Absicherung von Gesundheitsanbietern mit Proofpoint

Schutz von Menschen, Prozessen und Patientendaten

Die Zahl der Cyberangriffe auf das Gesundheitswesen nimmt immer weiter zu. Streng vertrauliche Patientendaten können finanziell äußerst lukrativ sein, was die entsprechenden Unternehmen zu einem attraktiven Ziel für Angreifer macht. Die COVID-19-Pandemie hat diese Branche noch angreifbarer gemacht. Heute müssen Ärzte und nicht-klinisches Personal die Patientenbetreuung verstärkt remote durchführen, was die Anfälligkeit für Cyberbedrohungen weiter verstärkt. Proofpoint kann Ihnen helfen. Unsere Lösungen für Cybersicherheit und Compliance schützen Sie, Ihre Mitarbeiter und Ihre Patienten.

Telemedizin und Home Office-Optionen sind leistungsfähige Hilfsmittel, die dem medizinischen Personal die Patientenversorgung erleichtern. Doch diese neuen Arbeitsmöglichkeiten öffnen Cyberbedrohungen Tür und Tor. Dadurch können medizinische Daten kompromittiert, die Patientenversorgung unterbrochen oder Patienten gefährdet werden.

Gesundheitseinrichtungen betrachten die Cybersicherheit mittlerweile als Problem für die Sicherheit der Patienten, das die Aufgabe des Gesundheitswesens grundlegend gefährdet. Ebenso wie viele Unternehmen in verschiedensten Branchen haben auch Gesundheitsanbieter in herkömmliche Sicherheitstools für den Schutz des Perimeters investiert. Diese Tools können hochentwickelte Bedrohungen, die medizinische Daten gefährden, weder erkennen noch abwehren.

Zudem sind Bedrohungen äußerst wandlungsfähig. Die Gesundheitsbranche hat den herkömmlichen Netzwerk-Perimeter hinter sich gelassen – und die Angreifer sind ihr gefolgt. Die Bedrohungen sind jedoch nicht nur beweglich, sondern nehmen auch andere Formen an und wählen neue Ziele aus. Jede Person in Ihrer Gesundheitseinrichtung stellt ein eigenes Sicherheits- oder Compliance-Risiko dar, das durch die zugänglichen Daten sowie die berufliche Technologienutzung bestimmt wird.

Krankenschwestern haben umfassenden Zugriff auf Patientendaten, was sie für Cyberangreifer besonders attraktiv macht. Klinische Forscher können auf wertvolles geistiges Eigentum zugreifen, was ihre Gefährdung erheblich steigert. Krankenhausmitarbeiter in der Lieferkette interagieren hingegen regelmäßig mit verschiedensten externen Systemen, sodass sie besonders von Bedrohungen betroffen sind. Bedrohungen wie Anmeldedaten-Phishing gewähren den Angreifern Zugriff auf viel mehr als nur E-Mail-Konten. Die Daten in der Cloud stellen den eigentlichen Schatz dar – und werden zudem von herkömmlichen Sicherheitstools nicht abgedeckt. Medizinisches Personal, Patienten, Ärzte und andere sind diesen personenorientierten Angriffen schutzlos ausgesetzt.

Wir dürfen jedoch nicht vergessen, dass Gesundheitsunternehmen gleichzeitig beliebte Ziele für Ransomware und andere Malware-Angriffe sind. Die Zahl dieser Bedrohungen ist zwar zurückgegangen, dafür erfolgen die Attacken zielgerichteter. Mehr als je zuvor müssen Unternehmen daher dieser Gefahr mit einem kombinierten Ansatz begegnen, der Technologie und Schulungen verbindet.

Cybersicherheitsprobleme im Gesundheitswesen

Bei der Suche nach innovativen Ansätzen für die Patientenbetreuung stehen Gesundheitsunternehmen vor neuen Herausforderungen. Schließlich geht es darum, weder das Unternehmen noch die Klinikmitarbeiter oder die Patienten zu gefährden. Die Herausforderungen für die IT- und Sicherheitsverantwortlichen im Gesundheitswesen im Jahr 2021 und darüber hinaus sind erheblich komplexer. Dadurch wird es für Gesundheitseinrichtungen noch schwieriger, eine sichere Umgebung für die digitale Gesundheitsversorgung zu schaffen.

Wechsel zu sicheren neuen Pflegemodellen

Die Angriffsfläche ist durch Gesundheits-Apps für Mobilgeräte, Telemedizin und das Internet of Things (IoT, Internet der Dinge) gewachsen. Kunden von Gesundheitsleistungen nutzen verschiedenste Mobile-Health-Anwendungen, medizinische Wearable-Geräte sowie medizinische Technologien für den Einsatz zu Hause. Klinikpersonal bringt private Geräte mit auf Arbeit und nutzt unternehmenseigene Geräte zu Hause. Gleichzeitig lassen neue Technologien die Grenze zwischen klinischen und privaten Umgebungen verschwimmen, was die Komplexität weiter steigert. Dies führte zu einer dezentralisierten und Perimeter-losen IT-Infrastruktur, deren Absicherung erheblich schwieriger ist.

Datenspeicherung und Datensicherung

Die Absicherung des Arzt-Patient-Verhältnisses ist ein wichtiger Teil der Gesundheitsversorgung. Wenn die Daten bei externen Parteien ungeschützt gespeichert oder unverschlüsselt versendet werden, kann es zur Kompromittierung von Patientendaten kommen. Während alle Gesundheitsunternehmen angeben, dass sie vertrauliche Daten erfassen, speichern und weitergeben, werden diese Daten nur bei 38 % verschlüsselt.[1]

Cloud-Sicherheit

In der Gesundheitsbranche sind die zahlreichen Vorteile von Cloud Computing, standardisierten Anwendungen, nutzungsabhängigen Zahlungsmodellen und reduziertem Kapitalaufwand durchaus bekannt. Doch wegen der wahrgenommenen Risiken von Cloud-Diensten wurden Cloud-Angebote nur zögerlich angenommen. Das ändert sich gerade. Sicherheitsverantwortliche in Gesundheitsunternehmen kennen die Vorteile von Cloud-Lösungen und suchen nach Produkten, die Compliance-Vorgaben einhalten und den Datenschutz sowie die Transaktionsintegrität gewährleisten. Zudem legen sie Wert auf Lösungen, die sich anpassen lassen, um Cloud-Anwendungen von Geschäfts- und Logistikpartnern zu schützen.

Gleichzeitig nutzen viele Gesundheitsanbieter weiterhin veraltete Systeme, da einige Komponenten proprietär sind und den Wechsel zu Cloud-Diensten nicht gestatten. Dies führt zu weiteren Risiken, da Kriminelle immer neue Schwachstellen zur Verbreitung von Malware finden. Dazu gehören Ransomware-Angriffe, die ein ganzes Unternehmen lahmlegen können.

Absicherung der Lieferkette

Der Geschäftsbetrieb von Gesundheitsanbietern ist von verschiedensten externen Lieferanten, Partnern und Geschäftsbeziehungen abhängig. Diese voneinander abhängigen Verbindungen bilden ein komplexes Drittanbieter-Ökosystem, das keinen Schutz vor Diebstahl und neuen Cyberrisiken bietet. Neue Einfallstore für Bedrohungsakteure können die gesamte Lieferkette des Krankenhauses kompromittieren. Das Sprichwort, wonach eine Kette nur so stark wie ihr schwächstes Glied sein kann, ist heute im Gesundheitswesen so relevant wie nie zuvor. Wenn eine einzige Schwachstelle in der Lieferkette eines Krankenhauses infiltiert und anschließend zum Exfiltrieren vertraulicher Daten missbraucht wird, können die Verluste verheerend sein.

Neue Cyberbedrohungen für das Gesundheitswesen

Durch den wachsenden Wert medizinischer Informationen werden Gesundheitsanbieter zu einem attraktiven Ziel. Deshalb müssen Sie Ihre Schutzmaßnahmen stärken und davon ausgehen, dass die Branche von Akteuren wie staatlich unterstützten Angreifern und Hackern attackiert wird. Einfache Viren und Malware sind Geschichte. Die schwerwiegendsten Cyberangriffe werden von den Akteuren gezielt gegen Menschen gerichtet, wobei strategische Einfallstore langfristig ausgekundschaftet werden. In ihrer Gesamtheit können sie großen Schaden anrichten. Tatsächlich dauert die Erkennung von Datenschutzverletzungen bei Gesundheitsunternehmen am längsten – im Durchschnitt ganze 329 Tage.[2]

1 Thales Data Threat Report (Thales-Bericht zu Datenbedrohungen), 2019

2 „2020 Cost of a Data Breach Report from IBM Security“ (Bericht zu den Kosten von Datenkompromittierungen 2020, von IBM Security), Ponemon Institute

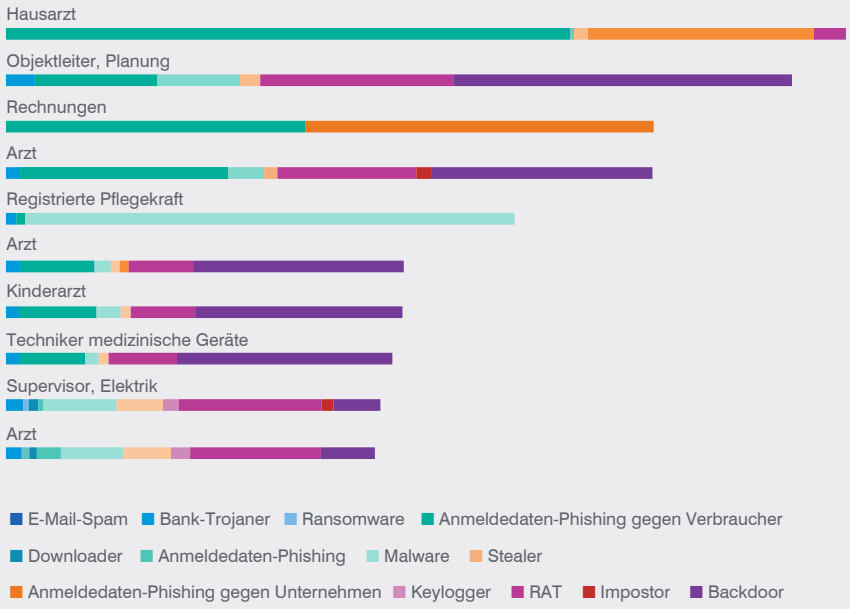

Abb. 1: Aufschlüsselung der Very Attacked People in einem bekannten Kinderkrankenhaus

Ein personenorientierter Ansatz

Heutige Cyberangriffe richten sich nicht gegen Technologien, sondern gegen Menschen. Aus diesem Grund müssen Gesundheitsanbieter für die Absicherung ihrer Klinikmitarbeiter und sonstigen Angestellten sowie der vertraulichen Daten, die sie nutzen und teilen, einen personenorientierten Ansatz implementieren. Klinische Arbeit erfordert volle Konzentration auf die optimale Patientenbetreuung, häufig auch unter Zeitdruck, sodass die Überprüfung von E-Mails nicht immer die erforderliche Aufmerksamkeit erhält. Dies ist einer der Gründe dafür, dass die Branche ein leichtes Ziel für schädliche Aktivitäten bleibt, zumal erfolgreiche Angriffe enorm lukrativ sein können.

Gleichzeitig müssen Gesundheitsunternehmen die strengen Anforderungen der EU-Datenschutzgrundverordnung einhalten, da sie genetische, biometrische und medizinische Daten verarbeiten und speichern. Diese Datenkategorien sind in der Liste der Kategorien enthalten, die besonders strenge Kontrollen erfordern. Für den Schutz dieser Daten müssen Unternehmen ausreichende Sicherheitskontrollen implementieren, um nicht nur Geldstrafen zu vermeiden, sondern auch den Patientendatenschutz zu gewährleisten.

In unserem Bericht „Bedrohungslandschaft im Gesundheitswesen“ von 2020 untersuchen wir die sogenannten Very Attacked People™ (VAPs) im Gesundheitswesen. Damit bezeichnen wir die Anwender in einem Unternehmen, die am häufigsten mit Cyberbedrohungen angegriffen werden. Abb. 1 zeigt ein Beispiel aus dem echten Leben.

Kinderkrankenhaus

In diesem Beispiel war „Arzt“ die am häufigsten angegriffene Position. Bei Kindern bereitet der Datenschutz besonders große Sorgen, weil Patientendateien von Minderjährigen im Dark Web und in der Schattenwirtschaft äußerst wertvoll und ein beliebtes Ziel für Identitätsdiebstahl sind. Für die meisten Kinder ist noch keine Kredithistorie vorhanden und sie beantragen zum Zeitpunkt der Kompromittierung weder Kredite noch Kreditkarten. Zudem wissen Cyberkriminelle, dass die meisten Menschen diese Daten nicht auf Hinweise für Betrug überwachen. Wie sich zeigte, waren die Backdoor-Aktivitäten im Bereich des Gebäudemanagements am stärksten, wo die Sicherheitskontrollen häufig schwach sind.

In diesen Umgebungen werden häufig Assets mit Zugangsrechten (z. B. IoT-Geräte und HLK-Anlagen) eingesetzt, die häufig als Ziel für Angriffe auf die IT-Infrastruktur des Unternehmens dienen.

Anwendungsszenarien im Gesundheitswesen: So kann Proofpoint helfen

Verteilte Sicherheit im Gesundheitswesen

Die Gesundheitsbranche umfasst eine Vielzahl von Unternehmen und IT-Umgebungen, die Informationen zwischen Patienten und Klinikmitarbeitern austauschen, um ein patientenorientiertes bzw. Connected Care-Modell umzusetzen. Die Weitergabe vertraulicher Informationen erfolgt häufig per E-Mail, und ein Großteil der bekannt gewordenen Datenschutzverletzungen im Gesundheitswesen beginnt mit gezielten Phishing-Angriffen.

Proofpoint bietet die richtigen Lösungen für die Gesundheitsbranche an, um die heutige Arbeitsweise der Menschen zu schützen:

- **Email Protection** gewährleistet hervorragende E-Mail-Sicherheit und die Abwehr von Malware-basierten und Malware-losen Bedrohungen.
- **Data Loss Prevention (DLP)** minimiert das Risiko von Datenverlusten durch E-Mails und schützt vor E-Mail-Betrug.
- **Targeted Attack Protection (TAP)** kann mithilfe von Sandbox-Analysen hochentwickelte Bedrohungen erkennen und blockieren.
- **Proofpoint Threat Response** ermöglicht Unternehmen die schnelle Behebung von Bedrohungen und die Entfernung schädlicher E-Mails.
- **Proofpoint Security Awareness Training** stellt Schulungen für Mitarbeiter bereit, damit diese Social-Engineering-Angriffe mit Gesundheitsbezug erkennen, z. B. raffinierte Phishing-Köder.

Schutz vor Impostor-Angriffen

E-Mails mit gefälschter Identität sind betrügerische Nachrichten, die dem Empfänger bekannte oder vertraute Personen imitieren sollen. Solche Angriffe lassen sich nur schwer erkennen, da sie keine technischen Schwachstellen ausnutzen. Sie sind gegen konkrete Tätigkeitsbereiche gerichtet, die Zugriff auf finanziell lohnende Aktivitäten haben. Das sind beispielsweise Pharmazeuten, klinische Forscher, Angestellte in der Lieferkette oder Klinikpersonal.

Proofpoint bietet eine integrierte, personenorientierte und durchgängige Lösung, die alle Formen von E-Mail-Betrug stoppt – unabhängig von der verwendeten Taktik oder der angegriffenen Person:

- **Erweiterte E-Mail-Sicherheit** blockiert Phishing- und Impostor-E-Mails, die gefälschte bzw. Doppelgänger-Domänen nutzen. Die Lösung nutzt Machine Learning und mehrschichtige Erkennungstechniken, um diese gezielten Angriffe zu erkennen, und stoppt die Angriffe, noch bevor sie den Posteingang der Anwender erreichen.
- **DMARC (Domain-based Message Authentication Reporting and Conformance)** ist ein Protokoll zur Authentifizierung von E-Mails, das gefälschte E-Mails stoppt, bevor Mitarbeiter, Klinikpersonal und Geschäftspartner darauf hereinfallen.

Absicherung von Microsoft 365 und anderen Cloud-Anwendungen

Ein CASB (Cloud Access Security Broker) ist ein unverzichtbarer Bestandteil jeder Cloud-Sicherheitsarchitektur. Immer mehr Gesundheitsunternehmen übertragen Daten sowie Anwendungen in die Cloud und nutzen mehr vertrauliche Daten über Internetverbindungen. Daher benötigen sie eine Übersicht über die Cloud-Aktivitäten in ihrem Ökosystem und der Lieferkette.

Proofpoint CASB ermöglicht Unternehmen schnelle Prüfungen und umgehende Reaktionen auf potenzielle Richtlinienverletzungen in Cloud-basierten E-Mails in allen Bereichen der Pflege und Behandlung. Dadurch wird das Risiko von Cyberangriffen oder Datenschutzverletzungen verringert. Zudem untersucht Proofpoint CASB den E-Mail-Verkehr des Unternehmens auf vertrauliche Daten in Cloud-Dateidiensten wie Microsoft 365, Dropbox, Box und Salesforce.

Sichere Zusammenarbeit bei der Gesundheitsversorgung

Das medizinische Personal muss bei der Patientenversorgung effektiv zusammenarbeiten und kommunizieren können. Dazu stehen Mobil-Lösungen zur Verfügung, die Klinikmitarbeiter und Patienten verbinden. Bei ihrer Entwicklung standen jedoch die benötigten Funktionen sowie Nutzungsaspekte und nicht deren Sicherheit im Vordergrund. Zudem werden die Lösungen häufig außerhalb des geschützten Unternehmensnetzwerks betrieben.

Ärzte können mit privaten Geräten auf klinische Anwendungen zugreifen und mit Unternehmensgeräten ihre privaten E-Mails lesen. **Proofpoint Browser Isolation** gewährleistet, dass die privaten Aktivitäten und gefährlichen Inhalte nicht mit Ihrer Umgebung in Berührung kommen.

Dazu werden Webmails und sämtliche darin vorhandenen URLs in einem geschützten Container isoliert. Anwender können mit dem normalen Webbrowser ganz einfach und vertraulich auf ihre privaten E-Mail-Konten zugreifen. Gleichzeitig werden alle potenziell schädlichen Inhalte und Aktionen blockiert, sodass Ihre Umgebung sicher geschützt bleibt.

Schutz vor Insider-Bedrohungen

Dass ein Insider Patientendaten aus einem Arztbüro oder Krankenhaus weitergibt, klingt wie eine Szene in einem schlechten Film. Bedrohungen durch Insider sind jedoch real: Fast die Hälfte aller Datenschutzverletzungen steht mit internen Bedrohungsakteuren in Zusammenhang.[3]

Die drei häufigsten Bedrohungen und Datenschutzverletzungen im Zusammenhang mit Insidern im Gesundheitswesen sind:

1. Diebstahl oder missbräuchliche Verwendung geschützter Patientendaten
2. Diebstahl oder missbräuchliche Verwendung elektronischer Gesundheitsdaten
3. Versicherungs- und sonstiger Finanzbetrug

Proofpoint Insider Threat Management (ITM) schützt vor Datenverlust, schädlichen Aktionen und Markenschädigung, die durch böswillig, fahrlässig oder unbewusst falsch handelnde Insider entstehen. ITM korreliert Aktivitäten und Datenbewegungen und unterstützt dadurch Sicherheitsteams bei der Identifizierung von Anwenderrisiken, bei der Erkennung von und Reaktion auf Datenschutzverletzungen durch Insider sowie bei der Beschleunigung von Reaktionen auf Sicherheitszwischenfälle.

3 2020 Verizon Data Breach Investigations Report (Untersuchungsbericht von Verizon zu Datenkompromittierungen für 2020)

Schutz von Patientendaten: Sicherheit für personenbezogene Daten

Der schwerwiegendste Bedrohungsvektor im Gesundheitswesen sind die Menschen, die per E-Mail angegriffen werden. Die richtige Lösung für E-Mail-bezogene Datenverlustprävention (DLP) gewährleistet, dass vertrauliche und wichtige Informationen klassifiziert werden und nur für die richtigen Personen zugänglich sind.

Mit **personenorientiertem DLP von Proofpoint** können Gesundheitsunternehmen schnell Datenrisiken erkennen und beheben, die durch fahrlässig handelnde, kompromittierte und böswillige Anwender entstehen. In der zentralen Proofpoint-Plattform können Kunden wichtige Daten definieren und diese Definitionen für die gesamte Proofpoint-Plattform anwenden. Parallel dazu schützen sie die Vertraulichkeit einzelner E-Mail-Nachrichten mit **Proofpoint Email Encryption**. Die Anwender können mit selbst definierten Schlüsselbegriffen in der Betreffzeile automatisch verschlüsselte Nachrichten auslösen. Ebenso haben sie die Möglichkeit, die Verschlüsselung für einzelne Nachrichten auf Basis von DLP-Regeln auszulösen.

Der gemeinsame Proofpoint Incident Manager bietet nicht nur eine zentrale Übersicht zum Anzeigen von DLP-Verstößen bei E-Mails, in der Cloud sowie am Endgerät. Zusätzlich kombiniert er diese Daten und kann auf diese Weise erweiterte Bedrohungs- und Kontextinformation darstellen.

Verwaltung von Compliance-Vorschriften mit minimaler Komplexität

Viele regulierte Unternehmen haben in folgenden Bereichen Schwierigkeiten:

- Erkennung, wo ihre Geschäftskommunikation stattfindet
- Gewährleistung, dass diese Inhalte erfasst und sicher archiviert werden
- Schnelles und kostengünstiges Suchen und Abrufen von Inhalten für Audits
- Überwachung und Kontrolle von Mitarbeitern, die diese Kanäle nutzen

Die **Proofpoint-Lösung für Archivierung und Compliance** bietet personenorientierte Rundum-Compliance:

- Vollständige Erfassung von dem Moment, wenn der Inhalt verteilt wird, bis zu seiner Indexierung, Archivierung sowie dem Abruf
- Automatische Anwendung aller vorgeschriebenen Richtlinien wie lokalen Vorschriften im Gesundheitswesen oder DSGVO-Vorgaben
- Zuverlässige Einhaltung der Kommunikations- und Aufbewahrungsregeln bei Ihren digitalen Interaktionen
- Einfache, schnelle und preisgünstige Überwachung, Behebung (Ändern oder Entfernen) sowie Archivierung von Inhalten

Fazit

Proofpoint bietet Unternehmen im Gesundheitswesen Schutz und Transparenz für ihr größtes Sicherheitsrisiko: die Mitarbeiter. Wir bieten die effektivste Cybersicherheit zum Schutz von medizinischem Personal, ganz gleich, ob es per E-Mail, Web, sozialen Netzwerken oder Cloud-Anwendungen angegriffen wird. Dabei stoppen wir Bedrohungen, bevor sie klinische und nicht-klinische Mitarbeiter erreichen, schützen Daten und gewährleisten, dass Patienten vor Cyberangriffen sicher sind. Führende Gesundheitsunternehmen aller Größen setzen auf Proofpoint für die Abwehr, Erkennung und Behebung von Sicherheitsproblemen, noch bevor sie dauerhaften Schaden anrichten können.

WEITERE INFORMATIONEN

Weitere Informationen dazu, wie Sie mit einem personenorientierten Sicherheitsansatz Ihre Daten, Prozesse und Ihren Pflegeauftrag schützen können, finden Sie unter **www.proofpoint.com/us/solutions/healthcare-information-security**.