

Attacchi ransomware agli ospedali: quando la cybersecurity diventa una questione di vita o di morte



Gli attacchi ransomware agli ospedali stanno trasformando la percezione del rischio nel settore sanitario, mettendo in pericolo non solo dati sensibili, ma anche vite umane. Dall'incidente all'Università di Düsseldorf del 2020 ai casi più recenti come l'attacco all'HSE irlandese, gli ospedali sono diventati bersagli privilegiati per i criminali informatici, attratti dal valore economico e dalla vulnerabilità intrinseca dei dati sanitari. Questo articolo analizza il panorama dei ransomware nel settore sanitario, evidenziando le conseguenze cliniche, morali ed economiche degli attacchi, le strategie di difesa disponibili e le sfide emergenti legate alla digitalizzazione della sanità.

Nel settembre 2020, l'Università di Düsseldorf visse una notte che avrebbe cambiato per sempre la percezione delle minacce informatiche in ambito sanitario. Un attacco ransomware devastante paralizzò completamente i sistemi informatici dell'ospedale, costringendo il personale sanitario a navigare alla cieca in un mare di incertezza digitale. Una paziente in condizioni critiche dovette essere trasferita d'urgenza in un'altra struttura a oltre trenta chilometri di distanza. Non sopravvisse. Inizialmente si pensò che fosse la prima morte direttamente collegabile a un cyberattacco sanitario, ma dopo un'indagine approfondita durata due mesi, i procuratori tedeschi conclusero che le condizioni della paziente erano così critiche che sarebbe deceduta comunque, indipendentemente dal ritardo nel trattamento.

Eppure, quel caso rimane un monito inquietante. Come dichiarò il procuratore capo Markus Hartmann, è solo questione di tempo prima che un attacco ransomware causi direttamente la morte di un paziente. Quella tragedia di Düsseldorf segnò comunque un punto di non ritorno nella consapevolezza collettiva: non si trattava più soltanto di dati rubati o sistemi paralizzati, ma di vite umane appese a un filo digitale, vulnerabili alle azioni di cybercriminali senza scrupoli.

Gli ospedali, luoghi storicamente consacrati alla cura e alla salvaguardia della vita, sono diventati uno dei bersagli preferiti degli hacker. E le ragioni dietro questa escalation sono tanto chiare quanto disturbanti, radicate in un valore nascosto che molti non sospettano nemmeno.

Il tesoro digitale che vale più dell'oro: i dati sanitari

Quando pensiamo ai furti di dati, la mente corre immediatamente alle carte di credito o alle password dei social media. Eppure, nel mercato nero del dark web, una cartella clinica completa può valere fino a cinquanta volte di più di un numero di carta di credito. Il motivo è disarmante nella sua semplicità: mentre una carta può essere bloccata in pochi minuti con una telefonata, i dati sanitari sono permanenti e incredibilmente dettagliati. Nome, data di nascita, codice fiscale, storia medica completa, diagnosi, prescrizioni, informazioni assicurative. Un tesoro inestimabile per chi vuole commettere frodi assicurative, creare identità false o ricattare pazienti con informazioni sensibilissime sulla loro salute.

Secondo Experian e Trustwave, mentre una carta di credito si vende per circa tre dollari sul dark web, una cartella clinica può raggiungere i mille dollari. Gli ospedali custodiscono montagne di questi dati, spesso in sistemi obsoleti e poco protetti. Molte strutture sanitarie operano ancora con

software legacy, talvolta risalenti a decenni fa, perché l'aggiornamento è complesso, costoso e rischia di interrompere servizi critici. Questa vulnerabilità tecnologica, unita alla natura insostituibile dei servizi ospedalieri, crea il contesto perfetto per l'estorsione digitale.

La questione non riguarda solo il valore economico dei dati. C'è qualcosa di profondamente più inquietante: le informazioni mediche rivelano la nostra vulnerabilità più intima. Diagnosi di malattie mentali, terapie oncologiche, interruzioni di gravidanza, test per malattie sessualmente trasmissibili. Sono informazioni che possono essere usate per estorsioni mirate, discriminazioni o ricatti personali. E una volta che questi dati finiscono nel dark web, non esiste modo di cancellarli: vengono copiati, redistribuiti e conservati su innumerevoli server anonimi sparsi per il mondo.

Il dilemma morale del riscatto: pagare o lasciar morire?

Quando un attacco ransomware colpisce un ospedale, crittografando i database e paralizzando le operazioni, i dirigenti si trovano di fronte a una scelta impossibile che nessun corso di management potrebbe mai preparare ad affrontare. Da un lato c'è la ferma raccomandazione delle autorità di non pagare mai i criminali, per non finanziare ulteriori attacchi e non incoraggiare questa economia criminale. Dall'altro c'è la consapevolezza devastante che ogni ora di inattività può significare interventi chirurgici rimandati, diagnosi critiche ritardate, terapie salvavita sospese. E, nei casi più gravi, vite perse.

Il caso dell'Ireland's Health Service Executive nel maggio 2021 rappresenta forse l'esempio più emblematico di questa impossibile equazione morale. Il gruppo criminale Conti, utilizzando il ransomware omonimo, penetrò nei sistemi informatici dell'HSE e crittografò circa l'ottanta per cento

dei dati. I criminali chiedevano venti milioni di dollari. Il governo irlandese, con una decisione coraggiosa ma dolorosa, rifiutò categoricamente di pagare. Il prezzo di questa scelta fu altissimo: i sistemi rimasero compromessi per settimane, migliaia di appuntamenti vennero cancellati, e il ripristino completo richiese fino a settembre 2021, quattro mesi dopo l'attacco iniziale. I costi totali superarono i cento milioni di euro. La decisione fu coraggiosa sul piano dei principi, ma devastante per i pazienti in attesa.

Altri ospedali hanno fatto scelte diverse. Alcuni hanno pagato somme a sei o sette cifre per riavere accesso ai propri sistemi nel giro di ore, giustificando la decisione con la necessità urgente di proteggere i pazienti. Ma anche il pagamento del riscatto non garantisce soluzioni rapide o complete. I tool di decrittazione forniti dai cybercriminali sono spesso difettosi, lenti o incompleti. E non c'è alcuna garanzia che i dati rubati non vengano comunque venduti o pubblicati sul dark web. Come dimostrano numerosi casi documentati, anche dopo aver pagato, solo il due per cento delle organizzazioni sanitarie recupera tutti i propri dati.

La questione del pagamento diventa ancora più complessa quando si considera che ogni transazione in Bitcoin verso questi gruppi criminali finanzia operazioni sempre più sofisticate, permettendo loro di investire in tecnologie migliori, reclutare più talenti e colpire più duramente. È un circolo vizioso che le autorità faticano a spezzare, intrappolate tra la necessità di proteggere i cittadini oggi e quella di smantellare queste reti criminali per il futuro.

Attacchi ransomware agli ospedali: quando tornare alla normalità diventa un'odissea

Persino quando un ospedale riesce a recuperare l'accesso ai

propri sistemi, sia pagando il riscatto sia ricostruendo tutto da backup, la strada verso la normalità è lunga, tortuosa e costellata di ostacoli imprevisti. Il ripristino completo delle operazioni può richiedere da settimane a mesi, con costi che secondo Comparitech possono raggiungere in media 2.57 milioni di dollari, escluso il riscatto. In alcuni casi documentati, come quello di OrthoVirginia, il recupero completo ha richiesto diciotto mesi.

Durante questo periodo di recupero, il personale sanitario deve fare affidamento su procedure manuali che sembrano riportare l'orologio indietro di decenni: cartelle cartacee scritte a mano, telefonate invece di messaggi elettronici, prescrizioni compilate manualmente. È un ritorno forzato al passato che rallenta drammaticamente ogni processo e aumenta esponenzialmente il rischio di errori medici. Un medico abituato a consultare istantaneamente la storia clinica completa di un paziente con un click si trova improvvisamente a dover cercare tra pile di fogli, con il rischio concreto di non individuare allergie critiche, interazioni farmacologiche pericolose o precedenti complicazioni.

Le ricerche dimostrano che ogni giorno di downtime costa alle organizzazioni sanitarie americane una media di 1.9 milioni di dollari. Questo dato include non solo i costi diretti del ripristino tecnico, ma anche le perdite derivanti da interventi cancellati, pazienti trasferiti ad altre strutture, personale pagato senza poter lavorare normalmente, e il crollo nella produttività generale. In molti casi, gli ospedali devono trasferire pazienti verso altre strutture o ridurre drasticamente i servizi offerti. Le conseguenze si ripercuotono non solo sull'ospedale colpito, ma sull'intero sistema sanitario regionale, creando sovraccarichi a catena che possono mettere a rischio la vita di pazienti in strutture mai direttamente attaccate.

E c'è un altro problema spesso sottovalutato ma potenzialmente devastante nel lungo periodo: la perdita di fiducia. Quando i

pazienti scoprono che i loro dati più intimi potrebbero essere stati rubati o compromessi, che le loro diagnosi oncologiche o le loro terapie psichiatriche potrebbero finire pubblicate sul dark web, il rapporto con la struttura sanitaria ne risente profondamente. Alcuni ospedali hanno visto cali significativi nelle ammissioni nei mesi successivi a un attacco, con pazienti che preferivano rivolgersi altrove per timore che la sicurezza non fosse adeguata. Ricostruire questa fiducia richiede anni di impegno costante e investimenti massicci in comunicazione e miglioramenti concreti della sicurezza.

Una minaccia in crescita esponenziale che non accenna a fermarsi

I numeri parlano un linguaggio inequivocabile e allarmante. Gli attacchi informatici al settore sanitario sono aumentati in modo drammatico negli ultimi anni. Secondo uno studio pubblicato su JAMA Network Open, nel 2021 gli attacchi ransomware hanno rappresentato il trentuno per cento di tutte le violazioni di dati sanitari negli Stati Uniti, con circa duecentoventidue attacchi confermati contro entità coperte dall'HIPAA. Un sondaggio di Sophos ha rilevato un incremento ancora più preoccupante: la percentuale di organizzazioni sanitarie colpite è passata dal trentaquattro per cento nel 2020 al sessantasei per cento nel 2021, registrando un aumento del novantaquattro per cento in un solo anno.

La pandemia di COVID-19 ha ulteriormente accelerato questa tendenza devastante. I criminali informatici hanno sfruttato cinicamente il momento di massima vulnerabilità del sistema sanitario globale, quando gli ospedali erano sopraffatti dall'emergenza e il personale IT era già sotto pressione insostenibile. Durante i mesi più critici della pandemia, alcuni gruppi ransomware dichiararono pubblicamente di voler sospendere gli attacchi agli ospedali, ma come dimostrano i

dati dell'FBI, molti continuarono imperterriti, persino intensificando le loro operazioni.

Le organizzazioni criminali dietro questi attacchi non sono più gli hacker solitari dell'immaginario comune. Si tratta di vere e proprie imprese del crimine dotate di modelli di business strutturati, reparti di customer service per "assistere" le vittime durante il pagamento del riscatto, e persino programmi di affiliazione simili a quelli delle aziende legittime. Gruppi come Conti hanno accumulato oltre centottanta milioni di dollari nel solo 2021, colpendo più di novecento vittime in tutto il mondo, inclusi numerosissimi ospedali. REvil, altro gruppo tristemente famoso, ha raggiunto profitti stimati di almeno ottantuno milioni di dollari entro la fine del 2020. LockBit, insieme a Conti, è diventato uno dei gruppi ransomware-as-a-service più attivi e redditizi del panorama criminale digitale.

Questi gruppi operano secondo il modello del Ransomware-as-a-Service, dove sviluppatori esperti creano il malware e lo "noleggiano" ad affiliati che si occupano di penetrare nei sistemi delle vittime e distribuire il ransomware. Gli affiliati ricevono una percentuale sostanziosa del riscatto, spesso tra il settanta e l'ottanta per cento, mentre i creatori del ransomware forniscono infrastruttura, supporto tecnico e persino servizi di negoziazione con le vittime. Alcuni gruppi, come Conti prima della sua dissoluzione, avevano strutture così sofisticate da includere stipendi fissi per i dipendenti, bonus per i migliori performer mensili, e persino ferie pagate.

Difendersi è possibile, ma richiede investimenti che molti ospedali faticano a sostenere

La buona notizia, se così può essere chiamata in un panorama

così cupo, è che esistono strategie efficaci per proteggere gli ospedali dagli attacchi informatici. Backup regolari e testati frequentemente, aggiornamenti costanti dei sistemi operativi e del software, formazione continua del personale sui rischi del phishing e dell'ingegneria sociale, segmentazione rigorosa delle reti per limitare la diffusione laterale di eventuali intrusioni, autenticazione a più fattori su tutti i sistemi critici, monitoraggio continuo delle minacce con sistemi di detection avanzati. L'arsenale difensivo esiste ed è ben documentato.

La cattiva notizia è che tutto questo richiede investimenti significativi, sia in termini economici sia di risorse umane specializzate che scarseggiano sul mercato. Molte strutture sanitarie operano con budget ristretti e priorità cliniche immediate che assorbono la maggior parte delle risorse disponibili. Diventa quindi difficile giustificare spese ingenti per la cybersecurity, specialmente quando il rischio viene percepito come astratto o remoto. Almeno fino a quando l'attacco non avviene. Solo allora diventa tragicamente evidente che la sicurezza informatica non è un optional tecnologico o un lusso per chi se lo può permettere, ma una componente fondamentale della sicurezza dei pazienti, al pari dell'igiene delle mani o della sterilizzazione degli strumenti chirurgici.

Alcuni governi hanno iniziato a riconoscere la gravità del problema, stanziando fondi specifici per migliorare la resilienza cyber delle strutture sanitarie. L'Unione Europea, ad esempio, ha introdotto la direttiva NIS2 (Direttiva UE 2022/2555), che impone standard di sicurezza più stringenti per le infrastrutture critiche, inclusi esplicitamente gli ospedali e le organizzazioni sanitarie. La direttiva, che gli Stati membri dovevano recepire entro ottobre 2024, stabilisce obblighi precisi di gestione del rischio cyber, reporting degli incidenti significativi, e persino responsabilità personali per i membri dei consigli di amministrazione. Per le

entità essenziali come gli ospedali, le sanzioni possono raggiungere i dieci milioni di euro o il due per cento del fatturato annuo globale.

Ma il divario tra le minacce in rapida evoluzione e le capacità difensive di molte strutture rimane preoccupante. Come evidenziato dal rapporto sulla HSE irlandese, l'organizzazione non aveva un unico responsabile senior per la cybersecurity al momento dell'attacco, mancava di un piano documentato di risposta agli incidenti cyber, e presentava lacune critiche in venticinque dei ventotto controlli di sicurezza più efficaci contro il ransomware. Peggio ancora, i sistemi antivirus avevano rilevato le intrusioni preliminari ma gli alert erano stati ignorati. Questa situazione non è affatto rara nel panorama sanitario globale.

Guardando al futuro: tra innovazione digitale e nuove vulnerabilità

La digitalizzazione della sanità è inarrestabile e, per molti versi, assolutamente necessaria. Cartelle cliniche elettroniche che permettono la condivisione istantanea di informazioni tra specialisti, telemedicina che abbatte le barriere geografiche nell'accesso alle cure, intelligenza artificiale per la diagnostica che può individuare tumori invisibili all'occhio umano, dispositivi medici connessi che monitorano costantemente i parametri vitali dei pazienti. Tutte queste innovazioni promettono cure migliori, più personalizzate ed efficienti. Ma portano con sé anche nuove vulnerabilità che i cybercriminali sono rapidi a sfruttare.

Ogni dispositivo connesso alla rete ospedaliera è un potenziale punto di accesso per un attacco. Ogni dato condiviso tra sistemi è un'opportunità per un'intercettazione o un furto. I pacemaker connessi, le pompe per insulina

controllate da remoto, i sistemi di monitoraggio fetale wireless. Tutti questi dispositivi salvavita sono anche potenziali vettori di attacco. La sfida per il settore sanitario non è arrestare il progresso tecnologico, sarebbe assurdo e controproducente, ma guidarlo con consapevolezza, costruendo sistemi che siano non solo avanzati e funzionali, ma anche resilienti e sicuri by design.

La morte di quella paziente a Düsseldorf, anche se non direttamente causata dall'attacco informatico secondo le conclusioni dell'indagine, dovrebbe comunque essere un campanello d'allarme che nessuno può permettersi di ignorare. Il procuratore tedesco aveva ragione: è solo questione di tempo prima che un attacco ransomware causi direttamente la morte di un paziente con condizioni meno critiche. Quando un ospedale non può accedere alla storia clinica di un paziente allergico a determinati farmaci, quando i sistemi di diagnostica per immagini sono offline durante un'emergenza stroke, quando le pompe di infusione intelligenti non possono essere programmate correttamente, il rischio di esiti fatali diventa concreto e immediato.

Quando la cybersecurity fallisce in un ospedale, le conseguenze non si misurano in termini di dati persi, sistemi offline o dollari evaporati dai bilanci. Si misurano in vite umane, in pazienti che non ricevono cure tempestive, in diagnosi mancate, in interventi rimandati che diventano irreversibili. È tempo di trattare la sicurezza informatica sanitaria con la stessa serietà riservata a qualsiasi altra minaccia per la salute pubblica. Perché nel ventunesimo secolo, proteggere i pazienti significa anche proteggere i sistemi digitali che li curano. E questa non è più un'opzione, ma un imperativo etico e clinico che il settore sanitario non può più permettersi di rimandare.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/attacchi-ransomwar-e-agli-ospedali/>