CLUSIT, ALLARME CYBER RISK

di GIACOMO CORVI

IL 2022, SECONDO L'ULTIMO RAPPORTO DELL'ASSOCIAZIONE, È STATO L'ANNO PEGGIORE DI SEMPRE PER LA SICUREZZA INFORMATICA. IMPENNATA DEGLI ATTACCHI A LIVELLO GLOBALE, MA MANCANO ANCORA PRESIDI ADEGUATI ALLA PORTATA DELLA MINACCIA. E ANCHE L'ITALIA FINISCE NEL MIRINO DEGLI HACKER

Il giudizio del **Clusit** è perentorio: il 2022 è stato "l'anno peggiore di sempre per la cyber security". L'ultimo rapporto dell'associazione italiana per la sicurezza informatica, presentato in anteprima alla stampa all'inizio di marzo, non sembra lasciare spazio a molti dubbi: lo scorso anno il fenomeno del cyber risk ha infatti raggiunto il nuovo massimo storico di 2.489 attacchi informatici di grande portata a livello globale, ossia 440 episodi in più (+21%) rispetto a quanto registrato nel 2021. Il 44% degli incidenti ha avuto una gravità definita elevata, il 36% addirittura critica.

Non si è trattato di un exploit momentaneo, ma dell'esito naturale di un trend che nel 2022, complice anche lo scoppio del conflitto in Ucraina, ha raggiunto il suo nuovo picco. La nota che accompagna la ricerca, a tal proposito, evidenzia che negli ultimi cinque anni si è verificato un cambiamento sostanziale nei livelli globali di quella che il comunicato stampa definisce "cyber-insicurezza", a cui tuttavia non sarebbe corrisposto "un incremento adeguato delle contromisure adottate dai difensori". Il risultato è che gli attacchi informatici hanno registrato una crescita del 60% dal 2018 a oggi.

L'ITALIA NEL MIRINO

Anche l'Italia è ormai finita nel mirino di hacker e criminali informatici. Nel 2022 si sono verificati nel nostro paese 188 cyber attack, il 7,6% del totale registrato a livello globale, dato che mette a segno uno stupefacente balzo del 169% rispetto all'anno precedente. Il bersaglio principale resta il comparto governativo (20%), ma preoccupa la crescente attenzione che hacker e criminali informatici stanno riservando a una componente fondamentale del nostro sistema produttivo come il settore manifatturiero. Il comparto, nel dettaglio, ha subito il 19% degli attacchi registrati in Italia nel 2022, dato in rialzo del 191,7% su base annua. Alla base del risultato, secondo gli esperti del Clusit, ci sono soprattutto l'assenza di tecnologia nel core business delle imprese, la mancanza di investimenti e la scarsità di personale dedicato alla sicurezza informatica.

A pesare nel bilancio complessivo in Italia ci sono sicuramente i nuovi obblighi normativi in materia di disclosure introdotti a livello europeo con il *Gdpr* e con la direttiva *Nis*. Resta tuttavia il fatto che, nonostante qualche miglioramento rilevato da un'indagine condotta da **Fastweb** e inserita all'interno del rapporto, il livello di protezione di aziende ed enti pubblici non è evidentemente adeguato alla portata di una minaccia che nel corso degli anni si è fatta sempre più massiccia.

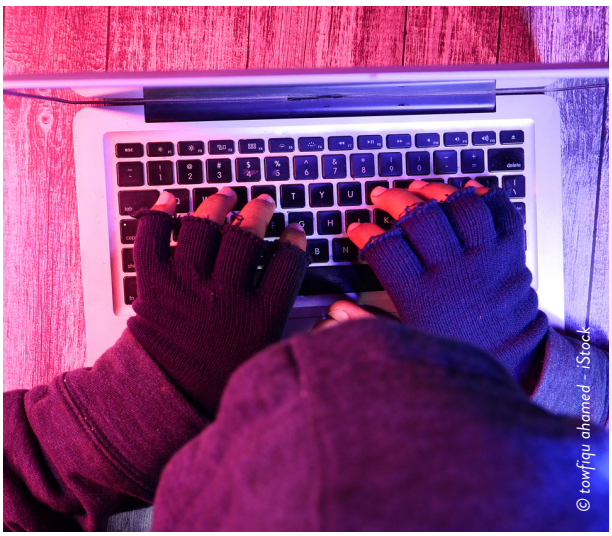
LA GUERRA ONLINE

Tornando al panorama mondiale, il cybercrime si conferma la causa principale di attacchi informatici, con oltre 2.000 episodi (82% del totale) attribuibili a semplici criminali del web. A stupire è tuttavia soprat-

tutto la crescita messa a segno da eventi riconducibili a forme di attivismo digitale, il cosiddetto *hacktivism* (+320%), e di *information warfare* (110%), nonché il nuovo massimo storico toccato da spionaggio e sabotaggio online (11%).
Secondo gli esperti del Clusit, tutto ciò può essere ricondotto all'invasione russa dell'Ucraina. E non è forse un caso se il nuovo record di attacchi mensili (238 episodi) sia stato raggiunto nel marzo del 2022, ossia proprio all'indomani dello scoppio delle ostilità. Il rapporto lo dice chiaramente. E suggerisce che il fenomeno potrebbe essere addirittura molto più esteso, visto che alcuni attacchi condotti da enti di spionaggio o enti governativi potrebbero essere stati perpetrati con modalità attribuibili ad altri tipi di attori, senza che tutto questo venisse chiaramente rivendicato a livello pubblico.

IL NUOVO DIRETTORE DELL'ACN

La presentazione del rapporto è avvenuta all'indomani delle dimissioni di **Roberto Baldoni** dalla carica di direttore dell'**Agenzia per cybersicurezza nazionale** (Acn). "È una decisione che non ci aspettavamo", ha commentato **Gabriele Faggioli**, presidente del Clusit, nel corso della conferenza stampa. "È fondamentale ora – ha proseguito – procedere a una rapida sostituzione, vista anche la situazione della sicurezza informatica in Italia". La nomina è arrivata pochi giorni dopo: **Bruno Frattasi** è il nuovo direttore dell'agenzia. "Lavoriamo a fianco delle istituzioni, pronti a supportare il nuovo corso dell'Agenzia per la cybersicurezza nazionale, consapevoli che in gioco ci sono continuità economica e sociale", ha commentato Faggioli in una nota. "Auguriamo al direttore Frattasi buon lavoro, convinti che le sue competenze e la sua esperienza – ha aggiunto Faggioli – apporteranno rapidamente grande valore al nostro paese anche nel nuovo, strategico ruolo".


© towfiqu ahamed - iStock

VITTIME E TECNICHE DI ATTACCO

Il bersaglio preferito degli attacchi informatici in tutto il mondo tornano a essere i cosiddetti *multiple targets* (22%), ossia enti e società non messi direttamente nel mirino degli hacker, ma oggetto di campagne indiscriminate che puntano a colpire il maggior numero possibile di soggetti. Seguono poi il settore governativo e le pubbliche amministrazioni (12%) e, su una percentuale analoga, le strutture sanitarie, mentre a breve distanza si fermano l'industria informatica (11%) e il settore scolastico e universitario (8%). Le crescite più significative si sono invece registrate nel settore manifatturiero (+79%), nell'industria dei media e dell'informazione (+70%) e nel comparto della finanza e delle assicurazioni (+40%).
Il malware, con il 37% degli episodi, si conferma infine la tecnica di attacco preferita da hacker e criminali informatici. In decisa crescita gli attacchi DdoS (+258%) e quelli basati su tecniche di phishing e social engineering (+52%), segnale quest'ultimo di una consapevolezza del rischio che, seppur in crescita, non ha ancora raggiunto livelli adeguati alla portata della minaccia informatica.