proofpoint.

PANORAMICA SULLA SOLUZIONE

Proteggere il settore della sanità contro il ransomware con Proofpoint

Previeni gli attacchi che prendono di mira le persone, difenditi dalle truffe basate sull'IA e proteggi i tuoi dati dalle estorsioni

Questa suite di soluzioni fa parte della piattaforma Human-Centric Security integrata di Proofpoint volta a proteggere persone e dati nell'ambiente di lavoro agentico.

Panoramica

Il ransomware è una delle minacce più devastanti che le aziende sanitarie devono affrontare oggi. Questi attacchi non si limitano più a crittografare i sistemi. Ora combinano il furto di credenziali d'accesso, la sottrazione di dati e l'estorsione per massimizzare l'impatto operativo e finanziario. Per gli ospedali e gli operatori sanitari, le conseguenze vanno ben oltre i semplici tempi di inattività e incidono direttamente sull'assistenza ai pazienti, sulla loro sicurezza e sulla fiducia che viene loro accordata.

La maggior parte degli attacchi ransomware ha inizio con un'email mirata, un account compromesso o un messaggio ingannevole che induce l'utente a compiere un'azione. Le email, le applicazioni cloud e le piattaforme di collaborazione rimangono i principali punti di accesso, con i criminali informatici che sfruttano il comportamento umano per ottenere l'accesso iniziale.

L'IA ora accelera questa minaccia. I criminali informatici utilizzano l'IA per creare messaggi di phishing estremamente convincenti, rubare l'identità di persone fidate e sferrare attacchi su larga scala contro le strutture sanitarie. Allo stesso tempo, gli operatori sanitari stanno adottando flussi di lavoro basati sull'IA e l'automazione, creando così nuove identità delle macchine e interazioni automatizzate che anche gli hacker possono sfruttare.

Proofpoint aiuta le aziende sanitarie a contrastare il ransomware impedendo la violazione degli utenti, rilevando le truffe basate sull'IA e proteggendo i dati sensibili da sottrazioni e estorsioni.

Impatto del ransomware sull'assistenza ai pazienti

Gli attacchi ransomware non sono dei semplici incidenti informatici, ma hanno un impatto diretto sulla sicurezza dei pazienti.

Quando i sistemi non sono disponibili o i dati vengono compromessi, le conseguenze sono immediate e hanno ripercussioni significative.

- Accesso ritardato o interrotto alle cartelle cliniche elettroniche (CCE)
- Riorientamento dei casi d'emergenza verso altre strutture
- Interruzioni della gestione dei pazienti in terapia intensiva e dei flussi di lavoro clinici
- Impossibilità di accedere ai sistemi di diagnostica, ai risultati di laboratorio o alle immagini diagnostiche
- Divulgazione di dati sensibili dei pazienti, con conseguente perdita di fiducia

1,2Mln $

Importo medio dei riscatti nel settore della sanità[1]

Le sfide poste dai ransomware nel settore della sanità

Il ransomware nel settore sanitario è particolarmente dannoso perché compromette sia il funzionamento delle strutture sanitarie sia l'assistenza ai pazienti. I criminali informatici prendono di mira deliberatamente gli ambienti in cui i tempi di inattività sono inaccettabili.

Questi attacchi seguono uno schema prevedibile. I criminali informatici ricorrono al phishing o al social engineering per rubare credenziali d'accesso, accedere ai sistemi e spostarsi lateralmente all'interno della struttura.

Una volta entrati, individuano i sistemi e i dati di maggior valore, sottraggono le informazioni sensibili, quindi rilasciano il ransomware per massimizzare il proprio vantaggio e, potenzialmente, bloccare le operazioni.

Ciò che è cambiato è il modo in cui questi attacchi vengono sferrati. Le campagne di ransomware ora presentano le seguenti caratteristiche:

- Estremamente mirate e incentrate su profili specifici come medici, team finanziari e dirigenti
- Ottimizzate dall'IA, il che favorisce furti d'identità più convincenti e uno sviluppo più rapido degli attacchi
- Basate sui dati, con priorità al furto dei dati dei pazienti e delle informazioni operative prima della crittografia
- Estese all'insieme degli ecosistemi, grazie allo sfruttamento di fornitori, partner e piattaforme condivise

Allo stesso tempo, le strutture sanitarie devono garantire la sicurezza non solo degli utenti, ma anche degli agenti di IA, dei flussi di lavoro automatizzati e delle identità non umane che interagiscono con sistemi e dati sensibili.

È proprio questa convergenza tra rischi umani, minacce ottimizzata dall'IA e esposizione dei dati che rende il ransomware moderno così efficace e difficile da contrastare con i controlli tradizionali.

Un approccio alla sicurezza sanitaria incentrato sulle persone e sugli agenti

Gli attacchi informatici odierni non prendono di mira solo la tecnologia. Sfruttano persone e agenti di fiducia. Per contrastare il ransomware, devi riorientare la tua strategia di sicurezza sulle prime fasi della catena di attacco piuttosto che sulla fase finale della crittografia.

Poiché il ransomware viene solitamente diffuso a seguito di un'interazione umana (clic su un link, apertura di un file o risposta a un messaggio), la difesa più efficace consiste nell'impedire la violazione prima che i criminali informatici ottengano accesso al sistema.

Ciò richiede un approccio alla sicurezza che:

- Comprende chi viene preso di mira
- Rileva le truffe nelle email e nei servizi cloud
- Garantisce la sicurezza delle interazioni basate sull'IA e dei processi automatizzati
- Protegge i dati sensibili dalle sottrazioni

Proofpoint raggiunge questo obiettivo grazie a una piattaforma unificata, incentrata sulle persone e sugli agenti, che mette in relazione comportamenti, identità e accesso ai dati per bloccare il ransomware durante l'intero ciclo di vita dell'attacco.

1. Ponemon Institute, *Study on Cyber Insecurity in Healthcare (Studio sulla sicurezza informatica nel settore della sanità)*, 2025.

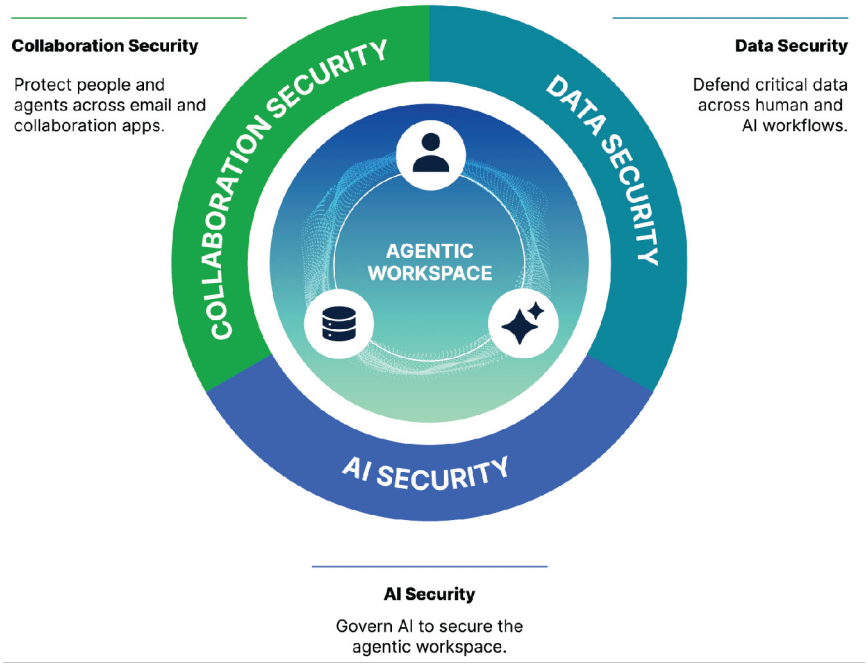

Figura 1. Un approccio basato su una piattaforma che blocca il ransomware lungo l'intero ciclo di vita dell'attacco

Soluzioni

- 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

Come Proofpoint può aiutarti

Adottato dal 67% delle aziende sanitarie della classifica Fortune 500, Proofpoint è l'unico fornitore a offrire una piattaforma integrata che protegge contemporaneamente persone, agenti e dati.

Prevenire la violazione iniziale

Proofpoint Collaboration Security Primeoffre un approccio end-to-end per bloccare gli attacchi che prendono di mira persone e agenti a livello di email, strumenti di collaborazione, applicazioni cloud, canali web e piattaforme social. Ottimizzato da Proofpoint Nexus®, utilizza IA avanzata, analisi comportamentale e threat intelligence per bloccare gli attacchi durante l'intero ciclo di vita della minaccia, prima della consegna, dopo la consegna e al momento del clic.

Difendersi dalle truffe e dal takeover degli account basati sull'IA

Proofpoint Account Takeover Protection e Proofpoint Insider Threat Management rilevano i comportamenti sospetti legati alle identità delle persone e degli agenti, inclusa la violazione delle credenziali d'accesso, l'uso improprio di privilegi, gli spostamenti laterali e la sottrazione di dati. Correlando identità, comportamenti e spostamenti dei dati, Proofpoint permette di intervenire in modo più rapido e preciso, prima che l'assistenza sanitaria venga interrotta.

Garantire la sicurezza dei dati dei pazienti

Le soluzioni Proofpoint Data Loss Prevention (DLP) prevengono la perdita accidentale e dannosa di dati tramite email, cloud ed endpoint, fornendo una visibilità approfondita sul comportamento degli utenti e sui contenuti.

Proofpoint Adaptive Email DLP utilizza l'IA comportamentale per analizzare i modelli normali di invio delle email e fornire avvisi contestuali in tempo reale a medici e personale sanitario, evitando così i messaggi inviati al destinatario errato e l'esposizione dei dati senza interferire con l'erogazione delle cure.

Proofpoint Data Security Posture Management (DSPM) identifica dove risiedono i dati sensibili, quali persone e agenti possono accedervi così come i casi in cui vengono concesse autorizzazioni eccessive o rischiose. I fornitori possono così ridurre l'esposizione e adottare in modo sicuro l'IA e l'automazione.

Proofpoint Satori™ completa Proofpoint DSPM gestendo la governance degli accessi ai dati in tempo reale negli ambienti sanitari. Proofpoint Satori monitora e controlla costantemente l'accesso ai dati sensibili dei pazienti negli archivi di dati cloud, piattaforme di analisi e pipeline di IA senza interferire con i flussi di lavoro clinici.

Grazie a Proofpoint Satori, gli operatori sanitari possono: Identificare e classificare i dati dei pazienti e i dati clinici sensibili sulle piattaforme di dati cloud

- Applicare il principio del privilegio minimo per i medici, il personale, le applicazioni e gli agenti IA
- Rilevare e correggere in tempo reale gli accessi ai dati a rischio o anomali
- Applicare controlli basati su policy per proteggere le informazioni di identificazione sanitaria consentendo l'analisi, la ricerca e l'innovazione in materia di IA

Ridurre i rischi legati agli utenti grazie al cambiamento dei comportamenti

Proofpoint ZenGuide offre formazione di sensibilizzazione alla sicurezza basata sui ruoli e sui rischi, pensata su misura per i medici e il personale. Rafforza i comportamenti sicuri utilizzando scenari di minacce reali per la sanità senza rallentare l'erogazione delle cure.

Conclusione

Gli attacchi ransomware nel settore della sanità sono inevitabili, ma questo non significa che il loro successo sia garantito. Concentrandosi sulle prime fasi della catena di attacco e affrontandone le cause alla radice, le strutture sanitarie possono impedire al ransomware di compromettere l'erogazione delle cure.

Proofpoint consente alle aziende sanitarie di prevenire gli attacchi, proteggere i dati dei pazienti e preservare la resilienza operativa grazie a un approccio moderno e incentrato sulle persone e sugli agenti per la protezione contro il ransomware.

proofpoint.

SCOPRILAPIATTAFORMA PROOFPOINT →