HACKER, RISCATTI E NUOVE NORME

# I cyberattacchi bloccano il medico come il carrozziere

Trivilini, responsabile dell'informatica forense, Supsi TI-PRESS

**Ovunque, il numero di aggressioni alle reti aziendali è aumentato bruscamente. A un garage, gli hacker hanno chiesto un riscatto di 700mila franchi. Nel mirino ospedali, studi medici, Comuni... Come difendersi e come prepararsi per la nuova legge sulla protezione dei dati. Entra in vigore tra 12 mesi.**

*di Simonetta Caratti*

L'ing. Paolo Lezzi (a sinistra) Ceo della InTheCyber e il legale Rocco Talleri

A una carrozzeria con 22 dipendenti hanno chiesto un riscatto di 700mila franchi per ripristinare l'attività e recuperare i dati sottratti. Ovunque, il numero di attacchi alle reti aziendali è aumentato bruscamente. In Svizzera del 65%. Nel mirino studi medici, ospedali, piccole e grandi aziende, amministrazioni pubbliche, Comuni, come quello di Rolle (nel canton Vaud) che non ha pagato il riscatto. Il risultato: numerosi dati sensibili degli abitanti sono finiti nel dark web. L'obiettivo dei cybercriminali è quello di batter cassa, coi ransomware ci riescono benissimo, con un minimo sforzo incassano milioni. Sono virus informatici che rendono inaccessibili i file dei computer infettati. Per ripristinarli, i criminali chiedono un riscatto, in genere in criptovaluta. Anche se la polizia sconsiglia di pagare, molte ditte lo fanno per poter continuare a lavorare. Un attacco blocca in media un'azienda per 23 giorni.

«È l'arma perfetta, collaudata, la monetizzazione di una truffa da ransomware è diventata ormai industriale. Si manda un'email e se va bene, a rischio e costo zero, si monetizza», ci spiega **Alessandro Trivilini**, responsabile del servizio informatica forense della Scuola universitaria professionale della Svizzera italiana (Supsi). Quasi una cyberpandemia. «Effettivamente è globale. Siamo all'inizio di una nuova sfida, purtroppo non si vede la fine, non ci salverà un antivirus; queste truffe saranno sempre più perfezionate sulla base di come evolvono le tecnologie, la consapevolezza delle persone e la quantità di dati».

Nel 2021 in Ticino si sono registrati 338 reati, la maggior parte legati alla cybercriminalità economica: 160 nel 2020 e 255 nel 2021. A questi va aggiunta la parte sommersa, quella in cui è stato pagato un riscatto. Quanti siano è difficile dirlo, ma secondo gli esperti è un numero elevato. «Le aziende oggi (ma cambierà tra un anno, con la nuova legge) non hanno obbligo di notificare l'attacco ai clienti, alcune lo fanno, altre tendono a lavare i panni in casa per evitare cattiva pubblicità, come dover ammettere che non erano pronte. In tanti casi il riscatto viene pagato, altrimenti l'azienda rischia di chiudere», precisa l'esperto. La polizia comunque sconsiglia di pagare per non alimentare reti criminali. «È corretto, ma è solo il 50% della verità. Se l'azienda non ha un piano di risposta per questi attacchi, se non è preparata ed equipaggiata per rimediare al danno, non potrà ripristinare servizi, dati, documenti dismessi. Non potrà lavorare».

Per questo motivo, in Ticino è nato un gruppo di lavoro trasversale a supporto di aziende e Comuni che comprende aspetti tecnici, assicurativi, di protezione dei dati e di validazione scientifica. «Siamo un'alleanza e ci muoviamo come squadra. Purtroppo chi non investe nella protezione rischia di pagare 2 volte e mezzo in più». Nell'ultimo anno ci sono state varie ondate di attacchi ransomware: «Infatti, il nostro servizio d'informatica forense è stato molto sollecitato da Comuni e aziende presi dal panico, ma anche da chi vuole scongiurare un attacco». Gli investimenti dipendono da molti fattori. «Viene fatta una radiografia della realtà aziendale, poco importa se è familiare o industriale, identifichiamo gli ambiti più fragili da mettere in sicurezza. Si valutano le tecnologie usate, quali processi e che tipo di dati sono utilizzati, chi usa quali tecnologie, quale formazione ha. Solo dopo una mappatura, possiamo stabilire quale è il livello di rischio più elevato e dove si posiziona».

In cima alla lista dei target c'è chi tratta dati sensibili: «Ospedali, studi medici e istituzioni (Comuni e pubbliche amministrazioni) non possono permettersi di non essere pronti». Ma da 0 a 10 quale è il rischio di un attacco per un'azienda? «Il rischio è dieci, basta avere un dispositivo aziendale allacciato a una rete internet. C'è chi si organizza e riduce il rischio, c'è chi lo snobba e chi non crede gli possa succedere», conclude Trivilini.

COME ASSICURARE IL RISCHIO

## Una ditta può restare ferma per 23 giorni

«Il cyberattacco ci sarà: è solo una questione di quando e quanto male farà. Aziende, Comuni ed enti pubblici devono fare il possibile per essere pronti e ridurre i danni». Uno degli ultimi casi, ci confida **Régis Dubied**, Ceo e fondatore di Assidu Lugano, è stata una carrozzeria con 20 dipendenti. «Hanno chiesto 700mila franchi per sbloccare i sistemi informatici. Due anni fa vedevamo riscatti per qualche decina di migliaia di franchi, oggi parliamo di centinaia di migliaia di franchi per piccole e medie imprese, di milioni per le grandi realtà economiche», precisa l'esperto. In media un'azienda vittima di un attacco ransomware può restare bloccata 23 giorni. «Non può più lavorare perché tutti i sistemi sono criptati e bloccati. C'è un riscatto da pagare. E non è finita, c'è un altro problema da risolvere: la responsabilità verso i dati sottratti dei clienti. Se sono sensibili, come ad esempio tassazioni, cartelle mediche, conti bancari, l'azienda o l'ente rischiano la denuncia dei clienti per non aver protetto a sufficienza i loro dati personali, che sono finiti sul dark web. Oltre a ingenti perdite economiche, c'è il danno d'immagine, la reputazione di un'azienda o la fiducia in un ente vengono pesantemente intaccate», precisa. Assidu offre in Svizzera consulenze neutre in ambito assicurativo e non solo.

**Quando la polizza copre il riscatto**

Proteggersi stipulando una polizza assicurativa è il pensiero di molti. Ma come funziona? «Serve a poco, ci spiega sempre Dubied, se il cliente non ha raggiunto un certo livello di sicurezza e protezione. A questo punto si possono trovare soluzioni per il trasferimento del rischio residuo attraverso coperture assicurative adeguate». La polizza non riduce la probabilità di un attacco ma può coprire il danno finanziario dell'azienda, come il periodo di fermo e in alcuni casi (non tutte le compagnie lo fanno) una quota del riscatto chiesto dai gruppi criminali. In un momento non facile per molte aziende significa dolorosi nuovi investimenti. «È un nuovo rischio. Le dirigenze devono analizzarlo e definire una strategia per riportarlo in una zona accettabile. È importante avere un protocollo, sapere cosa fare e come uscirne, formare il personale. Nel 90% degli attacchi, il virus entra da un'email, da un'errata manipolazione, da una chiavetta Usb inserita in un computer aziendale».


DEPOSITPHOTOS/LAREGIONE



LA NUOVA LEGGE

## Un anno di tempo per mettersi in regola

C'è un anno di tempo per mettersi in regola. Comuni, aziende, pubbliche amministrazioni devono adeguare, in molti casi introdurre da zero, protocolli di sicurezza informatica, adottando misure organizzative e tecniche per garantire la sicurezza dei dati ed evitare per quanto possibile il loro uso abusivo. Così da rispettare gli obblighi della nuova legge sulla protezione dei dati, che entrerà in vigore da settembre del prossimo anno. Un bel grattacapo per tante aziende. «Invece che una spesa, la sicurezza informatica deve essere considerata un investimento. Il mercato la richiede e lo farà sempre di più, esigerà delle certificazioni», ci spiega l'avvocato **Rocco Talleri** della Talleri Law Tech Service Gmbh (studio legale esperto anche di queste tematiche). Le nuove norme garantiscono la compatibilità col diritto europeo: sono importanti proprio per garantire che l'Ue continui a riconoscere la Svizzera come paese terzo con un livello adeguato di protezione dei dati.

Che cosa cambierà? La nuova legge rafforza molto i diritti degli individui, la protezione dei loro dati, e prevede nuovi obblighi e sanzioni più pesanti. «A dipendenza dei dati trattati si dovrà avere un regolamento (misure tecniche e organizzative adeguate) per trattarli. In caso di violazioni della sicurezza dei dati si dovrà informare gli interessati».

Le nuove spese saranno proporzionate al tipo di realtà: «Una farmaceutica di Basilea con 65mila dipendenti dovrà investire diversi milioni di franchi per adeguarsi, mentre uno studio medico o una piccola azienda avranno un altro tipo di approccio. Tutti dovranno proteggere i dati dei loro pazienti e clienti. Da qui il passo successivo: quello di proteggere i dati aziendali», aggiunge il legale.

### Multe fino a 250mila franchi

La risposta elvetica all'evoluzione normativa internazionale si articola su più punti: «Sono stati introdotti importanti strumenti di controllo, conferiti più poteri all'incaricato della protezione dei dati, ossia l'autorità di vigilanza fino a oggi considerata, forse a torto, una tigre coi denti di carta. Avrà più poteri investigativi e amministrativi». In caso di violazioni alla nuova legge, si rischiano multe fino a 250mila franchi (oggi fino a 10mila franchi) per non aver protetto i dati dei clienti.

### 'Ci sarà una selezione naturale'

La sensibilità al tema in Ticino, per il legale, è ancora bassa. «Alcuni clienti stanno dimostrando lungimiranza, altri vedono tutto questo come un mero costo». Non affrontare questi nuovi rischi e non prepararsi per le nuove normative potrebbe significare essere tagliati fuori dal mercato, che chiederà questo tipo di adeguamento. «Ci sarà una selezione naturale. Più si gestiscono dati sensibili (biometrici, sulla salute, tasse, bancari...), più dipendenti ci sono, maggiori sono i processi di elaborazione, più la protezione dovrà essere articolata».

L'attuale legge svizzera sulla protezione dei dati risale al 1992. In seguito, il trattamento e l'uso di dati personali sono cresciuti man mano che economia e società si sono digitalizzati. In seno all'Ue, la protezione dei dati è stata considerevolmente rafforzata. Per la Svizzera, si è dunque reso necessario adattare la sua legge del 1992 alle nuove abitudini di consumo (acquisti online, reti sociali), agli sviluppi tecnologici (digitalizzazione, intelligenza artificiale) e alle norme internazionali.

Col nuovo Centro nazionale per la cybersicurezza, Berna sta creando le condizioni quadro affinché le organizzazioni in Svizzera possano proteggersi.

L'ESPERTO DI TRUFFE

## Copiano la voce del capo e si fanno versare soldi

Non c'è limite alla fantasia dei criminali, l'attacco di un hacker può arrivare anche via cellulare. «A un nostro cliente è arrivata una telefonata dall'amministratore delegato che chiedeva un bonifico ed è stato fatto. Ma il manager non aveva mai chiamato. Con un sintetizzatore vocale è stata ricreata la voce del dirigente. Ci vogliono sempre controlli incrociati, solo così si riducono i rischi», ci spiega l'ingegnere **Paolo Lezzi**, fondatore e Ceo dell'InTheCyber Group. In Svizzera, per l'esperto, la difesa di aziende e istituzioni da cyberattacchi non è adeguata, andrebbe fatto di più. «Un attacco è fattibile, più o meno pesantemente. Dipende solo dal tempo e dallo sforzo che un hacker deve metterci. La consapevolezza delle direzioni delle aziende è ancora bassa, anche se negli ultimi 12 mesi c'è stata una notevole proliferazione degli attacchi e dunque l'attenzione si è alzata».

### Le aziende vanno nel panico e pagano

Non usa mezze parole Lezzi, la sua compagnia è una delle dieci aziende svizzere di riferimento per la cybersicurezza. Con la Supsi collabora a progetti di ricerca nel campo del monitoraggio nel dark web, del cyberterrorismo, del ransomware. Quei micidiali virus che possono bloccare l'attività di un'azienda o un ente, che per tornare operativo, per sbloccare i sistemi informatici deve pagare un riscatto. «Le aziende senza consulenti adeguati vanno spesso nel panico e pagano. Anche pagando, non sempre c'è la certezza di poter riavere i dati e tornare operativi». C'è chi, dopo un attacco, ha dovuto chiudere i battenti. Bisogna essere preparati: «Aziende e istituzioni, nessuno escluso, tutti sono potenzialmente sotto attacco. Limitare i danni significa non dover arrivare a pagare un riscatto, perché si è pronti su tre livelli: tecnologia, persone e processi». Che cosa significa, ce lo spiega così: «Serve la consapevolezza delle persone per evitare errori che permettono di bypassare le difese; le tecnologie vanno aggiornate di continuo e devono dialogare tra loro; i processi non devono permettere vie brevi per arrivare a un determinato punto».

Per Lezzi, sarebbe opportuno creare antenne regionali e il Ticino potrebbe fare scuola: «Il coordinamento deve essere federale, ma supportato da sentinelle regionali (realtà competenti e aziende con un team di cybersicurezza) che monitorano gli attacchi, che verificano ad esempio se stanno avvenendo in contemporanea a più enti o aziende».

### Mancano tecnici cyber, andrebbero formati

Il vantaggio di costruire una rete è quello di condividere le informazioni, aumentare la consapevolezza su questi rischi in una realtà purtroppo carente di professionisti in cybersicurezza. «Mancano operatori, le università non formano tecnici cyber, andrebbero sviluppati corsi più pratici per creare reali competenze di cyberdifesa».

Per le aziende significa fare grossi investimenti in un periodo non facile. «Occorre avere almeno un sistema di monitoraggio che ha costi contenuti e investire nella formazione dei dipendenti». Infatti la debolezza umana è spesso la porta d'entrata per i cybercriminali, abili nel manipolare gli altri per i propri fini. «Basta una e-mail per avere le credenziali, poi con una telefonata, circuiscono un dipendente ed è fatta», dice l'esperto.

Dietro questi attacchi, ci ricorda, ci sono organizzazioni criminali attive 24 ore su 24: analizzano costantemente la vulnerabilità di enti e aziende, quando trovano un potenziale target si inseriscono in modo silente, lo studiano anche per mesi, ne valutano la potenzialità economica e attaccano con l'obiettivo di fare il maggior danno possibile.