MAI PAGARE RISCATTI
SE IL CYBERCRIME ATTACCA

Amministratori, esperti informatici, legali e assicuratori concordano sulle strategie per contrastare il ransomware. Le dimensioni di un fenomeno in crescita

Andrea Galliano

Campania, Veneto e Lazio. Cambia la regione, ma resta costante la minaccia che negli ultimi mesi ha colpito il sistema sanitario italiano: il ransomware. Si tratta di un malware (software malevolo) che cripta i dati e chiede un riscatto per poterli decrittare. Pena la pubblicazione di quanto sottratto sul sito dell'attaccante nel deep web, una parte di internet non indicizzata dai motori di ricerca.

L'attacco più recente a un'azienda sanitaria si è verificato nei confronti dell'Asl Napoli 3 Sud alle tre del mattino dell'8 gennaio scorso. "Il sabato mattina i dipendenti hanno chiamato l'It dicendo che non riuscivano a fare il login. Così sono state fatte alcune verifiche: se c'è stato un calo di alimentazione e se il server era irraggiungibile. O se la password è stata dimenticata. Per esclusione i tecnici hanno dedotto che si trovavano davanti a un attacco informatico", ha spiegato l'ingegnere Massimo Bisogno, direttore dell'ufficio speciale per la Crescita e la Transizione digitale della Regione Campania. Di solito gli attaccanti lasciano alcune macchine libere per consentire l'accesso e in un file .txt mettono gli estremi per essere contattati. Che rimandano a chat che si trovano nel dark web.

LA TECNICA USATA IN CAMPANIA

"Fu trovato il file, ma non fu avviato alcun dialogo", ha precisato il dirigente. Gennaro Sosto, direttore generale dell'Asl Napoli 3 Sud, specifica che non era indicata una somma precisa per il riscatto. I dati oggetti dell'attacco erano le prenotazioni di alcune visite specialistiche e il riepilogo dei soggetti che si sono vaccinati. Il cryptolocker ha estratto questi file e li ha cifrati. E in parte sono stati pubblicati sul sito dell'attaccante come un trofeo. Il fatto assume una gravità maggiore perché si trattava di sanitari: è diverso conoscere il numero di telefono di una persona o la patologia da cui è affetta.

"Le vittime dei dati rubati per le prenotazioni sono state avvisate ed è stata preparata una bozza di comunicazione generalizzata per i soggetti vaccinati, che a maggio verrà diffusa all'interno dell'Asl e pubblicata sul sito web. Dati i numeri elevati, era improponibile una comunicazione puntuale", ha spiegato Sosto.

I cybercriminali sono riusciti a entrare nella rete della struttura sanitaria tramite l'account di un soggetto convenzionato con l'Asl, che ha accesso al sistema per motivi professionali. Gli attaccanti hanno usato le sue credenziali (user name e password) e poi con alcuni tool hanno scalato i privilegi (privilege escalation). Fino a diventare amministratori del sistema.

SERVONO DECALOGHI PER I DIPENDENTI

Secondo Bisogno "il problema di questi attacchi non è solo di natura tecnologica (aggiornare i sistemi operativi, i firewall e l'infrastruttura di rete) ma umana. I dipendenti, a prescindere dal ruolo che hanno, devono acquisire un minimo di competenze digitali. Anche un infermiere che usa una chiavetta usb in un apparato elettromedicale deve sapere che quella memoria va usata solo per quell'attività. Non va utilizzata anche a casa". Il dirigente paragona i decaloghi nell'uso degli strumenti tecnologici alle regole per la prevenzione dalla diffusione del covid. E invita a usare la stessa politica poiché "il comportamento rappresenta il 75-80% della tutela". In particolare sottolinea che "le password vanno costruite con delle logiche. Facili da ricordare, ma difficili da costruire. La lunghezza deve essere di almeno 10 caratteri e devono essere ricostruibili dal mio cervello anche se me le dimentico".

L'attacco è stato rivendicato dal gruppo Sabbath o, in linguaggio "leet", 54BB47h, come scritto nel loro sito. Non conoscono le regole italiane perché altrimenti saprebbero che un'azienda pubblica non può pagare alcun riscatto, per giunta in criptovalute. Pena l'apertura di un'indagine nei confronti del direttore generale da parte della Corte dei Conti. Invece è diverso attaccare un'azienda sanitaria americana dove vige l'autonomia dell'ente che può soddisfare la richiesta dei criminali. In Italia in questo settore l'unico vantaggio del gruppo attaccante è di natura reputazionale.

Anche perché nel caso dell'Asl Napoli 3 Sud sono stati ripristinati tutti i dati. Dopo che è stato rilevato l'attacco, una delle prime cose che fanno i tecnici è verificare che i backup siano disponibili e che non siano stati infettati. Si attiva il gruppo di sicurezza, si costituisce un'unità di crisi, si contattano la polizia postale, la magistratura, il Garante della privacy se c'è stato un data breach e si avvisa il Csirt (Computer security incident response team). C'era un backup completo fatto a cadenza almeno quotidiana e salvato su strutture scollegate dagli altri computer. In modo da proteggerlo da eventuali attacchi che la rete dell'ente può subire.

NESSUN DANNO ALLE APPARECCHIATURE

Però questa operazione non è avvenuta in un giorno solo: più complesso è l'attacco, più ci vuole tempo per ripristinare il tutto. Occorre verificare che il ransomware non sia nelle copie di sicurezza e nel frattempo sono state usate procedure emergenziali. "I referti sono stati scritti a mano", ricorda Sosto. Che aggiunge: "Eravamo preoccupati per le apparecchiature elettromedicali, perché il software è 'dedicato', sviluppato cioè sulla base delle richieste dell'azienda per l'utente finale e a volte datato. Ma l'attacco non le ha colpite". Il sistema di vaccinazione e quello dei tamponi non si sono mai bloccati poiché utilizzano la piattaforma regionale. Invece il sistema interno della gestione dei ricoveri non è stato utilizzabile per 3-4 settimane. La Regione ha diverse applicazioni nel cloud, come il Cup o il sistema di prenotazione dei vaccini. Perché così, se il cloud è protetto, vengono innalzati i livelli di sicurezza. Ma in questo caso i dati erano all'interno dell'Asl e non nel cloud.

IL RUOLO DEL CRISIS COORDINATOR

Nelle unità di crisi è fondamentale il ruolo svolto dal crisis coordinator. "È una figura nuova che gestisce tutte le attività di messa in campo, di disaster recovery per assicurare la business continuity e di comunicazione all'autorità giudiziaria, all'Agenzia per l'Italia digitale (Agid), all'Agenzia per la cybersicurezza nazionale e all'authority per la privacy", spiega l'avvocato Massimiliano Parla, presidente nazionale di Scudomed, società che si occupa di tutela del dato in contesti sanitari pubblici e privati. Il crisis coordinator fa da modem, rende fruibili le informazioni nella loro complessità tecnica a chi non ne ha dimestichezza. Spesso il linguaggio informatico è complesso, poiché è argomentato in bit e va destrutturato per renderlo di facile comprensione. Il legale sottolinea che "il ransomware di tipo crypto cifra i dati, mentre il locker rende impossibile l'accesso al dispositivo infettato e che a volte nel privato viene pagato un riscatto per decriptare i file e per evitare la pubblicazione dei dati esfiltrati sul sito dell'attaccante. Alcuni cybercriminali hanno siti nel dark web e hanno costituito servizi (una sorta di help desk) che aiutano l'attaccato a pagare la somma richiesta in criptovaluta. Magari il backup è stato fatto in maniera sporadica e si prende in considerazione il riscatto. Se l'attaccante pubblica i dati dopo il pagamento del riscatto ha un danno reputazionale". L'avvocato Parla evidenzia che spesso è sottovalutata la privacy e che il Garante può sanzionare l'attaccato se non dimostra di avere agito in accountability. La casistica è varia e può comprendere l'invio di referti medici a soggetti diversi dagli interessati, frequente nel periodo pandemico. Ma anche il trattamento illecito di dati personali e l'accesso illegittimo. Emblematico il fenomeno dell'insider misuse, che si verifica quando il personale sanitario non accede alle piattaforme per motivi di cura, ma per cercare dati di pazienti per la propria curiosità o per mettere a nudo le patologie delle persone. Viene sanzionato l'ente se non dimostra di avere adottato procedure e policy per evitare quanto accaduto. A partire da quelle relative alle password.

LA FORMAZIONE DEL PERSONALE

"Un canale tipico per gli attacchi però è costituito dall'email di phishing arrivata al dipendente che in maniera impropria clicca sul link o apre un allegato inserito nell'email stessa, che contiene codice malevole eseguito sul device del

malcapitato e che si diffonde, a cascata, all'interno della rete aziendale", ha spiegato Fabio Bonanni, Cyber Risk Partner di Deloitte ed esperto in ambito Life Sciences & Health Care. Per ridurre il rischio di questo tipo di attacchi è cruciale il tema della consapevolezza del dipendente. Fondamentali i programmi di formazione del personale. Vengono organizzati dalle risorse umane e l'it e la security ci mettono il contenuto. Bonanni ha evidenziato che "nei sistemi di controllo interno maturi la direzione security è separata dall'it, al fine di garantire la necessaria indipendenza tra chi definisce le regole di sicurezza (security) e chi è chiamato a implementarle sui sistemi (it). In tal senso l'it agisce da funzione di controllo di primo livello e la security di secondo". Nel sistema dei controlli c'è anche un terzo livello (internal audit). La sicurezza è un tema chiave e bisogna prevenire gli attacchi con la formazione e la gestione degli accessi ai sistemi informativi.

ALCUNI NUMERI

Il partner di Deloitte descrive la cybersecurity come un settore in grande crescita. Nel 2021 il valore globale del mercato è stato di 140 miliardi di dollari e le previsioni per il futuro sono rosee: 155,83 miliardi nel 2022 e 376,32 miliardi nel 2029.

Inoltre per Bonanni il riscatto non va pagato perché si entrerebbe in un giro di connivenza con l'attaccante. "Ci sono casi in cui, a fronte del pagamento del riscatto richiesto, l'attaccante non ha poi fornito l'algoritmo di decriptazione dei dati. L'indicazione è di rivolgersi sempre alle autorità competenti e a esperti certificati del settore", ha aggiunto il partner di Deloitte. Importante anche il tema dell'obsolescenza dei sistemi poiché ci sono aziende sanitarie con dati di 20-30 anni, non aggiornati e non aggiornabili. Si tratta di mine vaganti all'interno dell'ecosistema digitale. È necessario aggiornare e 'patchare' i sistemi informativi all'ultima release che il vendor ha fornito. Gli antivirus e gli antimalware vanno aggiornati realtime. Ed è fondamentale il sistema di segregazione delle reti. Non flat, ma bisogna isolare i segmenti di rete. Il paragone calzante è quello dei cluster Covid o del ruolo svolto dalla porta anti-incendio nel delimitare il pericolo.

Bonanni ha spiegato il concetto di architettura "Zero Trust", basata sul principio che non esiste fiducia implicita concessa ad alcun elemento di una rete o di un sistema. In altre parole, un'organizzazione non dovrebbe fidarsi di alcuna richiesta (per esempio di accesso ad una risorsa informatica) senza preventiva verifica, a prescindere dal fatto che la richiesta provenga dall'interno o dall'esterno del perimetro aziendale. Tra le misure di sicurezza più efficaci è da menzionare anche l'autenticazione basata sul rischio (Risk Based Authentication), un metodo di autenticazione dinamico multi-fattore che applica livelli di controllo incrementali a seconda del profilo di rischio dell'agente che richiede accesso ad un sistema. Così come accade nel mondo bancario quando avviene un pagamento anomalo dal conto corrente. Nel caso del phishing una possibile email finta del fornitore può contenere il messaggio "ho cambiato l'iban, fammi qui il bonifico". In questi casi bisogna contattare il fornitore e chiedere una lettera della banca. Non fidarsi e chiedere una verifica.

A RISCHIO TUTTA LA WHITE ECONOMY

A rischio non è solo il settore sanitario, ma anche quello farmaceutico e dei dispositivi medici. Il primo, che nel 2021 ha avuto una produzione di 34,4 miliardi di euro in Italia e di 1.423,5 miliardi di dollari a livello globale, è più avanti di quello sanitario. Il motivo è dato dai maggiori investimenti delle società farmaceutiche rispetto alle aziende pubbliche. Nel mondo della ricerca clinica tutti i dati sono digitali, per esempio quelli relativi alla sperimentazione di un farmaco. Ci sono stati attacchi ransomware anche qui, ma non se ne ha conoscenza perché vengono resi noti quelli alle aziende pubbliche o quelli che il cybercriminale decide di comunicare.

Il settore dei medical device ha un giro d'affari di 10,8 miliardi in Italia, 140 in Europa e 507 nel mondo. Questi dispositivi sono difficili da aggiornare, anche perché prodotti da vendor molto verticali. E possono rappresentare un veicolo di accesso per gli attaccanti se non sono segregati. Per Bonanni "è fondamentale che i dispositivi biomedicali, quali per esempio quelli in gestione all'ingegneria clinica, debbano essere isolati dalla rete it 'tradizionale' e debbano essere adottati protocolli diversi anche e soprattutto nell'ottica della continuità del servizio al paziente".

GLI EFFETTI DELLA GUERRA

Negli ultimi mesi, complice la guerra in Ucraina, è stato innalzato il livello di attenzione sulla sicurezza. Ci sono gruppi di cybercriminali su entrambi i fronti. I più noti sono Anonymous (pro Ucraina) e Conti (pro Russia). Quest'ultimo vittima di un leak che ha dimostrato come queste organizzazioni siano strutturate come delle vere e proprie multinazionali con tanto di risorse umane e premio per il "dipendente del mese". Inoltre questi gruppi possono mettere a disposizione il ransomware as a service. Un software che può essere acquistato da terzi per sferrare gli attacchi. Finora pochi cybercriminali sono stati presi poiché operano in maniera anonima. Per esempio Anonymous è di fatto gruppo mondiale di hacker che si appoggiano a questo brand. E chiedere il riscatto in criptovaluta è un escamotage per non essere rintracciati. Il conflitto iniziato dalla Russia ha accelerato lo sviluppo della cybersicurezza, così come "il Covid ha fatto con la digitalizzazione", ha spiegato Valeria Brambilla, Life Sciences & Health Care Industry Leader di Deloitte. Che ha aggiunto: "Il processo in corso nel settore sanitario al momento riguarda tecnologie diffuse, ma semplici. Come le prenotazioni e la virtualizzazione della cartella clinica (il fascicolo sanitario elettronico). Invece quelle più evolute, l'intelligenza artificiale, l'Iot e la blockchain, saranno un obiettivo implementabile appieno solo nel medio termine (3-5 anni)". Il Pnrr prevede fondi per la telemedicina, una tecnologia semplice. Ma si dovrà considerare anche per la preparazione del personale. "Prima bisogna dotare il settore dell'infrastruttura necessaria e poi, però, devo formare le persone. Hanno una formazione medica, ma dovranno averla anche tecnologica", ha sottolineato Brambilla. A latere c'è anche il tema regolatorio. È necessario seguire le normative in essere e quelle che verranno riviste. Il Gdpr va bene, ma bisogna rivedere i processi, le procedure, le mansioni e i ruoli. Va ripensato il disegno generale. E la gestione dei dati da manuale deve diventare digitale.

I DATI DEL RAPPORTO SOPHOS

Gli attacchi ransomware non riguardano solo il mondo healthcare, ma sono trasversali ai vari settori. Anche aziende come Campari, Enel, Luxottica o Trenitalia ne sono state vittime. Quest'ultima il 23 marzo scorso si è vista bloccare diverse macchine self service e biglietterie. Con disservizi per gli utenti. Il fenomeno è in netta crescita e il rapporto "State of Ransomware 2022" di Sophos, multinazionale attiva nel settore della sicurezza, lo testimonia. Il 61% del campione di aziende italiane oggetto della ricerca è stato colpito da ransomware nell'ultimo anno, mentre il 27% si aspetta di essere colpito in futuro. Delle aziende vittime di ransomware, il 63% ha subito l'encryption dei file mentre il 26% è riuscito a bloccare l'attacco prima che i dati venissero criptati. Il 43% ha pagato il riscatto e ha recuperato i propri dati mentre il 78% dichiara di essere riuscito a recuperare i dati grazie al proprio backup. Tra le aziende che hanno pagato il riscatto, il 24% ha recuperato circa la metà dei propri dati e solo il 3% è riuscito a recuperare la totalità dei dati sottratti dai cybercriminali.

ANCORA POCHE POLIZZE

Di crescente importanza il tema delle assicurazioni contro il rischio cyber, anche se "in Italia sono solo le aziende più grandi ad essersi assicurate perché manca la cultura", ha spiegato Remo Marini, responsabile sicurezza di Generali e amministratore delegato di GeneraliCyberSecurTech. Che ha aggiunto: "L'iter per le polizze cyber è complesso, non è come per l'rc auto. Bisogna fare un assessment dell'azienda ed è necessario discutere con il cliente se ha senso fare l'assicurazione o meno". Generali Italia gestisce il potenziale acquirente e vende le polizze (la prima nel settore è la Cyber Lion), mentre GeneraliCyberSecurTech si occupa dell'assessment e del post breach, la fuga di dati. In questo caso l'azienda li contatta e loro gestiscono, anche grazie a un accordo con Accenture. Anche loro non consigliano mai di pagare il riscatto perché il rischio è un furto di denaro senza sblocco dei dati. E, ha evidenziato Marini, "nel 95% dei casi il riscatto non è coperto dal risarcimento previsto dalla cyber polizza".

Il mercato globale, composto sia dalle polizze cyber autonome sia da quelle che fanno parte di assicurazioni it, nel 2020 è stato di 7,5 miliardi di dollari, con una proiezione per il 2028 di 36 miliardi. In Italia siamo indietro rispetto agli Stati uniti dove tutti sono coperti, infatti due anni fa il mercato del Nord America è stato di 5,3 miliardi, mentre quello europeo di un miliardo. I dati sono in crescita perché, come rilevato dal Risk Barometer di Allianz Global Corporate & Specialty, per il 2022 le aziende, sia a livello globale sia italiano, hanno messo i rischi informatici al primo posto della classifica delle proprie preoccupazioni.

Parole chiave
Cybersecurity, ransomware
Aziende/Istituzioni
Asl Napoli 3 Sud, Corte dei Conti, Regione Campania, Agenzia per l'Italia digitale (Agid), Agenzia per la cybersicurezza, Scudomed, Deloitte, Generali, Campari, Enel, Luxottica, Trenitalia