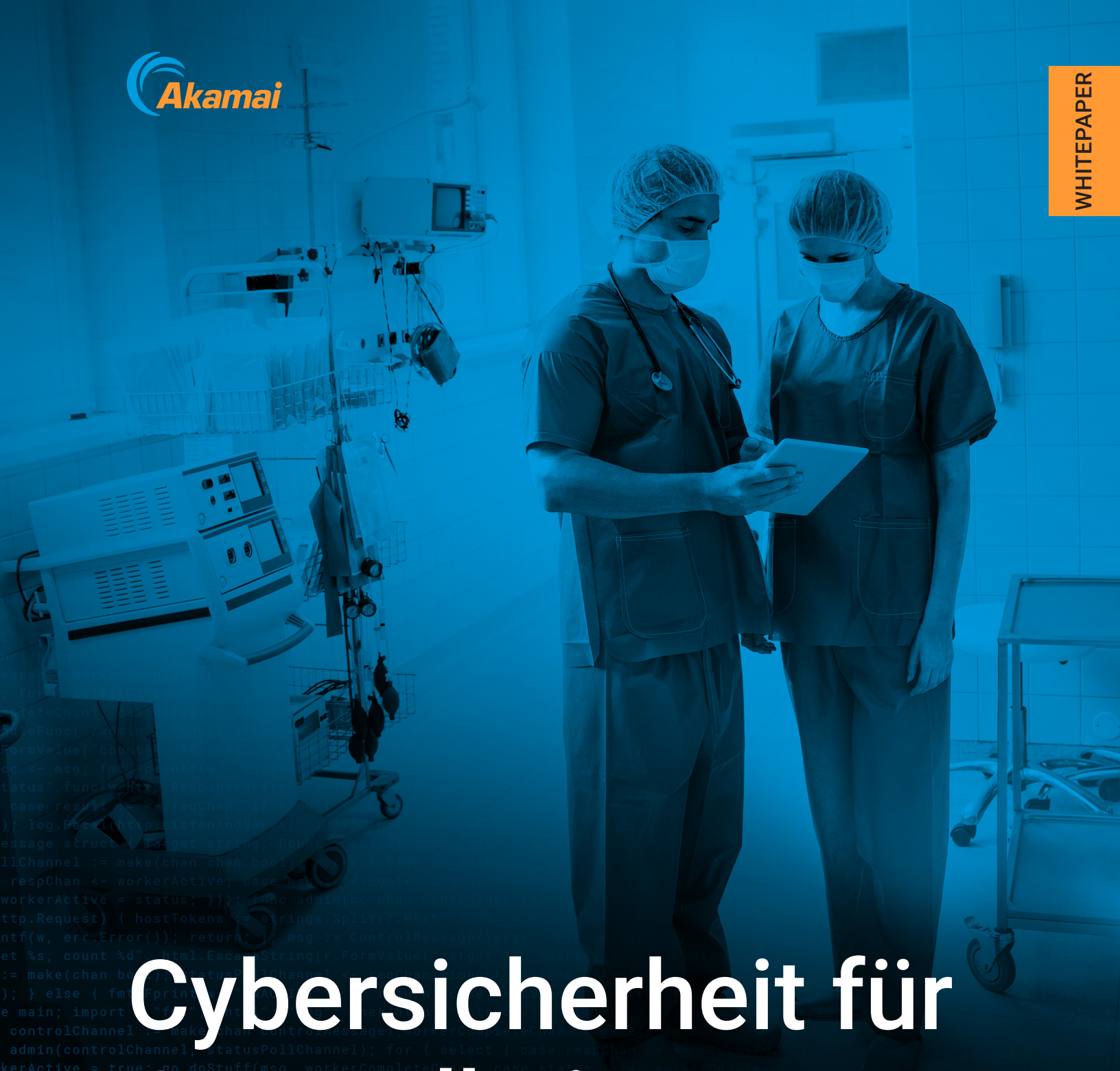
Akamai

WHITEPAPER



Cybersicherheit für Gesundheits-dienstleister

Einführung

Um in einem schnelllebigen Markt wettbewerbsfähig zu bleiben, setzen Gesundheitsdienstleister neue Geräte und Anwendungen ein, mit denen sie eine erstklassige Patientenversorgung und innovative Erlebnisse bieten können. Jedes neue Produkt bringt seinen eigenen Nutzen für die Patienten, aber auch eigene Sicherheitsrisiken für das Unternehmen mit sich.

Diese komplexe IT-Umgebung schafft in Verbindung mit dem hohen Wert geschützter Gesundheitsinformationen (Protected Health Information, PHI) eine unwiderstehliche Chance für Cyberkriminelle, die immer wieder Systeme angreifen. Laut einem Bericht des U.S. Department of Health and Human Services und einer Studie von IBM gab es seit dem Ausbruch der Pandemie im Gesundheitswesen einen Anstieg der Cyberangriffe von 50 %. Und diese Angriffe haben die Branche sehr viel Geld gekostet: Die durchschnittlichen Kosten lagen bei 7,13 Millionen US-Dollar pro Vorfall. Der IBM-Bericht betonte, dass Ransomware-Angriffe die häufigste Bedrohung waren, da Cyberkriminelle die Notwendigkeit, Krankenhaus- und Gesundheitssysteme schnell wiederherzustellen, ausnutzten. Den zweiten Platz belegen Datendiebstahl und Serverzugriff. Insbesondere Gesundheitsdienstleister sind attraktive Ransomware-Ziele, da elektronische Gesundheitsaufzeichnungen (Electronic Health Records, EHRs) im Dark Web bis zu 1.000 US-Dollar einbringen. Zum Vergleich: Kreditkarteninformationen werden für etwa 110 US-Dollar und Sozialversicherungsnummern für jeweils nur einen Dollar gehandelt.

Da die Anzahl der Bedrohungen für ihre Systeme ständig steigt, sind viele Unternehmen nicht ausreichend darauf vorbereitet, diese Bedrohungen zu mindern. Schlimmer noch: Einige Unternehmen wurden bereits infiltriert und wissen es nicht. Cyberkriminelle stehlen möglicherweise bereits Daten oder warten auf den richtigen Zeitpunkt, um zuzuschlagen.

Deshalb ist es jetzt an der Zeit, Klarheit über die Angriffsfläche Ihres Unternehmens zu gewinnen, indem Sie eine Bestandsaufnahme aller Geräte und ihrer Verbindung zu Ihrer Infrastruktur durchführen. Wenn Sie genau wissen, wo Sicherheitslücken bestehen, können Sie einen fundierten Plan zur Risikominderung implementieren, um die potenziellen Auswirkungen von Cyberangriffen zu verhindern oder zu minimieren.

So decken Sie die größten Cybersicherheitsrisiken für Ihr Unternehmen ab

Bedrohung 1: Phishing-Angriffe

Phishing ist einer der häufigsten Vektoren für Cyberangriffe in allen Branchen. Laut dem Health Sector Cybersecurity Coordination Center gab es 2021 einen deutlichen Anstieg von Phishing-Angriffen auf den Gesundheitssektor. Im Laufe des Jahres 2020 haben Kriminelle laut Akamai-Daten COVID-19 und das Versprechen finanzieller Hilfe oder finanzielle Schwierigkeiten ausgenutzt, um Menschen auf der ganzen Welt mit Phishing anzugreifen.

Bei Phishing wird versucht, vertrauliche Daten durch betrügerische E-Mails oder Webseiten zu erlangen. Wenn es erfolgreich ist, werden Nutzer dazu gebracht, ihre Anmeldedaten einzugeben, was den Tätern im Grunde freien Zugang zum Netzwerk verschafft.

Das ist auch Menschen passiert, die in New York Arbeitslosenhilfe beantragt haben. Laut einem Phishing-Bericht von Steve Ragan – ehemaliger Redakteur von CSO Online und derzeitiger Akamai-Sicherheitsforscher – gab es Anfang 2021 mehrere Phishing-Kits, die auf Programme für pandemiebedingte Arbeitslosenhilfe (Pandemic Unemployment Assistance, PUA) abzielten. Diese Programme sollten denjenigen helfen, die während der Lockdowns Hilfe brauchten, und unterstützten Millionen von US-Amerikanern.

In einem Beitrag von CBS News, der im ganzen Land ausgestrahlt wurde, sprach Ragan über ein solches PUA-Phishing-Kit, das auf Menschen in New York abzielte, und darüber, wie Kriminelle die persönlichen Daten sammeln und verkaufen, die sie durch den Betrug erlangen. Seit diesem Beitrag hat er PUA-Betrugsfälle entdeckt, die auf Menschen in Wisconsin, Indiana, Pennsylvania und Massachusetts abzielten.

So können Sie Phishing-Angriffe stoppen und ihre Auswirkungen mindern

Je nach Berechtigungseinstellungen und Sicherheitsvorkehrungen kann der Zugriff auf ein einzelnes Nutzerkonto Kriminellen möglicherweise freie Hand in wichtigen Teilen Ihres Netzwerks geben. Oftmals können sie ihre Reichweite im Netzwerk Ihres Unternehmens sogar erweitern.

Durch Mikrosegmentierung wird der Zugriff von Cyberkriminellen auf den Teil Ihres Netzwerks beschränkt, auf den sie zu Beginn Zugriff erhalten. So wird verhindert, dass sie sich lateral im Netzwerk bewegen und in weiteren Bereichen Schaden anrichten können. Mikrosegmentierung begrenzt die Auswirkungen eines Angriffs, indem sie verhindert, dass Kriminelle einen beliebigen Einstiegspunkt für den Zugriff auf das breite Unternehmensnetzwerk nutzen können.

Neben der Mikrosegmentierung ist Multi-Faktor-Authentifizierung (MFA) eine Ihrer wirksamsten Verteidigungsmaßnahmen gegen Phishing-Angriffe. Sie bietet eine zusätzliche Schutzebene, da eine zusätzliche Identitätsprüfung erforderlich ist, bevor der Zugriff auf ein Konto gewährt wird. Dadurch wird verhindert, dass kompromittierte Anmeldedaten ausgenutzt werden.

MFA, insbesondere eine von FIDO2 zugelassene Lösung, gewährleistet Schutz vor den neuesten Angriffen. Sie verlangt, dass Nutzer einen eindeutigen Code eingeben, der über eine Messaging- oder Authentifizierungs-App auf dem Mobilgerät des Nutzers generiert wird. Dieser zusätzliche Anmeldeschritt hilft, Phishing-Angriffe abzuwehren, selbst wenn Kriminelle über richtige Anmeldedaten verfügen.

Es ist wichtig, Ihre Mitarbeiter über die Taktiken von Social-Engineering-Angriffen wie Phishing zu informieren. Tatsächlich ist Phishing eines dieser Probleme, für die es keine Patentlösung gibt, weil es so viele Komponenten beinhaltet. Es ist schwer vorherzusagen, was Kriminelle als Nächstes tun werden. Da Menschen nach wie vor ein wichtiger Aspekt beim Phishing sind, bleiben sie das schwächste Glied in der Kette.

Das bedeutet, dass es entscheidend ist, Sicherheit einfach zu gestalten. Akamai bietet eine reibungslose, phishing-sichere MFA-Lösung, die selbst vor den klügsten Cyberkriminellen schützt.

Bedrohung 2: Nicht unterstützte ältere Software

Veraltete Software ist ein weiteres wichtiges Sicherheitsrisiko. Jedes neue Sicherheitsupdate (Patch), das nicht sofort installiert wird, erzeugt offene Backdoors in Ihrem Netzwerk. Das gilt insbesondere für ältere Geräte, die nicht mehr unterstützt werden und keine Updates mehr erhalten.

Nicht unterstützte Software kann Zero-Day-Schwachstellen aufweisen, die Unternehmen möglicherweise nur ungern selbst patchen. Die Erstellung eines nutzerdefinierten Patches kann manchmal zum Erlöschen der Garantie eines Geräts führen, was kostspielige Reparaturen nach sich ziehen kann, wenn etwas schiefgeht.

Medizinische Geräte haben einen langen Lebenszyklus. Wenn sie nicht sorgfältig mit der neuesten Version des Betriebssystems aktualisiert werden oder ein nicht unterstütztes Betriebssystem ausführen, können Hacker Schwachstellen ausnutzen, um Daten zu stehlen, ein Krankenhausnetzwerk zu infiltrieren und die Versorgung zu unterbrechen. Laut Fortune sind 83 % der mit dem Internet verbundenen medizinischen Bildgebungsgeräte – von Mammographie- bis hin zu MRT-Geräten – anfällig.

Je älter ein Gerät ist – insbesondere wenn sie über den Servicelebenszyklus hinausgehen –, desto wahrscheinlicher ist es, dass Kriminelle die Schwachpunkte kennen, mit denen sie über dieses Gerät auf das Netzwerk Ihres Unternehmens zugreifen können.

Windows 95 erhält beispielsweise seit Jahren keine Updates mehr und dennoch verlassen sich viele MRT-Geräte (unter anderem) immer noch auf dieses Betriebssystem, da es als letztes direktes Schreiben ermöglicht hat. Interne Entwickler können Schwachstellen zwar beheben, doch durch einen solchen Patch kann die Garantie für den Computer erlöschen. Die einzige sichere Option besteht darin, das MRT-Gerät vollständig zu ersetzen, aber das ist für viele Einrichtungen unerschwinglich.

Netzwerkadministratoren versuchen, nicht unterstützte Systeme vom Netzwerk fernzuhalten, aber das ist nicht immer möglich, insbesondere wenn Geräte für die Patientenversorgung benötigt werden und Ärzten schnell Daten bereitstellen müssen. Die Isolierung schlägt auch fehl, wenn nicht alle mit dem Netzwerk verbundenen Geräte bekannt sind, wodurch Backdoors entstehen. Was Sie nicht sehen können, können Sie nur schwer schützen.

So schützen Sie anfällige, nicht unterstützte Geräte

Um diese Geräte daran zu hindern, auf das Netzwerk Ihres Unternehmens zuzugreifen, ist der Umstieg auf eine Zero Trust Network Access-Architektur von entscheidender Bedeutung. Zero Trust Network Access ist ein Framework, das jede eingehende Anfrage als potenzielle Bedrohung behandelt, bis sie sich als sicher erwiesen hat. Angreifer werden effektiv gestoppt, bevor sie Zugriff auf das Gerät erhalten – selbst wenn Ihre Software veraltet ist.

Der Umstieg auf Zero Trust Network Access bedeutet einen grundlegenden Wandel vom alten Ansatz – bei dem jedem Gerät vertraut wurde, sobald es sich einmal im Netzwerk befand – hin zu einem Zero-Trust-Modell (erst prüfen, dann vertrauen). Während ein Zero-Trust-Ansatz wahrscheinlich keinen vollständigen Schutz vor Cyberangriffen bietet, begrenzt er den potenziellen Schaden von katastrophal auf überschaubar. HealthITSecurity sagt es am besten: „Wenn es einem Angreifer gelingt, Anmeldedaten zu stehlen und ein Gerät zu manipulieren, ist es mit einer Zero-Trust-Architektur unwahrscheinlich, dass er viel weiter kommt."

Akamai bietet einen zuverlässigen Plan, mit dem Dienstleister auf eine Zero-Trust-Architektur umsteigen können – ohne Ausfälle aktueller Workflows. Beginnen Sie noch heute mit Zero Trust Network Access – mit unserer Blaupause.

Bedrohung 3: Dienstleister im Homeoffice und BYOD

Die Patientenversorgung im 21. Jahrhundert ist dezentralisiert. Patienten werden heute oft bequem bei sich zu Hause betreut. Dienstleister versorgen sie über ihr Mobilgerät statt persönlich. Diese Zunahme der Verfügbarkeit bedeutet jedoch, dass die Cybersicherheitsrisiken für Dienstleister dramatisch zunehmen. Denn Mitarbeiter wechseln zwischen dem Netzwerkzugriff vor Ort und im Homeoffice und melden sich über nicht verwaltete Geräte an.

Während sich Ihre Teammitglieder vor der Pandemie nur gelegentlich über ihr Heimnetzwerk bei Ihrem System angemeldet hatten, hat die Anzahl persönlicher Geräte, die auf das Netzwerk Ihres Unternehmens zugreifen, während der Pandemie zwangsläufig zugenommen. Wenn diese Laptops, Tablets oder Smartphones mit Malware infiziert sind, könnten sie zu einem Einstiegspunkt für Ransomware-Angriffe werden.

Wenn z. B. eine Person aus Ihrem Team Opfer eines Phishing-Angriffs wird, indem sie versehentlich seine Anmeldedaten auf einer gefälschten Webseite eingibt, haben Cyberkriminelle denselben Zugriff wie dieser Nutzer. Und so können sie Dateien verschlüsseln, Ihr Team sperren und Ihr Unternehmen lahmlegen, indem sie ein hohes Lösegeld verlangen, um Ihre Dateien zu entschlüsseln.

So schützen Sie die Edge Ihres Netzwerks

Indem Sie genau überwachen, wer auf das Netzwerk Ihres Unternehmens zugreift (wo sich diese Nutzer befinden, wie ihre IP-Adresse lautet, welches Gerät sie verwenden usw.), können Sie die Wahrscheinlichkeit einer solchen Situation minimieren und Angriffe verhindern.

Wenn Ihr Team persönliche Geräte verwendet oder von zu Hause aus arbeitet, stellen Sie sich die folgenden Fragen:

- Verfügen wir über einen Zero Trust Network Access-Ansatz, um eingehende Anfragen möglichst genau zu prüfen und einen Angriff zu stoppen, bevor er auftritt?
- Haben wir Mikrosegmentierung implementiert, um den Zugang zu beschränken und laterale Netzwerkbewegungen zu verhindern, wenn ein Krimineller Zugang zum Unternehmensnetzwerk erhält?
- Verwenden wir ein SASE-Framework (Secure Access Service Edge), um unser Netzwerk zu schützen und gleichzeitig Latenzen zu minimieren und ein schnelles und angenehmes Nutzererlebnis zu gewährleisten?
- Verwendet unser Team Zugriffscodes, sichere und eindeutige Passwörter und Multi-Faktor-Authentifizierung (MFA) für jedes Gerät und jede Kontoanmeldung?

Mit unseren Sicherheitslösungen für Remote-Mitarbeiter erleichtert Akamai die Verwaltung des Netzwerkzugriffs.

Bedrohung 4: Schlechte Datenflussübersicht

Mit einer Kombination aus On-Premises und Cloud ist es fast unmöglich, herauszufinden, wo Ihre Daten gespeichert sind und wie sie durch Ihre Systeme fließen. Das hat verschiedene Gründe:

Zunächst einmal Volumen: Es kann überwältigend sein, mit der Anzahl der Geräte und Anwendungen Schritt zu halten, die täglich – wenn nicht stündlich – zum Netzwerk hinzugefügt und daraus entfernt werden, da Dienstleister, Auftragnehmer und Berater allesamt unterschiedliche Geräte, Tools und Lösungen verwenden.

Zweitens: Das System zur Nachverfolgung von Hardware und Software ist nicht mehr verfügbar und ist aufgrund von Fluktuation von Teammitgliedern, Prozessänderungen oder konkurrierenden Prioritäten nicht mehr genau oder zuverlässig.

Unabhängig vom Grund ist es wichtig, Ihr Netzwerk und die verbundenen Geräte zu visualisieren, da Sie nicht schützen können, was Sie nicht sehen.

So ordnen Sie den Datenfluss Ihrer verbundenen Geräte zu

Es ist von entscheidender Bedeutung, über ein Sichtbarkeitstool zu verfügen, mit dem eine Roadmap für vernetzte Geräte erstellt werden kann. Vor allem, da in einem Artikel im HIPAA Journal aus dem Jahr 2019 erwähnt wurde, dass 82 % der Gesundheitsorganisationen in den letzten 12 Monaten einen Cyberangriff auf ihre vernetzten Geräte erlebt hatten.

Die Wahl einer Lösung, die den Datenfluss in Ihrem Netzwerk verfolgt und Ihnen sagt, woher er kommt und wohin er geht – auch für Geräte, die nicht mit Ihrem Netzwerk verbunden sind –, ist der erste Schritt bei der Zuordnung Ihrer verbundenen Geräte. So erhalten Sie ein Echtzeitnetzwerkdiagramm davon, wie Informationen fließen, und können Geräte mit böswilligen Absichten erkennen, die sich möglicherweise in Ihrem Netzwerk befinden. Durch softwaredefinierte Mikrosegmentierungsringe um Kernsysteme, Assets und Daten (wie PHI) kann Ihr Unternehmen die lateralen Bewegungen von Angreifern innerhalb Ihres Netzwerks einschränken. Mit Mikrosegmentierungstools von Akamai erhalten Sie die erforderliche Transparenz.

Bedrohung 5: Bewältigung der Komplexität von Netzwerken, Anwendungen und Systemen

Wissen Sie, welche Anwendungen und Software Ihre Daten lesen können? Einige Softwareanwendungen, wie Social-Media-Plattformen, geben in ihren Datenschutzbestimmungen oder Nutzungsbedingungen deutlich an, wie invasiv sie sind. Andere, wie E-Mail-Anbieter, sind zwar unauffälliger, stellen aber dennoch ein erhebliches Risiko dar (z. B. Zugriff auf die Fotos eines Geräts, die PHI enthalten).

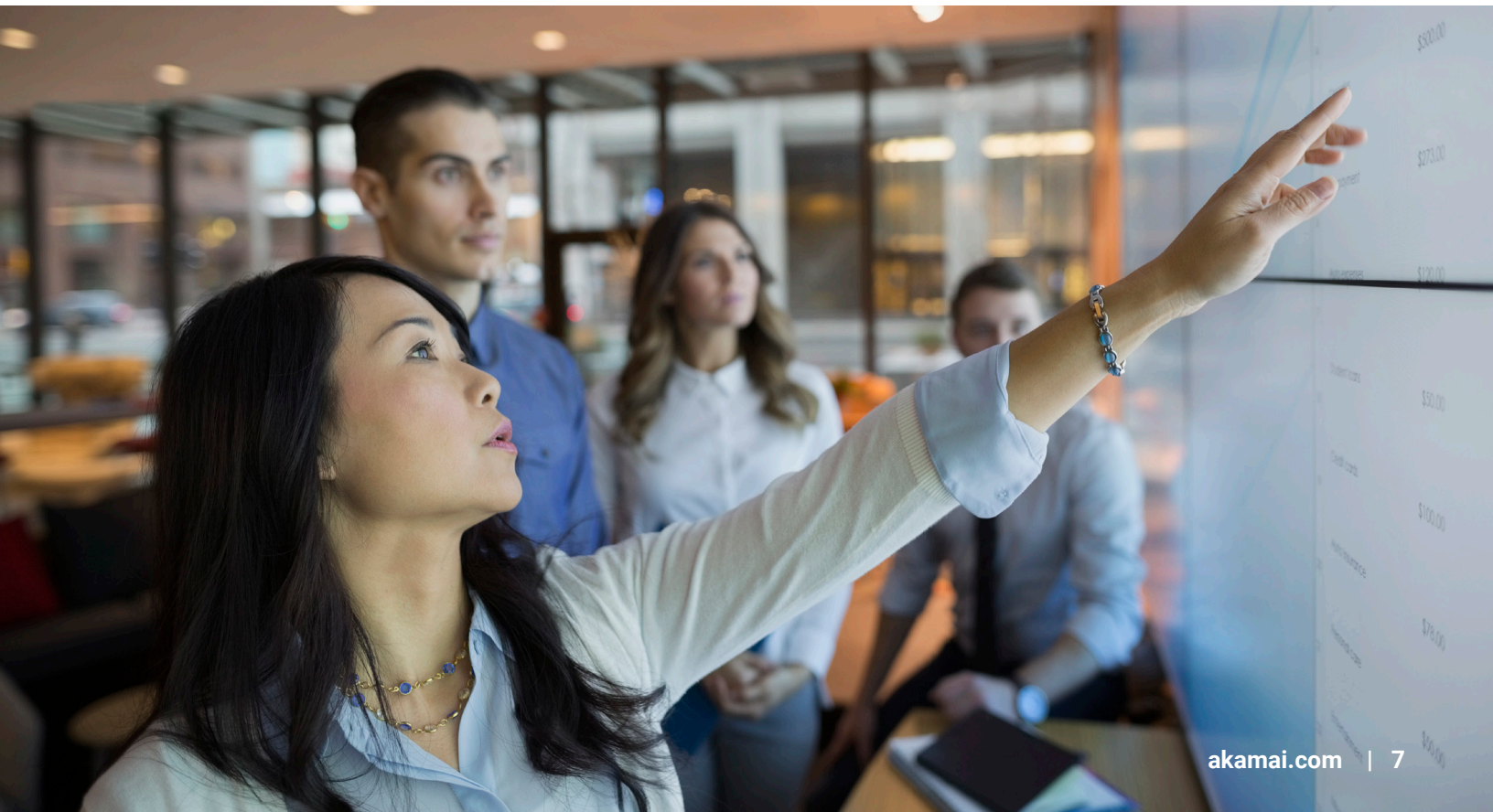
Anwendungen können möglicherweise auch Elemente anzeigen, die in die Zwischenablage kopiert wurden, z. B. Patienten-IDs oder Kennwörter. Wenn sich Patientendaten auf einem Gerät befinden, besteht die Möglichkeit, dass ein Drittanbieter (oder ein Cyberkrimineller) sie sieht (und aufzeichnet).

Schulen Sie Ihr Team, sehen Sie sich das gesamte Netzwerk an, schützen Sie Ihre Edge

Es ist von entscheidender Bedeutung, dass Sie alle Mitarbeiter Ihres Unternehmens über die Risiken der Verwendung persönlicher Geräte und über die Anforderungen informieren, die zum Schutz privater Patientendaten erforderlich sind.

Außerdem müssen Sie berücksichtigen, wie gut Ihr Unternehmen Einblick in Ihre Angriffsfläche und in potenzielle Vektoren hat. Überwacht Ihr Sicherheitsteam das gesamte Netzwerk über mehrere Cloudservice-Anbieter und On-Premises-Rechenzentren hinweg? Oder sind sie in verschiedene Gruppen und Silos unterteilt, die sich auf verschiedene Aspekte der Infrastruktur Ihres Unternehmens konzentrieren? Es ist unerlässlich, einen ganzheitlichen Überblick über das gesamte Netzwerk Ihres Unternehmens und dessen Aktivitäten zu erhalten, insbesondere während eines Angriffs.

Ähnlich wie bei Bedrohung 4 sind die besten Verteidigungsoptionen zum Schutz der Edge eine Zero-Trust-Architektur in Kombination mit Mikrosegmentierung und MFA für Kontoanmeldungen. Wenn Sie alle Systeme mit nur einem Anbieter schützen – unabhängig davon, von wem sie stammen und ob sie sich in der Cloud oder On-Premises befinden –, können Sie Ihr Netzwerk schützen, ohne das Nutzererlebnis zu beeinträchtigen.



Welche Auswirkungen hat es, wenn Sie nichts unternehmen?

Die Kosten können viele Formen annehmen. Am offensichtlichsten sind finanzielle Folgen: Laut dem IBM-Bericht „Cost of a Data Breach 2021“ erlitten Unternehmen des US-Gesundheitswesens insgesamt 9,23 Millionen US-Dollar an finanziellen Schäden für einen einzigen Datenschutzvorfall. Andere Kosten sind qualitativer Natur, darunter Patientensicherheit und Vertrauen. Diese Kosten sind in Gesundheitsorganisationen besonders wichtig.

Verringerte Patientensicherheit

Die Patientensicherheit ist das wichtigste Ziel der Cybersicherheit. Wenn IT-Systeme durch einen Angriff abgeschaltet werden müssen, wird die Patientenversorgung unterbrochen. Behandlungen und Termine werden verschoben, was für Patienten gesundheitliche Folgen haben kann. Tatsächlich war eine kürzliche Klage die erste Anschuldigung eines Patiententodesfalls, der direkt auf einen Ransomware-Angriff zurückzuführen war.

Gleichzeitig stellen vernetzte medizinische Geräte zur Fernüberwachung von Patienten (z. B. Herzfrequenz oder Blutzuckerspiegel) eine direktere Bedrohung für die Versorgung dar. Beispielsweise kann die Unterbrechung der Auslesung der Blutdruckwerte eines Patienten dazu führen, dass gefährliche Zustände unbemerkt und unbehandelt bleiben, was möglicherweise zu einem Sentinel Event führen kann.

Vertrauensverlust der Patienten

Die Unfähigkeit, eine zuverlässige Versorgung zu gewährleisten und Patientendaten zu schützen, führt zu einem Vertrauensverlust der Patienten. Mehr als 90 % der Patienten geben an, dass sie den Dienstleister wechseln würden, wenn ihre privaten Daten durch eine Datenschutzverletzung gefährdet würden. Die Zahl ist möglicherweise niedriger, wenn entsprechende Fälle tatsächlich eintreten, aber rechnen Sie selbst: Wenn nur die Hälfte dieser Patienten abwandern würde oder ein Zehntel, welche Auswirkungen hätte das auf Ihre Patientenpopulation? Und wie lange müssten Sie anhaltende Verluste erleiden, während Sie schrittweise neue Patienten gewinnen?

Umsatzverlust

Mit 38 % ist Umsatzverlust der größte Kostenfaktor, der mit einer Datenschutzverletzung verbunden ist. Wenn die zentralen Systeme der Dienstleister ausfallen (wie EHRs, E-Mail-Server usw.), kommt das Geschäft zum Erliegen. Das bedeutet keine Termine, keine Besuche und keine Einnahmen (ganz zu schweigen von den Auswirkungen auf die Patientenversorgung).

Scripps Health mit Sitz in San Diego erlitt im Mai 2020 einen großen Cyberangriff, der zu Umsatzverlusten in Höhe von 91,6 Millionen US-Dollar führte, hauptsächlich durch die Reduzierung von Notfallversorgung und elektiven Operationen.

Selbst wenn das Netzwerk Ihres Gesundheitssystems teilweise noch betriebsbereit ist, können Sie sich erst sicher sein, dass alles in Ordnung ist, wenn Sie den Vektor gefunden, die Schwachstelle gepatcht und die forensische Analyse abgeschlossen haben.

Erhöhter Overhead

Das Recruiting, die Einstellung und die Bindung begehrter Cybersicherheitstechniker ist teuer, doch die wahren Kosten gehen weit darüber hinaus. Wenn Sie in Ihrem Unternehmen ein internes Cybersicherheitsteam einsetzen, können hierdurch teure Sicherheitslücken entstehen.

Generell gilt: Je länger es dauert, bis Ihr Unternehmen einen Cyberkriminellen identifiziert und aus Ihrem Netzwerk wirft, desto höher sind die Kosten. Ein Bericht des Ponemon Institute besagt, dass die Erkennung eines Cyberangriffs innerhalb der ersten 200 Tage einem Unternehmen mehr als 1,26 Millionen US-Dollar einsparen kann. Leider dauert es laut demselben Bericht zufolge durchschnittlich 287 Tage, bis ein Angriff identifiziert und eingedämmt wird. *287 Tage!* Das bedeutet, dass sich Cyberkriminelle oft länger als neun Monate in der Netzwerkinfrastruktur befinden und ihre Angriffe planen, um den Ruf und das Geschäftsergebnis Ihres Krankenhauses maximal zu schädigen.

Es ist wichtig, die Zeit zu messen, die Ihr Sicherheitsteam benötigt, um einen Angriff zu identifizieren und entsprechende Maßnahmen zu ergreifen. Die Konsolidierung der Sicherheit bei einem Anbieter, der Managed Services und Engineering-Support für überlastetes Personal bereitstellt, kann erhebliche Kosteneinsparungen bedeuten.

Strafen für die Nichteinhaltung von Bestimmungen

Da sich viele wertvolle personenbezogene Daten in Ihrem Besitz befinden, könnte eine Datenschutzverletzung zu hohen Strafen durch Aufsichtsbehörden führen. Bis zum 30. November 2021 hat das Office of Civil Rights des Health and Human Services Department Sanktionen gegen 106 HIPAA-Unternehmen in Höhe von insgesamt mehr als 131 Millionen US-Dollar beschlossen oder verhängt. Das sind durchschnittlich mehr als 1,2 Millionen US-Dollar pro Strafe (zusätzlich zu den hier genannten zusätzlichen Kosten).

So bereiten Sie Ihre Gesundheitsorganisation am besten auf einen Cyberangriff vor

Moderne Cyberbedrohungen erfordern branchenführende Sicherheit für Dienstleisterunternehmen. Ihre Patienten und Ihr Unternehmen sind darauf angewiesen: Wenn Sie nichts tun, sind die Kosten einfach zu hoch.

Finanzielle Engpässe, konkurrierende Prioritäten oder Unsicherheit hinsichtlich der Risiken könnten Sie dazu bringen, ein zu hohes Risiko einzugehen. Doch Ihre Sicherheitsmaßnahmen müssen gründlich, strategisch, wachsam und agil sein.

Nur weil ein Ökosystem heute angemessen geschützt ist, heißt das nicht, dass es auch morgen geschützt sein wird. Bedrohungen entwickeln sich schnell. Ein Tag (oder weniger) kann ausreichen, bis Cyberkriminelle eine neue Schwachstelle ausnutzen.

Gesundheitsdienstleister, die diesen Bedrohungsbereich verringern und den im Sicherheitsratgeber dargelegten Backup-Ansatz umsetzen möchten – drei Kopien in mindestens zwei verschiedenen Formaten speichern, wobei eine Kopie offline bleibt –, suchen zunehmend nach einem hybriden Ansatz. Die Datenspeicherung vor Ort bietet ihnen zwar mehr Kontrolle über die Sicherheit, kann aber kostspielig sein. Außerdem kann es schwierig werden, sie mit dem erforderlichen Tempo voranzutreiben, insbesondere angesichts der aktuellen explosionsartigen Zunahme der Menge an Gesundheitsdaten und der digitalen Transformation in der Pflege, die durch die Pandemie noch verstärkt werden. Die Datenspeicherung in der Public Cloud ist kostengünstiger, doch Unternehmen riskieren Ausfälle und mangelnde Transparenz in Bezug auf den Schutz der Daten.

Ein hybrider Ansatz ermöglicht die Speicherung sensibler Daten vor Ort, während die weniger sensiblen Daten in der Cloud gespeichert werden. Auch das ist keine perfekte Lösung, da Schutzmaßnahmen geschaffen werden müssen, um die Übertragung der Daten zwischen den beiden Speicherarten abzusichern und zu gewährleisten, dass nur diejenigen auf die Daten zugreifen können, die berechtigt sind, die Übertragung durchzuführen und die Daten anzuzeigen. Der Übergang zu den sieben wichtigsten Anforderungen für die Implementierung einer Zero Trust Network Access-Architektur hilft Institutionen, ihre Daten zu schützen, indem sie Nutzern nur Zugriff auf die Anwendungen gewähren, die sie für ihre Rolle benötigen. Und durch MFA wird die Sicherheit weiter gesteigert.

Mit Akamai sind Sie optimal vorbereitet, wenn – nicht falls – ein Angriff stattfindet. Gemeinsam erstellen wir einen einheitlichen Überblick über Ihr Netzwerk, um Angriffe schnell zu erkennen und den Schaden effizient zu mindern. Unser Unternehmen beruht auf dem Schutz von Netzwerken vor DDoS- und Ransomware-Angriffen, um nahtlose, sichere Weberlebnisse bereitzustellen (einschließlich Anwendungen und APIs).

Wir stärken die Edge Ihres Netzwerks, um die Wahrscheinlichkeit einer Sicherheitsverletzung zu begrenzen und den Explosionsradius zu reduzieren, wenn doch eine Sicherheitsverletzung auftritt. Und hierbei behalten wir die Flexibilität für den Nutzerzugriff bei, damit sich Ihr Unternehmen angesichts immer neuer Betriebs- und Pflegeanforderungen auf die Bereitstellung optimaler Gesundheitsergebnisse konzentrieren kann.

Der Schutz von Patientendaten vor immer komplexeren Cyberangriffen und einer wachsenden cloudbasierten Angriffsfläche war noch nie so wichtig wie heute. Patientenorientierte Organisationen und Behörden vertrauen auf die Edge-Plattform von Akamai, um ihre digitalen Erlebnisse näher an Patienten zu bringen – und Bedrohungen fernzuhalten.

Vertrauen Sie Akamai, dem Partner, der Cybersicherheit von einer permanenten Belastung zu einem Wettbewerbsvorteil macht.

Kontaktieren Sie uns, um mehr zu erfahren, oder rufen Sie uns an unter +49 89 94006 308.

Akamai

Power und Sicherheit für das digitale Leben – mit Akamai. Die innovativsten Unternehmen weltweit setzen bei der Bereitstellung und beim Schutz ihrer digitalen Erlebnisse auf Akamai und unterstützen so täglich Milliarden von Menschen in ihrem Alltag, bei der Arbeit und in ihrer Freizeit. Mit der weltweit größten und zuverlässigsten Edge-Plattform bringt Akamai Anwendungen, Code und Erlebnisse ganz nah an die Nutzer – und hält dabei Bedrohungen fern. Möchten Sie mehr über die Produkte und Services von Akamai für Sicherheit, Content Delivery und Edge Computing erfahren? Dann besuchen Sie uns unter www.akamai.com und blogs.akamai.com oder folgen Sie Akamai Technologies auf X und LinkedIn. Veröffentlicht: 02/22.