DALLA MINACCIA INFORMATICA ALLA GUERRA IBRIDA: ECCO LA CYBER RESILIENZA

di FABRIZIO AURILIA

C'ERA UNA VOLTA L'HACKER SOLITARIO, CHIUSO NELLA SUA CAMERETTA. OGGI GLI STATI SI COMBATTONO CON GLI ESERCITI TRADIZIONALI E QUELLI VIRTUALI, I CUI DANNI SONO PERÒ MOLTO CONCRETI. COME PROTEGGERSI? OCCORRE COSTRUIRE UNA NUOVA RESISTENZA PER GARANTIRE LA SICUREZZA DELLE PERSONE E DEL SISTEMA ECONOMICO E FINANZIARIO SOTTO ATTACCO

Era la metà di febbraio quando la **Banca centrale europea** metteva in guardia gli istituti dell'Unione su un possibile attacco informatico della Russia diretto contro le istituzioni finanziarie europee, nei giorni in cui le tensioni tra Russia e Ucraina aumentavano e che, come tutti sappiamo, sarebbero poi deflagrate nella guerra.
La Bce era da tempo in allerta per la minaccia di attacchi informatici alle banche, uno scenario che, però, a distanza di due mesi dall'invasione non sembra essersi concretizzato, almeno nella portata temuta dalla presidente **Christine Lagarde**.
Ma i timori dell'autorità bancaria europea per gli attacchi cyber non sono certo nuovi, semmai quello che prospettava la Bce è un "salto di qualità". Mentre il regolatore si era concentrato sulle "truffe ordinarie", esplose durante la pandemia, la crisi ucraina ha portato la Banca centrale europea a interrogare direttamente gli istituti riguardo alla tenuta delle loro difese.

L'ALLERTA PER LE CYBER WAR

Le istituzioni finanziarie europee stanno quindi conducendo "giochi di guerra informatica" per testare la loro capacità di respingere un eventuale attacco. Del resto le preoccupazioni della Banca centrale europea rispecchiano quelle di tutto il mondo: il *Dipartimento dei servizi finanziari* di New York aveva emesso un avviso rivolto alle istituzioni finanziarie già a fine gennaio, in cui parlava di attacchi informatici russi che sarebbero scattati in caso di sanzioni statunitensi alla Russia, a seguito dell'invasione dell'Ucraina; cosa che poi effettivamente è avvenuta.
Ma la Russia, autentica superpotenza nella *cyber war*, aveva già fatto sentire la sua pressione proprio contro il Paese che poi avrebbe invaso. All'inizio di quest'anno, diversi siti web ucraini sono stati colpiti da un attacco informatico che aveva lasciato persino un avvertimento, una sorta di ultimatum: rivolgendosi agli ucraini, i soldati dell'esercito informatico russo avevano suggerito di "aver paura e di aspettarsi il peggio", poiché la Russia stava accumulando truppe vicino al confine. Il

***Christine Lagarde**, presidente della Bce*

servizio di sicurezza ucraino aveva subito comunicato che l'attacco informatico era collegato a gruppi di hacker associati ai servizi di intelligence russi.

ATTACCHI GLOBALI

Il *National cyber security center* britannico ha avvertito le grandi organizzazioni di rafforzare la loro resilienza alla sicurezza informatica, mentre il supervisore tedesco **BaFin** ha apertamente dichiarato che la guerra informatica è "interconnessa con la geopolitica e la sicurezza". Basta ricordare il caso *NotPetya* del 2017, quando un virus paralizzò buona parte dell'infrastruttura informatica ucraina, colpendo anche altri Paesi.
Una vulnerabilità, quella agli attacchi cyber, sottolineata ancora l'anno scorso, quando una delle più grandi campagne di hacking del mondo ha utilizzato **SolarWinds**, una società tecnologica statunitense, come trampolino di lancio per compromettere una serie di agenzie governative: un attacco che la Casa Bianca ha attribuito ai servizi di intelligence della Russia. L'attacco al software di SolarWinds diede agli hacker l'accesso a migliaia di aziende che utilizzano i prodotti informatici della casa americana, colpendo così in tutta Europa. La **Banca centrale danese** aveva affermato che tutta "l'infrastruttura finanziaria del Paese era stata colpita".

COME SI SPEZZA LA BLOCKCHAIN

Una delle più recenti evoluzioni del cyber crime riguarda ambienti tecnologici nuovi, come la *blockchain*, interessati sia da tipologie di attacco ordinarie, con relativi presidi di cybersecurity classica, sia da modalità più specifiche. Un esempio? In tema di attacchi specifici alla blockchain, ci sono i cosiddetti *consensus attack*. Il consensus è quell'insieme delle regole di convalida che forniscono ai partecipanti indipendenti della catena (la blockchain, appunto) la capacità di verificare la validità e l'integrità delle transazioni. Il *51% attack*, che riguarda le reti pubbliche, e il *Regulator's exploitation attack*, su reti private, sono meccanismi di manipolazione del consensus che possono portare a trasferimenti non autorizzati di risorse digitali (criptovalute), censura non autorizzata delle transazioni, doppia spesa o interruzione operativa della convalida della transazione. Gli attacchi contro gli algoritmi che governano il consensus possono agire su diversi *entry point* come le reti, nodi, i singoli utenti e il codice utilizzato.

CRIMINE INFORMATICO COME I CARTELLI DELLA COCA

"In questi primi mesi di guerra, gli attacchi informatici hanno continuato a colpire infrastrutture critiche, servizi governativi, banche e telecomunicazioni ucraini", ha affermato la società di analisi **CyberCube** in un recente report. Ma anche le istituzioni e le imprese governative russe sono prese di mira dagli attacchi cyber, portati sia da alleati, come la Bielorussia, sia da Paesi come Polonia, Lituania e Lettonia.

Lo accenniamo solo in questa introduzione, perché dell'argomento si tratterà ampiamente nelle prossime pagine, ma l'invasione sta ovviamente aumentando la pressione sui premi assicurativi delle polizze cyber, con tassi in forte aumento a causa di attacchi ransomware. La società di sicurezza informatica **Coveware** ha paragonato il margine di profitto, superiore al 90%, degli attacchi ransomware dello scorso anno ai guadagni dei cartelli della cocaina colombiani realizzati nel 1992.

Secondo **Marsh**, i tassi sono aumentati del 130% negli Stati Uniti e di oltre il 90% in Gran Bretagna, nel quarto trimestre dello scorso anno.

CHE COS'È LA CYBER RESILIENZA

Ma prima di ricorrere alle polizze, le istituzioni finanziarie devono mettere in campo quella che è stata definita, in ultima analisi, la *cyber resilience*, un concetto che va oltre la semplice difesa dagli attacchi. La cyber resilience comprende tutte quelle iniziative volte a garantire la continuità di servizio di un sistema, in questo caso quello finanziario. In questo contesto, la cyber resilienza diviene uno strumento centrale per prevenire e gestire eventi che possono intaccare la continuità del sistema, come ha spiegato bene un recente report di **Bankitalia** (*Cyber resilience per la continuità di servizio del sistema finanziario*).

Gli analisti spiegano che gli attacchi in ambito finanziario sono sempre più mirati allo sfruttamento di specifiche vulnerabilità e caratteristiche delle singole organizzazioni. Tra i fenomeni in marcato aumento ci sono le richieste di riscatto, le frodi e i furti (anche in ambito di criptovaluta), oppure operazioni contro la catena di approvvigionamento.

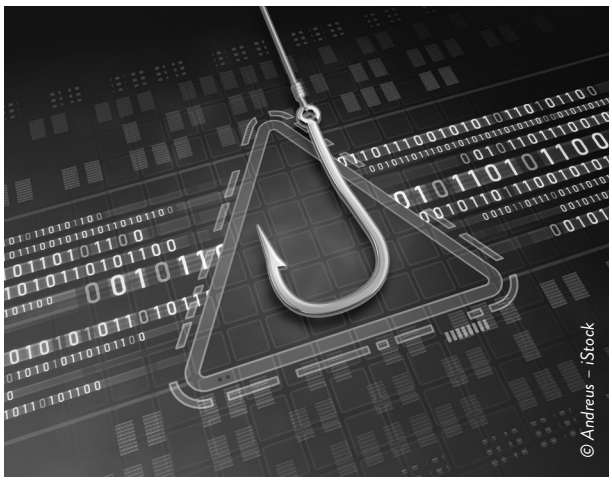
LA VIRALITÀ FA MALE PIÙ DELL'ATTACCO

Un aspetto interessante sottolineato dalla ricerca è che gli eventi cyber (sia i veri e propri attacchi, sia i malfunzionamenti del sistema) sono accompagnati da un'elevata velocità di propagazione: notizie vere, parzialmente vere o del tutto false diventano sovente incontrollabili. Fenomeni come la viralità e l'effetto *echo chamber* in rete sono in grado di influenzare i mercati finanziari in modo particolarmente rapido: "la gestione bilanciata e proporzionata delle notizie e dell'esposizione esterna può costituire un elemento centrale, tanto quanto la gestione resiliente degli eventi ai fini

della continuità operativa", precisa Banca d'Italia. Attacchi fisici e cyber, poi, vanno spesso insieme, ecco perché è sempre più urgente la necessità di potenziare i sistemi informatici, così da integrare in modo continuo il sistema fisico e quello virtuale: un attacco sofisticato e articolato è accompagnato quasi sempre da "attacchi semplici" a singole porzioni dell'infrastruttura.

LA CYBER SOVRANITÀ

Tornando al confronto geopolitico tra Stati, quello cui stiamo assistendo, le operazioni cyber sono spesso sotto-soglia (*below-the-threshold*), cioè fatte con l'intento di non provocare una risposta o una contro-offensiva da parte dell'attaccato, riuscendo in molti casi a eludere la rilevazione di tali operazioni.
"In un quadro di guerra ibrida – ricordano gli analisti – esse sono preferite a operazioni apertamente ostili, per via dei minori costi e rischi". In altri casi, l'attacco è invece palese, conclamato, proprio in virtù del fatto che è comunque difficilissimo sanzionare a livello internazionale un attacco cyber. In ambito cyber, il dibattito è ancora aperto, ed è di natura tecnica, politica e giuridica, sul concetto stesso di *soglia* e sulla sua precisa definizione.
In questo scenario, per far fronte alla minaccia cyber, gli Stati mettono in campo misure volte a rafforzare la loro autonomia strategica, l'indipendenza e la supremazia tecnologica, nonché la cosiddetta *cyber sovereignty*: emanano disposizioni nazionali in materia di sicurezza, compresi obblighi per le aziende private di condividere informazioni con l'intelligence; limitano l'utilizzo di piattaforme di file sharing e social network; oppure creano infrastrutture tecnologiche parallele, attuano censure, oscurano siti web, come abbiamo visto in Russia.


© Andreus – iStock

LE COMPETENZE TECNICHE NON BASTANO PIÙ

Nel caso del sistema finanziario, che si contraddistingue per la complessità delle interdipendenze tra gli elementi che lo compongono, è evidente come anche "piccoli eventi e minime perturbazioni di tipo cyber, anche solo a carattere locale, hanno la capacità di provocare ricadute di grande portata a livello sistemico, a volte con dinamiche di tipo caotico", si legge nel report.
In un sistema costituito da istituzioni, mercati e infrastrutture, finanziarie e tecnologiche, le numerose e profonde interconnessioni fisiche e digitali tra le diverse componenti travalicano i confini nazionali, estendendosi a una dimensione globale e dando luogo a innumerevoli reti di interdipendenze sia operative sia economico-finanziarie: "un attacco cyber su larga scala contro punti nodali del sistema finanziario – ricordano gli analisti – può pertanto innescare una crisi sistemica a livello globale".
Lo sviluppo di professionalità e capacità multidisciplinari in ambito cyber sarà un elemento chiave per la resilienza del sistema finanziario nel suo complesso, ma proprio per inquadrare la natura più profonda del cyber crime, la portata del rischio, occorre che alle investigazioni tecniche si affianchi una conoscenza sempre maggiore delle motivazioni e degli attori della minaccia: occorrono competenze complementari rispetto alle sole conoscenze tecnico-informatiche. "Sviluppare nel concreto unità e gruppi di lavoro composti da persone con competenze variegate è una delle misure che possono aiutare nella definizione e applicazione di politiche di cyber resilience", concludono gli analisti di Banca d'Italia.