investire

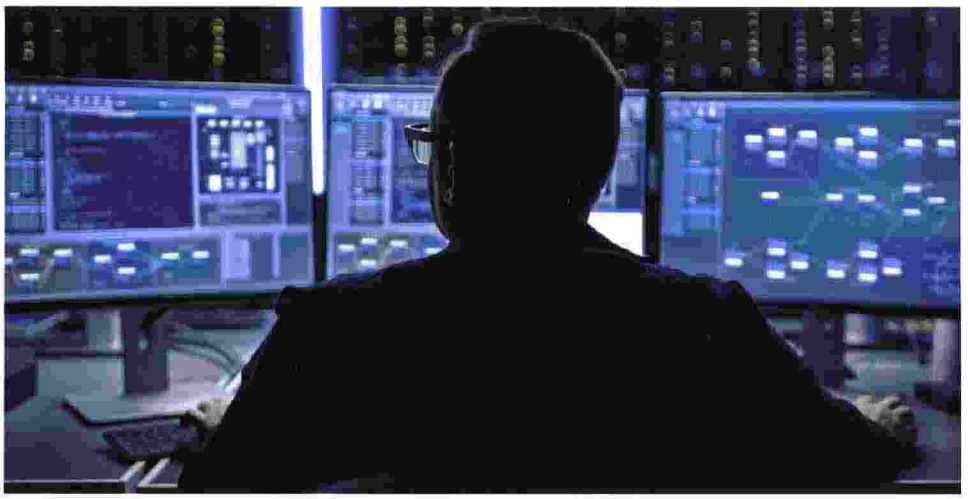
Data 03-2023
Pagina 56/57
Foglio 1 / 2

CYBERSICUREZZA

LA RETE INSICURA OFFRE BUONE OCCASIONI

di Gloria Valdonio

LA SICUREZZA DIGITALE GUIDERÀ SEMPRE PIÙ NEI PROSSIMI ANNI IL SETTORE TECH CHE OFFRE GIÀ OGGI UN BUON PUNTO DI INGRESSO PER TUTTI GLI INVESTITORI



Domenica 12 febbraio diversi siti della Nato, incluso quello del Quartier Generale delle Operazioni Speciali, hanno subito un attacco hacker che li ha mandati in tilt. A renderlo noto è stata la stessa Alleanza Atlantica attraverso l'agenzia di stampa tedesca Dpa. L'offensiva sembra essere stata attuata dal leggendario collettivo hacker **Killnet** (lo stesso che lo scorso maggio aveva colpito i siti del Senato e del Ministero della Difesa italiani), famoso per agire bloccando il funzionamento di un sito o di un servizio tramite un sovraccarico di richieste ai server. Solo sette giorni prima, il 5 febbraio, il massiccio disservizio di **Tim** e il blocco dei bancomat in gran parte dell'Italia è stato il risultato visibile di un attacco ramsomware su larga scala che ha colpito decine di Paesi occidentali. Il **Computer Security Incident Response Team Italia** - ovvero l'organismo che monitora e interviene su scala nazionale in caso di attacchi informatici - ha scoperto che i protagonisti di quell'incursione non erano comuni pirati informatici, ma che poteva trattarsi di qualcosa di diverso e molto più serio.

PRIVACY

La rete è un luogo insicuro, e questo si era capito. Quello che non era ancora chiaro invece è che la rete è a tutti gli effetti un campo di guerra potenzialmente illimitato nel quale ciascuno potrebbe cadere colpito. Gli esperti stanno lanciando infatti un monito: l'Internet of Things (IoT), che moltiplica la connettività e lo scambio di dati attraverso il 5G, sarà il nuovo terreno di caccia per i criminali informatici che cercano di accedere a informazioni private. L'IoT metterà infatti in rete tutti i nostri dispositivi - come cellulari, tv ed elettrodomestici - e quindi anche conti correnti, dati medici e informazioni personali sensibili. «La portata del pericolo rappresentato dagli attacchi informatici è molto alta, poiché l'incremento della dipendenza dalle tecnologie digitali ha aumentato la vulnerabilità delle aziende e delle infrastrutture soggette a questi attacchi», conferma **Annacarla Dellepiane**, head of sales Italy di **HANetf**. Che aggiunge: «Inoltre, la crescente insicurezza globale e le tensioni internazionali come la guerra in Ucraina tendono ad alimentare ulteriormente questi pericoli: secondo l'agenzia per la sicurezza informatica dell'Ucraina, nell'ultimo anno gli attacchi informatici nel Paese sono triplicati».

Nella foto in basso Annacarla Dellepiane, head of sales Italy di HANetf

DEBITO SOVRANO

Se la privacy non è popolare nell'era dei social e della visibilità, un report dello scorso ottobre di **S&P Global Ratings** avvertiva della portata di un attacco informatico sui debiti sovrani. "Come abbiamo visto recentemente nel conflitto Russia-Ucraina, gli attacchi informatici possono precedere o accompagnare l'azione militare come parte della guerra ibrida, con obiettivi chiave come infrastrutture o servizi", è scritto nel report. In caso di rischio politico esterno o interno imminente o in rapido aumento - come la guerra, l'escalation di un conflitto interno o il rischio crescente per la stabilità istituzionale - S&P Global Ratings potrebbe abbassare il rating sovrano indicativo sulla base del rischio di evento, a seconda dell'entità prevista del fenomeno. Secondo il recente rapporto Clusit, che raccoglie e analizza i dati globali relativi agli incidenti informatici, tra gli attacchi cyber più diffusi e frequenti rispetto al 2021 troviamo spionaggio/sabotaggio (+62,1%), informazioni di guerra (+119,2%) e hacktivismo (+414,3%), spesso utilizzato come un mezzo per supportare un conflitto bellico e diffondere messaggi propagandistici o rendere pubbliche informazioni riservate. Tali minacce hanno colpito principalmente i settori sanitario, pubblico e finanziario. Rispetto al primo semestre 2021, nel 2022 la crescita maggiore nel numero di attacchi gravi si osserva nei settori multiservizi (+108,3%), telecomunicazioni (+77,8%), finance/insurance (+76,7%), media (+50%), manifatturiero (+34%), seguiti da energia/utenze (+5,3%) e sanitario (+2,2%).

AZIENDE

Le aziende ovviamente sono ancora più esposte alle minacce informatiche. Nel 2021, le istituzioni finanziarie statunitensi hanno perso quasi 1,2 miliardi di dollari a causa dei soli attacchi ransomware, con un aumento di quasi il 200% rispetto all'anno precedente. Continuando a questo ritmo, nel 2023 i costi globali potrebbero avvicinarsi a 16 trilioni di dollari. Come conferma **Alpay Soytürk**, chief regulatory officer di **Spectrum Markets**, gli attacchi informatici rappresentano una minaccia a tutti i livelli, che non risparmia neppure gli intermediari finanziari. In uno studio sulla resilienza informatica, il Comitato per i pagamenti e le infrastrutture di mercato (Cpmi) e l'Organizzazione internazionale delle commissioni sui valori mobiliari (Iosco) hanno affermato che vi sono alcuni seri motivi di preoccupazione, che rappresentano chiare sfide per la resilienza informatica delle infrastrutture dei mercati finanziari.

Nelle foto da sinistra: Alpay Soytürk, chief regulatory officer di Spectrum Markets, e Mark Hawtin, investment director, disruptive growth equities di Gam

LA GUIDA DEL TECH

Vista l'entità del fenomeno e la sua evoluzione è facile prevedere che la sicurezza informatica guiderà il settore tech nei prossimi mesi e anni. «La sicurezza informatica resta un'opportunità di investimento attiva e in crescita», conferma **Mark Hawtin**, investment director, disruptive growth equities di **Gam**. Che aggiunge: «I consumatori devono proteggere la privacy online, le reti casalinghe e i loro dispositivi. Noi andiamo quindi alla ricerca delle società che offrono opportunità di cross selling per essere sempre più connessi online». Anche secondo Dellepiane è consigliabile diversificare il proprio portafoglio di investimenti, considerando tutti i titoli delle aziende che forniscono soluzioni di sicurezza cibernetica. Ma in che modo investire nel settore? Secondo la strategist, attraverso gli Etf, che consentono un approccio dedicato, ma anche diversificato al tema emergente. È importante inoltre pensare al futuro della cybersecurity, un tema oggi sempre più interconnesso ad altri sotto-settori come quello del Cloud, del Gaming e dell'intrattenimento digitale. «Si tratta di servizi che nel prossimo futuro potrebbero convergere con la sicurezza informatica. Già oggi moltissimi servizi cloud offrono un pacchetto unico con cyber security inclusa», aggiunge Dellepiane. Secondo Hawtin, le prospettive sono nel complesso positive per il segmento disruptive e per il processo di digitalizzazione in corso e il divario tra vincitori e vinti si amplierà ulteriormente, «pertanto si potrà generare più alpha se si sapranno scegliere le società vincenti». Ma quali saranno i titoli vincenti? **GDS Holdings Limited**, la data center cinese e **Okta Inc**, identity & access management company basata a San Francisco sono state le aziende più performanti nel 2022. Ma, secondo Dellepiane, alcuni leader nel settore della cybersicurezza da seguire con attenzione sono **Cisco Systems**, **Microsoft**, **FireEye** e **Palo Alto Networks**. «Queste aziende sono considerate interessanti perché offrono soluzioni di sicurezza cibernetica affidabili e innovative, hanno una forte presenza sul mercato e una buona crescita finanziaria», conclude Dellepiane.