Schutz von Gesundheitsdaten mit Proofpoint

So schützen Sie Patientendaten vor Insider-Bedrohungen, Datenverlust und Cloud-Risiken

Produkte

- Proofpoint Cloud App Security Broker (CASB)
- Proofpoint Email Data Loss Prevention
- Proofpoint Endpoint Data Loss Prevention
- Proofpoint Insider Threat Management
- Proofpoint Web Security
- Proofpoint Zero Trust Network Access (ZTNA)
- Proofpoint Managed Services für Informationsschutz

Wichtige Vorteile

- Identifizieren und Minimieren von Risiken, die durch fahrlässige und kompromittierte Anwender sowie durch böswillige Insider entstehen
- Verhindern von Datenverlust durch E-Mails, die Cloud und Endpunkte
- Ausweiten skalierbarer Schutzfunktionen auf die wachsende Zahl stark verteilter Cloud-Dienste

Das Gesundheitswesen ist schon lange ein bevorzugtes Ziel von Cyberkriminellen und dieser Trend hat sich durch die COVID-19-Pandemie noch verstärkt. Angreifer haben ihre Bemühungen intensiviert, um in den Besitz wertvoller Informationen (z. B. Impfstoffstudien), personenbezogener Gesundheitsdaten und Finanzdaten zu gelangen. Andererseits vergrößern Gesundheitseinrichtungen ihre Angriffsfläche, wenn sie in die Cloud wechseln und immer mehr Mitarbeitern und Patienten den Fernzugriff erlauben. Dadurch steigt das Risiko durch böswillige sowie durch wohlgesonnene Insider.

Proofpoint bietet einen personenzentrierten Ansatz, um vertrauliche Daten in stark verteilten Netzwerken des Gesundheitswesens zu schützen. Unsere Datenschutzlösungen können leicht bereitgestellt und gewartet werden und ermöglichen die Erstellung robuster SASE (Secure Access Service Edge)- oder SSE (Security Service Edge)-Systeme. Wir unterstützen Sie dabei, Ihre Mitarbeiter und deren vertrauliche Daten vor versehentlichen Fehlern, Angriffen und Insider-Risiken zu schützen. Unser Schutzschild erstreckt sich auf Cloud-Dienste, E-Mails, Endpunkte und lokale Dateifreigaben.

Eine wachsende Bedrohung

Eine Datenschutzverletzung kann Compliance-Strafen und Rechtsstreitigkeiten für Gesundheitseinrichtungen nach sich ziehen, den Markenruf beschädigen oder sogar Leben kosten. Leider musste das US-Ministerium für Gesundheitspflege und soziale Dienste für das erste Halbjahr 2020 bei Datensicherheitsverletzungen im Gesundheitswesen eine Zunahme von 50 % vermelden. Darüber hinaus hat sich die Zahl der Ransomware-Angriffe 2021 mehr als verdoppelt. Insgesamt war das Gesundheitswesen 2021 einer der beiden am häufigsten angegriffenen Sektoren.

Die wachsende Zahl medizinischer IoT-Geräte (Internet of Things) kann zwar Leben retten, führt aber auch zu mehr Komplexität. Zudem kommen aufgrund von COVID-19 verstärkt Telemedizin-Dienste zum Einsatz, die mitunter sogar direkt aus dem Homeoffice und nicht mehr von einer Klinik oder einem Krankenhaus aus bereitgestellt werden.

Daher wundert es nicht, dass Moody's Investors Service auf absehbare Zeit keine Entspannung bei den Cyberrisiken für das Gesundheitswesen sieht. Die Einrichtungen müssen trotz des bereits zwei Jahre dauernden Kampfes gegen die existenzbedrohende Krise auch weiterhin wachsam bleiben.

Herausforderungen im Datenschutz

Krankenhäuser, Kliniken, Krankenversicherungen und Biotech-Firmen sollten dem Datenschutz in dieser prekären Bedrohungslandschaft höchste Aufmerksamkeit widmen, um die personenbezogenen Gesundheitsdaten, personenbezogenen Informationen und Zahlungskartendaten der Patienten zu schützen. Dabei stehen sie vor verschiedenen Herausforderungen.

Ausspionieren elektronischer Gesundheitsdaten und andere Bedrohungen durch Insider verhindern

Mitarbeiter im Gesundheitswesen sind die wahren Helden der Pandemie. Obwohl die Krise immer schlimmer wurde, haben sie dem enormen Arbeitsstress Tag für Tag standgehalten, auch wenn kein Ende absehbar war. Stress dieser Art kann auch das Risiko von Insider-Bedrohungen erhöhen. Ein neugieriger Mitarbeiter kann in einer Pause schon mal einen kurzen Blick in die Patientenakte eines berühmten Patienten werfen. Dieses Schnüffeln in elektronischen Patientenakten birgt hohe Risiken für die Einrichtung, sollten die Informationen eines zahlungskräftigen Patienten den Weg in die Öffentlichkeit finden.

Wohlgesonnene, aber überarbeitete Mitarbeiter könnten versehentlich auf eine Phishing-E-Mail klicken, die sie unter normalen Umständen sofort erkennen würden, und emotionaler Stress kann sogar zu Insider-Bedrohungen gegen einen Arbeitgeber führen. Deshalb benötigen Sie einen proaktiven Ansatz, um alle diese Bedrohungen zu verhindern.

Wachsende Angriffsfläche durch Wechsel in die Cloud schützen

Viele Gesundheitseinrichtungen gingen den Wechsel in die Cloud nur zögerlich an. Inzwischen bieten jedoch fast alle Einrichtungen Dienste in Public und Private Clouds an, sodass sie ihre operative Effizienz deutlich steigern konnten. Zudem müssen sich die Einrichtungen nicht mehr um die Finanzierung der entsprechenden IT-Infrastruktur kümmern. Andererseits hat sich dadurch die Angriffsfläche der Gesundheitseinrichtungen vergrößert.

Selbst bei lokal gespeicherten elektronischen Patientenakten werden einzelne Informationen daraus unweigerlich an anderen Orten aufgerufen, geteilt und gespeichert. Denken Sie zum Beispiel an mobile Geräte, Endpunkte im Homeoffice, medizinische IoT-Geräte und Cloud-basierte E-Mail-Systeme. Da medizinische Informationen an immer mehr Ziele übertragen werden, gestaltet sich auch ihr Schutz immer problematischer.

Mit dem Wachstum der Cloud-Umgebungen steigt auch das Risiko von Anmeldedaten-Diebstahl. Büro-Software und Collaboration-Funktionen werden immer öfter über Cloud-Dienste wie Microsoft 365 und Google Workspace bereitgestellt, die für Cyberbedrohungen sehr anfällig sind. Hinzu kommt, dass Cyberkriminelle diese gängigen Dateifreigabe-Umgebungen verstärkt nutzen, um ihre Exploits zu verteilen.

Medizinisches Personal und Telemedizin-Patienten bei immer neuen Bereitstellungsmodellen schützen

Einige der plötzlichen Änderungen, die die Pandemie der Arbeitswelt Anfang 2020 aufzwang, waren zwar nur von vorübergehender Dauer – doch viele werden uns auch in den nächsten Jahren begleiten. Ein ungebrochener Trend im Gesundheitswesen ist die zunehmende telemedizinische Betreuung. Laut einer Studie lag die Nutzung von Telemedizin Ende Februar 2021 beim 38-fachen des Wertes von 2019. Dies bedeutete eine massive Zunahme von Patienten, die online auf die Ressourcen der Einrichtungen zugreifen.

Hinzu kommt, dass eine große Zahl von Mitarbeitern weiterhin zumindest teilweise im Homeoffice arbeitet. Viele von ihnen verwalten elektronische Patientenakten, finanzielle Patienteninformationen und Forschungsdaten. Die wachsende Zahl von Remote-Anmeldungen erhöht das Risiko von Angriffen auf Personen, die innerhalb einer Einrichtung spezielle Funktionen ausüben.

Ein personenzentrierter Ansatz

Ältere Datenschutzansätze konzentrieren sich nur auf die Daten. Informationen gehen jedoch nicht einfach so verloren. Hinter Datenverlusten stehen immer Personen, die einen Fehler machen oder böswillig handeln. Bei Cybersicherheit kommt es auf Transparenz an. Deshalb müssen Sie die Personengruppen kennen, die für Risiken besonders anfällig sind. Ein personenzentrierter Ansatz analysiert die Dynamik der Individuen, die mit diesen Daten interagieren.

So kann Proofpoint helfen

Die Information and Cloud Security-Plattform von Proofpoint kann Sie beim Schutz Ihrer vertraulichen Informationen unterstützen, denn sie konzentriert sich auf die Personen, die diese Daten verwalten.

Proofpoint Cloud App Security Broker (CASB)

Proofpoint Cloud App Security Broker (CASB) schützt Anwender vor Cloud-Bedrohungen. Die Lösung sichert vertrauliche Daten und verwaltet Cloud- und OAuth-Apps in Microsoft 365, Google Workspace sowie mehr als 900 von der IT genehmigten und tolerierten Cloud-Anwendungen. Sie dehnt die Transparenz von Proofpoint bei den VAPs (Very Attacked People™) auf Ihre Cloud-basierten Dienste aus, sodass Sie Cloud-Konten und -Daten besser schützen können. Proofpoint CASB bietet einen detaillierten Überblick über Cloud-Zugriffe, Anwenderverhalten und die Verwendung vertraulicher Daten (z. B. Gesundheitsdaten), sodass Sie Datenschutz- und Datensicherheitsbestimmungen leichter einhalten können.

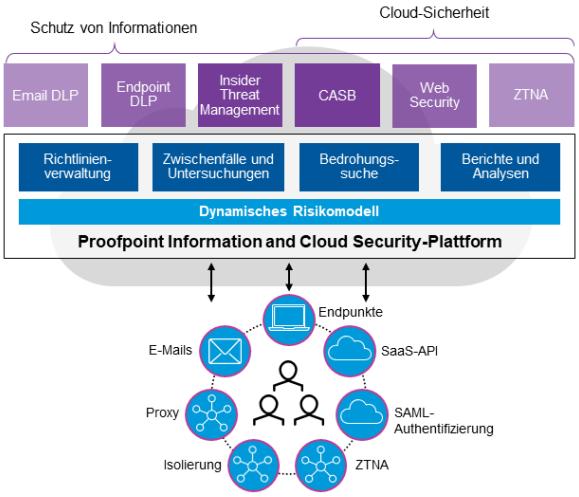

Abb. 1: Proofpoint Information and Cloud Security-Plattform.

Proofpoint CASB kann je nach Anwendungsszenario in verschiedenen Modi bereitgestellt werden. Um nahezu Echtzeit-Transparenz mit schneller Rendite zu ermöglichen, integriert sich CASB mit den APIs Ihrer Cloud-Apps und den Protokollen Ihrer Infrastruktur. Für Echtzeit-Kontrollen über Zugriffe und Daten stehen Ihnen risikobasierte SAML-Authentifizierung, Isolierung sowie Inline-Forward-Proxy-Funktionen zur Verfügung. Sie können CASB in echter SSE-Manier mit Proofpoint Web Security und Zero Trust Network Access (ZTNA) integrieren, um Homeoffice-Mitarbeiter über Web- und Cloud-Anwendungen hinweg zu verbinden und zu schützen.

Proofpoint Data Loss Prevention

Proofpoint Data Loss Prevention nutzt einen personenzentrierten Ansatz für die Datenverlustprävention (DLP). Die Lösung vereint Inhalte, Verhaltensweisen und Bedrohungen und stellt Kontext für alle drei Elemente bereit. Sie präsentiert ihre Einblicke in einer modernen Zeitleistenansicht, um Ihnen ein umfassenderes und nuancierteres Verständnis von konkreten Ereignissen zu vermitteln. Mithilfe dieser Informationen können Sie erkennen, ob ein gekennzeichneter Anwender kompromittiert wurde, böswillig oder fahrlässig handelt.

Proofpoint Insider Threat Management

Proofpoint Insider Threat Management (ITM) korreliert Anwenderaktivitäten und Datenbewegungen, damit Sicherheitsteams potenzielle Insider-Bedrohungen erkennen, untersuchen und abwehren können. Die Lösung ermöglicht die personenzentrierte Erkennung von Verhaltensweisen. Dazu bietet sie Funktionen zur Echtzeiterkennung von Datenexfiltrationen, Missbrauch von Berechtigungen und Anwendungen, unbefugten Zugriffen, riskanten versehentlichen Aktionen sowie ungewöhnlichen Verhaltensweisen – einschließlich Optionen zur schnellen Reaktion. Auf diese Weise können Sie Bedrohungen wie das Ausspionieren von elektronischen Patientenakten in zeitleistenbasierten Visualisierungen und Analysen erkennen, verhindern und abwehren.

Sobald eine Insider-Bedrohung erkannt wurde, stellt Proofpoint ITM Workflows und unwiderlegbare Beweise für Fehlverhalten bereit, um die Reaktion auf den Zwischenfall zu beschleunigen. Die Informationen werden durch ressourcenschonende Endpunktsensoren zusammengetragen und anschließend in einer modernen Architektur analysiert, die Skalierbarkeit, Sicherheit und Datenschutz gewährleistet. Darüber hinaus kann Proofpoint ITM flexibel als lokale Lösung oder per Software-as-a-Service (SaaS) bereitgestellt werden.

Proofpoint Web Security

Immer mehr Mitarbeiter melden sich von außerhalb des Netzwerkperimeters an. Proofpoint Web Security kann diese verteilte Belegschaft beim Surfen im Internet vor raffinierten Bedrohungen schützen. Dazu untersucht die Lösung den gesamten SSL-Datenverkehr, um Bedrohungen wie Ransomware- und Zero-Day-Phishing-Angriffe aufzudecken und zu blockieren. Zudem verhindert sie das Aufrufen gefährlicher und nichtkonformer Inhalte.

Proofpoint Zero Trust Network Access

Mit dem Wechsel von Anwendungen in die Cloud steigt die Mobilität der Mitarbeiter im Gesundheitswesen. Dieser Trend erfordert eine bessere VPN-Alternative für den sicheren Zugriff. Proofpoint ZTNA nutzt für jeden Anwender einen Software-definierten Perimeter, damit sie Cloud-basiert und sicher per Fernzugriff auf Ressourcen im Rechenzentrum und in der Cloud zugreifen können.

Dabei erhält jeder Anwender Zugriff auf konkrete Anwendungen, während das restliche Netzwerk unsichtbar bleibt. Proofpoint ZTNA überprüft Anwender, bevor sie Zugang zum Netzwerk erhalten, und erhöht damit die Sicherheit und Transparenz.

Proofpoint Managed Services für Informationsschutz

Managed Services für Informationsschutz (MSIP) verstärken Ihr Team mit unseren weltweit tätigen Datensicherheitsexperten. Wir haben jahrzehntelange Erfahrung und basierend darauf Best Practices und ein Reifegradmodell zur Optimierung Ihres Programms entwickelt. Wir decken Anwendungsverwaltung, Umfang und Richtlinien-Governance, Ereignisanalyse, Zwischenfallverwaltung und Berichte sowie Analysen ab. Dadurch werden Sie vor dem Diebstahl geistigen Eigentums und vor Verletzungen des Patientendatenschutzes bewahrt. Unsere Experten konzipieren, implementieren und betreiben ein Programm, das speziell für Ihre Sicherheits- und Compliance-Anforderungen maßgeschneidert wurde. Wir verwenden hochentwickelte Machine Learning-Techniken wie DLP, Cloud App Security Broker und ITM sowie menschliche Analysen, um die Sicherheit Ihrer medizinischen Informationen zu gewährleisten. Warnmeldungen werden untersucht und für schnelle Reaktionen auf Kompromittierungsversuche genutzt. Wir helfen Ihnen gern dabei, Ihre Sicherheit zu verbessern und Ihr Team optimal einzusetzen, sodass Sie sich auf andere Themen konzentrieren können.

Fazit

COVID-19 hat bei allen Gesundheitseinrichtungen zu massiven Veränderungen im Arbeitsalltag geführt. Die Angriffsflächen sind gewachsen, der Datenschutz muss für mehrere Clouds gewährleistet werden, Mitarbeiter und Patienten befinden sich zunehmend an anderen Orten und die Anzahl medizinischer IoT-Geräte am Netzwerkrand steigt.

Seit mehr als zwei Jahrzehnten versuchen Einrichtungen, den Perimeter zu sichern. Aufgrund der aktuellen explosionsartigen Zunahme bei der Nutzung von Cloud-Diensten und der verstärkten Arbeit im Homeoffice ist jeder einzelne Mitarbeiter gleichzeitig Perimeter und Netzwerkrand.

Diese rasanten Veränderungen erfordern eine mitwachsende Sicherheitsarchitektur. Der neue Ansatz wird oft als SSE bezeichnet. SSE ist der Sicherheitsteil eines SASE-Systems und bietet Anwendern den sicheren Zugang, den sie für alle Cloud-Dienste über Cloud-Rechenzentren benötigen. Hier finden der Zero-Trust-Netzwerkzugriff und das Identitäts- und Zugriffsmanagement statt. Zudem wird der Zugriff mithilfe zentraler Kontrollen von Administratoren überwacht.

Sie können mit der Information and Cloud Security-Plattform von Proofpoint eine robuste SSE- oder SASE-Architektur aufbauen. Dabei profitieren Sie von sicheren Zugriffen und Bedrohungsschutz, während Personen unabhängig von Standort oder Gerätetyp auf Anwendungen und Daten zugreifen. Sie schützen Ihre Einrichtung, indem Sie die Personen schützen, die mit Ihren vertraulichen Informationen arbeiten.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de**.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

proofpoint.

0207-005-01-01 12/21