L'Economia del Corriere della Sera

Gruppo Engineering

b19293b7-7f8c-4a24-92df-743170611122f

«Boom di attacchi informatici, ecco lo scudo digitale per le imprese»

Intervista al CEO Maximo Ibarra: "Attacchi cyber, lo scudo per le imprese"

Alessia Cruciani

Nel primo semestre del 2024 gli attacchi hackerin Italia sono aumentati del 23% rispetto al semestre precedente. In questo stesso periodo nel mondo si sono registrati più di1.600 attacchi «critici» o «gravi»: il 7,6% di questi sono avvenuti proprio nel nostro Paese colpendo in particolare sanità, servizi e difesa. I dati, resi noti dall'ultimo rapporto Clusit, rivelano anche quanto tutto ciò rappresenti un ricco affare per i pirati informatici: solo quest'anno gli attacchi Ransomware (quelli in cui si chiede un riscatto) hanno fruttato a livello mondiale un miliardo di dollari. E l'Interpol ha previsto che nel 2025 i costi derivanti dal cyber crime raggiungeranno i 10,5 trilioni di dollari. «La cybersecurity è un tema da affrontare con sempre più determinazione, negli ultimi anni gli attacchi hacker riusciti sono aumentati significativamente. Ma ci sono anche alcuni dati positivi che riguardano l'Italia in termini di risposta e prevenzione», afferma Maximo Ibarra, ceo di Engineering, azienda tecnologica leader in Italia con 14.000 dipendenti, oltre 80 sedi distribuite in Europa, Stati Uniti e Sud America e più di 50 nel nostro Paese, capace di guidare l'innovazione in tanti settori, dall'AI alla sanità, dalla cybersecurity allo spazio. A incoraggiare il manager è il fatto che nel 2023 gli investimenti in sicurezza informatica delle imprese italiane hanno raggiunto 2,15 miliardi di euro (+16%) e il 62% delle grandi aziende ha incrementato la spesa perla difesa digitale. Su quale aspettononsi è ancora lavorato abbastanza? «Tra le piccole e medie aziende c'è ancora un ritardo nell'adozione di adeguate misure di difesa digitale. Cominciano a seguire il tracciato seguito dalle grandi aziendema il primo punto è sempre capire quali sono le implicazioni di un attacco hacker. È il motivo per cui bisogna fare prevenzione, l'awareness, ossia la consapevolezza. Questa ormai c'è in gran parte delle aziende di medie dimensioni e mi aspetto che, acquisita questa consapevolezza, gli investimenti cominceranno ad aumentare. Un tema che però rallenta e ha limitato finora la possibilità di essere più efficaci è la carenza di persone che abbiano le competenze giuste. E non riguarda soltanto la cybersecurity, ma tutta la tecnologia». È un problema che interessa solo l'Italia? «Assolutamente no, è mondiale. Noi abbiamo un footprint internazionale ampio e quindi vediamo esattamente quello che succede in quel segmento di mercato. Le dinamiche sono sempre le stesse. Si parla anche all'estero di mancanza di competenze, della crescita della consapevolezza e di investimenti non sufficienti». Come si risolve questa emergenza? «Tutti gli operatori hanno le loro eccellenze e dovremmo riuscire a lavorare in network (che può essere italiano e poi europeo). Con la nostra Academy stiamo già collaborando con altre aziende private e non per forza del settore, così come con 50 università italiane e centri di ricerca. Così si può accelerare la formazione di competenze. Credo che da parte delle istituzioni ci sarà bisogno di un programma diformazione sulla cybersecurity che riguardi anche

le case perché sempre di più l'attacco arriverà attraverso telecamere, smart home, televisori connessi. Qualsiasi cosa collegata alla rete è chiaramente foriera di rischi». Oggi l'intelligenza artificiale rende più complessi e più sofisticati gli attacchi degli hacker. Ma rende più efficiente anche la difesa? «La minaccia cyber segue semplicemente un trend legato alla maggiore digitalizzazione dell'economia e degli ecosistemi produttivi nel loro complesso. Quindi, ci sarà sempre un incremento delle minacce cyberdigitali. Contemporaneamente, le aziende hanno iniziato a investire non solo in trasformazione digitale ma in sistemi che incorporano e integrano le difese digitali. In tal modo, la tecnologia di difesa riesce a essere un passo avanti rispetto a chi attacca. Non è un'azione stand-alone o separata ma fa parte della trasformazione digitale stessa, diventa chiaramente molto più solida. È come quando siristruttura una casa o la si costruisce da zero: se la difesa si incorpora da subito nel progetto iniziale, ha una certa efficacia; se la si aggiunge alla fine, bisogna sempre fare qualche adattamento ed è meno efficace». Questo significa anche che tuttinoidobbiamo essere consapevoli, non solo gli esperti di informatica? Ogni dipendente deve essere educato a utilizzare gli strumenti nel modo corretto? «Il cyberattacker in genere sfrutta la vulnerabilità di quello che io chiamo l'ultimo miglio. Cioè il dipendente che si collega a una rete wi-fi non autorizzata o non protetta, oppure installa nel proprio PC o laptop un software non riconosciuto tra quelli previsti da parte dell'azienda, dell'organizzazione. Bisogna preparare anche a un attacco di phishing, o a quelli più recenti che utilizzano i deep fake: l'attaccante finge di essere un collega e fa delle richieste, a quel punto si danno informazioni che non dovrebbero essere fornite. Questo tipo di informazione è essenziale per rendere meno vulnerabile questo ultimo miglio. Noi internamente abbiamo un sistema di autenticazione per tutti i nostri account su qualsiasi device. Talmente invasivo che capita spesso di dover rifare l'autenticazione più volte durante la giornata. Io mi muovo molto con quattro device e mi capita spesso di fare 16 autenticazioni al giorno». Questi reati non hanno confini, possiamo essere attaccati da qualsiasi parte del mondo. Non sarebbero utili in Europa regole comuni a tutti per un aiuto reciproco tra i Paesi dell'Unione? «Per quanto riguarda le tecnologie, tra cui l'intelligenza artificiale, bisognerebbe avere piattaforme che siano potenzialmente allenabili, che possano imparare da dati che provengono da Paesi diversi all'interno dell'Europa, offrendo una maggiore capacità di difesa. Visto che l'AI è utilizzata anche come strumento di difesa, più questi dispositivi possono essere allenati, più possono essere sofisticati, sfruttando un know-how di dati che è più ampio rispetto ai soli confini dell'Italia. Esiste ancora una forte frammentazione per la regolamentazione nell'uso dei dati: un Paese europeo non può usare quelli di un altro. La frammentazione deve essere risolta». Intanto avete completato l'acquisizione Cybertech. «Abbiamo costituito un centro di competenza in cyber sicurezza all'interno di Engineering. Ci sono oltre 300 professionisti. Non solo abbiamo aumentato il numero dei collaboratori, ma anche quello di persone con un'expertise specifica in cyber sicurezza. Siamo riusciti a lavorare tantissimo sui moduli dell'offerta Cybertech in sinergia con un altro nostro centro di competenza, Cloud Infrastructure. Con i nostritre data center assicuriamo

ai clienti un'infrastruttura con il massimo livello in termini di capacità computazionali e sicurezza. Le due aree lavorano insieme così da garantire alle aziende e ai nostri clienti un luogo sicuro dove poter fare lo storage dei propri dati. La combinazione tra data center, la nostra piattaforma di intelligenza artificiale EngGPT e Cybertech, comincia a essere particolarmente interessante come soluzione integrata per le aziende». Come agisce il vostro Security operations center? «È a Roma ed è fondamentale perla protezione dei nostri 450 clienti. La cosa da sottolineare è che i 450 clienti a cui offriamo servizi di cybersecurity, appartengono a settori molto diversi: energia, utilities, trasporti, infrastrutture, retail, banche. Si tratta di grandi clienti che il nostro Soc protegge perché, oltre a essere in grado di identificare velocemente e inanticipo tutte le potenziali minacce o attività sospette, attiva immediatamente un alert e si interviene subito». Che cosa prevede l'accordo raggiunto nei mesi scorsi con la Polizia? «È sostanzialmente una cooperazione e condivisione di informazioni. All'interno della Polizia di Stato c'è una struttura specializzata che funge da presidio per le infrastrutture strategiche del Paese, come ormai è anche a nostra. Se Engineering dovesse essere oggetto di un attacco, potremmo condividere le informazioni permettendo non solo alla Polizia di comprendere lo stato delle cose ma anche a noi di sfruttare la sua esperienza». Siete mai stati attaccati? «Come ogni azienda al mondo. Ma siamo in grado di intercettarli prima. Non dico quotidiani, ma i tentativi di attacco sono costanti. È quasi business as usual»