Cybersecurity 2023/ All'evento di Class Editori focus su un fenomeno in costante crescita

Lotta dura sul fronte informatico

Le imprese cercano di resistere. Ma servono investimenti

DI ANDREA BOERIS

Una minaccia sociale e politica, ma soprattutto economica e che tocca le imprese. Eppure l'Italia spende appena lo 0,1% del suo pil per contrastare gli attacchi informatici e la sfida è ancora tutta da giocare. Se n'è parlato all'evento Cybersecurity 2023 organizzato da Class Editori. Il cyber rischio aumenta e, come hanno spiegato **Ivano Gabrielli**, direttore del Servizio di Polizia Postale, e **Gianluca Ignagni** (Agenzia per la Cybersicurezza Nazionale), «con la guerra in Ucraina, il trend di crescita degli attacchi informatici è più che raddoppiato».

Negli ultimi due-tre anni «i cyber-criminali hanno fatto molti soldi», ha fatto notare **Dadi Gertler** (Israel Cyber), ma secondo **Igor Kranjec** (European Cyber Security Organisation) «gli attacchi cyber più pericolosi sono quelli che rubano le nostre informazioni».

Sicuramente sono le pmi quelle più esposte e «che più devono investire in cybersecurity», ha sottolineato **Eugenio Santagata**, chief public affairs & security officer di Tim e ceo di Telsy, spiegando anche che «le aziende sono il player primario nella strategia di cyber-resilience del paese perché subendo gli attacchi hanno poi informazioni importanti che possono e devono essere condivise». Se condividere informazioni permette di imparare dagli altri per essere immediatamente reattivi, «in futuro scriveremo le informazioni più importanti utilizzando i fotoni: rubare informazioni dai fotoni è contrastato dal fatto che decadono appena provi a manometterli», ha concluso ancora Santagata.

L'Italia spende lo 0,1% del suo pil per contrastare i cyberattacchi

Nel 2022 «in Italia c'è stato il 6% degli attacchi su scala globale», ha osservato **Gabriele Faggioli**, presidente di Clusit, «e siamo nel pieno del periodo dell'era dei ransomware». Sono la tipologia di attacco più diffusa, ha concordato **Francesco Teodonno** (Ibm Italia), «e prima per progettare un attacco ransomware servivano 3-4 mesi, ora bastano 3-4 giorni».

Cosa serve fare dunque? Secondo **Andrea Castellano**, country leader security di Cisco Italia, «nel 2023 sempre più aziende italiane prenderanno iniziative per migliorare il proprio livello di cybersecurity: investiranno di più anche perché cresce la consapevolezza sul tema». Leonardo ad esempio, come ha spiegato **Aldo Sebastiani** (Svp del Cyber security Center of Excellence del gruppo), «sta investendo sull'automazione della risposta agli attacchi attraverso le Ai, anche perché le minacce cyber sono sempre più pervasive e multi-dominio». Per **Paolo Prinetto**, direttore del Laboratorio nazionale di Cybersecurity, «serve mettere enfasi sulla formazione delle persone, dai ceo all'ultimo impiegato». E non a caso «nell'area cyber c'è una richiesta altissima di personale qualificato, non solo di figure ad alto profilo tecnologico ma anche legate al risk management», ha spiegato **Carlo Mauceli**, cto e cso di Microsoft Italia.

Le imprese affilano dunque le armi contro la minaccia informatica. «Negli ultimi anni abbiamo visto sempre più attacchi cyber nel nostro settore», ha evidenziato **Alessandro Menna**, chief security officer di Italgas, «e data l'infrastruttura che dobbiamo gestire, dobbiamo lavorare sulla capacità di anticipazione dei cyber-attacchi». Piaggio è invece impegnata «a mantenere costantemente aggiornati i livelli di sicurezza», ha confermato **Vittorio Boero**, cio del gruppo.

Il problema è che «l'Italia ha un triste primato, siamo al sesto posto per attacchi malware e ransomware», ha ricordato **Samuele Zaniboni**, senior manager of presales and tech engineers di Eset Italia. «Non si possono più evitare gli attacchi cyber, ma con le tecnologie a disposizione dobbiamo cercare di identificare gli attacchi, bloccarli e mitigarli». E cercare di farlo bene. «La miglior risposta a un attacco cyber», secondo **Marco Ramilli**, ceo Yoroi-Tinexta Cyber, «non è quella più veloce, ma quella più ragionata. Dobbiamo capire quali strumenti funzionano meglio in risposta e quali funzionano peggio». Anche perché ormai «i criminali usano l'Ai in varie forme e bisogna studiare queste nuove tecnologie per amplificare il perimetro della cybersecurity», ha concluso Ramilli.

Il mestiere della sicurezza tra scuola, impresa e finanza

A fronte di una vulnerabilità crescente, la cybersicurezza è uscita dal tracciato della competenza settoriale per trasformarsi in un dominio trasversale che interessa manager e dipendenti a tutti i livelli, ma anche scuola e mondo finanziario-assicurativo. L'obiettivo comune agli attori in campo lo ha messo in luce **Angelo Spalluto**, chief information officer di Mundys, in occasione della rassegna Cybersecurity 2023 di Class Editori: «Nella sicurezza informatica bisogna partire dalle persone. Le risorse umane non sono vulnerabilità, ma alleati strategici contro le minacce».

Il primo punto, gli ha fatto eco **Alessandro Curioni** (Di.Gi Academy), «è riuscire a far passare l'idea che quello che succede dentro uno schermo ha un impatto concreto nella realtà aziendale». E questo vale per tutte le fasi dell'impresa, tanto che una delle figure professionali più ricercate è quella «che si occupa della sicurezza applicata ai sistemi di automazione della fabbrica», ha raccontato **Alessandro Manfredini** (Aipsa). Figure che vengono formate anche negli Istituti tecnici superiori (Its). Così **Giulio Genti** (Rete Fondazioni Its Italia): «Il nostro ruolo è formare tecnici che forniscano alle imprese le competenze di cybersicurezza necessarie».

La formazione è un primo passo fondamentale che deve avvenire anche in azienda, partendo da piccoli accorgimenti. «Meglio che le chiavi di sicurezza le abbiano in pochi: condividere le utenze e le password tra tanti soggetti è una pratica pericolosa», ha sottolineato **Lorenzo De Francesco** (Italia Fintech). Ormai anche i piccoli imprenditori devono muoversi nella direzione della cybersecurity: «È un ambito che interessa tutti e in tutti i settori, compresi quello sanitario ed energetico», ha precisato **Stefano Scoccianti** (Hera).

Alla base di tutto, ovviamente, ci deve essere il supporto degli specialisti come Reevo, il cui obiettivo, nelle parole del founder e ceo **Antonio Giannetto**, è «costruire nel cloud una cassaforte digitale dei dati delle imprese che consentano alle aziende di proteggere il loro business dagli hacker».

Banche e assicurazioni sono chiamate a svolgere un ruolo decisivo nella partita, sia a livello di sicurezza dei clienti (retail o imprese) sia di offerta di prodotti dedicati. Anche perché, ha svelato **Simone Ranucci Brandimarte** (Italian Insurtech Association), «nel primo trimestre il 71% delle imprese e il 45% della clientela retail si sono detti interessati a sottoscrivere o valutare un prodotto di cyber insurance». Insomma, per le assicurazioni la cybersicurezza può essere un volano di crescita importante: «Il settore deve sfruttare l'opportunità di coprire tutto il mondo degli asset digitali con soluzioni ad hoc per le imprese ma anche per i singoli individui», ha evidenziato **Matteo Carbone** (IoT Insurance Observatory).

I grandi player si sono mossi in anticipo. Generali, ad esempio, ha elaborato un modello quantitativo di rischio cyber «sulla base di scenari predefiniti che vengono adattati dinamicamente ai contesti, interni ed esterni», ha raccontato **Rosangela D'Affuso** della sezione di IT & Security Governance. Anche per i broker assicurativi il tema è in cima all'agenda, come ha spiegato **Flavio Sestilli** di Aiba: «Bisogna lavorare tantissimo in formazione: nelle pmi tutti, a cominciare dal fondatore, devono sapere bene come comportarsi, quali mail non aprire, a quali messaggi non rispondere».

E le banche? **Romano Stasi** (Abi Lab e CertFin) sa bene che gli istituti di credito si sono mossi con prontezza (e bene) per ridurre il rischio, ma sa anche che bisogna spingere l'acceleratore sulla sensibilizzazione: «Nei comportamenti fraudolenti c'è sempre una corresponsabilità involontaria dei clienti: molte volte addirittura è il cliente stesso che dà informazioni agli hacker e li aiuta a fare l'operazione, ad esempio rispondendo a mail che pensa erroneamente siano state scritte dalla banca».

Infine, il nodo dei dati. «Privacy e sicurezza sono due temi strettamente connessi. In tale ottica ci sono presidi da adottare, anche semplici, come il backup dei dati che si stanno usando», ha detto **Ginevra Cerrina Feroni** (Garante della Privacy). «Alla base c'è un dovere di organizzazione da parte dei titolari di un sistema, che devono strutturarsi nel modo più efficiente possibile in un'ottica di cybersecurity», le ha fatto eco **Pierluigi Perri** (Chiomenti). Le regole valgono ovunque, anche nella nuova frontiera del metaverso? «Sì, perché c'è il Gdpr: una normativa matura, che per come è stata impostata dal legislatore europeo consente l'applicazione anche a nuovi contesti», ha concluso **Vincenzo Colarocco** (Studio Previti).

Marco Capponi