privilegierten Zugriffe nicht zu überwachen, würde große Sicherheitsrisiken bedeuten.

Eine weitere essenzielle Maßnahme, um das Missbrauchsrisiko zu minimieren und widerstandsfähiger zu werden, ist das Einschränken von Zugriffen nach dem Just-in-Time-Prinzip. Das bedeutet, dass Zugriffe nur ein einem eng begrenzten und für den jeweiligen Benutzer definierten Zeitraum, und niemals dauerhaft, gewährt werden. Viel zu viele Unternehmen halten Privilegien viel zu lange aufrecht, versäumen es, Passwörter und Konten auslaufen zu lassen und Privilegien zu löschen, wenn diese nicht mehr gebraucht werden, z.B. wenn Projekte enden oder Mitarbeiter ausscheiden. Das Gewähren von dauerhaftem privilegiertem Zugriff verstößt gegen das Least Privilege-Prinzip und birgt unkontrollierbare Risiken. Deshalb empfiehlt sich der Einsatz von PAM-Lösungen, die es Unternehmen ermöglichen, privilegierten Zugriff in Echtzeit oder aber nur bei Bedarf zu gewähren.

Die eigenen Cloud-Verantwortlichkeiten im Blick behalten

Bei der Absicherung der Cloud ist es zudem wichtig, die eigenen Verantwortlichkeiten genau zu kennen. Viele Unternehmen sind sich nicht bewusst, dass die meisten Cloud-Fehlkonfigurationen und inkonsistenten Kontrollen rechtlich gesehen die Schuld des Nutzers sind, nicht die des Cloud-Anbieters. Nur in seltenen Fällen kann es zu einer Mithaftung kommen, so dass es auch im Interesse des Cloud-Anbieters liegt, ihren Kunden bei der Umsetzung von Security-Best-Practices zu helfen. Die Hauptverantwortung liegt jedoch tatsächlich auf den Schultern des Unternehmens. Sie müssen dafür sorgen, dass Zugriffe und Berechtigungen für jede Identität und jedes System, das mit Cloud-basierten Systemen interagiert, angemessen verwaltet und geschützt werden.

Zu diesen Systemen können kritische Anwendungen oder Datenbanken gehören, die in der Cloud gespeichert sind, Plattformen für die Anwendungsentwicklung oder Tools, die von den Business- oder Technik-Teams verwendet werden. Unter Berücksichtigung dessen sollte der Cloud-Zugriff mit denselben PAM-Richtlinien, -Prozessen und -Lösungen, die für das gesamte Unternehmen verwendet werden, eingebunden und geprüft werden.

Dabei müssen die Unternehmen auch Veränderungen im Blick haben und in ihre Sicherheitsstrategie einplanen. Das zeigt auch der vermehrte Einsatz von Cloud-Services: So nutzen Unternehmen heute durchschnittlich etwa 2.000 Cloud-Dienste und damit bereits 15 Prozent mehr als noch im letzten Jahr, was hauptsächlich auf das Wachstum von SaaS zurückzuführen ist.

So schnell digitale Transformationsprojekte derzeit an Tempo gewinnen, so gut kann PAM hier helfen. In DevOps-Unternehmen, in denen eine breite Palette

an Cloud-Ressourcen kontinuierlich und in großem Umfang erstellt, verwendet und wieder lahmgelegt wird, unterstützt PAM durch die Automatisierung der schnellen Erstellung, Archivierung, Abfrage und Rotation von Secrets.

Fazit

In Zeiten einer verschärften Bedrohungslandschaft und zunehmender Cyber-Angriffe kann PAM die Arbeit von IT- und Security-Abteilungen erheblich vereinfachen. So verschafft PAM nicht nur einen besseren Überblick über hybride On-Premises- und Multi-Cloud-Umgebungen, Daten und Infrastrukturen sowie Privilegien im Allgemeinen. Ein gut durchdachtes PAM ermöglicht es auch, granulare Kontrollen, die eine kontinuierliche Authentifizierung und sichere Autorisierung unterstützen, über verschiedene Umgebungen hinweg einzurichten und umzusetzen. Gleichzeitig sorgt eine starke PAM-Strategie für eine klarere Auditierbarkeit, indem sie die Einhaltung von Vorschriften und Compliance erleichtert.

Inmitten der ständigen Transformation, die durch Covid-19 noch stärker vorangetrieben wird, und die den Einsatz von immer mehr Cloud-Diensten forciert, kann PAM Unternehmen eine zusätzliche wertvolle Sicherheitsebene bieten. Indem präzise gesteuert wird, was Benutzer in Cloud-Plattformen, -Diensten und -Anwendungen sehen und tun können, können Unternehmen die Angriffsfläche reduzieren und letztlich die Herausforderungen der Cloud-Sicherheit meistern.

Stefan Schweizer

1.7 USE CASES

Gesundheitswesen: Wie Unternehmen ihre Cybersecurity während der schnellen Digitalisierung sicherstellen

Das Gesundheitswesen befindet sich schon seit einiger Zeit inmitten der digitalen Transformation – die COVID-19 beschleunigt den Einsatz von Cloud-Services und digitalen Tools zusätzlich. Eine weitere Veränderung der Branche: Immer mehr digital native sogenannte „Health-Tech“-Unternehmen drängen auf den Markt und ermöglichen die Digitalisierung gesundheitlicher Dienstleistungen.

Die Vorteile der digitalen Transformation sind in der Branche unumstritten, dennoch wird gerade das Gesundheitswesen immer mehr zum Angriffsziel von Cyber-Attacken. Besonders in diesem Bereich können Cyber-Angriffe gravierende Folgen haben: Neben den Auswirkungen auf das angegriffene Unternehmen oder Institution, können ebensolche Attacken im Zweifelsfall

zu Verzögerungen bei der medizinischen Versorgung oder gar zum Verlust von Menschenleben führen.

Seit Beginn der COVID-19-Pandemie ist das Gesundheitswesen noch stärker in den Fokus der Hacker gerückt, um die anfällige Phase gezielt auszunutzen. Ein Beispiel aus den USA: Das U.S. Department of Health and Human Services berichtete vor Kurzem einen Anstieg von 50 Prozent bei den Verstößen gegen die Cybersecurity von Krankenhäusern und Netzwerken von Gesundheitsdienstleistern – dies deutet auf eine verstärkte Ausrichtung auf die Gesundheitsbranche hin. In Düsseldorf legte im September 2020 ein Ransomware Angriff das Universitätsklinikum lahm und führte zum Tod einer Patientin.

Die IT-Systeme des Gesundheitswesens sind einem erhöhten Sicherheitsrisiko ausgesetzt, denn immer mehr Endanwender setzen auf Technologien wie Telemedizin oder spezielle Gesundheits-Apps – und teilen damit sensible, persönliche Daten. Darüber hinaus besteht ein Großteil der medizinischen Infrastruktur aus veralteten und heterogenen Systemen mit offensichtlichen Sicherheitseinschränkungen.

Aber auch die Branche selbst ist ein attraktives Ziel für Cyber-Angriffe: Gesundheitsdienstleister bieten vermehrt Telemedizin, Apps, Services und vernetzte Endgeräte an und generieren damit große Datenmengen an sogenannten Protected Health Information (PHI). Diese sensiblen Daten werden im Dark Web hoch gehandelt. Und auch hochwertige Assets wie die Forschung und Entwicklung von Impfstoffen sind wertvolle Ziele für kommerzielle und politische Zwecke.

Das Gesundheitswesen ist ohne Zweifel systemrelevant und eine kritische Dienstleistung. Sowieso schon am Anschlag müssen Gesundheitsorganisationen und Dienstleister mitten in der Pandemie ihre Sicherheit verbessern und die Cybersecurity stärken. Während die meisten Cybersicherheitslösungen branchenunabhängig sind, gibt es bestimmte Nuancen, die die Gesundheitsbranche berücksichtigen muss.

IT-Hygiene

Organisationen des Gesundheitswesens müssen einen „Null-Toleranz-Ansatz“ in Sachen IT-Hygiene verfolgen und dabei für die notwendigen Systeme und Steuerung beim Risikomanagement von Dritten sorgen. Dabei müssen die vorhandenen Richtlinien für Hochrisikosysteme wie Lebenserhaltungssysteme oder sensible Assets wie Impfstoffversuche drastisch verschärft werden.

Organisationen sollten sich strikt an die Software- und Hardware-Security halten, indem sie etwa für aktuelle Anwendungen und Betriebssysteme sorgen, veraltete oder nicht unterstützte medizinische Geräte austauschen und Sicherheitsmaßnahmen für remote vernetzte Geräte implementieren.

Zero Trust-Modell

Mit der zunehmenden Verbreitung der Telemedizin und der vermehrten Remote-Arbeit von Fachkräften im Gesundheitswesen reicht es nicht mehr aus, ausschließlich die Sicherheit der Perimeter zu gewährleisten – vielmehr benötigen Unternehmen neue, belastbare Modelle, die an die neue Umgebung angepasst sind.

Organisationen des Gesundheitswesens sollten generell nur limitiert Privilegien vergeben. So erhalten beispielsweise ausschließlich Personen Zugriff auf Daten, die sie für die Erledigung ihrer Aufgaben benötigen. Darüber hinaus sollten nur notwendige Anwendungen für den Remote-Zugriff freigegeben werden. Mithilfe von Netzwerksegmentierung können Firmen außerdem sicherstellen, dass geschäftskritische Systeme – etwa zur Lebenserhaltung oder für Forschung und Entwicklung – vom restlichen IT-Setup separiert sind.

Datensicherheit

Unternehmen sollten sich auf Datenminimierung konzentrieren. Auf diese Weise werden nur unbedingt notwendige Daten gesammelt, verarbeitet und (wenn möglich) anonymisiert. Um die Sicherheit sensibler Daten wie PHI sowie Forschungs- und Entwicklungs-Assets sowohl im Ruhezustand als auch bei der Übertragung zu gewährleisten, müssen Unternehmen automatisierte Systeme zur Datenidentifizierung und -klassifizierung sowie zur Vermeidung von Datenverlusten aufbauen.

Die Gesundheitsbranche muss zudem auch strengere Datenzugriffskontrollen einführen. Diese beschränken den Zugriff nur auf die Einzelperson und den Gesundheitsdienstleister sowie gegebenenfalls auf eine Regierungsbehörde, um die kommunale Gesundheitsversorgung wie im Fall von COVID-19 zu verwalten. Hochentwickelte Verschlüsselungsstandards sowie Data Masking-Lösungen und regelmäßige Kontrollen gewährleisten darüber hinaus, dass nur autorisierte Benutzer Zugriff erhalten.

Secure by Design

Moderne Unternehmen müssen sicherstellen, dass Cybersecurity bereits in der Entwicklungsphase berücksichtigt wird (Security by Design) und nicht erst im Nachhinein. Dies erfordert die Etablierung sicherer Kodier-Richtlinien und die Einführung von Praktiken wie DevSecOps.

Ebenso ist ein fortlaufendes Compliance-Management mit Echtzeit-Patching und Fokus auf Bedrohungen, Schwachstellen, Risiken und Vorfällen essenziell. Auch die Mitarbeiter müssen involviert werden: Nur mit einem fundierten Verständnis und Sensibilität für IT-Security können Mitarbeiter Sicherheitsrisiken intuitiv entschärfen – eine starke Security-Unternehmenskultur rundet dies ab.

Vishal Salvi,
Chief Information
Security Officer &
Head of Cyber
Security Practice,
Infosys

Compliance und Risk Management

Das Ökosystem des Gesundheitswesens besteht aus einer Vielzahl von Partnern und Anbietern innerhalb der Wertschöpfungskette. In dieser vernetzten – aber ungleichen – Struktur muss jeder Beteiligte individuell für Cybersecurity sorgen.

Unternehmen müssen effektive Partner-Risikomanagement-Programme entwickeln und implementieren, um Daten zu sichern und vor Cyberangriffen zu schützen. Dies kann durch eine Bewertung der Sicherheitslage von Partnern erreicht werden, gefolgt von einer risikobasierten Partnersegmentierung sowie der Definition an „Zero-Trust“-Prinzipien in Sachen Konnektivität und Zugriffsmanagement für Partner.

Managed Detection and Response

Die Cyber-Bedrohungslandschaft entwickelt sich stetig weiter. Dies führt dazu, dass fast jeden zweiten Tag neue Bedrohungen auftauchen. Daher ist ein gut definiertes Playbook für die schnelle Erkennung von Bedrohungen und Sicherheitsverletzungen und die Reaktion darauf entscheidend.

Organisationen des Gesundheitswesens müssen KI-Systeme mit Machine Learning und Verhaltensanalysen einsetzen, um Anomalien und Bedrohungen proaktiv zu erkennen und schnelle Sandboxing- und Wiederherstellungsprozesse zu entwickeln. Nur dann können sie sich „cyber-resilient“ (widerstandsfähig) aufstellen und schützen.

Vishal Salvi

Cyber-Risiko Lieferkette: Warum die Cybersecurity Ihrer Partner auch Ihre Angelegenheit ist

Die Zahl der Cyberangriffe auf Industrieanlagen aller Größenordnungen nimmt seit Jahren deutlich zu. Dabei erstreckt sich das Risiko über die gesamte Lieferkette. Eine Studie mit 150 Cybersecurity- und IT-Fachleuten in mittelständischen und großen Unternehmen der Fertigungsindustrie hat unlängst gezeigt, dass jede zweite OT-Infrastruktur für Cyberangriffe anfällig ist. 53 Prozent der Befragten gaben zudem an, dass ihr Unternehmen in den letzten 12 bis 24 Monaten bereits von einem Cyberangriff oder einem anderen Sicherheitsvorfall betroffen war, der auch die OT-Netzwerke beeinträchtigte.

Moderne Lieferketten sind längst komplizierte, miteinander verflochtene Partnernetzwerke. Und wenn ein Partner kompromittiert wird, hat dies Auswirkungen auf alle Partner in der Lieferkette. Die Auswirkungen eines Angriffs auf einen First-Tier-Lieferanten können dabei genauso verheerend sein, wie ein Angriff auf die eigenen Systeme: Ganze Produktionslinien können ausfallen, was erhebliche Kosten verursacht, sich negativ auf den Umsatz auswirkt und den Ruf

des Unternehmens schädigt.

Seit Jahren nutzen Angreifer Schwachstellen in der Lieferkette als Sprungbrett, um andere Unternehmen zu infiltrieren. Vielleicht erinnert sich so mancher noch an den Datenvorfall beim US-amerikanischen Handelsunternehmen Target vor knapp zehn Jahren. Hier haben Angreifer gestohlene Zugangsdaten eines Klimaanlage-Herstellers genutzt, um auf das Netzwerk von Target zuzugreifen und sich lateral zu bewegen. Das Ergebnis: Millionen gestohlener Kundendaten, inklusive Zahlungsinformationen. Ein paar Jahre später sahen wir mit der Ransomware NotPetya einen weiteren hochkarätigen Angriff auf die Lieferkette, der zunächst Software einer ukrainischen Buchhaltungsfirma infizierte. Im weiteren Verlauf wurden multinationale Unternehmen getroffen und es entstand ein geschätzter Gesamtschaden von 10 Milliarden US-Dollar. Und erst kürzlich ermöglichte die Kompromittierung der SolarWinds Orion-Software und die SUNBURST-Backdoor Angreifern den Zugang zu zahlreichen Unternehmen und Behörden auf der ganzen Welt. Das Ausmaß und die Auswirkungen dieses Angriffs sind derzeit noch nicht abzusehen.

Maßnahmen der Industrie

Cybersicherheit in der Lieferkette wird mittlerweile als bedeutendes Thema von Führungskräften und Sicherheitsverantwortlichen in (nahezu) allen Branchen wahrgenommen. Entsprechend ergreifen Behörden, Branchenverbände und Regulierungsbehörden Maßnahmen, um das Risiko zu minimieren. Als ein Impfstoff für COVID-19 in greifbare Nähe rückte, gab IBM eine Warnung vor unbekannten Bedrohungsakteuren heraus, die auf die Lieferkette für den Impfstoff COVID-19 zielen. Die Security-Experten wiesen dabei besonders auf die gestiegenen Fähigkeiten von Angreifern sowie die Dringlichkeit und Schwere des Lieferketten-Risikos hin und mahnten, die Gefährdung von OT-Umgebungen zu reduzieren. Ab Juli 2024 werden neue Cybersecurity-Vorschriften für die Automobilindustrie für alle in der Europäischen Union produzierten Neufahrzeuge verpflichtend sein. Entsprechend sind derzeit neue Cybersicherheitsstandards zur Etablierung von „Cybersecurity by Design“ über den gesamten Lebenszyklus eines Fahrzeugs in der Entwicklung.

Was Sicherheitsverantwortliche tun können

Cyber-Risiken in der Lieferkette sind kompliziert und erstrecken sich über den gesamten Lebenszyklus eines Produkts – von der Entwicklung über die Herstellung, den Vertrieb und die Lagerung bis hin zur Wartung. Je umfangreicher und komplexer der Lebenszyklus ist, desto mehr Angriffsmöglichkeiten und Chancen, ein schwaches Glied in der Kette zu finden und auszunutzen, gibt es. Und da Lieferketten oft global sind und mehrere Ebenen von Lieferanten umfassen, liegt

Yaniv Vardi,
CEO,
Claroty