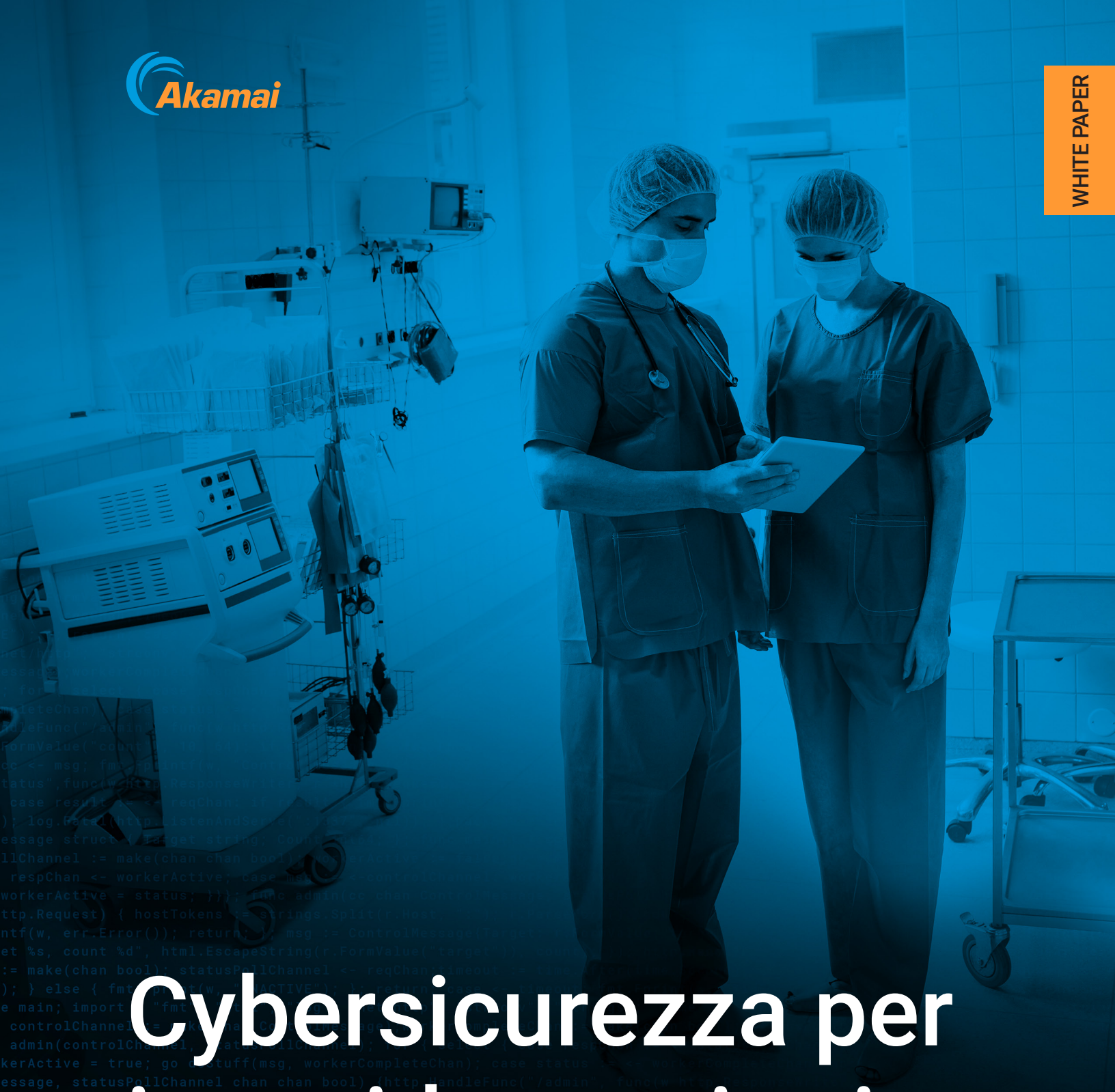
Akamai

WHITE PAPER



Cybersicurezza per i provider sanitari

Introduzione

Per competere in un mercato in rapida evoluzione, i provider di servizi sanitari devono adottare nuovi dispositivi e applicazioni in grado di fornire ai pazienti un'assistenza eccellente ed experience innovative. Ogni nuova aggiunta apporta i suoi vantaggi ai pazienti, ma anche specifici rischi per la sicurezza dell'organizzazione.

Questo complesso ambiente IT, insieme con l'elevato valore delle informazioni sanitarie protette (PHI), crea un'irresistibile opportunità per i criminali informatici, che continuano a colpire i sistemi. Secondo un rapporto stilato dal dipartimento della salute e dei servizi umani degli Stati Uniti e in base ad una ricerca condotta da IBM, il settore sanitario ha registrato un aumento del 50% nel numero di attacchi informatici dall'inizio della pandemia e questi attacchi sono stati i più costosi, con un costo medio di 7,13 milioni di dollari per incidente. Il rapporto di IBM ha messo in evidenza come la minaccia più comune sia stata rappresentata dai ransomware, in quanto i criminali sfruttavano la necessità degli ospedali e delle strutture sanitarie di ripristinare velocemente i sistemi, seguiti a ruota dal furto di dati e dall'accesso ai server. Le strutture sanitarie sono un bersaglio particolarmente allettante per i criminali perché è possibile vendere sul dark web le cartelle cliniche elettroniche a 1.000 dollari ciascuna rispetto ai dati delle carte di credito, che vengono venduti a circa 110 dollari o ai numeri di previdenza sociale venduti a 1 solo dollaro ciascuno.

Considerando il numero di minacce contro i sistemi sanitari in costante crescita, molte organizzazioni non sono adeguatamente preparate per mitigarli o, ancora peggio, potrebbero in alcuni casi essere già state violate senza saperlo. Magari i criminali hanno già esfiltrato i dati oppure stanno aspettando il momento giusto per sferrare il loro attacco.

Questo è quindi il momento giusto per fare chiarezza sulla superficie di attacco della vostra organizzazione stilando un inventario dei dispositivi e del modo con cui sono connessi all'infrastruttura. Conoscendo meglio le aree vulnerabili, sarà più semplice mettere in atto un appropriato piano di mitigazione per prevenire o minimizzare il potenziale impatto degli attacchi informatici.

Come coprire i rischi maggiori per la cybersicurezza della vostra organizzazione

Minaccia 1. Gli attacchi di phishing

Il phishing è uno dei più comuni vettori di attacchi informatici in tutti i settori. Secondo l'Health Sector Cybersecurity Coordination Center, il 2021 ha fatto registrare un aumento significativo di attacchi di phishing nel settore sanitario. In effetti, per tutto il 2020, Akamai ha osservato i criminali sfruttare il COVID-19 e la promessa di assistenza finanziaria o lo stress derivante dalle difficoltà economiche per prendere di mira gli utenti di tutto il mondo tramite il phishing.

Il phishing tenta di acquisire dati sensibili tramite e-mail o pagine web fraudolente. Se riesce nel suo intento, questo attacco forza gli utenti ad inserire inavvertitamente le loro credenziali di accesso, offrendo, in pratica, ai criminali una porta aperta sulla rete.

Questa situazione si è verificata ad alcune persone che stavano richiedendo il sussidio di disoccupazione a New York. Secondo un rapporto sul phishing stilato da Steve Ragan, in precedenza redattore per CSO Online e, attualmente, ricercatore della sicurezza di Akamai, molti kit di phishing hanno preso di mira i programmi di assistenza per la disoccupazione pandemica (PUA) agli inizi del 2021. Questi programmi sono stati concepiti per assistere chi ha perso il lavoro a causa dei lockdown durante la pandemia di COVID-19 e hanno fornito servizi essenziali per milioni di americani.

In uno spot apparso su CBS News trasmesso negli Stati Uniti, Ragan ha parlato di un kit di phishing che ha preso di mira alcuni disoccupati di New York e di come i criminali siano riusciti a raccogliere e vendere le informazioni personali violate durante la truffa. Non appena questa storia è stata trasmessa, Ragan ha scoperto che le truffe PUA hanno preso di mira varie persone in Wisconsin, Indiana, Pennsylvania e Massachusetts.

Come bloccare e mitigare gli attacchi di phishing

A seconda delle impostazioni dei permessi e dei sistemi di sicurezza messi in atto, guadagnare l'accesso all'account di un singolo utente può potenzialmente fornire ai criminali la libertà di agire in parti critiche della rete e quindi, spesso, la possibilità di ampliare il loro raggio d'azione una volta penetrati all'interno della rete di un'organizzazione.

La microsegmentazione confina l'accesso dei criminali solo alle parti della rete a cui inizialmente hanno effettuato l'accesso, impedendo loro di muoversi lateralmente e di infliggere ulteriori danni in altre aree. Così facendo, limita l'impatto di una violazione evitando che i criminali usino eventuali punti di ingresso per accedere in modo più ampio alla rete di un'organizzazione.

Oltre alla microsegmentazione, l'autenticazione multifattore (MFA) è una delle migliori linee di difesa dagli attacchi di phishing poiché fornisce un ulteriore livello di protezione richiedendo un'altra verifica delle identità prima di concedere l'accesso ad un account, impedendo così lo sfruttamento delle credenziali violate.

L'MFA, nello specifico una soluzione con approvazione FIDO2, garantisce la protezione dagli ultimi attacchi e richiede agli utenti di inserire un codice univoco generato tramite un'app di testo o di autenticazione sul dispositivo mobile dell'utente. Questo ulteriore passaggio nel processo di accesso aiuta a contrastare gli attacchi di phishing, anche quando i criminali dispongono di precise credenziali di accesso.

È fondamentale formare il personale sulle tattiche utilizzate negli attacchi di social engineering come il phishing. In realtà, il phishing è uno di quei problemi che non possono essere risolti completamente perché vi incidono troppe variabili. È difficile prevedere le future mosse dei criminali. Poiché l'uomo è comunque un aspetto vitale del phishing, rimane l'anello debole della catena.

Ecco perché è fondamentale semplificare la sicurezza. Akamai offre una soluzione MFA semplice e anti-phishing per proteggersi anche dai criminali informatici più scaltri.

Minaccia 2. Software legacy non supportato

I software obsoleti sono un'altra causa significativa di vulnerabilità. Ogni nuovo aggiornamento di sicurezza (patch) che non viene installato immediatamente crea una backdoor aperta nella rete, soprattutto nel caso di dispositivi obsoleti che non sono più supportati e non vengono più aggiornati.

Un software non supportato può presentare vulnerabilità zero-day e, pertanto, le organizzazioni potrebbero esitare ad applicare le patch autonomamente. La creazione di una patch personalizzata può, spesso, rendere nulla la garanzia di un dispositivo, causando costose riparazioni in caso di problemi.

Benché i dispositivi medici abbiano un lungo ciclo di vita, se non vengono scrupolosamente aggiornati con l'ultima versione del sistema operativo o se vengono eseguiti su un sistema operativo non supportato, gli hacker potranno sfruttare eventuali vulnerabilità per rubare dati, penetrare nella rete di un ospedale e bloccare l'assistenza sanitaria. In realtà, l'83% dei dispositivi di imaging medico connessi a Internet (dalle macchine per le mammografie alle apparecchiature per la risonanza magnetica) è vulnerabile, come segnalato da Fortune.

Più un dispositivo è obsoleto, specialmente quelli oltre il ciclo di vita della manutenzione, più probabilmente i criminali ne conoscono i punti deboli che possono consentire loro di accedere alla rete di un'organizzazione tramite un dispositivo di terze parti.

Ad esempio, la manutenzione di Windows 95 non viene eseguita da anni, tuttavia, molte apparecchiature per la risonanza magnetica (ma non solo) continuano a basarsi su questo sistema operativo poiché è stato l'ultimo a fornire la funzionalità di scrittura diretta. Gli sviluppatori in-house potrebbero riuscire a correggere una vulnerabilità, ma la loro patch potrebbe invalidare la garanzia dell'apparecchiatura. L'unica opzione sicura è sostituire l'apparecchiatura per la risonanza magnetica, che, tuttavia, per molte strutture è una soluzione proibitiva in termini di costi.

Gli amministratori di rete cercano di tenere i sistemi non supportati all'esterno della rete, ma non sempre ci riescono, specialmente se i dispositivi sono necessari per l'assistenza ai pazienti e se devono fornire rapidamente i dati ai medici. Inoltre, l'isolamento è fallace se la mappa dei dispositivi connessi alla rete è incompleta, una condizione che crea potenziali backdoor. È difficile proteggere ciò che non si vede.

Come proteggere i dispositivi vulnerabili non supportati

Per proteggere questi dispositivi impedendo che forniscano l'accesso alla rete di un'organizzazione, è cruciale passare ad un'architettura ZTNA (Zero Trust Network Access). Il sistema ZTNA tratta ogni richiesta in entrata come una potenziale minaccia finché non viene dimostrato che sia sicura, fermando in modo efficace i criminali prima che ottengano l'accesso al dispositivo, anche se il software è obsoleto.

Il percorso verso l'approccio ZTNA segna una svolta fondamentale, che implica il passaggio dal tradizionale vecchio approccio perimetrale alla sicurezza ad un modello Zero Trust (basato sulla verifica preliminare). Anche se un approccio Zero Trust probabilmente non protegge completamente dagli attacchi informatici, può limitare il potenziale danno catastrofico rendendolo gestibile. HealthITSecurity afferma giustamente: "Se un criminale riesce ad ottenere le credenziali e a manipolare un dispositivo, è improbabile che possa fare molto di più quando è implementata un'architettura Zero Trust".

Akamai offre un solido piano per aiutare i provider a passare ad un'architettura Zero Trust, senza problemi di downtime e la flessibilità dei workflow attuali. Per informazioni sull'approccio ZTNA, potete consultare questa guida visiva.

Minaccia 3. Provider che lavorano da casa e in modalità BYOD (Bring Your Own Device)

La continuità assistenziale nel 21° secolo è decentralizzata. I pazienti ricevono l'assistenza necessaria restando comodamente a casa. I provider di servizi sanitari forniscono l'assistenza richiesta tramite il proprio dispositivo mobile piuttosto che di persona. Tuttavia, questo aumento di accessibilità implica un aumento notevole dei rischi per la cybersicurezza osservato dai provider di servizi sanitari, mentre i membri del personale oscillano tra varie modalità di accesso alle reti (on-site e da casa o da dispositivi non gestiti).

Se prima della pandemia i membri del vostro team effettuavano l'accesso al vostro sistema dalla rete di casa solo occasionalmente, il numero di dispositivi personali che accedono alla rete della vostra organizzazione ha inevitabilmente raggiunto oggi un picco. Se questi dispositivi (laptop, tablet o smartphone) fossero infettati da malware, potrebbero diventare un punto di ingresso per un attacco ransomware.

Ad esempio, se un membro del vostro team subisce un attacco di phishing perché ha inserito senza volere le proprie credenziali di accesso in una pagina web fittizia, i criminali potranno guadagnare lo stesso livello di accesso di questo utente, riuscendo, potenzialmente, a crittografare i file, a bloccare l'accesso al team e a paralizzare la vostra organizzazione richiedendo un cospicuo riscatto per decrittografare i file.

Come proteggere il perimetro della rete

Monitorando attentamente gli utenti che accedono alla rete della vostra organizzazione (dove si trovano, qual è il loro indirizzo IP, quale dispositivo utilizzano, ecc.), potete minimizzare la probabilità che si verifichi una situazione simile e agire per bloccare un attacco prima che venga sferrato.

Se il vostro team utilizza dispositivi personali o lavora da casa, dovreste farvi queste domande:

- Abbiamo messo in atto un approccio ZTNA (Zero Trust Network Access) per massimizzare il controllo sulle richieste in arrivo e fermare un attacco prima che si verifichi?
- Abbiamo adottato la microsegmentazione per limitare l'accesso e impedire il movimento laterale se un criminale riesce ad entrare nella rete dell'organizzazione?
- Stiamo usando un sistema SASE (Secure Access Service Edge) per proteggere la nostra rete, minimizzando, al contempo, la latenza e mantenendo user experience rapide e piacevoli?
- Il nostro team utilizza codici di accesso, password complesse e univoche e l'autenticazione multifattore (MFA) per l'accesso a tutti i dispositivi e gli account?

Akamai aiuta a semplificare la gestione degli accessi alla rete con le sue soluzioni per la sicurezza dei collaboratori da remoto.

Minaccia 4. Scarsa mappatura del flusso dei dati

Con un piede nell'ambiente on-premise e l'altro nel cloud, può risultare quasi impossibile capire deve risiedono i dati e come avviene il loro flusso. Questo aspetto si verifica per un paio di diversi motivi.

Innanzitutto, il volume, che può risultare enorme per stare al passo con il numero di applicazioni e dispositivi aggiunti e rimossi dalla rete ogni giorno (se non ogni ora) poiché vendor, collaboratori e consulenti utilizzano tutti diversi dispositivi, strumenti e soluzioni.

In secondo luogo, il sistema di tracciamento di hardware e software è ormai defunto e non è più accurato o affidabile a causa dell'avvicendamento dei membri del team, dei cambiamenti dei processi o delle altre priorità.

Indipendentemente dal motivo, è importante avere la massima visibilità sulla rete e sui dispositivi connessi perché è impossibile proteggere ciò che non si vede.

Come mappare il flusso dei dispositivi connessi

È cruciale disporre di uno strumento di visibilità in grado di creare una roadmap dei dispositivi connessi, specialmente considerando che un articolo del 2019 pubblicato nel HIPAA Journal ha riportato che l'82% delle organizzazioni sanitarie ha subito un attacco informatico contro i propri dispositivi connessi nei 12 mesi precedenti.

La scelta di una soluzione in grado di monitorare il flusso dei dati sulla rete, fornendo informazioni sulla loro provenienza e sulla loro destinazione, inclusi i dispositivi non connessi alla rete, è il primo passo che consente di mappare i dispositivi connessi. In tal modo, potete disporre di un diagramma di rete in tempo reale in cui è visibile la destinazione del flusso delle informazioni e tramite cui potete rilevare i dispositivi eventualmente presenti sulla vostra rete che mostrano intenti dannosi. Se vengono inseriti livelli di microsegmentazione definiti da software intorno ai sistemi, alle risorse e ai dati principali (come le informazioni PHI), la vostra organizzazione può limitare il movimento laterale dei criminali all'interno della propria rete. Ottenete la visibilità che vi serve con gli strumenti di microsegmentazione offerti da Akamai.

Minaccia 5. Gestione delle complessità di reti, app e sistemi

Sapete quali applicazioni e software possono leggere i vostri dati? Alcune applicazioni software, come le piattaforme dei social media, dichiarano chiaramente quanto saranno invasive nei confronti degli utenti nella loro informativa sulla privacy o nei termini di servizio. I provider dei servizi e-mail, invece, ad esempio, sono più discreti, ma comunque pongono rischi significativi (come nel caso di accesso alle foto memorizzate su un dispositivo se le immagini contengono informazioni PHI).

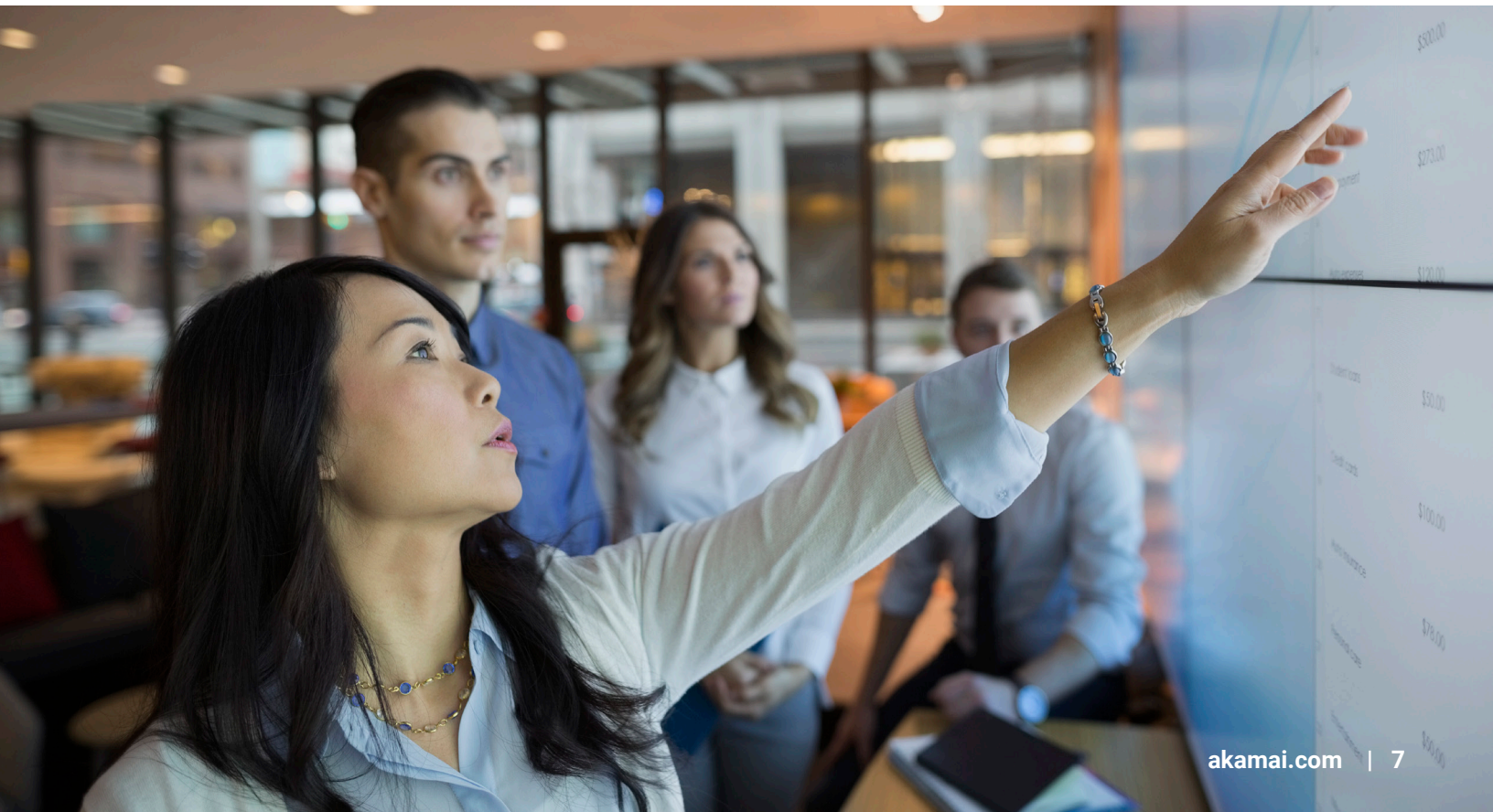
Alle app viene anche consentito di visualizzare elementi copiati negli appunti, inclusi ID o password dei pazienti Se su un dispositivo sono memorizzate informazioni sui pazienti, esiste una possibilità che altri utenti (o criminali) possano vederle (e registrarle).

Formazione del team, visibilità su tutta la rete e protezione del perimetro

È fondamentale formare tutti i membri dell'organizzazione del vostro provider sui rischi derivanti dall'utilizzo di dispositivi personali e su ciò che è richiesto per proteggere le informazioni private dei pazienti.

È anche importante considerare la visibilità della vostra organizzazione sulla propria superficie di attacco e sui potenziali vettori. Il vostro team addetto alla sicurezza sta monitorando tutta la rete nei diversi provider di servizi cloud e nei data center on-premise? O invece questi vari gruppi sono separati tra loro in base ai diversi aspetti dell'infrastruttura della vostra organizzazione? È fondamentale mantenere una visione olistica di tutta la rete della vostra organizzazione e delle sue attività, specialmente durante un attacco.

Analogamente alla minaccia 4, le migliori opzioni di protezione del perimetro della vostra rete sono l'adozione di un'architettura Zero Trust combinata con funzionalità di microsegmentazione e l'utilizzo dell'autenticazione MFA per gli accessi agli account. L'utilizzo di un solo provider per proteggere tutti i sistemi indipendentemente dai loro proprietari e dalla loro posizione (on-premise o nel cloud) vi consentirà di proteggere la vostra rete senza compromettere le user experience.



Cosa succede se non si fa nulla?

Si può incorrere in costi di vario tipo, di cui il più ovvio è rappresentato dalle spese finanziarie, se consideriamo che le strutture sanitarie negli Stati Uniti devono affrontare in media 9,23 milioni di dollari di costi nel caso di una sola violazione di dati, secondo il rapporto stilato da IBM sui costi di una violazione di dati nel 2021. Altri costi sono di tipo più qualitativo, come la fiducia e la sicurezza dei pazienti, che possono influire ugualmente, se non maggiormente, sulle strutture sanitarie.

Minore sicurezza dei pazienti

Quando si tratta di cybersicurezza, la sicurezza dei pazienti è l'obiettivo più significativo. Se i sistemi IT vengono costretti a bloccarsi mediante un attacco, si interrompe anche l'assistenza ai pazienti. Le cure e gli appuntamenti vengono posticipati e ci possono essere conseguenze negative sulla salute dei pazienti. In realtà, una recente azione legale ha portato all'attenzione per la prima volta la morte di un paziente causata direttamente da un attacco ransomware.

Intanto, i dispositivi medici connessi, che vengono utilizzati per il monitoraggio remoto dei pazienti (ad esempio, per controllare il battito cardiaco o i livelli di glucosio), pongono una minaccia più diretta sull'assistenza sanitaria. Ad esempio, l'interruzione della visualizzazione dei valori relativi alla pressione sanguigna di un paziente potrebbe far ignorare, e quindi non trattare con farmaci, condizioni pericolose, causando potenzialmente un evento di allerta.

Perdita della fiducia dei pazienti

L'impossibilità di fornire un'assistenza sanitaria affidabile e di proteggere le informazioni dei pazienti conduce ad una perdita della fiducia da parte loro. Più del 90% dei pazienti afferma che cambierebbe provider se le loro informazioni private venissero compromesse in una violazione di dati. Il numero effettivo potrebbe diminuire quando arriva il momento, ma facciamo comunque un po' di calcoli: anche se solo metà (o un decimo) di questi pazienti cambiassero provider, quale impatto ci sarebbe sugli altri pazienti? E per quanto tempo dovreste incorrere in perdite fino ad acquisire gradualmente nuovi pazienti?

Perdita di ricavi

Per il 38% dei pazienti, la perdita di affari è il tipo di costo maggiormente associato ad una violazione di dati. Quando i sistemi principali di un provider si bloccano (come le cartelle cliniche elettroniche, i server di posta elettronica, ecc.), si interrompono bruscamente anche le opportunità commerciali, il che si traduce in una perdita di appuntamenti, visite, colloqui e ricavi (per non parlare dell'impatto sull'assistenza sanitaria ai pazienti).

Scripps Health, una struttura sanitaria con sede a San Diego, ha subito un imponente attacco informatico a maggio 2020 che le ha causato la perdita di 91,6 milioni di dollari di ricavi, principalmente per la diminuzione dell'assistenza sanitaria in pronto soccorso e degli interventi non urgenti.

Anche se alcune parti della rete del sistema sanitario rimangono operative, non si può avere la certezza che tutto sia al sicuro finché non viene individuato il vettore di attacco, non viene corretta la vulnerabilità e non si effettuano analisi e indagini.

Incremento dei costi fissi

Il reclutamento, le assunzioni e il mantenimento di tecnici dedicati alla cybersicurezza sono operazioni costose, anche se i costi effettivi possono essere superiori. L'utilizzo di un team addetto alla cybersicurezza formato internamente alla vostra organizzazione può lasciarvi con costose lacune nella copertura.

In genere, più tempo serve alla vostra organizzazione per identificare ed esfiltrare un criminale dalla rete, più saranno elevati i costi associati. Un rapporto stilato dal Ponemon Institute afferma che il rilevamento di un attacco informatico entro i primi 200 giorni può far risparmiare ad un'organizzazione più di 1,26 milioni di dollari. Purtroppo, secondo lo stesso rapporto, sono richiesti, in media, 287 giorni per identificare e contenere un attacco. *287 giorni!* Ciò significa che i criminali rimangono spesso all'interno dell'infrastruttura di rete per più di nove mesi per poter progettare e pianificare il loro attacco in modo da arrecare il massimo danno alla reputazione e al fatturato del vostro ospedale.

È fondamentale, pertanto, quantificare il tempo richiesto al team addetto alla sicurezza per identificare e adottare le azioni appropriate contro un attacco. Consolidare i vendor di soluzioni per la sicurezza che offrono servizi gestiti e supporto tecnico in caso di aumento del personale può implicare notevoli risparmi in termini di costi.

Sanzioni normative

Poiché la vostra organizzazione è responsabile di una notevole quantità di preziose informazioni personali, una violazione dei dati può condurre a pesanti sanzioni imposte dalle agenzie di regolamentazione. A partire dal 30 novembre 2021, l'ufficio per i diritti civili del dipartimento della salute e dei servizi umani degli Stati Uniti ha stabilito o imposto sanzioni contro 106 entità che rientrano nell'HIPAA per un totale di oltre 131 milioni di dollari, con una media di più di 1,2 milioni di dollari per sanzione (oltre ai costi aggiuntivi qui menzionati).

Come preparare al meglio la vostra azienda sanitaria per fronteggiare un attacco informatico

Le odierne minacce informatiche richiedono alle aziende sanitarie un sistema di sicurezza leader del settore. I vostri pazienti e le vostre attività aziendali dipendono da questo: non agire ha un prezzo troppo alto.

I vincoli finanziari, le priorità concorrenziali o l'incertezza dei rischi potrebbero spingervi ad assumere troppi rischi. Tuttavia, il vostro sistema di sicurezza deve essere accurato, strategico, sicuro e agile.

Un ecosistema adeguatamente protetto oggi potrebbe non essere protetto domani. Le minacce si evolvono rapidamente. Un giorno (o meno) può bastare ai criminali per sfruttare una nuova vulnerabilità.

Le aziende sanitarie stanno cercando di ridurre l'area delle minacce e di accogliere il suggerimento di un approccio basato sui backup evidenziato nell'avviso federale, ossia salvare tre copie in almeno due formati diversi, con una copia offline, e stanno guardando sempre più a un approccio ibrido. L'archiviazione dei dati on-premise offre loro un maggior controllo sulla sicurezza, ma può essere costosa e difficile da espandere quando necessario, soprattutto con l'esplosione corrente di dati sanitari e la trasformazione digitale in atto nelle cure, entrambe spinte dalla pandemia. L'archiviazione dei dati nel cloud pubblico è più economica, ma le organizzazioni rischiano interruzioni e mancanza di trasparenza nel modo in cui i dati vengono protetti.

Un approccio ibrido consente di tenere i dati sensibili on-premise e di archiviare quelli meno sensibili nel cloud. Ma anche questo approccio non è perfetto, in quanto è necessario mettere in atto la sicurezza per proteggere il trasferimento dei dati tra due tipi di archiviazione e garantire che l'accesso sia limitato a coloro che sono autorizzati a trasferire e visualizzare i dati. Passare ai 7 requisiti chiave per implementare un'architettura ZTNA aiuta le istituzioni a proteggere i loro dati, concedendo agli utenti l'accesso solo alle applicazioni di cui necessitano per il loro ruolo, con un'ulteriore sicurezza offerta dall'autenticazione MFA.

Akamai è qui per aiutarvi a prepararvi quando (non se) si verificherà un attacco. Collaboriamo per costruire una visione coesa della vostra rete per consentirvi di individuare rapidamente un attacco e mitigare il danno in modo efficiente. Le nostre attività aziendali si basano sulla protezione delle reti dagli attacchi DDoS (Distributed Denial-of-Service) e ransomware per offrire web experience semplici e sicure (incluse app e API).

Rafforziamo il perimetro della vostra rete per limitare le possibilità di una violazione e, nel caso si verifichi, per ridurne la portata, mantenendo, al contempo, la flessibilità per gli accessi degli utenti al fine di consentire alla vostra organizzazione di focalizzarsi sull'ottimizzazione dei risultati sanitari nel contesto di esigenze operative e assistenziali in continua evoluzione.

Proteggere le informazioni dei pazienti da criminali informatici sempre più sofisticati e da una crescente superficie di attacco basata sul cloud non è mai stato così importante. Le organizzazioni incentrate sui pazienti e gli enti governativi si affidano alla piattaforma edge di Akamai per avvicinare le loro experience digitali ai pazienti e per allontanare le minacce.

Fidatevi di Akamai, il partner con cui l'onere perpetuo della cybersicurezza si trasforma in una forza competitiva.

Per ulteriori informazioni, potete contattarci o chiamare il numero +1-877-425-2624.