di Fabrizio Fratoni*

# L'aumento della minaccia cyber e la necessità di rafforzare la sicurezza dei sistemi informatici

Negli ultimi mesi il panorama nazionale ed internazionale evidenzia problematiche emergenti che per natura, gravità e dimensione travalicano i confini del settore delle tecnologie riguardanti i sistemi integrati di telecomunicazione ICT e della stessa *cyber security*, fino a determinare impatti profondi e sistemici su ogni aspetto della società, della politica e dell'economia. I rischi informatici costituiscono, infatti, soprattutto per le conseguenze immediate e successive, la maggiore preoccupazione per le aziende a livello globale, dalla minaccia di attacchi ransomware, le violazioni di dati fino alle lunghe sospensioni dei sistemi IT, rispetto all'interruzione di attività, al fermo della catena logistica, delle catastrofi naturali o della Pandemia di Covid-19, tutti i fattori che hanno pesantemente colpito le aziende nell'ultimo anno[1]. Tutto ciò, anche perché, la forza lavoro nelle aziende opera sempre più spesso da remoto, e questa nuova modalità lavorativa aumenta il rischio *cyber* dalle *e-mail di phishing* (per raccogliere credenziali e ottenere un facile accesso ad ambienti *business-critical*) e gli attacchi *malware/ransomware* finalizzati a bloccare il sistema operativo e tenere in ostaggio i dati, bloccare servizi/produzione, divulgare informazioni riservate e soprattutto chiedere il pagamento di un riscatto alle aziende, ma anche ai liberi professionisti e normali utenti della rete. La crescita delle perdite derivanti da questa situazione di f*ar west* digitale, che sono state stimate in oltre 1 trilione di dollari per il 2020 e 6 trilioni per il 2021, evidenzia chiaramente un andamento esponenziale degli attacchi informatici[2] che fa registrare crescenti dinamiche deleterie.

La situazione rappresenta un'emergenza globale concreta visto che le minacce informatiche incidono con una percentuale significativa del prodotto economico globale mondiale, con un tasso di peggioramento annuale a 2 cifre ed un valore totale pari a 3 volte il PIL italiano. A causa dell'esponenziale incremento degli attacchi informatici, sia a livello quantitativo che qualitativo per la gravità del loro impatto, che impone necessita di una costante attenzione, l'Associazione Italiana per la Sicurezza Informatica Clusit[3] nel 2021 ha deciso di pubblicare, per la prima volta un rapporto di metà anno con contenuti inediti rispetto alle analisi precedenti. Tale rapporto riferito al 1° semestre 2021 evidenzia, in tema di distribuzione geografica delle vittime, che rimangono sostanzialmente invariate le vittime di area americana (dal 45% al 46%), ma aumentano sensibilmente gli attacchi verso realtà basate in Europa passando dal 15% al 25%, mentre sono stabili quelli rilevati contro organizzazioni asiatiche. Sotto il profilo della gravità del fenomeno, definita tecnicamente *severity*[4], specie nei confronti di alcune categorie di vittime è contestualmente peggiorata, agendo da moltiplicatore dei danni, tanto da confermare che da 3-4 anni sta avvenendo un'evoluzione degli hacker, sia nelle modalità, che nella pervasività e nell'efficacia degli attacchi, al quale, purtroppo non è corrisposto un incremento sufficiente delle contromisure adottate dai difensori. In particolare, la *severity* media degli attacchi informa-

tici, definibile come l'indice di gravità degli attacchi analizzati, ha evidenziato la crescita maggiore verso le categorie "Transportation / Storage", facendo registrare un preoccupante aumento del +108,7%, e "Professional, Scientific, Technical" con un +85,2%, seguono poi i significativi trend di crescita sui settori "News & Multimedia" (+65,2%), "Wholesale / Retail" (+61,3%) e "Manufacturing" (+46,9%). Aumentano, anche, gli attacchi verso le categorie "Energy / Utilities" cresciuti del +46,2%, "Government" (+39,2%), "Arts / Entertainment" (+36,8%) ed infine il delicato settore "Healthcare" che registra un +18,8%.

Per quanto riguarda l'incisività delle conseguenze degli attacchi informatici, se nel 2020 gli attacchi con impatto "critico" rappresentavano il 13% del totale, quelli di livello "alto" il 36%, quelli di livello "medio" il 32% ed infine quelli di livello "basso" il 19%, nel primo semestre 2021 la situazione è risultata di allarmante gravità dato gli attacchi informatici con effetti devastanti ad impatto " critico " rappresentano il 25% , quelli a livello alto costituiscono il 49%, quelli di impatto "medio" si attestano al 22%, ed infine quelli a basso impatto solo il 4%. Il fenomeno più preoccupante[5] è l'incremento degli attacchi di tipo ransomware[6] con richiesta di riscatto, con una crescita dell'attività di questo malware di circa il 350% rispetto allo stesso periodo dello scorso anno, anche per le conseguenze causate da questa tipologia di attacchi, sono sempre più aggressivi e diventano in qualche modo ancora più evidenti, quando riguardano enti pubblici o settori delicati come quelli della salute e dei servizi pubblici al cittadino. Tristemente celebre tra gli attacchi in danno di strutture pubbliche, che hanno bloccato l'operatività quotidiana degli utenti con gravi danni specie per i cittadini delle fasce più deboli, è quello che il 30 luglio 2021 ha interessato la rete informatica della Regione Lazio, mandando in tilt i servizi a privati e aziende, tra cui il sistema informatico sanitario e quello dedicato alla vaccinazione contro il COVID-19[7].

Se si analizza l'aspetto degli attaccanti si può evidenziare, come dal rapporto del Clusit del primo semestre 2021, si registra un aumento esponenziale di attività degli *hacker* rientranti nelle categorie per finalità di "*cybercrime*" (con un +21,1%) e di "*information warfare*"[8] (con un +18,2%), che fanno comunque registrare il numero di attacchi più elevato degli ultimi 10 anni, mentre diminuiscono gli attacchi classificati come attività di "*cyber espionage*" (registrandosi un -36,7% dopo il picco straordinario del 2020 dovuto principalmente a spionaggio relativo allo sviluppo di vaccini e cure per il Covid-19) e le attività riferibili ad attacchi della categoria "*hacktivism*" che diminuiscono sensibilmente (-66,7%). Peraltro, non sorprende il fatto che, in percentuale, il maggior numero di attacchi classificati come "*critici*" riguardi le categorie *espionage ed information warfare*, perché la prevalenza di attacchi con impatto di tipo "alto" e "medio" si spiega con la necessità, degli hacker di rimanere relativamente sottotraccia, guadagnando sui grandi numeri più che sul singolo attacco, che spesso viene attuato con normali strumenti di aggressione. La situazione descritta dimostra che il tempo della sottovalutazione dei problemi, del rimandare l'adozione di contromisure efficaci, evitando spesso di investire quanto necessario, debba al più presto terminare, anche alla luce del fatto che il PNRR (Piano nazionale di ripresa e resilienza), il quale che complessivamente alloca circa 45 miliardi di euro per la "transizione digitale", possa rappresentare per l'Italia l'occasione di mettersi al passo e colmare le proprie lacune in ambito cyber, e non abbia come esito un ampliamento della superficie di attacco esposta dal Paese, ma una sua complessiva, significativa riduzione.

Per realizzare questo fondamentale obiettivo di potenziamento strategico delle difese informatiche, che oggi più che mai, deve essere inteso come assolutamente prioritario e strategico, richiederà la predisposizione e l'attuazione una *governance* stringente in ottica *cyber security* di tutti i progetti di digitalizzazione previsti dal piano, una *vision* politica che non accetti compromessi e pressioni esterne, e miri finalmente alla valorizzazione delle risorse umane con competenze cyber del Paese, ed il loro sviluppo in termini quantitativi e qualitativi. Ma soprattutto si deve puntare sulla formazione, non solo del personale tecnico, ma di tutti i collaboratori e personale dell'azienda, prevedento in alcuni casi, anche delle procedure di orientamento per gli utenti esterni e gli stakeholders, oltre per i clienti, al fine di salvaguardare, al massimo, la sicurezza dei rispettivi sistemi informatici. Spesso gli attacchi cybercriminali vanno a buon fine, non soltanto delle scarse difese approntate, ma anche a causa comportamenti non corretti e di dipendenti ed utenti, di cui purtroppo ancora, si denota la carenza di consapevolezza relativa alla sicurezza IT[9].

Si è accertato che solo un utente su dieci è pienamente consapevole delle policy e delle regole di sicurezza informatica stabilite dall'azienda per cui lavora, infatti, i comportamenti in violazione delle regole di policy da parte del personale disattento, di regola contribuisce agli incidenti di cyber sicurezza nel 46% dei casi. La priorità delle organizzazioni pubbliche e private, dovrebbe essere dunque quella di impegnarsi nell'educazione dello staff oltre che nell'installazione di soluzioni adeguate, ma anche semplici da usare e gestire, che permettano di migliorare la protezione dell'azienda, anche a chi è meno esperto di sicurezza informatica. Anche le aziende di piccole e medie dimensioni dovrebbero avvalersi di regolari training di formazione sull'importanza della sicurezza IT per lo staff e dell'individuazione di soluzioni personalizzate, in considerazione del fatto che le tecniche più utilizzate sono in grande maggioranza conosciute, a partire dal classico malware prodotto ormai in quantità industriale dai cybercriminali, e salvo casi sporadici non ci sono nuovi prodotti, ma più che altro

vi è un facile adattamento a nuovi bersagli da aggredire. I tentativi delle aziende di innalzare i propri livelli di protezione dotandosi di strumenti tecnologici, come ad esempio *firewall* o *virtual private network* per garantire la continuità operativa, con una conseguente riduzione della superficie di attacco, hanno spinto i criminali informatici a spostare la loro attenzione verso un punto più debole della catena ovvero verso l'endpoint, il pc del dipendente. Si è, infatti, evidenziata una crescita del numero di attacchi indirizzati ai PC personali stimati in oltre 85.000 nel 2021, un fenomeno spiegabile dal fatto che molte aziende non sono riuscite a dotare i propri dipendenti di laptop aziendali, con conseguente utilizzo di dispositivi personali, solitamente maggiormente vulnerabili a malware e virus. In questi casi le aziende dovrebbero attivare delle mirate procedure al fine di contenere l'attacco informatico, isolando, tempestivamente, i dispositivi interessati al fine di proteggere i sistemi critici, notificare l'accaduto internamente, esternamente e ai propri stakeholders in maniera tempestiva e trasparente, denunciando l'accaduto alle forze dell'ordine per poter attivare celermente le investigazioni. Nell'immediatezza è necessario che ogni ente metta in atto il proprio meccanismo di *disaster recovery* e *business continuity* per far in modo di garantire la funzionalità aziendale, contemporaneamente all'attivazione delle operazioni necessarie ad analizzare l'attacco ricevuto e mettere in atto le necessarie contromisure da prendere nel breve termine, quali l'azione di bonifica dell'area colpita e il ripristino dei sistemi in sicurezza. Tale panificazione di misure susseguenti dovrebbero anche comprendere la possibilità di minimizzare il danno di immagine, offrendo, ove possibile, anche servizi di protezione e di assistenza, non solo ai fornitori, ma soprattutto agli utenti più deboli, maggiormente danneggiati dalle conseguenze dell'attacco informatico. ■

***Ufficiale dell'Arma dei Carabinierl**

**1** - Come emerge dall'Allianz Risk Barometer 2022, il sondaggio annuale di Allianz Global Corporate & Specialty (AGCS) raccoglie le opinioni di 2.650 esperti provenienti da 89 Paesi, tra cui CEO, risk manager, broker ed esperti assicurativi, tanto che i rischi informatici si posizionano in cima all'indice delle gravità (44% delle risposte), l'interruzione di attività scende di poco al secondo posto (42%) e le catastrofi naturali sono al terzo posto (25%), mentre i pericoli inerenti la pandemia scende al quarto (22%).
**2** - In particolare, gli attacchi rilevati dal Security Operations Center (SOC) di FASTWEB, che nella prima metà del 2021 (dal 1° gennaio al 31 agosto), ha registrato 36 Milioni di eventi malevoli, con un aumento del +180% rispetto allo stesso periodo dell'anno precedente.
**3** - L'Associazione Italiana per la Sicurezza Informatica è un'associazione senza fini di lucro costituita a Milano il 4 luglio 2000 presso Università degli Studi di Milano – Dipartimento di Informatica "Giovanni Degli Antoni".
**4** - Che consente di realizzare un'analisi dei differenti impatti causati dalle diverse categorie di attaccanti rispetto alle varie tipologie di vittime, e di offrire interessanti spunti di riflessione a coloro che si occupano di *threat modeling*, di *cyber risk management* e di *cyber strategy*, sia a livello aziendale che istituzionale, grazie ad una migliore "fotografia" dei rischi attuali resa possibile da questo ulteriore elemento di valutazione.
**5** - Oltre agli attacchi di tipo "*Proxy Logon*" che consente di accedere ai server di posta elettronica, con tecnologia Exchange, delle vittime riuscendo a violare gli account di posta elettronica e veicolando, attraverso di essi, un ulteriore software malevolo per aumentare la portata dell'attacco.
**6** - Tipo di malware che viene utilizzato per bloccare l'accesso ai dati o a un sistema informatico, solitamente facendo ricorso alla crittografia, finché la vittima non paga un riscatto all'estorsore, ultimamente anziché tenere in ostaggio un singolo computer portatile o dispositivo, ora i criminali informatici puntano all'azienda nel suo complesso, fino a bloccarne completamente l'attività.
**7** - Secondo le indagini del Centro nazionale anticrimine informatico per la Protezione delle infrastrutture critiche, l'anello debole, in questo attacco, è stato un dipendente di Frosinone di LazioCrea, a cui sono stati rubati i dati di accesso al sistema, in fase di accertamento sono ancora le modalità tecniche di attacco presumibilmente di phishing mirato o attraverso un PDF infetto ovvero una pagina web con uno script malevolo. Ben noti, invece, sono i danni provocati dall'attacco: un mese di interruzioni dei servizi, dal sistema sanitario online per i cittadini ai registri dei dati delle farmacie e perfino di altri settori come quello urbanistico, cui maggiori danni si sono riscontratiti per l'emergenza sanitari con notevoli ritardi avendo interessato il database delle vaccinazioni e di rilascio dei green pass.
**8** - Guerra dell'informazione è una metodologia di approccio imperniato sulla gestione e l'uso dell'informazione in ogni sua forma e a qualunque livello con lo scopo di assicurarsi il decisivo vantaggio specialmente in un contesto combinato e integrato. spaziando dalle iniziative atte a impedire all'avversario di acquisire o sfruttare informazioni, fino alle misure mirate a garantire l'integrità, l'affidabilità e l'interoperabilità del proprio assetto informativo, nonostante la connotazione tipicamente militare, la guerra basata sulle informazioni ha manifestazioni di spicco anche nella politica, nell'economia, nella vita sociale ed è applicabile all'intera sicurezza nazionale inibendo il normale funzionamento delle strutture informatiche soprattutto in tema di comando e controllo delle funzionalità strategiche ed operative. Si compone di sette diverse forme dal command and control warfare (C2W), quella guerra di comando e controllo, che mira a colpire la testa e il collo dell'avversario; all' intelligence-based warfare (IBW), ovverosia guerra basata sulle informazioni, che consiste nel progettare e proteggere propri sistemi per la gestione dell'informazione e nell'ingannare quelli avversari al fine di dominare la situazione; l'electronic warfare (EW) la guerra elettronica che sfrutta sofisticati apparati radioelettronici e strumenti di crittografia; la psychological warfare (PSYOP), la guerra di operazioni psicologiche sui singoli o sulla massa, in cui l'informazione è adoperata per influire e per modificare pensieri e opinioni di soggetti amici neutrali o nemici; l' hacker warfare (HW) tipica degli esperti informatici, che prevede l'attacco a computer, reti telematiche e sistemi di elaborazioni dati ed infine l'economic information warfare (EIW) (guerra delle informazioni a rilievo economico) con la paralisi delle informazioni o il loro pilotaggio volto a garantire la supremazia economica ed infine la guerra cibernetica, che è la sintesi delle operazioni più futuribili sul campo di battaglia con l'utilizzo di alta tecnologia informatica, elettronica, satellitare.
**9** - Secondo una recente indagine di Kaspersky Lab e B2B International, che ha coinvolto 7.993 impiegati, ben il 24% dei crede che la propria azienda non abbia stabilito alcuna policy, anche l'ignoranza delle regole non venga considerata una scusante: quasi la metà degli intervistati (49%) pensa, infatti, che tutti i dipendenti – se stessi inclusi – dovrebbero assumersi la responsabilità della protezione delle risorse IT aziendali dalle minacce informatiche.