

Cyberattacchi, Severino ad Adnfinance: â??Le istituzioni sono un bersaglio geopolitico. Danni immensi, intervenire con diritto internazionaleâ?•.

Descrizione

default watermark

(Adnkronos) â?? â??Quando si arriva a colpire le grandi istituzioni, quelle che tendenzialmente hanno un livello di protezione estremamente elevato, ci rendiamo conto che dal privato al pubblico il tema dellâ??attacco hacker puÃ² riguardare tutti noi, nessuno escluso. Lo ha sottolineato ad Adnfinance, il format tv di Adnkronos, Paola Severino, presidente della Luiss School of Law e giÃ ministra della Giustizia, commentando il presunto attacco alla Dia. Un fenomeno che, secondo lâ??ex Guardasigilli, assume contorni sempre piÃ¹ preoccupanti anche sul piano geopolitico. â??Sembra che questa forma di delinquenza voglia colpire gli interessi fondamentali dei Paesiâ?•.

Il salto di qualitÃ della criminalitÃ informatica emerge soprattutto quando nel mirino finiscono le istituzioni pubbliche e i loro archivi riservati. Se gli attacchi rivolti a imprese e privati sfociano frequentemente in estorsioni e ricatti, quelli contro le strutture dello Stato possono avere finalitÃ ben piÃ¹ ampie.â??Gli attacchi alle strutture pubbliche possono rappresentare vere e proprie minacce di tipo geopolitico. Si vuole minacciare un Paese e gli si fa comprendere che anche le istituzioni piÃ¹ importanti, anche quelle che detengono i dati piÃ¹ segreti e riservati, possono essere colpiteâ?•, spiega Severino. Particolarmente delicata Ã¨ la sottrazione di informazioni giudiziarie e investigative. Dallâ??iscrizione di una persona nel registro degli indagati alle indagini sulla criminalitÃ organizzata, fino alle informazioni relative alla prevenzione del terrorismo, la diffusione di dati riservati puÃ² produrre conseguenze difficilmente quantificabiliâ?•. Le conseguenze di un cyberattacco possono essere rilevantissime e molto diversificate. Ed Ã¨ praticamente impossibile prevederne tutti gli esiti e quindi lâ??entitÃ del danno che si potrebbe provocareâ?•. Severino richiama anche il ruolo della disinformazione. La diffusione di notizie false, soprattutto quando riguarda la sicurezza dei trasporti e delle infrastrutture, puÃ² contribuire a generare panico e alimentare quella che definisce una possibile â??strategia del terroreâ?•.

Ma il cybercrimine rappresenta anche una minaccia diretta per il sistema economico e finanziario. Quando una banca o una compagnia assicurativa subisce un attacco informatico, il danno non si limita alla possibile sottrazione di dati o denaro. A essere compromesso Ã¨ soprattutto il rapporto fiduciario

con i clienti. Alla domanda su quale possa essere lâ??impatto di una violazione informatica sulla fiducia dei risparmiatori, Severino risponde con un solo aggettivo: â??Immensoâ?•. â??Ogni cliente di una banca, ogni persona che conta su unâ??assicurazione, a quel punto pensa che i propri dati non siano custoditi, non siano tutelatiâ?•.â?•Il rischio, spiega, Ã¨ che il timore di un attacco si trasformi in sfiducia generalizzata verso gli intermediari finanziari e le istituzioniâ?•. Sfiducia nelle istituzioni, sfiducia nellâ??economia, sfiducia nelle grandi entitÃ come le banche e le assicurazioni. Una destabilizzazione che puÃ² diventare essa stessa uno degli obiettivi di chi utilizza gli strumenti digitali per colpire lâ??economia e la societÃ .

Sul fronte normativo, il problema non Ã¨ soltanto la capacitÃ delle leggi di tenere il passo con lâ??evoluzione tecnologica. Secondo Severino, negli ultimi anni sono stati compiuti progressi importanti sia sul piano legislativo sia su quello investigativo. Ma resta una debolezza strutturale: la difficoltÃ di perseguire criminali informatici che operano oltre i confini nazionali. â??Il problema piÃ¹ grande Ã¨ quello della giurisdizione, perchÃ© gli autori degli attacchi hacker spesso si trovano in Paesi che hanno un basso livello di protezione normativaâ?•. Anche quando gli investigatori riescono a individuare i responsabili, infatti, non Ã¨ sempre possibile assicurarli alla giustizia. â??Se questi soggetti si trovano in un Paese nel quale non esistono norme adeguate a tutela della cybersicurezza, Ã¨ quasi impossibile perseguirliâ?•, precisa Severino.

default watermark

Ã? il fenomeno del cosiddetto forum shopping della criminalitÃ : la ricerca degli ordinamenti nei quali le regole sono meno stringenti e i controlli piÃ¹ deboli. â??La criminalitÃ andrÃ a cercare i luoghi nei quali i controlli sono minoriâ?•, avverte , sottolineando la necessitÃ di rafforzare la cooperazione internazionale. Lâ??Unione europea, osserva, dispone giÃ di un quadro normativo articolato. Il vero nodo riguarda i Paesi esterni allâ??Europa e la difficoltÃ di costruire accordi efficaci in uno scenario internazionale segnato da guerre e tensioni geopolitiche. â??Questa Ã¨ la grande debolezza del sistema. Un sistema che oggi dovrebbe essere gestito a livello internazionaleâ?•.

Un altro fronte particolarmente delicato riguarda le criptovalute e il loro possibile utilizzo per attivitÃ illecite, dal riciclaggio al finanziamento del terrorismo. Secondo Severino, la disintermediazione finanziaria ha aperto nuovi spazi di rischio. FinchÃ© i trasferimenti di denaro venivano controllati e governati dalle banche, câ??era qualcuno che registrava, scriveva e sapeva chi stava effettuando quel versamento o quellâ??incasso. Con alcune tipologie di criptovalute, invece, i trasferimenti possono avvenire senza una preventiva identificazione dei soggetti coinvolti. â??Io credo che il riciclaggio abbia trovato degli spazi immensi, delle praterie sconfinateâ?•, ha precisato Paola Severino. Il rischio riguarda non soltanto il denaro proveniente dalla criminalitÃ organizzata e dalla corruzione, ma anche i flussi destinati al finanziamento del terrorismo.â?•Io non credo, ha precisato, che possa esistere un mondo sotterraneo nel quale un soggetto non identificato possa determinare spostamenti di valuta, di denaro o comunque di valoriâ?•. In questo contesto, lâ??ex ministra valorizza il ruolo dellâ??Italia nella lotta al riciclaggio e lâ??esperienza maturata dal sistema bancario nazionale nel contrasto alla criminalitÃ organizzata. â??Lâ?•Italia da questo punto di vista Ã¨ molto avantiâ?•, osserva, ricordando come le banche italiane siano state chiamate a dotarsi di sistemi antiriciclaggio fin dal 1992. Unâ??esperienza che oggi puÃ² rappresentare un vantaggio anche nella nuova stagione della finanza digitaleâ?•. â??La nuova autoritÃ europea antiriciclaggio, Amla, presieduta dallâ??italiana Bruna Szego, Ã¨ uno degli strumenti fondamentali per rafforzare il contrasto ai flussi finanziari illecitiâ?•, ha evidenziato.

La trasformazione dei sistemi di pagamento pone nuove sfide anche sul fronte dellâ??euro digitale. Severino invita a distinguere il progetto di una moneta digitale emessa dalle autoritÃ monetarie dalle

criptovalute il cui valore Ã¨ determinato dalle oscillazioni del mercato. â??La differenza tra lâ??euro digitale e una criptovaluta sarÃ appunto questa: un valore che Ã¨ determinato dalle autoritÃ monetarie e non dal flusso di mercato di un giornoâ?•. La prospettiva dellâ??innovazione, secondo lâ??ex ministra, non deve perÃ² tradursi in unâ??accelerazione priva di adeguate garanzie. â??Prima di attivare qualunque meccanismo digitale, senza naturalmente impedirne lo sviluppo, credo che si debba essere molto prudentiâ?•. La condizione essenziale Ã¨ che gli strumenti di controllo siano giÃ disponibili al momento dellâ??introduzione delle nuove tecnologie.

La cybersecurity, infine, non puÃ² essere delegata esclusivamente alle istituzioni, alle imprese o alle autoritÃ di vigilanza. Anche i cittadini hanno un ruolo decisivo nella protezione dei dati personali e nella prevenzione degli attacchi. Severino invita a prestare maggiore attenzione alle autorizzazioni concesse attraverso smartphone, tablet e altri dispositivi, evitando di fornire indiscriminatamente accesso alle proprie informazioni. â??Ognuno di noi puÃ² rappresentare un punto di ingresso per lâ??accesso illegale ai propri datiâ?•. Il rischio Ã¨ che una singola violazione possa consentire ai criminali di raggiungere informazioni ulteriori, in una catena di accessi illegali. Nonostante lâ??aumento delle minacce, Severino invita a non cedere al panico, ricordando che i sistemi di controllo hanno finora, nel complesso, funzionato. Il messaggio conclusivo Ã¨ un appello alla responsabilitÃ individuale e collettiva:â?•Dobbiamo evitare di provocare un effetto domino. La parola dâ??ordine Ã¨ massima prudenzaâ?•.

default watermark

â??

economia

webinfo@adnkronos.com (Web Info)

Categoria

1. Comunicati

Tag

1. Ultimora

Data di creazione
Novembre 9, 2026
Autore
redazione