La sicurezza informatica alla base della privacy?

Giovanni Reccia
Colonnello della Guardia di Finanza, plurilaureato ed abilitato alle professioni di avvocato, di revisore legale dei conti e di giornalista pubblicista, già comandante del Nucleo Frodi Tecnologiche

Fabio Pascucci
Dottore in Giurisprudenza, Scienze politiche, Economia e Scienze della sicurezza economico finanziaria, è Ufficiale superiore della Guardia di Finanza e ha svolto numerosi incarichi pluriennali presso Uffici e C.E.D. del settore informatico

Un altro attacco hacker suscita il risentimento e il timore dell'opinione pubblica; questa volta è toccato alla SIAE. I banditi informatici hanno rubato 60 gigabyte di dati, pari a 28mila file, con lo scopo di metterli in vendita sul dark web, se la società non fosse stata pronta a pagare un riscatto di 3 milioni di euro in criptovalute. Allo stesso modo, nel luglio 2021, la società Garmin, nota nell'ambiente dei corridori di tutto il mondo per i suoi prodotti d'avanguardia sul tracciamento sportivo, ha ammesso di essere stata vittima di un attacco informatico. Cybercriminali russi, denominati Evil Corp, avrebbero chiesto e ottenuto un riscatto di 10 milioni di euro per sbloccare i servizi aziendali. La Garmin ha prontamente smentito, anche se il virus inoculato, WastedLocker[1], ha lasciato traccia che sia stata eseguita un'azione finalizzata a decrittografare file bloccati.

Questi attacchi vengono spesso condotti senza l'utilizzo di alcun software malevolo e sono noti come attacchi fileless: utilizzano tecniche chiamate LotL – Living Off The Land[2], attraverso le quali gli attaccanti possono sfruttare

[1] P. Tarsitano, *WastedLocker, il ransomware nascosto in finti aggiornamenti software che chiede riscatti milionari*, cybersecurity360.it, 24 giugno 2020.
[2] C. Kastan, *Living Off The Land Attacks: Tools, Tactics, and Prevention*, frsecure.com, 2 agosto 2021.

01_PwC_aprile_2022.indd 5 19/05/22 14:45

qualsiasi strumento già installato e in uso nel sistema della vittima. I data breach per la sottrazione dei dati, spesso attuati con la tecnica del phishing, non rappresentano solo un fenomeno italiano, ma si tratta di un'emergenza ormai all'attenzione internazionale. Un recente rapporto negli Stati Uniti ha fornito una stima di 5 miliardi di dollari drenati così dai criminali. Questo significa che le aziende e gli enti devono strutturarsi in maniera più attenta per elevare i livelli di sicurezza informatica ed attivare un efficace impianto tecnologico di prevenzione e contrasto, come antimalware e firewall, per proteggersi dagli attacchi mirati.

Oltre alle strutture di sicurezza, bisogna prendere in considerazione anche il fattore umano, coinvolgendo tutti i dipendenti nella puntuale adesione alle policy di sicurezza. I "buoni" comportamenti sono alla base della protezione aziendale, tuttavia l'efficace sicurezza informatica limita i comportamenti dei dipendenti incauti.

In Italia, lo scorso settembre, sono state gettate le basi per la creazione del Polo Strategico Nazionale, un'infrastruttura per la gestione di tutti i dati e le applicazioni della Pubblica Amministrazione, all'interno di uno spazio virtuale in cloud. L'infrastruttura si inserisce nell'ambito del piano complessivo di accelerazione della trasformazione digitale a garanzia della sicurezza dei dati. Con la conversione in legge del decreto n. 82 del 14 giugno 2021, infatti, è nata l'Agenzia per la Cybersicurezza Nazionale - ACN[3], creata specificamente per la gestione della security. Essa ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria. Ha l'obiettivo di sviluppare capacità nazionali di prevenzione, monitoraggio, rilevamento e mitigazione in materia di cybersecurity, per contribuire all'innalzamento della sicurezza dei sistemi di Information and Technology ed assumere le funzioni di interlocutore unico nazionale per i soggetti pubblici e privati in materia di misure di sicurezza informatica.

In altri Paesi, agenzie simili all'ACN esistono da oltre un decennio; ciò induce ad auspicare la massima condivisione delle informazioni sugli attacchi informatici tra le strutture preposte alla gestione degli incidenti a livello internazionale. A tal riguardo, è utile ricordare la recente vicenda "Log4shell", ossia una vulnerabilità presente nella libreria Log4j, un framework di logging, open source distribuito da Apache Software Foundation e presente su circa 3 miliardi di dispositivi (probabilmente la libreria di "log" più usata nel mondo Java), in cui Check Point, l'azienda di sicurezza informatica israeliana, ha subito condiviso a livello mondiale i seguenti dati:

[3] M.Iaselli, *Nasce l'Agenzia per la cybersicurezza nazionale*, altalex.com, 23 giugno 2021.

01_PwC_aprile_2022.indd 6 19/05/22 14:45

- il 10 dicembre sono stati registrati qualche migliaio di tentativi di attacco informatico;
- l'11 dicembre sono diventati 40.000;
- il 12 dicembre 200.000;
- il 13 dicembre erano già più di 840 mila.

Questo ci fa comprendere come sia assolutamente indispensabile disporre della più ampia condivisione delle informazioni a livello internazionale, alla stregua di quanto sta accadendo per la diffusione del Covid, in cui, come abbiamo visto, una variante sviluppatasi in Sud Africa ha avuto ripercussioni in pochissimo tempo su tutto il globo terrestre. Il Log4j, infatti, è stato definito il Covid della cybersecurity", considerato che un malware è come un virus pronto a diffondersi se trova sistemi non "vaccinati"[4]. L'unico strumento per fermare questi attacchi è l'installazione di patch, per andare a modificare un programma, aggiornarlo e risolvere le sue vulnerabilità[5]. Nonostante sia difficile capire chi stia attaccando i singoli bersagli, tutte le aziende che hanno esposto servizi su Internet dovrebbero aver ben chiaro il concetto che bisogna aggiornare Log4J sempre all'ultima versione, utilizzando preferibilmente un test specifico per verificare che non ci siano software che usano vecchie versioni di Log4J.
Se la nuova frontiera del cyberattack è costituita dal modello del ransomware-as-a-service (RaaS)[6], ovvero un sistema composto da una rete di affiliati che utilizzano un ransomware creato da un gruppo di criminali informatici, non può esserci altra alternativa se non quella di colmare un ritardo inevitabilmente accumulato dall'Italia rispetto ad altri Paesi. La creazione di un'Agenzia per la cybersicurezza nazionale è un enorme passo avanti. D'altro canto, sappiamo che purtroppo non ci troviamo in una situazione di stasi, ma gli attacchi continuano ininterrottamente e il livello di tecnicismo aumenta sempre di più. A questo dobbiamo aggiungere la triste constatazione che, in settori attualmente strategici come quello sanitario e della ricerca, si sta diffondendo a dismisura la tecnica della disinformazione, all'interno della quale si muovono attori intenzionati a modificare il *sentiment* di intere

[4] Da notare che il 13 dicembre 2021, la Apache Foundation ha subito rilasciato una versione correttiva, la 2.15.0, ma, in pochissimo tempo sono stati rilevati attacchi anche negli stessi sistemi aggiornati. Di conseguenza, Apache ha dovuto fare gli straordinari per realizzare la versione v2.16.0 già il 14 dicembre, risolvendo i problemi emersi nella 2.15.0.
[5] G. Calzetta, *Log4Shell: la tempesta è ancora in corso, ma non si sa chi ne sta approfittando*, ilsole24ore.com, 26 dicembre 2021.
[6] A. Pontrelli, *Maze e Ransomware as a Service: sanità sotto minaccia della doppia e tripla estorsione*, cybersecurity360.it, 21 giugno 2021.

01_PwC_aprile_2022.indd 7 19/05/22 14:45

popolazioni con notizie artefatte e decontestualizzate. Lo scopo spesso non è puramente economico, ma determina comunque forti ripercussioni sulla stabilità dei mercati internazionali che movimentano in un attimo volumi enormi di disponibilità finanziarie, causando notevoli scossoni alla solidità delle economie dei Paesi.

Ma allora come intervenire?

Ciò che conta è l'abilità di introdurre misure di sicurezza adeguate in grado di proteggere gli asset strategici, per evitare che il progresso dell'economia digitale sia seriamente compromesso. Pertanto, in termini di governance, le sfide alla sicurezza informatica richiederanno uno sforzo di gruppo organizzato, essendo le debolezze della sicurezza più difficili da proteggere nella complessità degli ecosistemi internet di oggi, costretti ad adottare nuove tecnologie sempre più velocemente rispetto alla capacità di proteggerle.

Sugli attacchi con "riscatto" deve prevalere una strategia della fermezza atteso che pagare un riscatto a un gruppo cybercriminale comporta una duplice conseguenza negativa: ingenera nei clienti una sensazione di insicurezza e inaffidabilità della società bersagliata; la medesima azienda, considerata ormai vulnerabile e soprattutto "disponibile a pagare", potrebbe essere facilmente oggetto di ulteriori attacchi hacker. Inoltre, i cybercriminali, una volta incassato il "malloppo" (solitamente in valuta virtuale non tracciabile), svaniscono nel nulla e i sistemi rimangono comunque compromessi.

In tali circostanze si potrebbe qui fare riferimento alla soluzione adottata alla fine degli Anni '80 contro i sequestri di persona: l'obiettivo primario era quello di rendere improduttiva l'industria del rapimento, colpendo all'origine la possibilità del profitto. Considerato che all'epoca si disponeva il sequestro obbligatorio e preventivo dei beni della vittima e dei suoi parenti, nonché la nullità di ogni prestito o transazione stipulati per il pagamento del riscatto, si potrebbe pensare di applicare una misura simile nei confronti delle imprese che subiscono un attacco hacker, al fine di tutelare i loro interessi finanziari: in sostanza, un blocco temporaneo delle movimentazioni finanziarie che non abbiano una giustificazione contabile, per disincentivare i cybercriminali dal perpetrare azioni finalizzate esclusivamente alla richiesta di un riscatto con pagamento monetario.

Sugli attacchi che determinano un furto di dati o informazioni o che causano blocchi ai sistemi informativi la soluzione è soltanto nello scambio informativo tra i Paesi coinvolti (danneggiati e da cui provengono le intrusioni), profilo che presuppone un rilancio della convenzione di Budapest[7] e

[7] Convenzione del Consiglio d'Europa sulla criminalità informatica (STE no. 185), Budapest 23/11/2001, entrata in vigore il 1 luglio 2004.

01_PwC_aprile_2022.indd 8 19/05/22 14:45

la sua estensione al maggior numero di Stati esistenti nel mondo. Rimanere ancorati alle proprie infrastrutture informatiche od alle proprie strutture nazionali di contrasto appare utile nel breve periodo, ma probabilmente rimarrà improduttivo ai fini della soluzione definitiva.

È di tutta evidenza che la sicurezza informatica è alla base della privacy: i sistemi di sicurezza informatica devono essere in grado di impedire l'alterazione diretta o indiretta delle informazioni, sia da parte di utenti non autorizzati, sia a causa di eventi accidentali; inoltre devono bloccare l'accesso abusivo ai dati, favorendo un approccio euristico ai comportamenti umani. Per identificare tutti i contesti organizzativi in cui c'è un trattamento di dati personali, è necessario allestire dei sistemi *ad hoc*, nei quali coinvolgere consulenti legali e informatici, DPO, esperti di sicurezza ed operatori IT, per la definizione del rischio inteso sia come costruzione dei processi necessari a identificarlo sia come strumenti idonei a limitarlo.

La tecnologia si evolve più rapidamente della legge e per le aziende non è semplice mappare l'ecosistema digitale in cui operano; peraltro, non sono solo gli uomini a produrre, consumare e diffondere dati, ma anche le macchine, le cosiddette intelligenze artificiali, connesse in un internet delle cose sempre più in espansione e intriso di blockchain e big data. Di conseguenza, la sicurezza informatica diventa fondamentale per garantire l'efficace azione della privacy che dovrebbe essere ripensata in un'ottica di *compliance* integrata con il contesto aziendale, ove il sistema organizzativo non può più prescindere dall'ambiente tecnologico.

In tale ottica va visto il Protocollo d'Intesa recentemente stipulato tra Agenzia per la Cybersicurezza Nazionale e Garante Privacy in cui lo scambio d'informazioni è, sì, finalizzato a definire e migliorare i contesti di entrambi gli Organi, ma i cui scenari fanno presagire un diritto alla riservatezza combinato alla cybersecurity. La sicurezza informatica deve quindi rappresentare un modello culturale a carattere generale che consenta la condivisione di informazioni essenziali sia per le amministrazioni pubbliche, senza frenarne l'assolvimento delle funzioni istituzionali, sia per le aziende private, senza ostacolarne la produttività.

01_PwC_aprile_2022.indd 9 19/05/22 14:45