proofpoint.

KURZVORSTELLUNG

Schutz des Gesundheitswesens vor Ransomware mit Proofpoint

Verhindern Sie gezielte Angriffe auf Menschen, wehren Sie KI-gesteuerte Täuschungen ab und schützen Sie Daten vor Erpressung

Überblick

Ransomware ist eine der gravierendsten Bedrohungen, denen sich Gesundheitseinrichtungen heute gegenübersehen. Diese Angriffe beschränken sich nicht mehr auf die Verschlüsselung von Systemen, sondern sie kombinieren jetzt Diebstahl von Anmeldedaten, Datenexfiltration und Erpressung, um maximalen betrieblichen und finanziellen Schaden zu erreichen. Für Krankenhäuser und Gesundheitsdienstleister gehen die Folgen weit über Ausfallzeiten hinaus und betreffen direkt die Patientenversorgung, Sicherheit und das Vertrauen.

Die meisten Ransomware-Angriffe beginnen mit einer gezielten E-Mail, einem kompromittierten Konto oder einer betrügerischen Nachricht, die einen Anwender zu einer Aktion verleitet. E-Mail, Cloud-Anwendungen und Collaboration-Plattformen sind auch weiterhin die Haupteinfallstore, wobei Angreifer menschliches Verhalten ausnutzen, um Erstzugriff zu erlangen.

KI verschärft jetzt diese Bedrohung. Gegner erstellen mithilfe von KI äußerst überzeugende Phishing-Nachrichten, geben sich als vertrauenswürdige Personen aus und weiten Angriffe auf Gesundheitseinrichtungen aus. Gleichzeitig integrieren Gesundheitsdienstleister KI-gesteuerte Arbeitsabläufe und Automatisierung, wodurch neue Maschinenidentitäten und automatisierte Interaktionen entstehen, die auch von Angreifern ausgenutzt werden können.

Proofpoint hilft Gesundheitseinrichtungen bei der Abwehr von Ransomware, indem Kompromittierungen von Mitarbeitern verhindert, KI-gesteuerte Täuschungen erkannt und vertrauliche Daten vor Datenexfiltration und Erpressung geschützt werden.

Auswirkungen von Ransomware auf die Patientenversorgung

Ransomware-Angriffe sind nicht nur IT-Vorfälle, sondern Ereignisse, die die Patientensicherheit gefährden.

Wenn Systeme nicht verfügbar sind oder Daten kompromittiert werden, sind die Auswirkungen sofort spürbar und weitreichend.

- Verzögerter oder unterbrochener Zugang zu elektronischen Gesundheitsakten (EHRs)
- Umleitung von Notfallpatienten zu anderen Einrichtungen
- Unterbrechungen der kritischen Patientenversorgung und klinischen Arbeitsabläufe
- Unterbrochener Zugriff auf Diagnosesysteme, Laborergebnisse oder Bildgebung
- Offenlegung geschützter Gesundheitsdaten, was zu Vertrauensverlust führt

Diese Lösung ist Teil der integrierten Proofpoint Human-Centric Security-Plattform, die Menschen und Daten an agentenbasierten Arbeitsplätzen schützt.

1,2 Mio. $

Durchschnittliche Lösegeldzahlung im Gesundheitswesen.[1]

Herausforderungen durch Ransomware im Gesundheitswesen

Ransomware im Gesundheitswesen ist besonders schädlich, da sie sowohl die Abläufe als auch die Patientenversorgung angreift. Angreifer konzentrieren sich absichtlich auf Umgebungen, in denen Ausfallzeiten keine Option sind.

Diese Angriffe folgen einem vorhersehbaren Muster. Bedrohungsakteure nutzen Phishing oder Social Engineering, um Anmeldedaten zu stehlen, Zugang zu Systemen zu erlangen und sich lateral innerhalb des Unternehmens zu bewegen.

Sobald die Angreifer sich Zugang verschafft haben, identifizieren sie wertvolle Systeme und Daten, exfiltrieren vertrauliche Informationen und installieren dann Ransomware, um maximalen Druck zu erzeugen und möglicherweise den Betrieb lahmzulegen.

Geändert hat sich die Art und Weise, wie diese Angriffe ausgeführt werden. Ransomware-Kampagnen sind heute:

- Hochgradig zielgerichtet, mit Fokus auf spezifische Rollen wie Klinikmitarbeiter, Finanzteams und Führungskräfte
- KI-unterstützt, was überzeugendere Nachahmung und die schnellere Entwicklung von Angriffen ermöglicht
- Datengestützt, wobei der Diebstahl von Patientendaten und Betriebsinformationen vor der Verschlüsselung priorisiert wird
- Ökosystem-übergreifend, wobei Lieferanten, Partner und gemeinsame Plattformen ausgenutzt werden

Gleichzeitig müssen Gesundheitseinrichtungen nicht nur Anwender, sondern auch KI-Agenten, automatisierte Arbeitsabläufe und nicht-menschliche Identitäten absichern, die mit vertraulichen Systemen und Daten interagieren.

Durch diese Kombination aus personenbezogenem Risiko, KI-gesteuerten Bedrohungen und Datenkompromittierung ist moderne Ransomware so effektiv und lässt sich so schwer mit klassischen Kontrollen stoppen.

Ein personen- und agentenzentrierter Ansatz für die Sicherheit im Gesundheitswesen

Heutige Cyberangriffe richten sich nicht nur gegen Technologie, sondern nutzen vertrauenswürdige Anwender und Agenten aus. Um Ransomware zu stoppen, müssen Sie Ihren Sicherheitsansatz von der letzten Phase der Verschlüsselung auf die frühesten Phasen der Angriffskette verlagern.

Da Ransomware typischerweise durch menschliche Interaktion (Klicken auf einen Link, Öffnen einer Datei oder Reagieren auf eine Nachricht) verbreitet wird, besteht die effektivste Verteidigung darin, eine Kompromittierung zu verhindern, bevor Angreifer Zugang erhalten.

Dies erfordert einen Sicherheitsansatz, der folgende Kriterien erfüllt:

- Versteht, wer angegriffen wird
- Erkennt Täuschungsversuche über E-Mail- und Cloud-Kanäle
- Sichert KI-gesteuerte Interaktionen und automatisierte Prozesse ab

1. Ponemon Institute: *Study on Cyber Insecurity in Healthcare* (Studie zur Cyber-Unsicherheit im Gesundheitswesen), 2025.

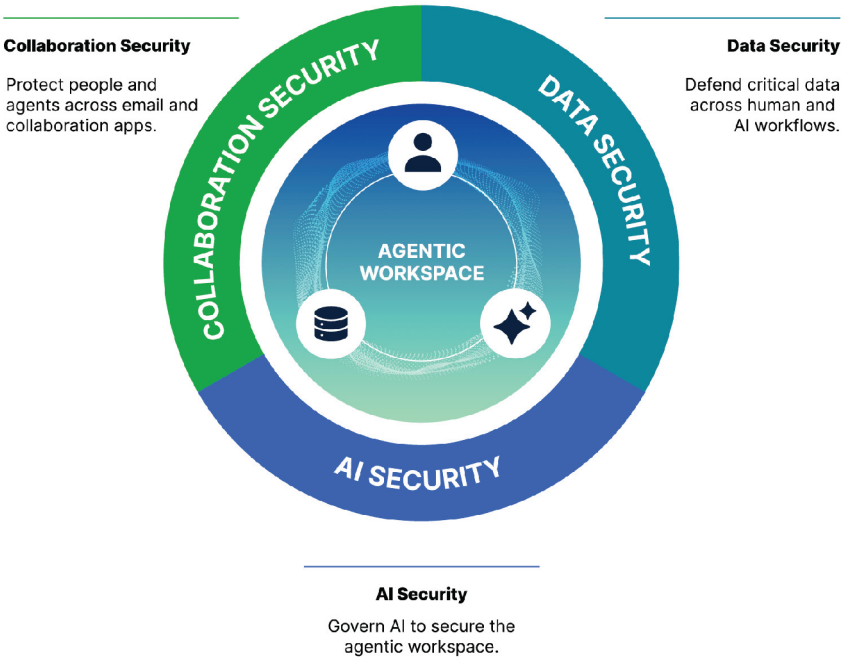

Abb. 1: Ein Plattformansatz, der Ransomware über den gesamten Angriffslebenszyklus hinweg stoppt.

Produkte

- Proofpoint Collaboration Security Prime
- Proofpoint Nexus
- Proofpoint Data Loss Prevention (DLP)
- Proofpoint Adaptive Email DLP
- Proofpoint Data Security Posture Management (DSPM)
- Proofpoint Satori
- Proofpoint Account Takeover Protection
- Proofpoint Insider Threat Management
- Proofpoint ZenGuide

Wie Proofpoint helfen kann

Proofpoint genießt das Vertrauen von 67% der Fortune 500-Unternehmen im Gesundheitswesen. Nur Proofpoint bietet eine integrierte Plattform, die Menschen, Agenten und Daten gleichermaßen schützt.

Verhinderung der Initial-Kompromittierung

Proofpoint Collaboration Security Prime bietet einen umfassenden Ansatz zur Abwehr von Angriffen, die auf Menschen und Agenten abzielen und dazu E-Mails, Collaboration-Tools, Cloud-Anwendungen, Webkanäle und Social-Media-Plattformen missbrauchen. Die Lösung nutzt Proofpoint Nexus® für fortschrittliche KI, Verhaltensanalysen und Bedrohungsdaten, um Angriffe über den gesamten Bedrohungszyklus hinweg zu blockieren – von vor der Zustellung bis nach dem Klick.

Schutz vor KI-gesteuerten Täuschungen und Kontoübernahmen

Proofpoint Account Takeover Protection und Proofpoint Insider Threat Management erkennen verdächtiges Verhalten bei Anwender- sowie bei Agentenidentitäten sowie Kompromittierungen von Anmeldedaten, Missbrauch von Berechtigungen, laterale Bewegungen und Datenexfiltrationen. Durch die Korrelation von Identität, Verhalten und Datenbewegungen ermöglicht Proofpoint schnellere und genauere Reaktionen, bevor die Patientenversorgung beeinträchtigt wird.

Sichere Speicherung von Patientendaten

Proofpoint Data Loss Prevention (DLP)-Lösungen verhindern versehentlichen oder böswilligen Datenverlust per E-Mail, Cloud und über Endpunkte, indem sie umfassende Einblicke in das Anwenderverhalten und Inhalte liefern.

Proofpoint Adaptive Email DLP nutzt verhaltensbasierte KI, um normale E-Mail-Versandmuster zu analysieren und Klinikpersonal sowie Mitarbeitern kontextbezogene Warnungen in Echtzeit zu übermitteln, Dadurch werden fehlgeleitete Nachrichten und Datenkompromittierungen verhindert, ohne die Patientenversorgung zu beeinträchtigen.

Proofpoint Data Security Posture Management (DSPM) identifiziert, wo vertrauliche Daten gespeichert sind, welche Menschen und Agenten darauf zugreifen können und wo übermäßige oder riskante Berechtigungen bestehen. Dadurch können Gesundheitsdienstleister ihre Angriffsfläche verringern und KI sowie Automatisierung sicher einführen.

Proofpoint Satori™ erweitert DSPM durch Governance für Echtzeit-Datenzugriffe in Gesundheitseinrichtungen. Proofpoint Satori überwacht kontinuierlich und kontrolliert den Zugriff auf vertrauliche Patientendaten in Cloud-Datenspeichern, Analyseplattformen und KI-Pipelines, ohne die klinischen Arbeitsabläufe zu beeinträchtigen.

Proofpoint Satori bietet Gesundheitsanbietern folgende Vorteile: Erkennung und Klassifizierung vertraulicher Patientendaten und klinischer Daten über Cloud-Datenplattformen hinweg

- Durchsetzung von Least-Privilege-Zugriffen für Mediziner, Mitarbeiter, Anwendungen und KI-Agenten
- Erkennung und Behebung riskanter oder ungewöhnlicher Datenzugriffe in Echtzeit
- Anwendung richtlinienbasierter Kontrollen, um personenbezogene Gesundheitsdaten zu schützen und gleichzeitig Analysen, Untersuchungen und KI-Innovationen zu ermöglichen

Reduzierung personenbezogener Risiken durch Verhaltensänderung

Proofpoint ZenGuide bietet rollenbasierte, risikoorientierte Security-Awareness-Schulungen an, die auf Klinikpersonal und Mitarbeiter zugeschnitten sind. Die Lösung fördert sicheres Verhalten durch die Simulation realer Bedrohungsszenarien im Gesundheitswesen, ohne die Patientenversorgung zu beeinträchtigen.

Fazit

Ransomware-Angriffe im Gesundheitswesen sind unvermeidlich, aber ihr Erfolg ist nicht garantiert. Wenn sich Gesundheitseinrichtungen auf die frühesten Phasen der Angriffskette konzentrieren und die Ursachen angehen, können sie Ransomware stoppen, bevor diese die Patientenversorgung beeinträchtigt.

Proofpoint kann Angriffe verhindern, Patientendaten schützen und die betriebliche Resilienz mit einem modernen, personen- und agentenzentrierten Ansatz zur Abwehr von Ransomware aufrechterhalten.

proofpoint.

LERNEN SIE DIE PROOFPOINT-PLATTFORM KENNEN →