Garantire la sicurezza delle strutture sanitarie con Proofpoint

Protezione di persone, processi e dati dei pazienti

Gli attacchi informatici che colpiscono il settore della sanità sono in costante ascesa. I dati altamente sensibili dei pazienti possono avere un valore economico elevato, rendendo così le organizzazioni sanitarie un obiettivo primario dei criminali informatici. Il COVID-19 ha reso il settore ancora più vulnerabile. Ora medici e personale non medico offrono ai pazienti servizi di assistenza in remoto, aumentando la loro esposizione alle minacce informatiche. Proofpoint può aiutarti. Le nostre soluzioni di sicurezza informatica proteggono la tua struttura, il tuo personale e i pazienti.

La telemedicina e il telelavoro sono strumenti potenti che hanno facilitato al personale sanitario l'erogazione delle cure ai pazienti. Ma queste nuove modalità di lavoro in remoto aprono anche le porte alle minacce informatiche, che potrebbero mettere a repentaglio i dati medici, interrompere le cure ai pazienti o anche compromettere la loro salute.

Le istituzioni sanitarie ora considerano la sicurezza informatica una priorità assoluta per l'incolumità dei pazienti. Ma, come molte aziende nei più diversi settori, hanno investito in strumenti di sicurezza tradizionali che proteggono il perimetro della rete. che però non sono in grado di rilevare, ancor meno di bloccare, le minacce che mettono a rischio i dati sanitari.

Inoltre, le minacce stesse stanno cambiando. Dato che il settore sanitario si espande oltre il perimetro della rete, i criminali informatici fanno altrettanto. Le minacce però non si limitano a spostarsi, ma assumono nuove forme e colpiscono nuovi bersagli. Ogni persona nella tua struttura sanitaria rappresenta un differente livello di sicurezza o rischio per la conformità, in funzione dei dati a cui hanno accesso e del modo in cui usano la tecnologia per svolgere il proprio lavoro.

Il personale infermieristico è quello che ha maggiore accesso alle informazioni dei pazienti, per cui rappresenta un bersaglio primario. I ricercatori medici hanno accesso a preziose proprietà intellettuali, il che ne innalza notevolmente il livello di vulnerabilità. Il personale ospedaliero addetto alle forniture interagisce regolarmente con svariati sistemi di terze parti e ciò aumenta il loro livello di esposizione alle minacce. Le minacce come il phishing delle credenziali permettono ai criminali informatici non solo di prendere il controllo di un account email ma anche di accedere a una miriade di dati archiviati nel cloud, che va oltre la portata dei tradizionali strumenti di sicurezza. Gli operatori della sanità, i pazienti, i medici e altri membri del personale sono esposti a questo nuovo tipo di attacchi concentrati sulle persone.

Inoltre, non dobbiamo dimenticare che le istituzioni sanitarie restano i bersagli preferiti del ransomware e degli altri attacchi basati sul malware che, benché ridotti in volume, sono ora più mirati. Più che mai, le istituzioni sanitarie devono combattere questo tipo di minaccia con un approccio che combini tecnologia e formazione.

Le sfide della sicurezza informatica nel settore della sanità

Nella loro ricerca di approcci innovativi all'erogazione dell'assistenza senza mettere sé stesse, i propri medici e i pazienti a rischio, le organizzazioni sanitarie si trovano ad affrontare delle nuove sfide. I problemi che attendono i responsabili di informatica e sicurezza della sanità nel 2021 e oltre sono ora molto più complessi. Di conseguenza, per le istituzioni sanitarie sarà quindi più difficile mantenere un ambiente sicuro per la telemedicina.

Adozione di nuovi modelli sicuri di assistenza

L'uso della diagnostica mobile, della telemedicina e dell'Internet of Things ha ampliato la superficie di attacco. Gli utenti della sanità usano un'ampia gamma di applicazioni sanitarie mobili, dispositivi medicali portatili e tecnologie utilizzabili in casa. I medici portano i loro dispositivi personali sul lavoro e i loro dispositivi professionali a casa. Inoltre, le tecnologie emergenti e i confini meno definiti fra contesto clinico e domestico aumentano ulteriormente la complessità, contribuendo alla creazione di una infrastruttura informatica decentralizzata, priva di perimetro e molto più difficile da proteggere.

Archiviazione e protezione dei dati

La protezione del rapporto medico-paziente è una parte fondamentale della sanità. Se i dati non vengono conservati in modo sicuro presso le terze parti, oppure vengono trasmessi senza una prima essere crittografati, si corre il rischio di esporre le informazioni dei pazienti. Tutte le strutture sanitarie dichiarano di raccogliere, conservare e condividere dati sensibili, ma solo il 38% afferma di crittografare tali dati[1].

La sicurezza del cloud

Il settore sanitario è consapevole dei molteplici vantaggi del cloud tra cui l'utilizzo di applicazioni standardizzate, i modelli di fatturazione in base all'uso e la riduzione delle spese in conto capitale. A causa del rischio percepito, il settore della sanità è stato lento nell'adottare i servizi cloud, ma ora sta recuperando terreno.

Riconoscendo gli ovvi vantaggi del cloud, i responsabili della sicurezza nella sanità sono alla ricerca di soluzioni che offrano una solida conformità, mantengano la riservatezza e l'integrità delle transazioni e infine che possano essere adattate per proteggere le applicazioni cloud dai dipendenti e dai partner della supply chain.

Allo stesso tempo, molte istituzioni sanitarie continuano a usare sistemi obsoleti, data la natura proprietaria di alcuni componenti, il che impedisce loro di passare ai servizi cloud. A sua volta, ciò introduce ulteriori rischi poiché i criminali informatici sfruttano le nuove vulnerabilità per diffondere il malware, compresi gli attacchi ransomware, che possono mettere offline un'intera organizzazione.

Protezione della supply chain

Per svolgere il proprio lavoro, le società operanti nel settore della sanità dipendono da numerosi fornitori esterni, partner e associati. Queste relazioni interdipendenti formano un complesso ecosistema di terze parti, vulnerabile ai furti e ai rischi informatici emergenti. Si tratta di nuovi punti di ingresso, utilizzabili dai criminali informatici per compromettere la catena di fornitura ospedaliera. Più che mail la sicurezza di una struttura sanitaria si misura all'anello più debole della catena. Quando un solo anello debole della catena di fornitura ospedaliera viene compromesso e poi utilizzato per estrarre dati sensibili, le conseguenze possono essere drammatiche.

Evoluzione del panorama delle minacce informatiche nel settore della sanità

La crescita del mercato ad alto valore delle informazioni mediche rende le strutture sanitarie un obiettivo interessante. È necessario quindi adottare un approccio difensivo e supporre che il settore verrà aggredito da minacce quali gli attacchi da parte di Stati e la pirateria informatica. I virus e il semplice malware sono un ricordo del passato. Gli attacchi informatici più devastanti sono quelli incentrati sulle persone e perpetrati da hacker che hanno individuato nel corso del tempo punti strategici di ingresso, che collettivamente possono provocare danni considerevoli. Secondo una ricerca, sono le strutture sanitarie quelle che impiegano il tempo maggiore per rilevare una violazione dei dati, con una media di 329 giorni[2].

1 2019 Thales Data Threat Report (Report 2019 di Thales sulle minacce ai dati)

2 Ponemon Institute, 2020 Cost of a Data Breach Report from IBM Security (Report 2020 sul costo di delle violazioni dei dati) di IBM Security

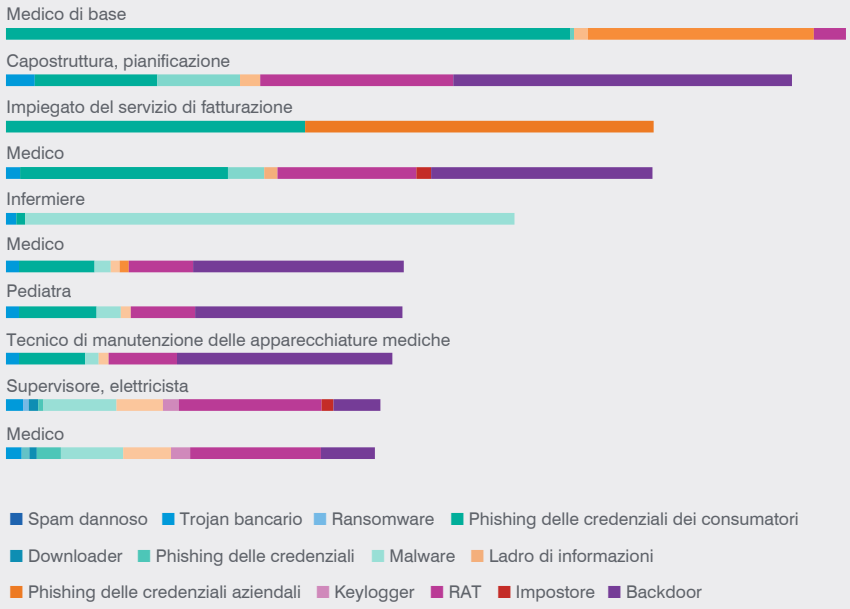

Figura 1: ripartizione dei VAP in un prestigioso ospedale pediatrico.

Adozione di un approccio incentrato sulle persone

Gli attacchi informatici attuali prendono di mira le persone, non la tecnologia. Ecco perché le strutture sanitarie devono adottare un approccio incentrato sulle persone per difendere il personale medico e non medico e i dati sensibili che utilizzano e condividono. La missione delle strutture sanitarie è quella di fornire un'assistenza ottimale ai pazienti, spesso in tempi brevi, che non concede loro di soffermarsi a considerare la legittimità di un'email. Questa è una delle ragioni per le quali il settore resta un facile bersaglio dei criminali informatici oltre al fatto che il potenziale guadagno in caso di successo di un attacco è elevato.

Allo stesso tempo, le strutture sanitarie devono soddisfare gli stringenti requisiti del Regolamento Generale sulla Protezione dei Dati (GDPR) dell'Unione Europea, soprattutto per quanto riguarda il trattamento e la conservazione dei dati genetici, biometrici e medici, tutte categorie incluse nell'elenco dei dati considerati sensibili, per i quali è necessario attuare livelli di controllo più elevati. Le strutture sanitarie devono implementare adeguati controlli di sicurezza per proteggere tali dati, non solo al fine di evitare potenziali sanzioni, ma anche per tutelare la privacy dei pazienti.

Il nostro report del 2020 sul panorama delle minacce nel settore della sanità prende in esame quelle che definiamo VAP (Very Attacked People™ ovvero le persone più attaccate) nel settore della sanità. Utilizziamo questo termine per indicare gli utenti all'interno di un'azienda che sono più duramente colpiti dalle minacce informatiche. La Figura 1 mostra un esempio concreto.

Ospedale pediatrico

In questo esempio, i medici occupano la posizione più attaccata. Le preoccupazioni per la privacy aumentano quando si tratta di bambini perché sono un bersaglio popolare per i furti di identità.

La cartella clinica di un minore è estremamente preziosa nel dark web o nell'economia sommersa. La maggior parte dei bambini non ha ancora una storia creditizia e sicuramente non avrà presentato una richiesta di prestito o di carte di credito al momento della violazione. I criminali informatici sanno che la maggior parte delle persone non controlla se loro dati vengono utilizzati per scopi fraudolenti. È interessante notare che il il numero di backdoor è più elevato nell'ambito della gestione delle strutture, dove i controlli di sicurezza sono spesso meno solidi ed efficaci.

Questi ambienti utilizzano sovente delle risorse permissive, come i dispositivi IoT e gli impianti di filtraggio dell'aria. Non è raro che fungano da vettori di attacco per infiltrarsi nella struttura informatica di un'azienda.

Scenari di utilizzo nel settore della sanità

Sicurezza distribuita

La sanità abbraccia un'ampia gamma di organizzazioni e di ambienti informatici, che condividono informazioni fra pazienti e personale medico per migrare a un modello assistenziale connesso o incentrato sul paziente. L'email è un metodo molto diffuso per la distribuzione di informazioni riservate e la maggioranza delle più clamorose violazioni di dati nel settore della sanità inizia infatti con attacchi di phishing mirati.

Proofpoint offre soluzioni su misura per il settore sanitario, per proteggere gli utenti nel contesto attuale:

- **Proofpoint Email Protection** è una soluzione di email security ad alte prestazioni per bloccare il malware e le altre minacce.
- **Proofpoint Data Loss Prevention (DLP)** limita il rischio delle perdite di dati via email e protegge contro le frodi via email.
- **Proofpoint Targeted Attack Protection (TAP)** rileva e blocca le minacce avanzate grazie alle funzionalità di sandboxing.

- **Proofpoint Threat Response** consente alle organizzazioni di rispondere rapidamente per neutralizzare le minacce e rimuovere le email dannose.
- **Il programma Proofpoint Security Awareness Training** offre corsi di formazione per insegnare ai dipendenti a individuare gli attacchi di social engineering che colpiscono il settore sanitario, incluse le sofisticate tecniche di phishing.

Protezione contro gli attacchi fraudolenti

Le email fraudolente sono messaggi ingannevoli, concepiti per sembrare provenienti da qualcuno che il destinatario conosce o di cui si fida. Tali attacchi possono essere difficili da rilevare perché non sfruttano le vulnerabilità tecniche. I loro bersagli sono specifiche mansioni che hanno accesso ad attività monetizzabili: farmacisti, ricercatori medici, operatori della supply chain o personale ospedaliero di base.

Proofpoint offre una soluzione integrata, incentrata sulle persone, end-to-end, che blocca tutte le forme di frode via email, a prescindere dalla tattica usata o dalla persona presa di mira:

- **La soluzione di sicurezza avanzata dell'email di Proofpoint** blocca il phishing e le email fraudolente che utilizzano nomi di dominio cugini o falsificati. Si basa su un sistema di machine learning avanzato e su diversi motori di rilevamento per individuare tali attacchi mirati e bloccarli prima che raggiungano le caselle email degli utenti.
- Il protocollo **DMARC (Domain-based Message Authentication Reporting and Conformance)** viene utilizzato per agevolare l'autenticazione dell'email. Blocca le email falsificate prima che ingannino dipendenti, personale medico e collaboratori dell'azienda.

Protezione di Microsoft 365 e di altri ambienti cloud

Una soluzione CASB (Cloud Access Security Broker) è un elemento critico di un'architettura di sicurezza cloud. Sempre più organizzazioni sanitarie stanno migrando dati e applicazioni nel cloud e accedono a un maggior numero di dati sensibili tramite una connessione a Internet. Hanno quindi bisogno di visibilità sulle attività nel cloud in tutto l'ecosistema sanitario e la supply chain.

Proofpoint CASB aiuta le organizzazioni ad analizzare e neutralizzare rapidamente le potenziali violazioni delle policy email nel cloud, per garantire la continuità delle cure. Riduce il rischio di un attacco informatico o di una violazione dei dati e sfrutta il flusso delle email di un'azienda per identificare i dati riservati nei servizi di hosting dei file nel cloud, come Microsoft 365, Dropbox, Box e Salesforce.

Protezione della collaborazione nel settore sanitario

Per fornire un'assistenza ottimale, il personale sanitario deve essere in grado di collaborare e comunicare efficacemente. Dispone pertanto di soluzioni mobili che mettono in contatto medici e pazienti, ma che sono concepite per essere funzionali e comodi piuttosto che sicuri e spesso vengono utilizzate oltre i confini della rete aziendale protetta.

I medici possono accedere alle applicazioni cliniche anche dai loro dispositivi personali oppure utilizzare i loro account email personali su un dispositivo fornito dall'azienda. **Proofpoint Browser Isolation** mantiene le attività personali degli utenti e i contenuti pericolosi fuori dal tuo ambiente, isolando la webmail e gli URL presenti nelle email all'interno di un contenitore protetto. Gli utenti possono ancora accedere ai propri account personali liberamente e privatamente, tramite il loro consueto browser web, ma le azioni e i contenuti potenzialmente dannosi sono disattivati, per preservare la sicurezza del tuo ambiente.

Protezione dalle minacce interne

Un utente interno che trafuga le informazioni dei pazienti da uno studio medico o da un ospedale è una scena degna di una serie TV. Eppure, le minacce interne sono molto reali. Anzi, quasi la metà di tutte le violazioni nel settore della sanità ha visto il coinvolgimento di un utente interno[3].

Tre dei più comuni rischi di minaccia interna e di perdita di dati per le istituzioni sanitarie sono i seguenti:

1. Furto o uso improprio di informazioni sanitarie protette
2. Furto o uso improprio di cartelle cliniche elettroniche
3. Frode finanziaria e assicurativa

Proofpoint Insider Threat Management (ITM) protegge contro la perdita di dati, atti dolosi e danni al marchio causati dalle azioni dannose, negligenti o inconsapevoli degli utenti interni. La nostra soluzione ITM correla attività e spostamenti dei dati, permettendo agli addetti alla sicurezza di identificare i rischi legati agli utenti, rilevare e contrastare le violazioni dei dati causate dal personale interno e accelerare la risposta agli incidenti di sicurezza.

3 Verizon, 2020 Data Breach Investigations Report (Report 2020 sulle violazioni dei dati)

Sicurezza delle informazioni sanitarie personali: protezione dei dati dei pazienti

Nel settore della sanità l'email è il principale vettore delle minacce. Perciò è essenziale disporre di una soluzione adeguata per la prevenzione della perdita dei dati (DLP) per garantire che le informazioni sensibili e critiche siano classificate e accessibili solo dalle persone giuste.

Grazie alla soluzione **DLP incentrata sulle persone di Proofpoint**, le istituzioni sanitarie possono identificare e neutralizzare rapidamente ai rischi associati a utenti negligenti, compromessi e malintenzionati. La piattaforma unificata di Proofpoint consente ai clienti di definire e i dati di valore e di usare tali definizioni in tutto l'ambiente e quindi proteggere la privacy di ogni singola email grazie a **Proofpoint Email Encryption**. Gli utenti possono attivare automaticamente la crittografia dei messaggi aggiungendo una parola chiave a propria scelta nella riga dell'oggetto oppure attivare la crittografia a livello di messaggio sulla base delle regole DLP.

Lo strumento di gestione degli incidenti unificato di Proofpoint non solo permette agli utenti di visualizzare le violazioni alle policy DLP a livello di email, cloud ed endpoint da una postazione centralizzata, ma fornisce anche informazioni dettagliate sulle minacce e sul contesto, combinando questi dati.

Gestione degli standard di conformità normativa e riduzione della complessità

Molte aziende regolamentate stentano a:

- identificare i canali di comunicazione utilizzati;
- assicurarsi che il contenuto generato da tali comunicazioni sia acquisito e archiviato in modo sicuro;
- cercare e recuperare i contenuti per le verifiche in modo rapido ed economico;
- monitorare e supervisionare i dipendenti che utilizzano questi canali.

La soluzione **di archiviazione e conformità di Proofpoint** offre una conformità onnicomprensiva e incentrata sulle persone.

Potrai così godere dei seguenti vantaggi:

- Copertura dal momento in cui il contenuto viene distribuito fino a quando viene indicizzato, archiviato e recuperato
- Applicazione automatica delle tue policy normative, compresi le norme sanitarie locali e le regole correlate al GDPR
- Certezza del fatto che le attività di interazione digitali rispettino le regole di comunicazione e conservazione
- Possibilità di supervisionare, correggere (rivedere o rimuovere) e archiviare i contenuti in modo semplice, rapido ed economico

Conclusioni

Proofpoint offre alle strutture sanitarie visibilità e protezione per il loro rischio più grande per la sicurezza informatica: le loro persone. Offriamo la sicurezza informatica più efficace per proteggere i professionisti della sanità, sia che vengano colpiti tramite l'email, il web, i social media o le applicazioni cloud. Contribuiamo a bloccare le minacce prima che raggiungano il personale medico e di supporto, a proteggere i dati e in ultima analisi a proteggere i pazienti dagli attacchi informatici. Importanti strutture sanitarie di tutte le dimensioni si affidano a Proofpoint per prevenire, rilevare e neutralizzare le minacce critiche prima che provochino danni.

PER SAPERNE DI PIÙ

Per scoprire come adottare un approccio incentrato sulle persone per proteggere i tuoi dati, le tue operazioni e la tua missione assistenziale visita il sito **proofpoint.com/us/solutions/healthcare-information-security**.