ATTACCHI HACKER, “CYBER SECURITY FONDAMENTALE PER NOSTRA SOCIETA'”. PARLANO GLI ESPERTI

15 Maggio 2023



L’AQUILA – Tiene inevitabilmente banco in Abruzzo la drammatica vicenda dell’attacco hacker ai sistemi informatici della Asl 1 di Avezzano-Sulmona-L’Aquila che ha messo in ginocchio l’azienda sanitaria, con gravi conseguenze sull’utenza e sui malati, che la stessa Asl sta cercando di limitare al massimo, cercando al tempo stesso di ripristinare in ogni settore una situazione che sia il più vicino possibile alla normalità.

Mentre i pirati informatici continuano a diffondere sul cosiddetto dark web, per costringere le istituzioni a pagare un riscatto, i dati sensibili di molti utenti, motivo per cui sono già arrivate cento richieste di risarcimento danni alla Asl.

Ed è quindi necessario trattare un tema, quello della cyber security, dando la parola a chi se ne occupa dal punto di vista diretto, quindi professionale.

A spiegare, anche in dettaglio, ad *AbruzzoWeb.it*, cosa sia il rischio cyber, sono gli esperti di Securnow, Alessio Deiana e Claudio Lisi, Security Manager certificati Uni 10459:2017, che si occupano di sicurezza cibernetica. Securnow è un gruppo di consulenti partner della Faraone Group dell’imprenditore aquilano Luigi Faraone, che nel capoluogo di regione abruzzese e non solo da oltre vent’anni si occupa di sicurezza a trecentosessanta gradi.

Una Asl provinciale abruzzese viene colpita da un attacco hacker. E improvvisamente una grossa fetta di cittadinanza viene messa di fronte a un evento molto grave. È il caso, dunque, di spiegare l’importanza della cyber security, ossia quell’insieme di tecnologie, processi e misure di protezione progettate per ridurre il rischio di attacchi informatici.

In un mondo estremamente interconnesso, dove la nostra vita, i nostri interessi, le nostre informazioni personali e aziendali viaggiano in un millesimo di secondo da una parte all’altra del globo, è fondamentale avviare un processo di sicurezza informatica all’interno della propria azienda. Si pensi che solo nel primo semestre dell’ultimo anno si sono verificati 757 casi di attacchi cyber gravi, provenienti soprattutto da fattori interni alle aziende e tante sono state le vittime illustri nel panorama internazionale. Ma l’escalation di rischi e pericoli legati alla gestione del dato colpisce tutte le organizzazioni, a prescindere da dimensioni e settore di competenza.

Le statistiche non mentono.

Secondo il Rapporto Clusit 2023, a livello globale il numero di attacchi continua a crescere anno dopo anno e confrontando il

2022 con il 2018 la crescita è stata del 60 per cento, passando da un totale di 1.554 a 2.489 con una variazione sulla media mensile da 130 a 207. In particolare, l'aumento degli attacchi è stato sia nella quantità sia nella severità degli attacchi: l'80 per cento di essi è stato classificato con severità alta o critica, con l'aumento dell'incidenza degli attacchi critici, pari al 36 per cento, anche questo un record.

La situazione nel nostro Paese?

Sono stati registrati 373 attacchi a realtà presenti in Italia tra il 2018 e il 2022, di cui ben 188 eventi nell'ultimo anno, +169 per cento rispetto al 2021 e +527 per cento rispetto al 2018. Altro dato degno di nota è che proporzionalmente a tale crescita in Italia è stato registrato il 7,6 per cento degli attacchi globali (era il 3,4 per cento nel 2021), elemento che pone un'elevata attenzione al fatto che il nostro Paese stia diventando un target prioritario per gli attaccanti.

Domanda banale: perché si verificano gli attacchi informatici?

Gli attacchi informatici subiti da un'azienda hanno l'obiettivo di acquisire informazioni di tipo finanziario, gestionale, personale e molte altre ancora. Possono attaccare individui, aziende ed enti governativi acquisendo conversazioni telefoniche, e-mail, hacking di siti web per estrarre informazioni riservate. Secondo quanto dichiarato dal Segretario Generale dell'Interpol Jurgen Stock, durante la 90esima Assemblea Generale dell'Interpol ad ottobre 2022, il costo globale della criminalità informatica raggiungerà i 10.5 trilioni di dollari entro il 2025.

Il costo di un attacco cyber è solo di tipo economico?

Un attacco cyber andato a segno può causare gravi danni all'infrastruttura: operativo, finanziario, reputazionale e legale. Un'azienda che non cura la propria sicurezza informatica rischia in termini di interruzione della propria operatività, anche per diversi giorni, con conseguenze finanziarie e reputazionali. A tutto ciò si aggiunge l'aspetto legale correlato ad eventuale diffusione di dati in violazione della privacy. Secondo alcune stime della National Cyber Security Alliance degli Stati Uniti, il 60 percento delle piccole imprese fallisce sei mesi dopo un attacco informatico.

Come si può gestire un rischio cyber?

La gestione del rischio cyber è un approccio strategico per dare priorità alle minacce. Le organizzazioni implementano la gestione del rischio di sicurezza informatica per garantire che le minacce più critiche vengano gestite in modo tempestivo. Questo approccio aiuta a identificare, analizzare, valutare e affrontare le minacce in base al potenziale impatto che ciascuna minaccia pone. Una strategia di gestione del rischio riconosce che le organizzazioni non possono eliminare completamente tutte le vulnerabilità del sistema o bloccare tutti gli attacchi cibernetici. Stabilire un'iniziativa di gestione del rischio cyber aiuta le organizzazioni ad occuparsi prima dei difetti più critici, delle tendenze delle minacce e degli attacchi.

Che cos'è una valutazione del rischio cyber?

Si tratta di processo che aiuta le organizzazioni a determinare gli obiettivi aziendali chiave e quindi a identificare le risorse IT (ogni componente hardware e software in grado di offrire delle funzionalità all'interno del sistema informatico, es. server, software gestionali, pc, notebook, eccetera) appropriate necessarie per realizzare i propri obiettivi. Ciò implica l'identificazione di attacchi informatici che possono avere un impatto negativo su queste risorse IT. L'organizzazione è tenuta a determinare la probabilità che si verifichino questi attacchi e definire l'impatto che ogni attacco può causare. Una valutazione del rischio cyber dovrebbe portare alla mappatura dell'intero ambiente delle minacce e il modo in cui può influire sugli obiettivi di business dell'organizzazione. Il risultato della valutazione dovrebbe aiutare i team di sicurezza e le parti interessate a prendere decisioni informate sull'attuazione delle misure di sicurezza che mitigano questi rischi.

Quali sono le minacce cyber?

Il termine minaccia cyber si applica generalmente a qualsiasi vettore che può sfruttare una vulnerabilità presente nel sistema IT per violarne la sicurezza, causare danni all'organizzazione o esfiltrarne o criptarne i dati. Elenchiamo le minacce comuni che le organizzazioni moderne devono affrontare includono attacchi cyber:
• Cyberterrorismo: Il termine "cyber terrorismo" indica l'utilizzo del cyberspazio (Internet) per fini terroristici, ovvero, diffondere la paura e il panico nella popolazione destabilizzando l'ordine e la sicurezza pubblica, per ragioni politiche, ideologiche o religiose.
• Malware: questa minaccia comprende ransomware, spyware, virus e worm. Malware o "software malevolo" è un termine generico che descrive un programma/codice dannoso che mette a rischio un sistema. I malware cercano di invadere,

danneggiare o disattivare computer, sistemi, reti, tablet e dispositivi mobili, spesso assumendo il controllo parziale delle operazioni del dispositivo. Proprio come l'influenza, interferiscono con il loro normale funzionamento. Lo scopo dei malware è lucrare illecitamente a spese degli utenti.
• Trojan: come il leggendario cavallo di Troia della mitologia, questo attacco induce gli utenti a pensare che stiano aprendo un file innocuo. Al contrario, una volta installato, il trojan attacca il sistema, stabilendo in genere una backdoor che consente l'accesso ai criminali informatici.
• Botnet: comporta attacchi informatici su larga scala condotti da dispositivi infetti da malware controllati a distanza. Assumendo il controllo di centinaia o perfino migliaia di computer, le botnet vengono generalmente utilizzate per inviare spam o virus, rubare i dati personali o lanciare attacchi DDoS. Sono considerate una delle principali minacce online odierne.
• DDoS (Denial of Service): Gli attacchi DDoS cercano di disattivare singoli siti web o intere reti sommergendoli di traffico causato da migliaia di computer infettati, noti collettivamente come botnet. I siti bancari, i siti di informazione e anche i siti governativi rappresentano i bersagli principali degli attacchi DDoS, causando un'interruzione nel servizio fornito. Dato che sia l'obiettivo dell'attacco sia i computer utilizzati per lo stesso sono entrambi vittime, i singoli utenti diventano danni collaterali dell'attacco, vedendo i propri PC rallentati o bloccati a causa del lavoro che devono svolgere per gli hacker.
• Adware: questa minaccia è una forma di malware. Viene spesso chiamato software supportato da pubblicità. L'adware è un tipo di software gratuito supportato da pubblicità che vengono visualizzate in finestre pop-up o sulla barra degli strumenti di un computer o di un browser. Gran parte degli adware sono fastidiosi, ma innocui. Tuttavia, alcuni adware vengono utilizzati per raccogliere informazioni personali, tracciare i siti web visitati o registrare le digitazioni.
• SQL injection: una SQL è una richiesta di eseguire un'azione su un database, in genere una pagina web che richiede un nome utente o una password. Tuttavia, dato che gran parte dei siti web non monitora le immissioni diverse dal nome utente e dalla password, un hacker può utilizzare le caselle di immissione per inviare le proprie richieste, finendo per "iniettare" codice SQL nel database. In questo modo, gli hacker possono creare, leggere, aggiornare, alterare o eliminare i dati memorizzati nel database back-end, in genere per accedere a informazioni sensibili come codici fiscali e numeri delle carte di credito, oltre ad altre informazioni finanziarie.
• Phishing: gli hacker utilizzano comunicazioni false, in particolare e-mail, per ingannare il destinatario inducendolo ad aprirle e seguire istruzioni che in genere richiedono informazioni personali. Alcuni attacchi di phishing installano anche malware.
• Attacco man-in-the-middle (MITM): gli attacchi MITM coinvolgono gli hacker che si inseriscono in una connessione tra due utenti. Una volta entrati, gli hacker possono filtrare e rubare i dati desiderati. Gli attacchi MITM si verificano spesso su reti Wi-Fi pubbliche non protette.
Vista la situazione attuale risulta doveroso approfondire la minaccia del Ransomware.
Il Ransomware è un malware (come sopra descritto) che oltre ad insediarsi nelle nostre risorse IT ha due obiettivi principali:
1. criptare i file (file/cartelle con dati sensibili, progetti, file backup, ecc.) per renderli indisponibili al proprietario
2. esfiltrare i dati.
Non è un attacco di spionaggio industriale, il suo scopo è bloccare l'operatività sui dati di nostro interesse (in quanto criptati non sono utilizzabili se non si conosce la chiave di decifratura) per poi chiedere il riscatto (ransom).

Perché l'attaccante/hacker cerca di esfiltrare i dati?

Perché qualora non si dovesse procedere con il pagamento del riscatto, l'attaccante intimerà una divulgazione dei dati sulla rete, dark web (azione di doppio riscatto) con molteplici conseguenze di natura reputazionale e legale (es. privacy) per l'azienda. A tal proposito se un Ransomware, per la sua natura, ha la necessità di manifestarsi all'interno di un sistema poiché ricordiamo che il suo obiettivo è chiedere un riscatto, altre tipologie di attacco di alto livello (APT Advanced Persistent Threat) hanno l'obiettivo di mantenersi all'interno del sistema per più tempo possibile Secondo le stime del rapporto IBM Cost of a data breach infatti il tempo medio di scoperta (cd. finestra di compromissione) di un attacco APT è di oltre 200 giorni dove ci vogliono in media 75 giorni per "rimediare", o riparare, ai danni di un attacco informatico una volta scoperto.

Come chiedono il riscatto i cyber criminali?

Facciamo un passo indietro. Prima di rispondere alla domanda sfatiamo prima l'idea dell'hacker "nerd smanettone" nella sua piccola e buia stanzetta di casa con felpa e cappuccio tirato su. I cyber criminali o le cd. cyber-gang sono delle vere e proprie organizzazioni ben strutturate, dotate di sistemi all'avanguardia, a volte sponsorizzate da Stati-Nazione, ma soprattutto in continua evoluzione. Una volta portato a termine l'attacco, inviano delle precise istruzioni da seguire per procedere con il pagamento: al fine di preservare la loro identità, vengono utilizzate le criptovalute come canale di pagamento. Viene richiesto alla vittima, qualora non ne fosse già in possesso, di aprire un wallet (portafoglio in criptovaluta) e di acquistare il corrispettivo del riscatto in Bitcoin (più famosi) o in altre cryptovalute. In seguito di andare sul sito indicato nel Dark Web e procedere con il pagamento. Avendo a che fare, appunto, con dei criminali, si deve prestare attenzione alle

conseguenze del pagamento:
1. secondo alcune stime solo circa il 20% dei paganti ottiene il ripristino dei dati e talvolta solo parzialmente;
2. per aziende/enti pubblici o privati possono esserci ripercussioni di natura legale. Infatti, per gli Enti Pubblici si rischierà di essere chiamati a rispondere per danni all'erario dello Stato, per le aziende private potrebbero emergere delle valutazioni relative all'applicazione del D.Lgs. 231/2001 – Responsabilità amministrativa delle società e degli enti.
3. Come si evince dall'ultimo studio della società Trend Micro, Il 10% delle organizzazioni che subisce un attacco ransomware paga il riscatto ai cybercriminali e finanzia in questo modo una media di altri nove attacchi.

Cosa si intende per errore umano?

Se le vulnerabilità non risolte rappresentano la causa primaria più frequente di accesso iniziale a un sistema, in seconda posizione troviamo l'utilizzo di credenziali compromesse fornendo all'attaccante un accesso diretto ai nostri sistemi. Qualsiasi utente può scaricare accidentalmente malware o essere ingannato da schemi di ingegneria sociale come le campagne di phishing, uno dei tipi di truffa su internet. Una configurazione errata dell'infrastruttura può quindi esporre alla perdita di dati sensibili. Per prevenire e mitigare queste minacce, è fondamentale istituire un programma di formazione e sensibilizzazione dei dipendenti e applicare severi controlli di sicurezza. Ad esempio, utilizzare i gestori di password e monitorare i sistemi critici per riscontrare le configurazioni errate.

Per gestire un rischio cyber, quali strumenti occorre utilizzare?

Esistono diversi modelli (framework) di gestione del rischio cyber, ciascuno dei quali fornisce standard specifici che le organizzazioni possono utilizzare per identificare e mitigare i rischi. L'alta dirigenza e i responsabili della sicurezza utilizzano questi modelli per valutare e migliorare la posizione di sicurezza dell'organizzazione. Un framework di gestione del rischio informatico può aiutare le organizzazioni a valutare, mitigare e monitorare efficacemente i rischi, definire processi e procedure di sicurezza per affrontarli. Prendendo in esame il modello dell'Agenzia per l'Italia Digitale (AgID), https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict vengono indicate le misure minime di sicurezza per le Pubbliche Amministrazioni, cit. "un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle amministrazioni, al fine di contrastare le minacce informatiche più frequenti". Altri framework di gestione del rischio informatico comunemente usati sono il NIST CSF (National Institute of Standards and Technology Cybersecurity Framework che fornisce una serie completa di best practice che standardizzano la gestione del rischio. La ISO27001 che offre un insieme certificabile di standard definiti per gestire sistematicamente i rischi posti dai sistemi informativi, lo standard ISO 31000, che fornisce linee guida per la gestione del rischio aziendale e il CSIRT istituito presso l'Agenzia per la cybersicurezza nazionale (ACN).

In che modo si pone rimedio ad un attacco cyber?

È difficile porre rimedio ad un attacco cibernetico andato a segno. Nel linguaggio tecnico esistono due termini anglosassoni utilizzati quando avviene un attacco, Disaster Recovery e Business Continuity.

Tradotto per noi umani?

Il Disaster Recovery è un servizio che indica tutte le misure tecniche utili a gestire un possibile disastro che potrebbe colpire il sistema informativo aziendale e che potrebbe essere generato da diverse cause: calamità naturali come alluvioni o terremoti, errori umani, furti o hacking. Il piano di Disaster Recovery stabilisce innanzitutto quali sono i processi critici per l'azienda, indicando quali di essi devono essere meglio protetti e monitorati. Lo scopo della strategia di Business Continuity è quello di ridurre al minimo l'interruzione delle attività conseguenti ai danni, nonché assicurare l'efficacia delle procedure di ripristino. Ogni piano di continuità aziendale è diverso e altamente personalizzato in base al tipo di attività e alle sue particolari esigenze. La Business Continuity, infatti, deve assicurare la sopravvivenza globale dell'azienda in caso di disastri e include non solo la protezione del sistema informatico ma la salvaguardia della continuità di tutte le funzioni aziendali essenziali. La strategia di Business Continuity conta tutti i possibili eventi che potrebbero minacciare la vita dell'azienda ed è utile anche con piccole interruzioni delle attività. Inoltre, è in grado di fornire una visione strategica complessiva per aumentare la resilienza del business e la competitività sul mercato.

In sintesi, e per concludere: quanto è importante la cyber security?

Ad oggi la cyber security è fondamentale perché aiuta a proteggere le organizzazioni e gli individui dagli attacchi informatici e può aiutare a prevenire le violazioni dei dati, il furto di identità e altri tipi di criminalità informatica. Le organizzazioni devono disporre di solide misure di sicurezza informatica per proteggere i propri dati e quelli dei propri clienti.

© 2026 Abruzzo Web Enfasi srl - Quotidiano digitale registrato presso il Tribunale dell'Aquila con decreto n°501 del 3 settembre 2003
Iscrizione al ROC n. 26362 - P.IVA 01812420667
Direttore responsabile Berardo Santilli