Attacchi hacker. Lucchetti (Cyber 4.0): “Per la cybersecurity potenziamento delle competenze specialistiche e formazione di base nella popolazione”

L’ultimo attacco, il 16 maggio, al sito della Polizia di Stato “ma prima o poi toccherà a tutti”. Non si scompone **Matteo Lucchetti,** direttore operativo di Cyber 4.0, il Centro di competenza nazionale ad alta specializzazione sulla cybersecurity promosso dal ministero dello Sviluppo economico, con il quale, all’indomani dell’approvazione da parte del Governo della Strategia nazionale di cybersecurity, facciamo il punto sugli attacchi hacker di questi giorni e sul livello di sicurezza del nostro Paese. Ultimo in ordine di tempo, dopo il tentato blocco del sistema di voto Eurovision, l’attacco del 16 maggio contro il sito della Polizia di Stato rivendicato su Telegram dal collettivo di cyberattivisti filorussi Killnet. Nel mirino la scorsa settimana i siti di ministero della Difesa, Senato, Istituto superiore di sanità. Nei mesi scorsi, solo per citare i più clamorosi, i siti della Asl di Padova, della Regione Lazio, del San Raffaele di Milano. “Non bisogna fare terrorismo, ma sicuramente occorre creare ‘awareness’, consapevolezza a tutti i livelli”, sostiene Lucchetti che ha alle spalle una lunga esperienza in materia di cybercrime e cybersecurity, ambiti di cui si è occupato precedentemente anche presso l’Abi e il Consiglio d’Europa. **Direttore, qual è il livello di sicurezza della nostra PA?** Da un’analisi effettuata nel 2021 dall’Agid (Agenzia per l’Italia digitale) sui Data center della PA, circa 11mila tra Pubbliche amministrazioni centrali e locali, è emerso che il 95% di questi Data center non era in linea con i requisiti minimi di sicurezza e affidabilità, e quindi a rischio attacco informatico ma anche fault tecnologico. Questo ha impresso un’ulteriore spinta al progetto già in corso di realizzazione di

> un Cloud nazionale per la Pubblica amministrazione sul quale verranno gestiti tutti i dati della PA.

In questo modo verranno garantiti livelli di sicurezza ben superiori rispetto a quelli che il singolo può prevedere e un sistema di ridondanza in caso di attacco per recuperare dati e operatività dei sistemi in modo più efficiente. Si eviterà inoltre il cosiddetto vendor lock-in, ossia la dipendenza da un unico fornitore. **Quali potrebbero essere i tempi per il Cloud nazionale?** La migrazione del 75% della Pubblica amministrazione, sia locale sia centrale, dovrebbe avvenire entro il 2026. Quest’anno è stato lanciato il bando per la costruzione e la realizzazione del Polo strategico nazionale, consorzio di aziende che si occuperà della realizzazione del Cloud. I primi passaggi saranno effettuati appena questo sarà operativo. Il 75% della PA entro il 2026 è un obiettivo molto sfidante, ma utilizzando anche i fondi aggiuntivi che il Pnrr destina a questo tipo di progetto, appare raggiungibile. **Come si sta muovendo il nostro Paese nel contrasto al cybercrime?** In termini di strategie di contrasto l’Italia ha fatto nell’ultimo periodo passi significativi. Il primo e più rilevante è certamente l’istituzione dell’Acn (Agenzia nazionale per la cybersicurezza). Arriviamo un po’ in ritardo rispetto ad altri Paesi come Francia e Germania, ma questo consente anche di imparare da chi ha avviato questo percorso prima di noi. L’Agenzia accentra tutte le funzioni di cybersecurity; in altri termini ha raccolto sotto la sua egida quello che prima era un panorama di azioni molto frammentato: attività di difesa delle infrastrutture critiche nazionali, attività di collaborazione con altre entità omologhe estere, attività di promozione delle formazione e di una awareness a livello nazionale, ma anche attività più operative di risposta agli attacchi e di gestione degli incidenti che possono interessare infrastrutture critiche o sensibili a livello nazionale. **Il 17 maggio il Governo ha varato la Strategia nazionale di cybersecurity. Di che si tratta?** L’Acn sta per pubblicarla: si tratta di

> 85 obiettivi da conseguire da qui al 2026 attraverso azioni messe in campo dall’Agenzia per rafforzare i presidi di cybersecurity nazionale.

La Strategia certamente promuoverà una forte attenzione alla difesa delle infrastrutture critiche e alla gestione di possibili crisi cibernetiche, e quindi alle attività dello Csirt nazionale (Computer Security Incident Response Team), la struttura operativa di risposta agli attacchi alle infrastrutture nazionali. Sicuramente prevederà attività volte a conseguire l'autonomia strategica nazionale delle soluzioni di cyber sicurezza ma anche un rafforzamento delle attività di information sharing, perché molta dell'attività di prevenzione e contrasto del cybercrime può essere facilitata dalla condivisione delle informazioni tra soggetti vittime attuali o potenziali di attacchi, e coloro che monitorano lo scenario di cybersecurity a livello nazionale e internazionale. Per questo c'è necessità di incentivare ulteriormente la partnership tra pubblico e privato. Infine, punto centrale della cybersecurity nazionale sarà il potenziamento delle competenze, inteso sia come formazione specialistica per una transizione digitale sicura, sia come innalzamento della consapevolezza di base a livello nazionale di tutta la popolazione. **Come Cyber 4.0 avete un progetto in questo senso?** Noi ci occupiamo fondamentalmente di formazione di competenze e di promozione di attività di ricerca e innovazione in materia di cybersecurity. Tra le molte iniziative in corso, stiamo ragionando con la Regione Lazio su un possibile progetto di awareness a livello delle scuole. La Regione Lazio avvierà a settembre un'Accademia di cyber sicurezza (Acl - Accademia cyber sicurezza Lazio). Stiamo collaborando per lo sviluppo delle attività e dei programmi formativi prevedendo diversi livelli di corsi. **Quanto è importante che la cybersecurity diventi accessibile a tutti?** È fondamentale.

Per un'adeguata transizione digitale occorre un'educazione capillare che parta dal basso.

Si parla di adozione di nuove tecnologie a tutti livelli: intelligenza artificiale per incrementare la produttività di impianti industriali, utilizzo di block chain, utilizzo di tecniche di analisi dei Big data. La transizione 4.0 deve però essere necessariamente accompagnata da un'adeguata formazione e informazione sul corretto utilizzo di queste tecnologie e sui rischi di sicurezza che esse comportano. **La missione 1 "Transizione digitale" del Pnrr prevede circa 50 miliardi di euro di investimenti in digitalizzazione e innovazione, di cui 9,72 per digitalizzazione, innovazione e sicurezza nella PA (linea M1C1). Tra questi, 620 milioni destinati in modo specifico alla cyber security. Sono sufficienti?** Questo budget di 620 milioni, considerato molto basso, riguarda in realtà solo attività specifiche di cybersecurity condotte dall'Acn. Ma tutti gli investimenti per la trasformazione digitale della PA devono in realtà prevedere misure di rafforzamento per le difese cyber; pertanto la cybersicurezza sarà incorporata in tutto quello che è transizione digitale. Ecco perché il budget reale che il Pnrr alloca per la cybersecurity è molto più alto di quello esplicitato specificamente a questo fine. **Che cosa c'è dietro gli attacchi hacker?** Gli "attaccanti" sono principalmente mossi da motivazioni economiche; lanciano attacchi indiscriminati verso tutti i settori e quelli che ne subiscono maggiori danni sono quelli sui quali c'è stato negli anni un investimento minore in termini di protezione. Il settore bancario, ad esempio, riceve molti più attacchi rispetto ad altri ma si sa difendere meglio perché ha investito molto di più e da molto tempo in sicurezza. Il primo attacco italiano di phishing fu a marzo 2005, me lo ricordo perché all'epoca lavoravo all'Abi. Da allora questo settore ha sviluppato una serie di presidi di sicurezza, non da ultimo l'istituzione di un organismo di risposta agli incidenti centralizzato – il CERTFin - gestito da Banca d'Italia e da Abi. **Oggi quali sono gli obiettivi degli hacker?** Non più il profitto immediato, le credenziali dell'home banking, ma i dati. Il problema più significativo ad oggi sono gli attacchi di ransomware, una tipologia di malware che codifica i dati delle vittime – come accaduto in Regione Lazio – rendendoli inaccessibili a meno che non se ne abbia una chiave di decodifica. Il secondo passo è la richiesta di un riscatto per riaverli e/o anche per non divulgarli alla concorrenza, ai media o ad altri soggetti che ne potrebbero fare un uso illecito; insomma a qualsiasi canale sensibile per quel tipo di dati. L'accesso ad archivi di dati sensibili ha pertanto un cospicuo valore economico, e il settore sanitario in questo è sicuramente molto esposto. **La guerra In Ucraina si è spostata anche nel cyber spazio…** Gli ultimi attacchi, sferrati da gruppi che supportano la Russia, vanno in una doppia

direzione: attivismo pro-Russia e scopo estorsivo per ottenere fondi. Le gang russe stanno attaccando indiscriminatamente molti Paesi per poi accanirsi sulle realtà particolarmente vulnerabili. Colpito in modo massiccio dalla gang Conti è il Costa Rica che ha addirittura dichiarato lo stato di emergenza nazionale perché molte infrastrutture – e quasi tutte le infrastrutture governative – sono state messe totalmente fuori uso.

Giovanna Pasqualin Traversa