IL RISCHIO CYBER SI CONTROLLA CON VISIONE E UN APPROCCIO STRUTTURATO

di MARIA MORO

GLI ATTACCHI INFORMATICI SONO IN CRESCITA COSTANTE E AUMENTA LA SEVERITÀ DEGLI IMPATTI. CHE SI TRATTI DI CYBER CRIME, DI AZIONI POLITICHE O DI ATTIVISMO, NEL MIRINO CI SONO SOPRATTUTTO LE IMPRESE E GLI ENTI PUBBLICI. SE DA UN LATO LA NORMATIVA EUROPEA PUÒ COSTRUIRE UNA CORNICE DI PROTEZIONE, DALL'ALTRA È NECESSARIO CHE TUTTI I POSSIBILI BERSAGLI SI DOTINO DI STRUMENTI DI DIFESA, DALLA FORMAZIONE AL SUPPORTO DI COMPETENZE ESTERNE

Gli attacchi informatici sono in crescita costante da alcuni anni e si possono giovare oggi delle risorse dell'intelligenza artificiale. A farne le spese sono tanto le imprese quanto gli enti della pubblica amministrazione, due ambiti presi di mira con obiettivi differenti ma che presentano analogie quando si parla di difficoltà per le realtà meno strutturate e di cultura del rischio. Due aspetti positivi, in un panorama ancora di grande vulnerabilità e caratterizzato da un continuo inseguimento agli attaccanti da parte di chi difende, sono la normativa sulla cyber sicurezza e il supporto, fatto di competenze e prodotti, che può arrivare anche dal settore assicurativo.

L'analisi di **Federico Lucia**, chief risk officer & business continuity manager di **Csi Piemonte**, è ad ampio spettro e prende in considerazione tutti gli aspetti del

rischio informatico. Il cyber risk ha molte sfaccettature e la gestione del rischio per un'impresa o un ente pubblico deve partire anche da alcune considerazioni: "Innanzitutto le tipologie di attacco, che sono riconducibili a quattro macrocategorie. Il tipo più diffuso è il *cyber crime*: di pura natura criminale, ha scopi di lucro o di danneggiamento di un competitor, e nonostante sia aumentata la cultura della sicurezza e siano migliorati i sistemi di difesa è in costante crescita. Un secondo fenomeno sono gli attacchi a scopo politico e bellico, promossi in maniera più o meno manifesta da un paese con l'obiettivo di danneggiarne un altro o di affermare la propria proiezione di potenza: è il caso della guerra cibernetica (*information warfare*), a cui si affianca la terza categoria che riguarda gli episodi di sabotaggio e spionaggio (*espionage/sabotage*), tecniche viste all'opera con gli attacchi della Russia all'Ucraina ma pure in altri casi che quotidianamente colpiscono i paesi occidentali, così come quelli più recenti attribuiti a Israele ai danni dell'Iran. La quarta tipologia è l'*hacktivism*: in un contesto di tensioni crescenti sui temi sociali, dal *climate change* ai diritti umani, fino al sostegno a forze politiche, l'attivismo può dare origine a forme di pressione nei confronti dei governi, fino ad arrivare a veri e propri sabotaggi".

ATTACCANTI DIVERSI, STESSE VITTIME

Oltre ad avere motivazioni diverse, le tipologie di *cyber attack* si differenziano per le loro caratteristiche: il cyber crime è messo in atto da persone o gruppi che agiscono in incognito, con sistemi sia semplici ed economici sia complessi e dispendiosi e con l'obiettivo di ottenere un vantaggio economico. Gli attacchi che rispondono a tensioni geopolitiche hanno alle spalle l'organizzazione governativa e militare di un paese, sono sofisticati, possono contare su investimenti notevoli e su strutture organizzate e in genere non vengono rivendicati. Al contrario, i gruppi che praticano l'hacktivism sono soliti rivendicare i propri attacchi, per i quali usano in genere budget ridotti a danno di target specifici di natura prevalentemente istituzionale.

Guardando alle vittime degli attacchi, il recente *Rapporto Clusit 2024* afferma che tra i settori più colpiti vi è quello sanitario, in crescita del 30% rispetto all'anno precedente e raddoppiato rispetto al 2019: un ambito che, secondo Lucia, "interessa per i suoi dati sensibili, perché si tratta di asset strategici a supporto della società e perché, nel complesso, le sue strutture si rivelano spesso vulnerabili in termini di sicurezza, anche in virtù di una forte dipendenza dalle catene di fornitura". In forte aumento, e attrattive per le questioni di sicurezza nazionale, sono le organizzazioni amministrative e militari dello Stato. Sono invece motivi di interesse differente che fanno del settore finanziario e assicurativo il quarto in classifica per percentuale di attacchi subiti, nonché quello con il più alto tasso di crescita, aumentato del 300% rispetto al 2019, "non a caso l'Unione Europea ha risposto a questa criticità con l'emanazione del regolamento *Dora*, che ha l'obiettivo di consolidare la resilienza cyber del comparto *Finance*", commenta Lucia.

Gli obiettivi per eccellenza da parte del cyber crime rimangono i cosiddetti *multiple target*: "sparare nel mucchio è una tattica che paga sempre e che risponde alla strategia di attaccare un fornitore critico, specialmente nella supply chain informatica, con l'obiettivo di colpire contemporaneamente quante più organizzazioni possibili tra i clienti e all'interno della sua catena di fornitura. Un esempio è l'attacco del dicembre scorso a Westpole, che ha provocato, a cascata, danni informatici a oltre 1.000 enti pubblici italiani".

MANCA UNA RISPOSTA DI SISTEMA A LIVELLO PAESE E UE

La battaglia tra gli attaccanti cyber e le loro vittime si svolge sul fronte delle tecniche di difesa: "senz'altro migliora la qualità degli antivirus, ma in parallelo crescono gli attacchi *malware* e la capacità di penetrazione, a cui si aggiunge il punto debole del cosiddetto *fattore umano*". Inoltre, sono in crescita gli attacchi sulle vulnerabilità e i DDoS, i blocchi del sistema che generano indisponibilità. Come esito dell'aumento della digitalizzazione e della qualità delle difese da parte di imprese ed enti, si è assistito negli ultimi anni a un salto di qualità delle aggressioni, con un aumento esponenziale degli attacchi a impatto alto o critico. "Tra le disponibilità degli attaccanti – osserva Lucia – rimane rilevante l'ingegneria sociale, oggi migliorata dall'intelligenza artificiale che la rende più precisa, accessibile ed economica. A tutela delle potenziali vittime e del sistema paese, le normative europee quali Dora, *Nis 2* e *AI Act* si riveleranno utili: esse vanno nella direzione giusta ma manca ancora, a livello di Unione Europea, una piena capacità di leadership nel settore rispetto ad altri soggetti geopolitici come Stati Uniti, Cina, Russia e Israele. Questi sono paesi consapevoli di avere un ruolo

IL SUPPORTO DI CSI PIEMONTE

Nato negli anni '70 del secolo scorso come centro elaborazione dati per la PA piemontese, Csi Piemonte è oggi un consorzio per il sistema informativo a cui partecipano circa 140 enti pubblici, da anni sempre più su scala nazionale, oltre che regionale. Da Ced, negli anni, l'attività è evoluta e Csi è oggi una *Cloud* e *AI company* e supporta i propri enti nei programmi di trasformazione digitale. Tra le attività principali vi è la formazione, che ha portato alla creazione del Csi Digital Campus, un asset su cui il consorzio sta investendo molto e che è stato annoverato tra i finalisti agli *European Risk Management Award* di **Ferma** (la Federazione europea delle associazioni nazionali di risk manager) nella categoria *Training & Education Excellence*.

all'interno del contesto geopolitico globale, laddove noi europei abbiamo sempre portato avanti un approccio orientato alla *pax commerciale*, mettendo in secondo piano la possibilità di una recrudescenza delle tensioni tra gruppi e tra paesi. In qualche modo, abbiamo per un certo tempo sottovalutato l'importanza di organizzare sistemi di difesa strutturati, anche nel mondo cibernetico".

TRA CULTURA CYBER E RISCHIO GENERAZIONALE

Per quanto riguarda l'Italia c'è poi un *vulnus* particolare che è la quantità di micro, piccole e medie imprese, fondamentali nel tessuto economico ma che mostrano un deficit di risorse e di strumenti idonei a tutelarsi. "La cultura del rischio cyber – ammette Lucia – sta sicuramente crescendo, aiutata dai regolamenti, dalla trasformazione digitale, dai finanziamenti del Pnrr. Il punto critico sono sempre le risorse. Le nostre Pmi fanno parte di un'economia di trasformazione ed esportazione e sono inserite in catene di approvvigionamento molto estese e che spesso transitano da paesi con cui, in questo momento storico, non siamo in ottimi rapporti, aspetto che può aumentare i rischi per il nostro sistema produttivo". A questa debolezza strutturale si aggiunge il tema generazionale, che colpisce doppiamente le Pmi: "l'invecchiamento della popolazione rende più competitivo il mercato del lavoro a scapito delle aziende meno attrattive, ciò significa anche che le persone all'interno delle imprese, e a maggior ragione della PA, sono sempre più anziane e mostrano una maggiore resistenza al cambiamento, incluso quello tecnologico".
In questo panorama, il settore assicurativo può fornire alle Pmi un supporto importante, con l'obiettivo di condividere un rischio di migliore qualità, "a partire dalle azioni per la diffusione della cultura della sicurezza fino ad affiancare aziende meno strutturate nella valutazione del rischio o offrire proposte congiunte di prodotto e servizio che possano includere, ad esempio, il supporto in qualità di *Soc as-a-service*", osserva Lucia.

SEGUIRE UNA STRATEGIA DI SICUREZZA A 360 GRADI

Se per le imprese le criticità sono nella cultura del rischio e nel reperimento di risorse economiche e umane, la pubblica amministrazione si trova invece in un processo di trasformazione digitale che fa talvolta fatica a governare, "anche se, come per le aziende, molto dipende dalle dimensioni e dalla centralità dell'ente, considerando che si va dai ministeri ai piccoli comuni. Molti non hanno ancora accesso alla banda larga, hanno scarse risorse e poca cultura digitale. Ci sono organizzazioni, come Csi Piemonte, che operano come *in-house* e riescono a supportare la PA pure in termini di sicurezza, ma non per tutti i territori questo accade. Va detto, inoltre, che solo recentemente la PA ha scoperto l'approccio decisionale *risk based* e solo dal Covid in poi ha iniziato a mettere in atto i piani di business continuity pur richiesti da anni dal *Codice di amministrazione digitale"*.
Il consiglio per le Pmi, chiuse tra carenza di risorse, contesto competitivo e vulnerabilità, è di ricercare all'esterno le competenze necessarie, appoggiandosi a società di *Soc as-a-service* (*Security operations center*) e di *Ciso as-a-service* (*Chief information security officer*), e di puntare a ridurre il rischio legato al fattore umano con adeguati piani di formazione del personale. La chiave, conclude Lucia, è nell'avere "per la *security* lo stesso approccio che c'è nella *safety*, in piena integrazione, con una strategia del rischio a 360 gradi come richiesto dalla Nis 2". E una particolare nota va proprio alla direttiva Ue: è vero che si rivolge a precisi target di imprese ma "ha una tale estensione del perimetro per cui è difficile pensare che le altre possano esserne totalmente escluse".