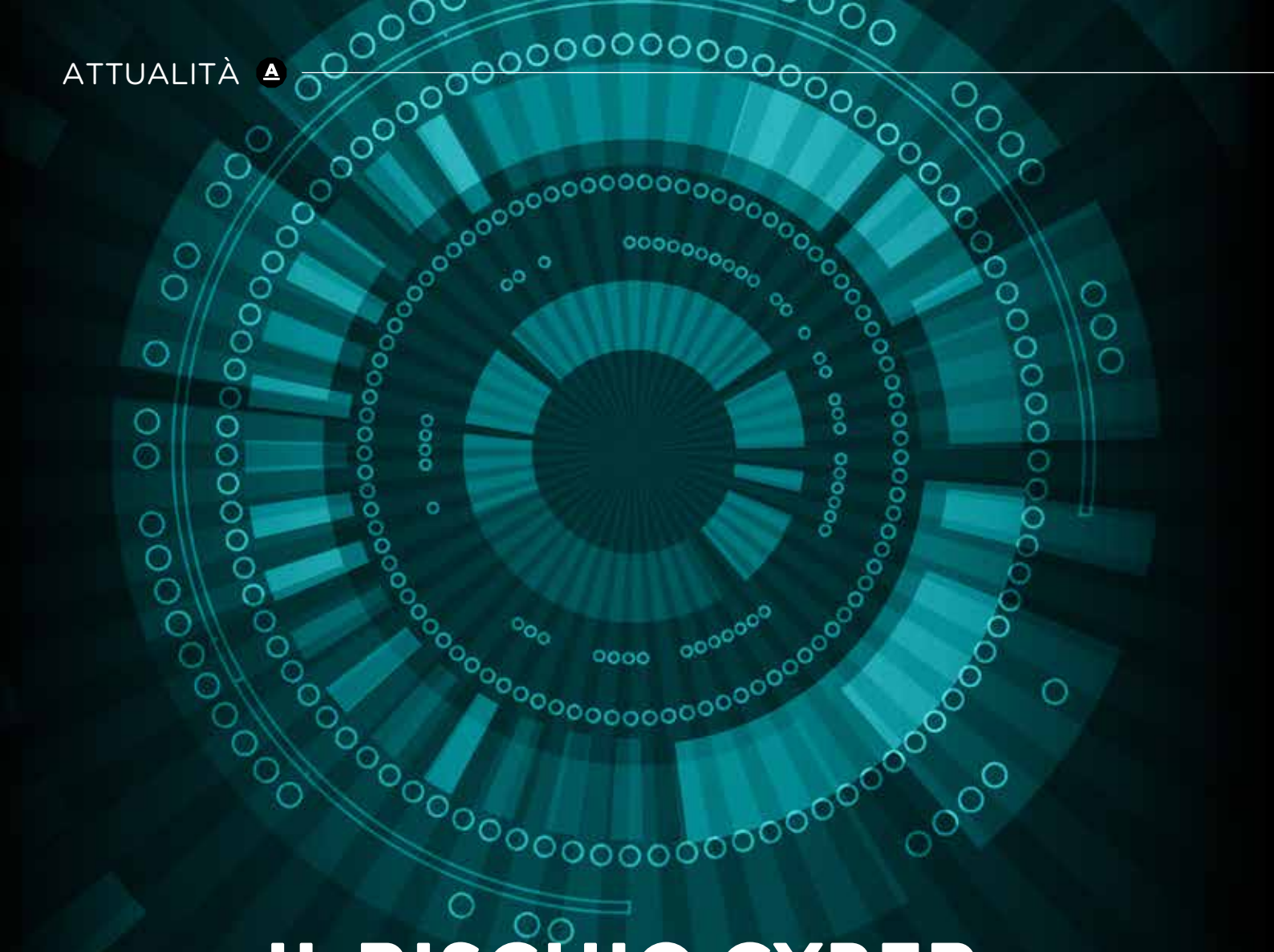


IL RISCHIO CYBER È DAPPERTUTTO

di FABRIZIO AURILIA

IL NOSTRO È UN MONDO DIGITALE: QUASI OGNI COSA CHE FACCIAMO È ABILITATA DALLA TECNOLOGIA, DA UNO SMARTPHONE, DA UN COMPUTER, DA UNA CONNESSIONE INTERNET. PIERGUIDO IEZZI, CEO DI SWASCAN E TRA I PRINCIPALI ESPERTI ITALIANI IN MATERIA, RACCONTA COME LA SVOLTA, IN NEGATIVO, SIA ARRIVATA CON LA PANDEMIA

© KruIUA - iStock

Oggi la tecnologia non è solo una parte del nostro quotidiano ma è, di per sé, la nostra quotidianità. Il mondo digitale è il mondo che viviamo e, esattamente come quello fisico, è esposto ai rischi. Qualsiasi asset digitale è un veicolo per i criminali informatici: il digitale è lo strumento. "Nel momento in cui i nostri valori si smaterializzano, e non parlo solo del conto corrente ma di tutti i nostri dati, è ovvio che il nostro rischio sta nel mondo digitale. Occorre averne la consapevolezza ed evolvere per comprendere come difenderci in questo contesto, esattamente come abbiamo fatto e facciamo nel mondo fisico". Parola di **Pierguido Iezzi**, ceo di **Swascan**, società di cyber security, punto di riferimento a livello internazionale che collabora con i privati (settore finanziario, Pmi, ecc.) e le pubbliche amministrazioni. Iezzi si occupa di tecnologia e cyber da oltre 25 anni, è un ex ufficiale di carriera all'Accademia militare e lavora da anni con **Raoul Chiesa**, "il padre dell'hacking europeo".

LA SVOLTA DOPO IL COVID-19

Insomma, il rischio cyber è pervasivo e ormai consustanziale alle vite di aziende e individui e questo, ne scriviamo da tanto tempo, non è più così sorprendente. Tuttavia, negli ultimi anni è cambiato qualcosa. "l'escalation l'abbiamo avuta nel periodo della pandemia – spiega Iezzi – con tutte quelle famiglie che hanno approcciato soluzioni come e-commerce e i sistemi di teleconferenze". Ma la stessa cosa è successa con le aziende, che per la prima volta si sono trovate a dover gestire rischi inattesi. "Anche prima del 2020 – ricorda l'esperto – si parlava tanto di trasformazione digitale ma nessuno concretamente ci stava arrivando: con il Covid-19, dall'oggi al domani, le imprese hanno dovuto permettere ai dipendenti di lavorare da remoto. Però non è stato fatto adeguatamente: abbiamo accettato il rischio di aver condotto la trasformazione digitale non in sicurezza, valutando costi e benefici".
Ma anche i criminali informatici ragionano per costi e benefici: la presenza di una nuova serie di vulnerabilità ha permesso loro di accedere ai sistemi, frodare, ricattare con i ransomware.

***Pierguido Iezzi**, ceo di Swascan*

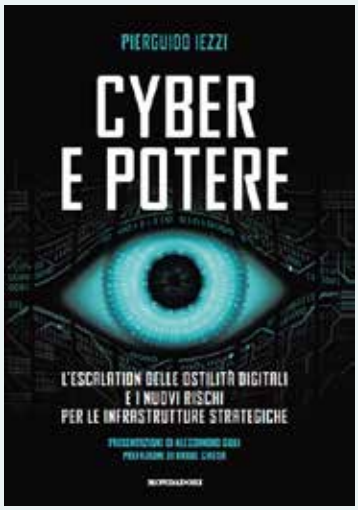
I TRE LIVELLI DI VULNERABILITÀ

"Oggi – sottolinea Iezzi – siamo sommersi dal cyber risk ma non abbiamo ancora la consapevolezza che si tratta di un rischio più probabile di quello di essere scippati, perché lo scippatore necessita di una presenza fisica vicino alla vittima, mentre nel mondo digitale chiunque abbia un computer e una connessione a internet è un possibile attaccante".
Del resto, come spiega l'autore del libro *Cyber e potere* (Mondadori, 2023), la maggior parte degli attacchi dei *criminal hacker* è effettuata senza avere informazioni sulla vittima, ecco perché uno degli errori più comuni è credere di essere al riparo dagli attacchi in quanto poco visibili. "Al contrario, i criminali digitali cercano semplicemente un'opportunità per penetrare nelle aziende", dice Iezzi. E quindi, quali sono queste opportunità? Ci sono tre livelli: il primo è la vulnerabilità di un oggetto digitale, magari un sistema di posta elettronica, una Vpn o il firewall non aggiornati o configurati correttamente.
L'altro livello è il *social engineering*: l'attacco attraverso la mail, o più in generale gli strumenti di comunicazione, come i messaggi o whatsapp: "questo perché le

mail e i dati sono disponibili online: ci sono luoghi su internet in cui si vendono o addirittura si regalano liste di mail o numeri di telefono per organizzare campagne di *phishing* o *smishing*".
Il terzo livello sono i portali che vendono direttamente le credenziali di accesso: "le chiavi per entrare dentro le aziende". Il senso è che oggi il criminale informatico non cerca il target ma l'informazione che permette di valutare qual è la tecnica più efficace. "Le aziende e i cittadini dovrebbero domandarsi quali sono le informazioni che un attaccante all'esterno potrebbe avere", argomenta Iezzi.

COME FARE ANALISI DEL RISCHIO

Per proteggersi, spiega il ceo di Swascan, bisogna utilizzare strumenti di *Threat intelligence*, attraverso tecnologie che permettono all'azienda di sapere quanto è a rischio, in base alla presenza sul web di propri dati e credenziali. "In questo modo – precisa Iezzi – le aziende possono capire quali potrebbero essere le tattiche o le tecniche che un potenziale criminale potrebbe utilizzare". Quindi occorre fare analisi del rischio, fare prevenzione, e capire se i sistemi sono in grado di resistere a un attacco portato con quelle modalità. "Un'analisi del rischio – continua – riguarda sia la componente tecnologica, e quindi occorre svolgere i cosiddetti *penetration test* sugli asset digitali, sia il rischio umano, per cui bisogna verificare che dipendenti e collaboratori sappiano riconoscere i tentativi di inganno, di frode e verificare che le policy e le procedure siano allineate alla legge. Infine, occorre prevedere la sicurezza proattiva: strumenti che facciano il monitoraggio 24 ore su 24 dei sistemi, garantendone la sicurezza: il presidio in azienda deve rimanere sempre alto", chiosa Iezzi.



CYBER WAR: IL RISCHIO DI UN PATTO CRIMINALE

Poi c'è stata un'ulteriore escalation in occasione dell'invasione russa dell'Ucraina e si è cominciato a parlare di guerra cibernetica, di infrastrutture critiche. Gli attacchi informatici filorussi alla vigilia dell'invasione hanno preparato il terreno, nello stile della guerra ibrida: hanno avuto un ruolo di supporto operativo alle operazioni sul terreno, colpendo gli strumenti di comunicazione o le infrastrutture elettriche. "In questo conflitto – spiega Iezzi – ci sono stati i collettivi filorussi che hanno scatenato rappresaglie contro Stati Uniti ed Europa, attacchi che non hanno causato danni gravi: avevano lo scopo di dare visibilità ai loro autori. Questi attacchi, però, sono stati rapidamente accantonati dai media e quindi quello che era l'obiettivo principale, cioè la visibilità, è venuto meno". Sta aumentando il rischio che questi collettivi alzino la posta: preoccupa, in questo senso, l'alleanza tra **KillNet**, **Anonymous Sudan** e **REvil**, quest'ultima una gang ransomware storica. "REvil – mette in guardia Iezzi – ha le competenze e le tecnologie per fare danni, accedere alle aziende e cancellare ogni dato attraverso malware specifici".

CYBER E POTERE? CYBER È POTERE

Dallo *shipping* alla *supply chain*, dal settore energetico alla sanità, passando per il dark web, per la cyber war russa, per finire con le soluzioni, i protocolli, le partnership che possono salvare il nostro mondo fisico dalla minaccia dei cyber criminali. *Cyber e potere* (Mondadori, 2023), di Pierguido Iezzi, è un libro illuminante che, oltre a mettere in fila e dare un senso generale, una visione d'insieme, agli attacchi degli ultimi anni, racconta e analizza le possibilità di difesa che ognuno ha, di fronte al dilagare, incontrollato, del cyber risk.