Bitdefender

L’importanza della sicurezza informatica nella Sanità. Come affrontare gli attacchi informatici in costante aumento

di Denis Cassinerio, Regional Director SEUR di Bitdefender

A causa della pandemia, il settore sanitario ha accelerato il processo di digitalizzazione anche se in netto ritardo rispetto ad altri settori.
In questo periodo la telemedicina e l’assistenza domiciliare da remoto stanno assumendo un ruolo sempre più importante grazie al supporto della tecnologia e delle nuove infrastrutture basate sul cloud.

Una ricerca di Accenture mette in evidenza come nell’inizio del 2020, solo il 7% dei pazienti intervistati ha avuto un consulto medico con un operatore sanitario mentre nel 2021 la percentuale è salita al **32%**. Anche l’uso delle cartelle cliniche elettroniche EHR (Electronic Health Records) ed EMR (Electronic Medical Records) è aumentato drasticamente dalla loro introduzione. Nel 2020, **l'89% dei medici** intervistati ha riferito di utilizzare sistemi EHR o EMR.

L’accelerazione alla digitalizzazione del settore sanitario ha portato però ad una maggiore esposizione agli attacchi informatici. La ricerca *“Healthcare Cybersecurity”* di Bitdefender, realizzata in Italia lo scorso maggio 2021, ha valutato lo status di efficienza della sicurezza informatica nel settore sanitario. In particolare tra i risultati più importanti, troviamo che il 93% delle aziende del settore sanitario ha subito attacchi informatici in passato mentre il 64% ritiene probabile, o altamente probabile, un attacco informatico nel prossimo futuro. Nonostante ciò, dalla ricerca emerge che l’efficienza delle strutture sanitarie italiane per affrontare i rischi di sicurezza informatica raggiunge solo il 49%.

Il COVID-19 ha accelerato la digitalizzazione ma ha anche aumentato gli attacchi informatici contro il settore della sanità

Nel giro di poche settimane, la pandemia COVID-19 ha portato alla chiusura degli uffici in tutto il mondo, riempito gli ospedali e trasformato il settore sanitario in un servizio di teleassistenza virtuale. Di conseguenza, l’adozione di fornitori e tecnologie cloud per la sanità è aumentata in modo considerevole senza però, comprensibilmente, considerare con la dovuta attenzione la sicurezza informatica.

L'introduzione accelerata di tecnologie, servizi di infrastruttura e fornitori cloud computing e ha aumentato in modo esponenziale la superficie di attacco e l'esposizione ai rischi per il settore sanitario. Queste aziende ora devono considerare la sicurezza e la gestione dei rischi di terzi, assicurandosi anche che questi fornitori, se hanno in gestione anche dati privati, li stiano trattando secondo gli standard di conformità.

Con il telelavoro, l'avvento del BYOD (Bring Your Own Device) e l'aumento della cosiddetta Shadow IT (l'uso di sistemi, dispositivi, software, applicazioni e servizi IT senza l'esplicita approvazione del reparto IT), tenere sotto controllo le proprie risorse, i fornitori e i dispositivi è

una sfida quasi impossibile. E questo vale anche quando tutti gli endpoint sono già protetti e la rete è adeguatamente protetta.

L'uso di sistemi EHR e di altri sistemi sanitari basati sul cloud per soddisfare le esigenze infrastrutturali e di archiviazione dei dati pone anche un rischio in termini di potenziali perdite. Che sia a causa di un'errata configurazione da parte del provider di servizi cloud o del proprio team interno, le cartelle cliniche possono essere accidentalmente esposte o diffuse su Internet, mettendo i dati e la reputazione del brand in pericolo.

All'inizio di quest'anno, gli esperti di sicurezza informatica hanno trovato più di un miliardo di record disponibili in un database appartenente a CVS Health che non richiedeva alcuna password di accesso. Questo tipo di incidenti non passano inosservati agli utenti, preoccupati di quanto siano sicuri i propri dati nelle mani delle strutture sanitarie. Nello stesso rapporto di Accenture sopra menzionato, il 64% dei pazienti intervistati ha dichiarato che l'assistenza sanitaria virtuale li ha resi più consapevoli delle loro esigenze di privacy e di sicurezza dei dati.

Il settore sanitario è sempre più preso di mira dai criminali informatici

Non è un segreto che il settore sanitario sia preso di mira sempre più spesso da criminali informatici e malintenzionati. Ancora una volta, nel 2020, il numero di attacchi informatici nel settore sanitario è salito del 42% rispetto all'anno precedente e il Dipartimento della Salute e dei servizi alla persona degli Stati Uniti ha segnalato che ogni mese nel 2020 sono state violate oltre 1 milione di cartelle dei pazienti. Inoltre la ricerca *"Healthcare Cybersecurity"* realizzata da Bitdefender in Italia lo scorso maggio 2021 per valutare lo status di efficienza della sicurezza informatica nel settore sanitario, ha rivelato che, il 93% delle aziende del settore sanitario ha subito attacchi informatici in passato mentre il 64% ritiene probabile, o altamente probabile, un attacco informatico nel prossimo futuro. Infine, la telemetria Bitdefender ha registrato per il solo mese di aprile *in Italia circa 7 mila attacchi.*

Alcuni di questi attacchi possono essere attribuiti all'aumento dell'uso da parte delle strutture sanitarie di fornitori cloud. L'impiego di terze parti porta ad avere una superficie di attacco più ampia, complicata da tenere sotto controllo, in quanto è difficile sapere se una terza parte sta adottando le migliori prassi e gli standard di sicurezza informatica in ambito sanitario.

Di questa situazione sono perfettamente consapevoli anche gli hacker che stanno prendendo di mira le strutture sanitarie con l'esplicito scopo di accedere ed esfiltrare i dati sanitari e dei pazienti. Nel giugno 2021, Forefront Dermatology ha annunciato che una violazione dei dati ha portato all'esposizione di oltre 2 milioni di cartelle cliniche dei pazienti. L'"Healthcare Cybersecurity Report" di Bitdefender rivela che l'efficienza delle strutture sanitarie italiane per affrontare i rischi di sicurezza informatica raggiunge solo il 49% e ne emerge una preparazione nettamente insufficiente sia in termini di tecnologie che di competenze professionali.

È evidente quindi la necessità di aggiornare e adeguare la sicurezza informatica al l'attuale contesto del settore sanitario.

Modernizzare la sicurezza informatica nel settore sanitario

l settore sanitario ha bisogno di modernizzare la propria sicurezza informatica nello stesso modo in cui ha modernizzato le sue infrastrutture e i suoi servizi. Devono essere adottati nuovi modelli e strutture di sicurezza all'avanguardia che incorporino la gestione del rischio di terzi, l'uso di fornitori di servizi e infrastrutture cloud in grado di offrire strategie di mitigazione dei rischi e di recovery per le attuali minacce che le strutture sanitarie si trovano ad affrontare.

Dare la priorità alla sicurezza di terze parti e fornitori di soluzioni cloud

La tua azienda è al sicuro tanto quanto il tuo fornitore meno sicuro. Occorre fare un inventario dei propri fornitori, specialmente i partner che forniscono servizi e infrastruttura cloud, classificandoli per priorità in base a quanto sono critici in termini di funzione aziendale e se hanno o meno accesso a informazioni sensibili. È importante capire quanto siano sicuri questi fornitori e quanto si è esposti attraverso di loro.

Ampliare la visibilità sulle proprie risorse per prendere in considerazione ulteriori endpoint e partner

È necessario un processo attivo per fare un inventario completo dei propri dispositivi, reti, partner ed endpoint, in modo da poter garantire che qualsiasi nuovo progetto o attività non abbia vulnerabilità esposte. È naturalmente necessario includere i dispositivi IoT, i dispositivi dei dipendenti, i dispositivi usati per il telelavoro e i partner che stanno interagendo con la rete o l'ambiente aziendale.

Cercare un partner per la sicurezza del cloud specializzato in ambito sanitario
Se si sta adottando un nuovo fornitore di infrastrutture cloud o se si sta adottando un sistema EHR, è probabile che si abbia bisogno di una soluzione dedicata per garantire che questi dati siano protetti e gestiti correttamente. Si tratta di uno degli investimenti più incisivi che si possa fare nel dipartimento di cybersecurity.

Creare un piano di risposta in caso di violazioni o incidenti

Nessuna organizzazione è sicura al 100%, quindi è necessario disporre di un piano e di un processo in caso di attacco. Occorre avere una soluzione di rilevamento e risposta che controlli la rete, gli endpoint e i file sensibili, un piano di risposta agli incidenti e le risorse per facilitare e velocizzare il recovery e l'implementazione di misure correttive.
Questa necessità può portare alla scelta di un partner che abbia gli strumenti, il personale e le risorse per intervenire in caso di incidente.

Come affrontare la sfida della sicurezza informatica del cloud in ambito sanitario

Non stiamo cercando di sminuire i nuovi sviluppi e i progressi tecnologici fatti dal settore sanitario. Queste innovazioni e adattamenti erano necessari per rispondere alle esigenze globali di "pazienti sempre più digitali". Tuttavia, l'aumento della digitalizzazione ha anche attirato l'attenzione di

criminali informatici senza scrupoli che sanno gli operatori del settore sono più propensi a pagare riscatti prima di altri.

Il prossimo passo per il settore sanitario sarà quello di proteggere i dati, le organizzazioni, i nuovi partner di servizi cloud e i fornitori di infrastrutture. Date le limitazioni in termini di budget, sarebbe difficile per queste aziende creare un dipartimento interno pronto per affrontare tutte le nuove minacce e i rischi posti a queste organizzazioni.

Bitdefender consiglia a queste aziende di affidarsi a partner dedicati con una solida esperienza nella protezione dei dati aziendali, fornendo strumenti di rilevamento e risposta e offrendo soluzioni di sicurezza cloud. Questo è il passo successivo del percorso di trasformazione digitale ed è necessario farlo ora.

A proposito di Bitdefender

Bitdefender, leader riconosciuto nel settore della cybersecurity, offre le migliori soluzioni di prevenzione, rilevamento e risposta alle minacce in tutto il mondo. Responsabile della protezione di milioni di sistemi in ambienti consumer, business e governativi, Bitdefender è l'esperto più affidabile del settore* per eliminare le minacce, proteggere la privacy e i dati per favorire la resilienza informatica. Grazie agli investimenti in ricerca e sviluppo, Bitdefender Labs rileva 400 nuove minacce ogni minuto con 30 miliardi di query giornaliere. L'azienda ha rilasciato innovazioni rivoluzionarie in materia di antimalware, IoT, analisi comportamentale e intelligenza artificiale e la sua tecnologia viene concessa in licenza a oltre 150 brand di cybersecurity, i più conosciuti al mondo. Fondata nel 2001, Bitdefender vanta clienti in 170 paesi e ha uffici in tutto il mondo. Per maggiori informazioni https://www.bitdefender.it.

*Bitdefender si è classificata al primo posto nel 54% di tutti i test di AV-Comparatives 2018-2021 per protezione del mondo reale, prestazioni, protezione dai malware & protezione dalle minacce avanzate.