in der Vergangenheit Ransomware oder einen anderen Cyberangriff erkannt hat? Das Diagramm zeigt die Basisgrößen nach Jahr, nicht alle Antwortoptionen werden angezeigt; aufgeschlüsselt nach historischen Daten (2021 = 112, 2023 = 157), nur Daten des Gesundheitssektors.

Segmentierung ist allgemein als Eckpfeiler von Zero Trust anerkannt.

Die Befragten aus dem Gesundheitswesen und im Bereich Life Sciences sind sich einig, dass Segmentierung wichtig ist, um die Sicherheit der Organisation zu gewährleisten, insbesondere bei der Abwehr von Malware.

Zero Trust ist eine Netzwerksicherheitsstrategie basierend auf der Philosophie, dass keine Person oder kein Gerät innerhalb oder außerhalb des Organisationsnetzwerks Zugang zu IT-Systemen oder Arbeitslasten erhalten sollte, wenn dies nicht ausdrücklich als notwendig erachtet wird. Kurz gesagt: Es gibt kein (zero) implizites Vertrauen (trust).

64 % der Befragten geben an, dass Segmentierung äußerst wichtig ist, und 94 % glauben, dass sie entscheidend ist, um schädliche Angriffe abzuwehren.

Die Einführung von Zero Trust wird häufig durch Umstände verursacht, die sich außerhalb des Einflussbereichs der IT-Verantwortlichen im Gesundheitswesen befinden. Ein Drittel (33 %) der Befragten aus dem Gesundheitswesen geben an, dass der Fokus ihrer Regierung auf Cybersicherheit lag, und fast ebenso viele (29 %) sagen, dass dies darauf zurückzuführen war, dass sie bereits Opfer eines Ransomware-Angriffs geworden waren.

Aber nur etwa einer von drei (34 %) Befragten aus dem Gesundheitswesen gibt an, dass ihr Zero-Trust-Framework vollständig sowie definiert und daher ausgereift ist. Dies gehört zu den niedrigsten in allen Branchen, wobei einige Sektoren (wie Baugewerbe und Finanzdienstleistungen) mit einer besonders hohen Wahrscheinlichkeit ein ausgereiftes Zero-Trust-Framework haben (53 % bzw. 47 %). Die Zero-Trust-Reife wird wahrscheinlich von Organisationen im Gesundheitswesen in den USA vorangetrieben. Hier geben 50 % an, dass sie über ein vollständiges und definiertes Framework verfügen, im Vergleich zu den anderen Ländern und Regionen, in denen nur 23 % angeben, dass ihr Zero-Trust-Framework vollständig und definiert ist. Dies spiegelt den allgemeinen Trend wider, bei dem US-Unternehmen und -Organisationen aus allen Branchen im Vergleich zu anderen Regionen häufiger Opfer von Cyberangriffen sind (115 in den letzten 12 Monaten im Vergleich zum Gesamtdurchschnitt von 86).

Organisationen im Gesundheitswesen stehen daher vor großen Herausforderungen, wenn es um Zero Trust geht. Die Befragten aus dieser Branche haben häufiger Probleme mit proprietären Technologien bei der Segmentierung ihres Netzwerks (41 % im Vergleich zu insgesamt 32 %) und sehen sich bei der Umsetzung von Zero Trust häufiger mit Budgetproblemen konfrontiert (47 %, verglichen mit durchschnittlich 37 % in allen Branchen). Die Unterstützung durch einen erfahrenen Partner kann dabei helfen, einige Herausforderungen zu meistern: Zu den schwierigsten Aspekten eines Zero-Trust-Frameworks, das für Organisationen im Gesundheitswesen implementiert werden muss, gehört der Anwendungs-Workload (68 % im Vergleich zu 60 % insgesamt). Ein Partner kann Qualifikationslücken schließen, die von 45 % der Organisationen im Gesundheitswesen gemeldet wurden.

Die Mehrheit der befragten Organisationen im Gesundheitswesen möchte noch weiter gehen und eine Mikrosegmentierung implementieren, die Anwendungs-Workloads auf einer granularen Ebene schützt

92 % der Befragten aus dem Gesundheitswesen geben an, Mikrosegmentierung habe mindestens eine hohe Priorität, und 43 % nennen sie als ihre oberste Priorität. Im Vergleich dazu geben 34 % der Befragten aus allen Branchen Mikrosegmentierung als oberste Priorität an. Dies zeigt, dass Organisationen im Gesundheitswesen im Durchschnitt eher ein Zero-Trust-Framework schätzen – und dafür eintreten.

Implementierungen gehen langsam voran, doch Beharrlichkeit zahlt sich aus

Selbst wenn man sich weithin bewusst ist, dass Segmentierung entscheidend für die Verhinderung von Cyberangriffen ist, wird sie nur langsam implementiert.

Nur 36 % der Organisationen im Gesundheitswesen haben mehr als zwei kritische Geschäftsbereiche im Jahr 2023 segmentiert, und 43 % haben vor zwei oder mehr Jahren ein Netzwerksegmentierungsprojekt gestartet, was darauf hindeutet, dass die Bemühungen zum Stillstand gekommen sind.

Die unternehmenskritischen Bereiche

- Kritische Anwendungen
- Öffentlich zugängliche Anwendungen
- Domaincontroller
- Endpunkte
- Server
- Geschäftskritische Assets/Daten

Dies kann auf viele der größten Hindernisse zurückgeführt werden, mit denen die Befragten im Gesundheitswesen konfrontiert sind – mangelnde Fähigkeiten/Fachkenntnisse bei der Implementierung der Segmentierung (45 %), erhöhte Leistungsengpässe (z. B. durch die Notwendigkeit der manuellen Fehlersuche, 44 %) und der Einsatz proprietärer Technologien (41 %, Abbildung 3). Insbesondere mangelnde Kompetenzen/Fachkenntnisse sind ein Problem für Organisationen im Gesundheitswesen, mehr als für Organisationen in anderen Branchen (alle liegen unter den 45 % für das Gesundheitswesen, wobei der vertikale Durchschnitt bei 39 % liegt). Diese Ergebnisse stimmen mit den jüngsten Erkenntnissen des Ponemon Institute, einem führenden Forschungsunternehmen für IT-Sicherheit, über die vorherrschenden Bedrohungen für das Gesundheitswesen überein, zu denen in erster Linie Ransomware und Business Email Commitment (BEC) zählen. Während eine wettbewerbsfähige Bezahlung für IT-Fachkräfte im Gesundheitswesen eine Herausforderung darstellt, ist die wachsende Menge komplexer regulatorischer Anforderungen eine weitere Herausforderung.

Organisationen im Gesundheitswesen auf der ganzen Welt spüren nach wie vor die Folgen der COVID-19-Pandemie und die Belastung, die sie auf das menschliche und treuhänderische Kapital ausübte, was diese Herausforderungen noch verstärkt.

Hindernisse bei der Segmentierung des Netzwerks in den Bereichen Gesundheitswesen und Life Sciences

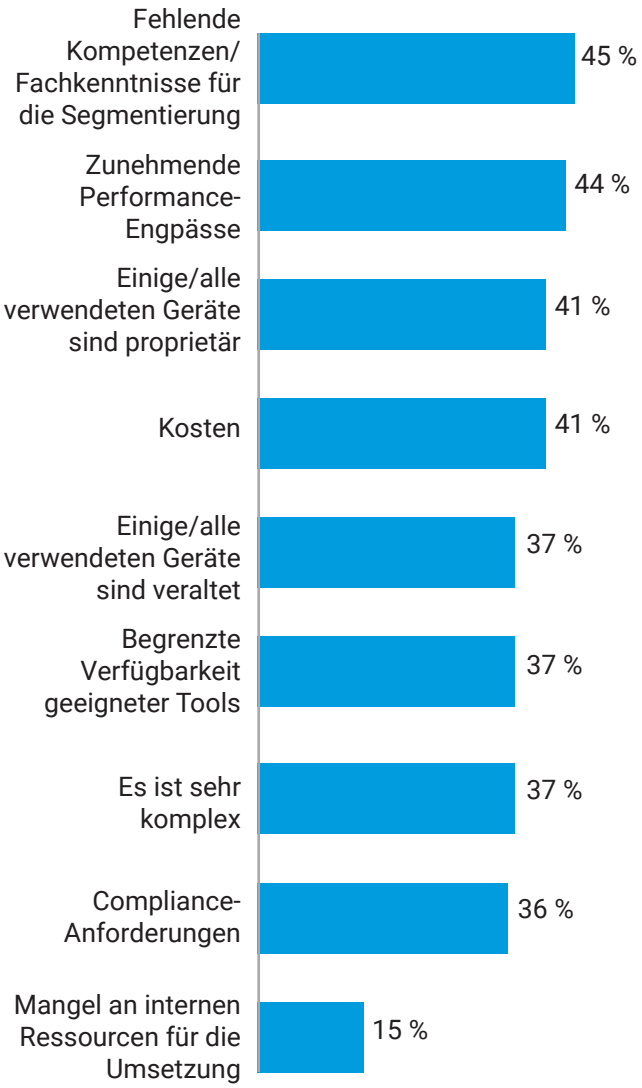


Abb. 3: Mit welchen Problemen war Ihr Unternehmen bei der Segmentierung des Netzwerks konfrontiert bzw. mit welchen Problemen rechnen Sie? Das Diagramm zeigt die Basisgröße von 157 für das Jahr 2023 und zeigt nicht alle Antwortoptionen an. Diese Frage wurde nur den Befragten in Organisationen gezeigt, die ihr Netzwerk zu einem bestimmten Zeitpunkt segmentiert haben (nur Daten des Gesundheitssektors).

Trotz des langsamen Fortschritts nehmen die Segmentierungsraten über alle Branchen hinweg allmählich zu. Im Gesundheitswesen stieg der Prozentsatz der Organisationen mit segmentierten geschäftskritischen Anwendungen/Daten von 2021 bis 2023 um 20 % und die segmentierten Server um 18 %. Doch während diese Steigerungen die durchschnittlichen Steigerungen aller Branchen (12 % bzw. 8 %) übertreffen, sorgen die häufigsten Schwachstellen dafür, dass die Segmentierungsraten noch stärker beschleunigt werden müssen. Im Gesundheitswesen ist es wahrscheinlich, dass ein Mitarbeiter/Nutzer im Büro der Grund/die Quelle für den Zugriff von Angreifern auf das Netzwerk war (47 %, verglichen mit 26 % insgesamt). Dies ist mehr als doppelt so viele Branchen wie Finanzdienstleistungen und Energie (beide 19 %). Die Auswirkungen solcher Angriffe können durch Segmentierung minimiert werden. Angesichts der Bedeutung, die so viele Systeme innerhalb von Organisationen im Gesundheitswesen – wo Leben auf dem Spiel stehen – haben können, verdeutlicht dies den Wert einer schnellstmöglichen Segmentierung.

Erkenntnisse aus der Segmentierung von sechs kritischen Geschäftsbereichen

Mehr Transparenz verringert Risiken, was in einer risikoscheuen Branche von entscheidender Bedeutung ist. Durch den Schutz und die Segmentierung von mehr Ressourcen werden Organisationen im Gesundheitswesen sicherer, sodass Sicherheitsteams Bedrohungen schneller erkennen und wesentlich effektiver reagieren können.

Die Ergebnisse von Vanson Bourne zeigen, dass mit Segmentierung die Wiederherstellung nach einem Angriff 11 Stunden schneller erfolgt. Die Mathematik dahinter: Bei Organisationen im Gesundheitswesen, die eine Segmentierung in sechs organisationskritischen Bereichen implementiert haben, dauert es durchschnittlich vier Stunden, bis ein Ransomware-Angriff vollständig gestoppt ist. Bei denjenigen, die nur ein Asset segmentiert haben, sind es 14 Stunden.

Mit Segmentierung beschleunigt sich auch die Eindämmung lateraler Netzwerkbewegungen um 11 Stunden. Für diejenigen, die Segmentierungen über alle sechs unternehmenskritische Bereiche hinweg implementiert haben, dauert es durchschnittlich drei Stunden, die laterale Netzwerkbewegung eines Ransomware-Angriffs signifikant zu begrenzen. Bei Unternehmen mit einer Segmentierung für nur ein Asset dauert dies durchschnittlich 14 Stunden.

Überlegen Sie, welchen Unterschied 11 Stunden für Ihr Team und für die Eindämmung von Kosten und Markenschäden in den beiden Szenarien machen.

Einen Angriff stoppen
3 Stunden

Die durchschnittlich erforderliche Zeit, um einen Ransomware-Angriff vollständig zu stoppen (für diejenigen, die alle sechs Organisationsressourcen segmentiert haben) Für diejenigen, die nur ein Asset segmentiert haben: **14 Stunden**

Bewegung begrenzen
3 Stunden

Die durchschnittlich erforderliche Zeit, um die laterale Netzwerkbewegung eines Ransomware-Angriffs signifikant zu begrenzen (für diejenigen, die alle sechs Organisationsressourcen segmentiert haben) Für diejenigen, die nur ein Asset segmentiert haben: **14 Stunden**

Wie eine softwarebasierte Mikrosegmentierungslösung Herausforderungen meistert

Mikrosegmentierung ermöglicht nicht nur eine fortschrittlichere, detailliertere Segmentierung, sondern erleichtert auch deren 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 für die Durchsetzung von Richtlinien nicht auf das zugrunde liegende Betriebssystem angewiesen ist, 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 aktuellen IoMT-Geräten (Internet der medizinischen Dinge) und Container-Technologien. Das bedeutet, dass Sie nur eine einzige Lösung mit einer Schnittstelle verwalten, um Verbindungen, die von verschiedenen Betriebssystemen und Geräten in Ihrer gesamten Umgebung hergestellt werden, unabhängig von ihrem physischen Standort zu visualisieren und zu steuern.

Wie sie die Bereitstellung erleichtert

Akamai Guardicore Segmentation 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 von technischen Belastungen eines Systems, die durch eine Segmentierungslösung verursacht werden, sondern vielmehr durch Personalengpässe. Der Zeit- und Arbeitsaufwand, der für die manuelle Segmentierung von Geschäftsbereichen und die manuelle Fehlerbehebung in diesen Bereichen aufgewendet werden muss, kann enorm sein. 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 Segmentierungsfachleute arbeiten während des gesamten Implementierungsprozesses mit Ihnen zusammen, um sicherzustellen, dass Sie die Segmentierungsziele in Ihrer speziellen IT-Umgebung erreichen.

Unterstützung bei der Implementierung bietet auch die Lösung selbst: Die auf KI basierenden Kennzeichnungs- und 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 Kunden konnte Akamai mit einem einzigen Ingenieur ein Projekt zur granularen Segmentierung, für das eine Dauer von zwei Jahren und Gesamtkosten von 1 Million US-Dollar veranschlagt waren, in nur sechs Wochen umsetzen. Dadurch konnten die Gesamtkosten des Projekts um 85 % gesenkt werden. Das Beispiel macht deutlich, dass eine granulare Segmentierung schnell und einfach ohne Belastung durch Engpässe implementiert werden kann.

So vereinfacht Mikrosegmentierung die Compliance

Viele Organisationen im Gesundheitswesen und im Bereich Life Sciences setzen Akamai Guardicore Segmentation ein, um die Einhaltung einer Reihe nationaler und internationaler Compliance-Auflagen zu gewährleisten, wie HIPAA, DSGVO, PCI DSS und viele mehr. Diese gesetzlichen 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. Außerdem sind nach einem Angriff die Wiederherstellungsmaßnahmen gesichert und benötigen weniger Zeit.

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 Fachleuten 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

Cyberangreifer richten sich zunehmend gegen Organisationen des Gesundheitswesens: Ransomware-Angriffe auf Organisationen im Gesundheitswesen nahmen von 2021 bis 2023 um 162 % zu. Im Vergleich dazu stiegen die Zahlen im Energiesektor in diesem Zeitraum um 69 %, und im Bereich Finanzdienstleistungen um 43 %.

Die Befragten im Gesundheitswesen geben häufiger an, dass ihre Organisation nach einem Cybersicherheitsangriff finanzielle Verluste erlitten hat: 43 % geben dies an, im Vergleich zu 36 % bei Befragten in allen Branchen.

Segmentierung und Mikrosegmentierung sind im Gesundheitswesen wichtiger als in vielen anderen Branchen: Entscheidungsträger im Bereich IT-Sicherheit in Organisationen im Gesundheitswesen (64 %) geben häufiger an, dass die Netzwerksegmentierung äußerst wichtig ist, um die Sicherheit ihrer Organisation zu gewährleisten, im Vergleich zu vielen anderen Sektoren, wie Bauwesen (58 %), Fertigung (53 %) und E-Commerce (48 %). Die Einschätzung der Entscheidungsträger im Bereich IT-Sicherheit im Gesundheitswesen entspricht den Zahlen der Befragten in den Bereichen Finanzdienstleistungen und Energie (beide 66 %).

Organisationen im Gesundheitswesen sind bei der Implementierung des Zero-Trust-Frameworks wahrscheinlich nicht ausgereifter: Die Befragten aus dem Gesundheitswesen geben weniger häufig an, dass die Zero-Trust-Einführung vollständig und definiert ist (34 %), im Gegensatz zu den Bereichen Finanzdienstleistungen (47 %), Energie (46 %) und E-Commerce (42 %).

Die Umfrageteilnehmer

Für die vollständige Studie haben wird 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 den IT-Sicherheitsansätzen, Segmentierungsstrategien und zu den Bedrohungen gestellt, denen die Organisationen 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 Befragten stammen aus der ganzen Welt, darunter aus den USA, Indien, Mexiko, Brasilien, dem Vereinigten Königreich, aus Frankreich, Deutschland, China, Japan und Australien. Die befragten Personen arbeiteten für Organisationen mit mehr als 1.000 Mitarbeitenden und repräsentierten unterschiedliche Branchen und Unterbranchen.

Hinweis: Diese Stichprobe unterschied sich geringfügig von der des Jahres 2021. Beispielgrößen: 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. 2023 richteten wir einen speziellen Fokus auf den digitalen Handel als eigenen Sektor.

Für die Zwecke dieses Berichts zu Gesundheitswesen und Life Sciences haben wir die Antworten von 157 (2023) und 112 (2021) befragten Organisationen aus diesem Sektor ausgewertet.
Die Umfrage berücksichtigte die gleichen Länder wie der Hauptbericht: USA, Indien, Mexiko, Brasilien, Vereinigtes Königreich, Frankreich, Deutschland, China, Japan und Australien.

Die vollständige Forschungsstudie umfasste die folgenden zusätzlichen Branchen: E-Commerce (190), Finanzdienstleistungen (173), IT, Technologie und Telekommunikation (125), Energie, Öl/Gas und Versorgungsunternehmen (94), Herstellung und Produktion (91), Einzelhandel, Vertrieb und Transport (81), Medien, Freizeit und Unterhaltung (63), Bau und Immobilien (60), Unternehmensdienstleistungen und Professional Services (58), öffentlicher Sektor (46), Verbraucherdienstleistungen (33), sonstige Wirtschaftszweige (29).

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 für Gesundheitswesen und Life Sciences erfahren? Dann besuchen Sie uns unter akamai.com/healthcare 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.