CYBER ATTACK E CYBER CRIME

Aziende sotto attacco di pirati del web furti di dati anche dai dipendenti

Ad alcuni imprenditori è stato chiesto un riscatto per rendere nuovamente utilizzabili i file

In alto a sinistra Paolo Rossetti

RIMINI
NICOLA STRAZZACAPA

Cyber attack e cyber crime sono in cima all'agenda di tutti i governi. Il tema del giorno, in Italia e nel mondo. In Usa Joe Biden, fra i suoi primi atti ha firmato un ordine esecutivo per obbligare le aziende in contatto con la sua amministrazione a rafforzare la sicurezza informatica. In Italia, il ministro per l'Innovazione Colao afferma che «il 95% dei server della nostra pubblica amministrazione non è protetto» e Palazzo Chigi fa nascere l'agenzia tricolore per la cyber security. E la Romagna e tutta la regione non fanno differenza. Anzi, crescono i cyber attack, che non risparmiano imprese di grandi e piccole dimensioni o studi professionali. A rivelarlo attraverso una serie di esempi concreti che riguardano società vittime tra Rimini e Forlì è Paolo Rosetti, chief excutive officer & DPO di 'Consulenti Privacy', società riminese in costante crescita sul territorio nazionale tanto che negli ultimi tre anni di attività ha aperto sedi in diverse città, tra cui Milano, Roma, Bologna e San Marino.

Siamo tutti sotto attacco

«Il cyber crime non colpisce solo imprese di grandi dimensioni o governi. Siamo tutti sotto attacco. I dati sensibili, commerciali, bancari, contenuti nei nostri Pc e server, possono diventare una miniera d'oro, per i criminali informatici. Il dipartimento della giustizia Usa dice che i primi 6 mesi del 2021 hanno già registrato un balzo in avanti delle attività di hacker e criminalità sul web del 102%. Nel mirino è finito addirittura tutto il servizio sanitario irlandese, grandi multinazionali hanno sborsato cifre milionarie dopo essere state colpite da ramsonware» spiega Rosetti, passando al panorama locale: «Un mese fa una delle aziende clienti di Consulenti Privacy è stata infettata da un ransomware. Il malware ha limitato l'accesso ai Pc, cifrato i file dell'utente rendendoli illeggibili e ha chiesto il pagamento di un riscatto, per disinstallarsi. Strategia fallita perché su suggerimento del nostro team di professionisti e a seguito di un'analisi del loro sistema informatico, era stato appena adottato un sistema di business continuity e backup all'avanguardia che ha consentito di riprendere la piena operatività in poche ore: zero perdita di dati e nessun riscatto».

Sventato il "furto" degli ex dipendenti

In un'altra impresa sempre seguita da Consulenti Privacy Srl si sono accorti invece che il Crm, quello con dentro tutti i dati dei clienti, girava lento e grazie a questo è stato sventato un vero e proprio furto di informazioni. «Appena avvisati, siamo intervenuti e abbiamo scoperto che degli ex dipendenti, ancora in possesso delle password di accesso, stavano trafugando sottotraccia l'intero Crm, con i suoi migliaia di contatti e i dati correlati. Quindi, fatta la notifica di legge al Garante per la privacy e aperta un'azione nei loro confronti, abbiamo implementato nell'azienda politiche di sicurezza più stringenti per gli accessi e il monitoraggio degli utenti al Crm, per impedire il ripetersi di fatti del genere in futuro».

E' caccia ai dati

Buona parte della pirateria informatica è infatti a caccia anche di semplici informazioni. Conoscere in tempo la politica commerciale di un'impresa (prezzi, sconti, incentivi, tempi e modi di fatturazione e pagamento) può valere valere molto per ogni competitor: è un vantaggio fraudolento che altera il mercato e per questo viene ben pagato. Ma va considerato anche il danno reputazionale e d'immagine a cui si va incontro, se non si è attenti a quanto accade sulle proprie piattaforme web. E anche a questo proposito, il chief excutive officer & Dpo fa un esempio concreto: «Un'azienda ci ha chiamato perché gli sono stati segnalati flussi spamming provenienti dall'account aziendale. Qualche giorno prima, un dipendente, aveva infatti inavvertitamente aperto un file zip allegato a una mail proveniente da un loro fornitore, nel frattempo già hackerato da pirati della rete. Così un software aveva iniziato a girare sul service aziendale e dopo essere stato silente per qualche giorno, aveva iniziato a inviare mail di spam a tutti i contatti aziendali: interni ed esterni». Il caso si è risolto con bonifica dei computer aziendali e avviso a tutti i soggetti spammati di non aprire le mail ricevute. Niente di grave, ma è facile pensare a dubbi e interrogativi che possono nascere sulla sicurezza informatica di un partner commerciale che si trasforma in spammer.

«Da quest'ultimo episodio appare evidente come la cyber security non sia solo questione di firewall, antivirus, backup o cloud. C'è bisogno anche di formazione su un terreno nuovo e insidioso, dove una semplice distrazione crea danni molto gravi. L'errore umano, spesso dovuto a scarsa o nulla formazione in ambito privacy e cyber security, è il più frequente generatore di cyber attacchi. Spesso, senza rendercene conto, siamo noi stessi ad aprire le porte ai criminali del web. Il tema della sicurezza dei dati, del loro trattamento, della sicurezza di reti, connessione e hardware non è più fantascienza. È una necessità quotidiana. Nel dark web è facilissimo entrarci, basta installare un programma a disposizione di chiunque, che fa scomparire il nostro IP, la nostra carta d'identità digitale e i criminali vendono il loro prodotti informatici illegali. Chi li compra li usa per furti, alterazioni d'identità, frodi, spionaggio commerciale e finanziario» conclude Rosetti, evidenziando come «un malware bancario per Android costa mille dollari, per Bancomat 2 mila un Kronos 3 mila (dati Trend Micro Reserch)» e concludendo: «Molto meglio proteggersi».

> «Spesso siamo noi stessi ad aprire le porte ai criminali del web Il tema della sicurezza dei dati non è più fantascienza»
>
> «Nel dark web è facilissimo entrarci: basta un programma a disposizione di chiunque»
>
> **Paolo Rosetti** Consulenti Privacy

Caserma "Giulio Cesare" affidata all'Agenzia del demanio

RIMINI

Un altro passo (questa volta ufficiale) verso la creazione della Cittadella della sicurezza. La caserma "Giulio Cesare" ieri ha completato il suo completo distacco dall'Esercito.

Infatti. Il ministero della difesa ha formalizzato la dismissione dell'area che da ieri è nella disponibilità dell'Agenzia del Demanio regionale. Un passaggio ufficializzato dalla sottoscrizione a Bologna di un verbale fra Stato Maggiore dell'Esercito e Demanio, che sancisce la consegna all'ente regionale del complesso in via Flaminia, una superficie che si estende per circa 70mila metri quadrati e su cui sorgono una dozzina di costruzioni oltre a ulteriori strutture minori.

Con la consegna al Demanio si apre così la possibilità di conferire all'ex caserma riminese una nuova destinazione, progetto su cui da tempo l'amministrazione comunale sta lavorando in sinergia con la Prefettura.

L'intenzione è di trasformare l'edificio nel nuovo "Federal building" di Rimini, diventando cioè sede delle forze dell'ordine, soluzione che consentirebbe di sanare un vulnus storico del territorio provinciale.

La caserma Giulio Cesare

A questo proposito si ricorda che il primo luglio in Tribunale va all'asta il complesso in via Ugo Bassi in origine destinato a diventare la sede della nuova questura e invece, dopo anni di abbandono e degrado, finito nell'oblio delle procedure fallimentari della società Dama.