EXECUTIVE BRIEF

Sfide, complessità e trasformazione della sicurezza informatica nel settore sanitario

I quattro problemi di cybersicurezza principali che interessano oggi la sanità.

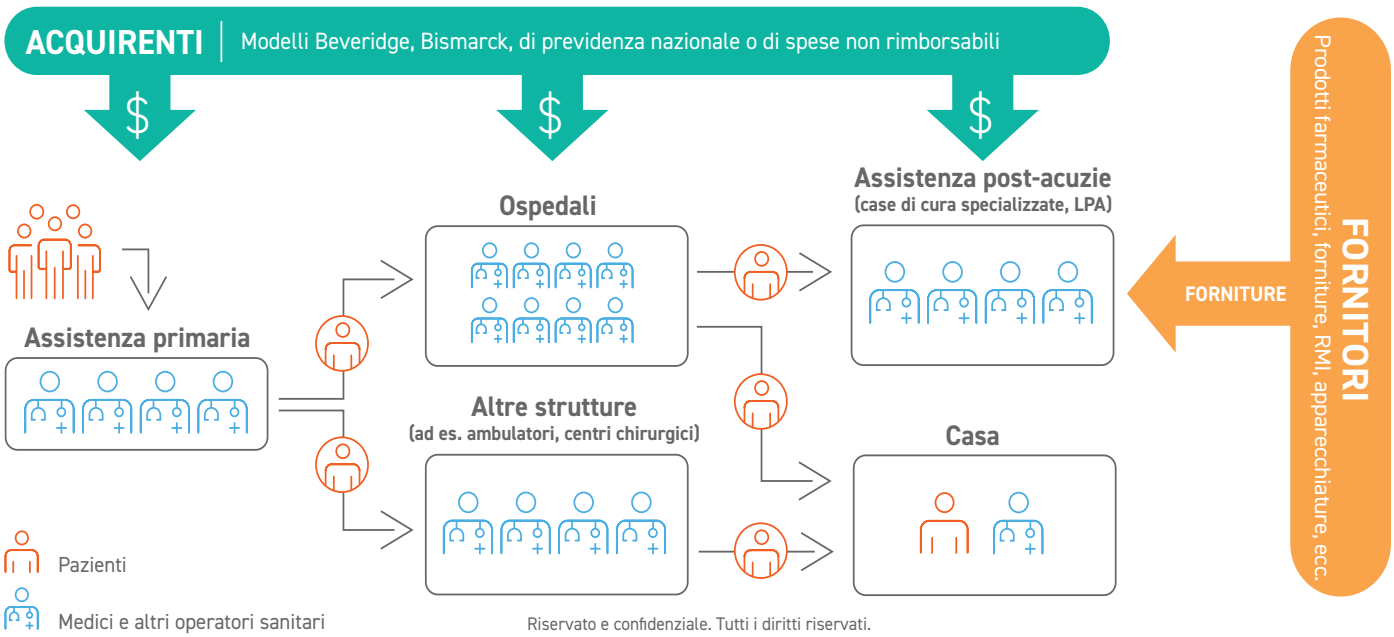
Abstract

Dall'inizio della pandemia di COVID-19, i fornitori di servizi sanitari hanno modificato e ampliato il proprio approccio alla tecnologia. Tale cambiamento è avvenuto in risposta alla rapida diffusione della telemedicina, all'afflusso di professionisti dell'assistenza remota, al passaggio a processi aziendali e di gestione dati basati sul cloud nonché alla proliferazione di dispositivi connessi per il monitoraggio remoto dei pazienti. Tutti questi fattori hanno permesso ai professionisti di offrire assistenza di alta qualità di persona, in modo virtuale o a domicilio da qualsiasi luogo, ma hanno anche creato – e in alcuni casi aggravato – una serie di problemi di sicurezza informatica. Il presente documento esamina le sfide e le complessità di questa trasformazione della sicurezza informatica nel settore sanitario, che riguardano l'intero settore a livello globale.

Introduzione

La posta in gioco nel settore sanitario è molto alta, con nuove tecnologie e applicazioni medicali che influiscono sul benessere e sulla sicurezza dei pazienti nel loro intero percorso di assistenza continua.

Gli effetti a cascata degli attacchi informatici sulle infrastrutture sanitarie critiche e sulla gestione delle cartelle cliniche elettroniche possono avere conseguenze devastanti sull'assistenza ai pazienti:



- I pazienti non ottengono le cure necessarie se il loro fornitore di servizi sanitari è offline a causa di un attacco ransomware o DDoS.
- I chirurghi devono rimandare gli interventi perché le informazioni necessarie per eseguire un delicato intervento chirurgico sono inaccessibili.
- L'interruzione di procedure diagnostiche e test di laboratorio provoca ritardi nel trattamento medico.
- I centri di pronto soccorso bloccati obbligano le ambulanze a dirigersi verso strutture sanitarie a chilometri di distanza, con conseguenze gravi e talvolta irreversibili.

Le informazioni sanitarie protette sono più preziose nel dark web

Gli ospedali e altre aziende che forniscono assistenza sanitaria sono tra gli obiettivi più ricercati per i cyber attacchi interni ed esterni, in quanto le informazioni sanitarie protette (PHI) sono molto richieste sul dark web e quindi possono essere vendute a un prezzo più alto rispetto ad altre informazioni personali.

Ad esempio, i numeri delle carte di credito rubate vengono disattivati e sostituiti non appena vengono rilevate spese sospette, con un conseguente calo del loro valore sul mercato nero. Le cartelle sanitarie hanno invece un valutazione più elevata perché contengono dati immutabili che non possono essere modificati o cancellati facilmente. I cybercriminali possono trarne un vantaggio a lungo termine, mentre i pazienti colpiti, oltre a subire un danno economico ed emotivo, impiegano parecchio tempo per rimediare ai danni causati da attività fraudolente. Tali danni possono includere l'acquisto di medicinali con ricette false, la richiesta di cure, il rimborso di spese mediche inesistenti o l'erogazione di prestiti personali o carte di credito utilizzando i dati sanitari rubati ai pazienti.

Il ransomware resta un problema grave

Gli autori delle minacce continuano a trovare nuovi metodi per sfruttare i punti deboli che i centri operativi di sicurezza (SOC) delle aziende sanitarie non hanno risolto o notato, proprio perché le tecniche di hacking avanzate sono un passo avanti rispetto agli investimenti per rafforzare i controlli di sicurezza. I cybercriminali sfruttano attivamente vulnerabilità non corrette, come Log4j, come vettore principale per lanciare attacchi ransomware. Il ransomware rimane quindi la minaccia più significativa per il settore sanitario.

Questa tendenza proseguirà probabilmente per tutto il 2022, considerando che negli ultimi due anni il 42%[1] delle aziende che erogano servizi sanitari ha subito attacchi. Inoltre, circa il 36%[2] di questi incidenti è avvenuto tramite terze parti, come gli attacchi alla catena di fornitura ampiamente riportati dai media che sfruttavano vulnerabilità del software di gestione dell'infrastruttura critica.

Vulnerabilità dei server di rete tra le cause principali delle violazioni di dati

Il 2021 è stato uno degli anni peggiori per il settore sanitario, con un numero record di violazioni di dati e furti di informazioni sanitarie protette. Ad esempio, l'Ufficio per i diritti civili del Dipartimento della sanità e dei servizi sociali degli Stati Uniti ha riferito che oltre 700 (figura 1) degli enti esaminati hanno subito una violazione, con conseguente furto, perdita o divulgazione di informazioni sanitarie protette di oltre 42 milioni di persone (figura 2). Gli incidenti[3] segnalati di recente rivelano che le violazioni e le vulnerabilità proseguono a buon ritmo nel 2022 (figura 3).

Figura 1
Violazioni di dati sanitari con 500 o più cartelle

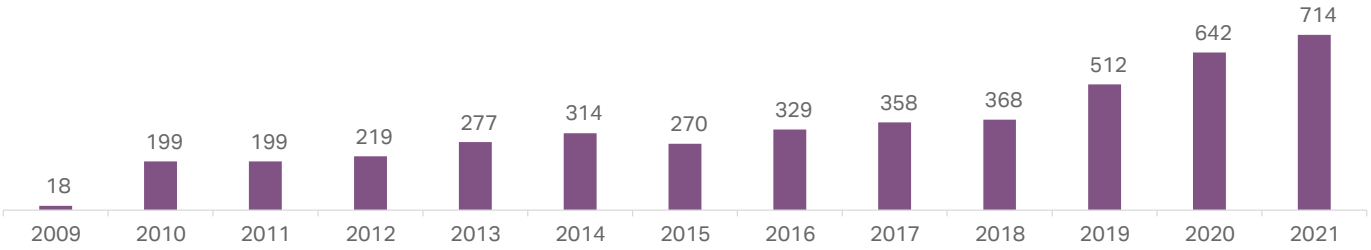
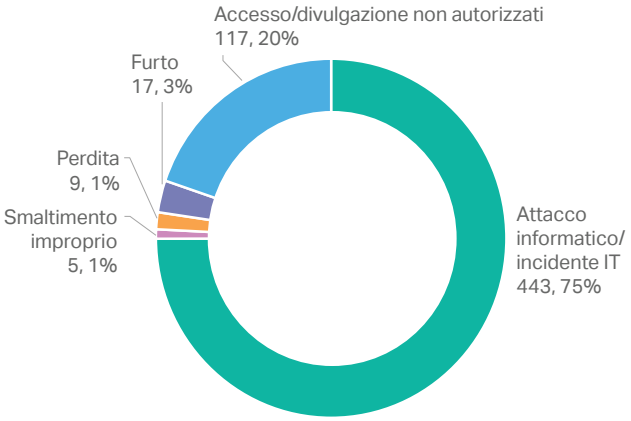


Figura 2

Violazioni di dati rilevate nel 2021, Ufficio per i diritti civili del Dipartimento della sanità e dei servizi sociali (USA)
Totale: 5



Persone colpite nel 2021, Ufficio per i diritti civili del Dipartimento della sanità e dei servizi sociali (USA)

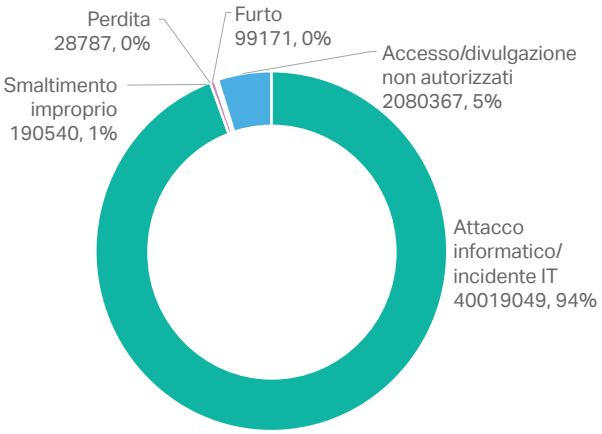
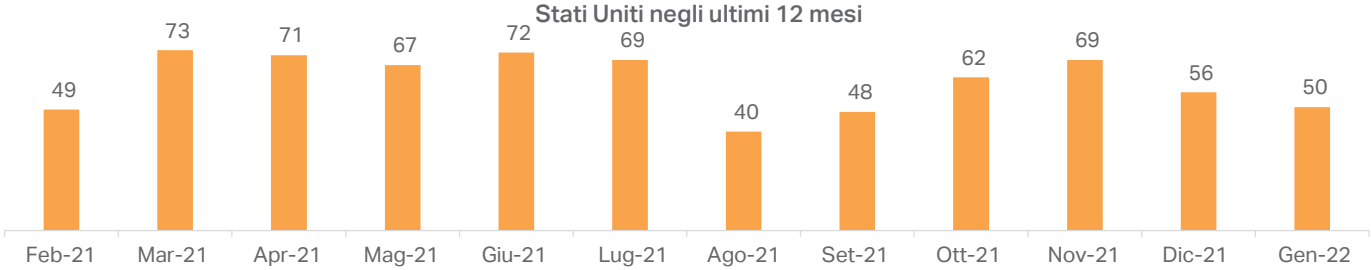


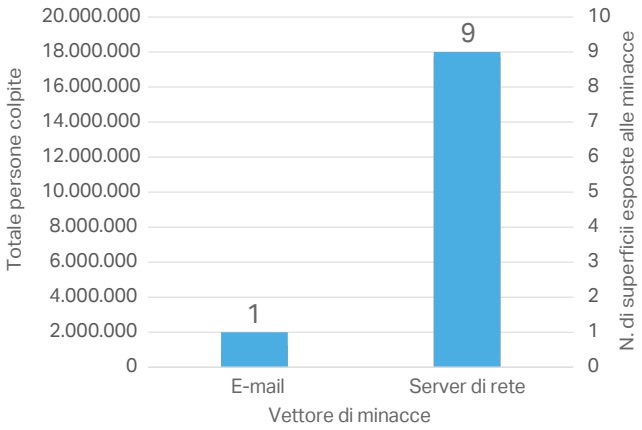
Figura 3
Violazioni di dati nel settore sanitario degli Stati Uniti negli ultimi 12 mesi



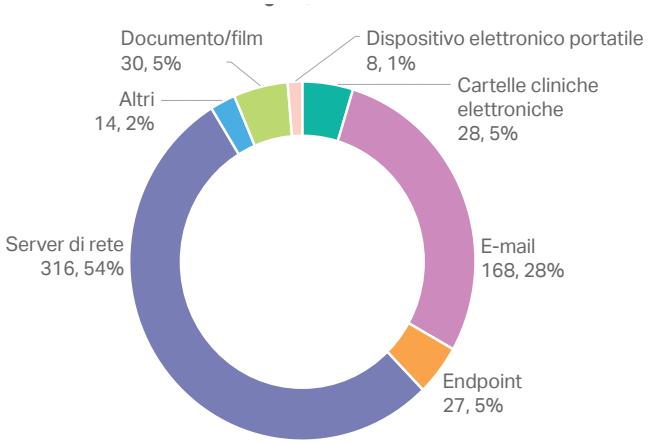
Le dieci violazioni di dati sanitari più gravi registrate nel 2021 sono state attribuite a cyber attacchi andati a buon fine, e la loro gravità è stata misurata in base al numero di persone colpite. Il 90% di queste violazioni si è verificato sui server di rete dei fornitori di servizi (figura 4). Inoltre, i server di rete e la posta elettronica rappresentano insieme l'80% dei vettori di attacco, con un impatto negativo sui trattamenti urgenti e con possibili esiti non soddisfacenti.

Figura 4

10 violazioni di dati sanitari più gravi registrate nel 2021 negli Stati Uniti



Superficie di attacco nel 2021, Ufficio per i diritti civili del Dipartimento della sanità e dei servizi sociali (USA)



SONICWALL

Quattro rischi di cybersecurity critici che mettono a dura prova l'assistenza sanitaria

Nonostante i numerosi vantaggi che le tecnologie offrono all'assistenza sanitaria, l'adozione di nuovi dispositivi di assistenza medica e l'interconnessione tra diversi sistemi sanitari comportano numerosi rischi. Le aziende che forniscono assistenza sanitaria si trovano ad affrontare quattro sfide di sicurezza informatica comuni a tutto il settore sanitario:

1. Mantenere le infrastrutture critiche operative e continuamente disponibili
2. Proteggere la privacy dei pazienti dai rischi interni
3. Preservare l'integrità dei dati sanitari
4. Prevenire le violazioni di dati causate da attacchi ransomware e phishing

Un investimento insufficiente nella sicurezza dell'infrastruttura critica può creare una situazione insostenibile nel momento in cui si decide di ampliarla. Eventuali carenze di sicurezza informatica come la gestione delle patch e delle configurazioni, il controllo degli accessi, la crittografia dei dati e la sicurezza del portale per i pazienti mettono a rischio l'impegno delle aziende sanitarie di fornire qualità, assistenza tempestiva e protezione della privacy dei pazienti. In base alle leggi e ai regolamenti vigenti sulla protezione dei dati, una falla nella protezione dei dati personali può comportare gravi conseguenze per i fornitori di servizi sanitari, come ad esempio: violazione dei dati, interruzione dell'assistenza, trattamenti inefficaci, interruzione della fatturazione, perdite finanziarie, costi di riparazione, spese legali e di liquidazione, pesanti sanzioni, erosione della fiducia, danni alla reputazione, e altro ancora.

Conclusioni

Mentre la pandemia non accenna a scomparire, le aziende che forniscono servizi sanitari soffrono di carenza di personale e di risorse e sono impegnate a gestire la tecnologia e la trasformazione digitale nel settore sanitario per servire meglio i propri pazienti. Le soluzioni di cybersecurity per il settore sanitario di SonicWall semplificano la transizione e rafforzano la sicurezza delle infrastrutture sanitarie, rendendo l'erogazione di prestazioni sanitarie ai pazienti più efficiente, resiliente e sicura. Queste soluzioni integrate e gestite centralmente garantiscono la sicurezza di postazioni periferiche, data center, accessi, connettività wireless, e-mail ed endpoint, e consentono ai fornitori di servizi sanitari di ottenere risultati positivi nella cura dei pazienti nel loro percorso di assistenza continua.

Leggi il nostro whitepaper "Cybersecurity senza confini per una sanità più sicura" per scoprire come le soluzioni di sicurezza SonicWall per il settore sanitario proteggono la disponibilità delle infrastrutture critiche, l'integrità dei dati sanitari elettronici e la riservatezza e la privacy delle informazioni sanitarie personali.

1 Fonte: The Impact of Ransomware on Healthcare During COVID-19 and Beyond, Ponemon Institute.
2 Fonte: The Impact of Ransomware on Healthcare During COVID-19 and Beyond, Ponemon Institute.
3 Fonte: Healthcare Data Breach Report, HIPAA Journal, Gennaio 2022, https://www.hipaajournal.com/january-2022-healthcare-data-breach-report/

SonicWall

SonicWall fornisce soluzioni di cybersecurity innovative che si adattano perfettamente alla nuova "normalità iperdistribuita", in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e in cui la sicurezza dei dati rappresenta un elemento fondamentale. SonicWall colma le lacune della cybersecurity per ospedali, cliniche e fornitori in ogni parte del mondo e rende possibile economie innovative grazie alla capacità di individuare le minacce più elusive e offrendo una visibilità in tempo reale. Per maggiori informazioni visitare www.sonicwall.com/healthcare.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

SONICWALL