

- Luiss Open - <https://open.luiss.it> -

Scudi digitali. Quali sono le nuove strategie per la cybersecurity (e perché la pubblica amministrazione deve adottarle al più presto)

Policy Brief n. 10/2021 della School of Government

1 marzo 2021. Nella "Relazione annuale sulla politica dell'informazione per la sicurezza", il capitolo dedicato alla "minaccia cibernetica" si apre con alcune considerazioni sul settore sanitario. Secondo l'intelligence italiana, "attori statuali" hanno "tentato di sfruttare le debolezze connesse all'ondata pandemica per porre in atto attacchi sofisticati miranti ad esfiltrare informazioni sensibili su terapie e stato della ricerca". Poi la stessa intelligence, a proposito degli attacchi cibernetici complessivamente intesi, rileva "un generale incremento delle aggressioni (+20%), che, quanto alla tipologia di target, hanno riguardato per lo più, a conferma di una tendenza già rilevata negli ultimi anni, sistemi IT di soggetti pubblici (83%, in aumento di 10 punti percentuali rispetto al 2019). Tra questi ultimi, quelli maggiormente interessati dagli eventi risultano le Amministrazioni locali (48%, valore in aumento di oltre 30 punti rispetto all'anno precedente), unitamente ai Ministeri titolari di funzioni critiche (+2% nel confronto anno su anno)".

15 febbraio 2021. I computer dell'ospedale pubblico di Villefranche-sur-Saône, vicino Lione, in Francia, vanno in tilt. Un episodio simile, una settimana prima, si verifica a Dax, nel sud-ovest del Paese. In entrambi i casi, racconta il quotidiano italiano La Stampa, alle strutture arriva la richiesta di pagare un riscatto per riottenere dati sensibili trafugati: "Si sono volatilizzati la banca dati con i nomi dei pazienti, il loro storico, le tabelle con le future visite e gli interventi chirurgici. (...) I due ospedali sono stati oggetto di cyberattacchi, una consuetudine ormai nel Paese: a destinazione di imprese private e amministrazioni pubbliche, le aggressioni degli hacker si sono quadruplicate nel 2020, intensificandosi contro gli ospedali (27 l'anno scorso e a un ritmo di uno a settimana dall'inizio del 2021". Una dinamica così preoccupante da spingere il Presidente, Emmanuel Macron, a intervenire pubblicamente sul tema, precisando che lo Stato non pagherà mai riscatti ma piuttosto investirà maggiori risorse sulla cybersicurezza.

6 dicembre 2020. I vertici francesi dell'associazione ecologista Greenpeace fanno sapere di essere entrati in possesso di documenti riservati riconducibili alla centrale nucleare di Flamanville, nella bassa Normandia. Il gruppo di attivisti ecologisti parla di "diverse migliaia di pagine di documenti, compresi piani precisi del sito del reattore nucleare europeo ad acqua pressurizzata (EPR), la localizzazione delle telecamere di sicurezza e anche la descrizione del sistema elettronico di sorveglianza". Tutte informazioni, precisa Greenpeace, ottenute tramite una persona che non ha alcun motivo professionale per esserne in possesso. Documenti, inoltre, che fanno esplicito riferimento a convalide ottenute da strutture ministeriali ad hoc; file inviati come allegati a e-mail non sufficientemente protette. Il tutto testimonia, secondo Greenpeace, le

défaillance strutturali e i rischi potenziali del sito nucleare in questione. Dalle analisi sulla minaccia cibernetica appena pubblicate dall'intelligence italiana, così come dai recenti attacchi cyber che hanno colpito la Francia e che abbiamo pur sommariamente sintetizzato, possiamo trarre alcune considerazioni sulle prossime sfide che attendono la Pubblica amministrazione del nostro Paese in materia di rischi cyber e tutela degli asset strategici.

Gli attori malevoli, presenti nella sfera cyber e rafforzatisi nel tempo, rendono inadeguate le classiche misure di controllo "passive" dei nostri asset strategici, misure concepite fino a un recente passato per mitigare il rischio di eventi accidentali. Si prenda il caso di una centrale atomica o di una infrastruttura ferroviaria: entrambe, se costruite secondo tutti i crismi del "safety engineering", saranno pensate per evitare una "failure" totale. Cosa vuol dire? Tenta di spiegarlo con due esempi. Primo: un cortocircuito in un settore specifico della centrale atomica potrebbe portare allo spegnimento parziale del reattore in nome della sicurezza di chi lavora sul sito e di chi abita nelle vicinanze, dando così il tempo di rimediare al cortocircuito senza compromettere in modo irreparabile l'infrastruttura e l'ambiente circostante. Secondo esempio: nel caso di un grave incidente ferroviario su una linea ad alta velocità, la rete è progettata per mantenere comunque un funzionamento minimo, magari a velocità ridotta in attesa di approfondimenti e riparazioni (come accaduto in Italia col tragico incidente ferroviario di Livraga, vicino Lodi, nel febbraio dello scorso anno). Una "failure" totale, in presenza delle dovute attenzioni, può essere evitata perché singoli incidenti del tipo citato sono localizzati, dunque i loro effetti possono essere contenuti grazie a un'attenta progettazione degli asset. Nel mondo cyber, però, le condizioni cambiano e si complicano. A minacciare un'infrastruttura critica oggi potrebbe essere – invece del semplice caso – un attore malevolo, in grado di causare e coordinare un numero multiplo di incidenti, colpendo obiettivi su tutto il sistema. Alla già temibile e classica minaccia di stampo terroristico, dunque, si aggiunge un andamento potenzialmente "pandemico" di un attacco simile. Il classico "safety engineering" non basta più, nemmeno per quelle che in letteratura sono chiamate "high reliability organizations", cioè organizzazioni (per esempio del settore energetico-nucleare, aereo o medico-sanitario) che mettono in cima alle loro priorità l'affidabilità e la sicurezza del proprio operato, anche a discapito dell'efficienza e del profitto nel breve periodo. Se perfino simili organizzazioni, da sempre preparate al peggio, devono riorganizzare le proprie difese a causa della nuova natura degli attacchi cyber, cosa fa pensare che un percorso simile non diventi obbligato per la nostra P.A., spesso in controllo di strutture strategiche?

- **Le conseguenze distruttive dei cyber-attacchi non sono più confinate alle frodi informatiche, ma possono investire la sicurezza fisica dei cittadini**, come evidenziato dagli episodi che nelle ultime settimane hanno riguardato le centrali nucleari e gli ospedali in Francia. Nemmeno un anno fa, anche una struttura italiana d'eccellenza come l'Ospedale Spallanzani di Roma è stata vittima di un attacco hacker, per limitarci ai casi assurti agli onori delle cronache. Ovviamente è impossibile sottostimare la gravità di un eventuale incidente nucleare, così come di una possibile violazione delle strutture sanitarie specialmente in tempi di pandemia, per la stessa incolumità fisica dei cittadini.
- **Quando si affronta il tema della sicurezza cibernetica, occorre ormai ragionare in termini di "catene del valore globali" e non di singole strutture ritenute sicure**. Di primo acchito qualcuno potrebbe ritenere un po' forzato il legame tra P.A. e asset strategici. Tuttavia,

come si deduce dal caso Flamanville, per esempio, nella realizzazione o nel rinnovamento di una centrale nucleare sono coinvolti tanto attori privati quanto attori pubblici. Si pensi solo ai permessi di costruzione necessari, ai nulla osta per la tutela dell'ambiente o per la sicurezza del sito scelto. Ampia parte della documentazione sensibile, di conseguenza, viene prodotta o in qualche modo rielaborata dalla stessa P.A., a tutti i livelli, dallo Stato fino al Municipio. Non solo, anche la sorveglianza su certe utilities potrebbe essere in parte demandata alle autorità locali, e in tempi di spending review non si può escludere la tentazione di risparmiare anche alla voce "sicurezza". Queste "catene del valore", che uniscono attori pubblici e privati per garantire l'esistenza e il funzionamento di certi asset strategici, spesso travalicano i confini nazionali. Si pensi soltanto a quanto tra le società partecipate italiane (da Fincantieri a ENI) sono esposte a possibili intrusioni malevole. Tale processo accresce dunque i potenziali punti di attacco a disposizione di eventuali attori ostili. La P.A., in tutte le sue articolazioni, dovrebbe smettere vecchi riflessi di presunta "invulnerabilità" e ricordarsi in ogni istante del proprio nuovo ruolo, come uno dei tanti anelli che formano le catene del valore. Il principio della "security-by-design" ("sicurezza fin dalle fondamenta"), ormai radicato nel mondo dell'ingegneria del software, deve informare anche l'operato della nostra P.A. La buona notizia è che oggi ci sono gli strumenti per farlo: con la tecnologia blockchain e gli smart contract, per esempio, si possono creare infrastrutture che – a prescindere dall'organizzazione che di volta in volta le sta usando – garantiscono sicurezza, immutabilità e tracciabilità delle transazioni. L'approfondimento di scenari d'uso che prevedano il coinvolgimento della P.A. potrà certamente servire a individuare le condizioni per implementazioni di successo.

• **Nella P.A., i processi umani che garantiscono l'erogazione dei servizi essenziali dovrebbero applicare il principio della "collective mindfulness"**. L'inclusione del principio "security-by-design" in ogni decisione della P.A., soprattutto nell'ambito dei servizi essenziali, è un passaggio necessario ma non sufficiente. Dovrebbe essere accompagnato da avanzamenti altrettanto radicali nel tipo di processi umani che rendono possibile il funzionamento della P.A. Come sostenuto in un precedente scritto ("La Pubblica amministrazione e la sfida delle piattaforme digitali", Policy Brief n.03/2021), "alle capacità tecniche vanno affiancate capacità organizzative di risposta rapida, sempre trasversali alle singole amministrazioni. Una risposta rapida consiste naturalmente nella tempestiva individuazione dell'incidente e nella soluzione del danno subito. Essa comporta anche la capacità di comunicare efficacemente quanto accaduto, per rassicurare gli utenti, per tutelare allo stesso tempo il buon nome e dunque l'attrattività di società partecipate strategiche che fossero state vittime di attacchi, insomma per non aggravare con un danno d'immagine l'agibilità futura delle piattaforme della P.A.". Si tratta, per dirla in altre parole, di trasferire un know-how tipico del mondo militare e della Difesa al mondo dell'amministrazione civile. Le organizzazioni militari, infatti, attribuiscono estrema importanza a ogni segnale di allarme. Secondo la logica della "collective mindfulness", a essere decisiva non è soltanto la destrezza del singolo che opera in prima linea ma la possibilità che il suo "chi va là" – lanciato come tempo fa avrebbe fatto la sentinella di una fortezza – sia trasmesso rapidamente all'interno di tutta la struttura militare interessata, consentendo una verifica tempestiva dell'eventuale rischio, verifica che conduca infine a risolvere il problema oppure a non ritenerlo tale. È un atteggiamento di questo tipo, cioè di difesa tutt'altro che passiva, che la nostra P.A. potrebbe mutuare dalle strutture militari, considerata la vulnerabilità strutturale crescente di tante infrastrutture. Per tornare agli esempi di cronaca da cui abbiamo avviato la nostra

riflessione, è indubbio che la sicurezza dei pazienti ricoverati sia sempre stata al centro delle attenzioni dei nostri ospedali. Oggi però una concezione della sicurezza che si limitasse a considerare i pazienti protetti all'interno di un singolo reparto ospedaliero potrebbe mettere a rischio la loro stessa incolumità, lasciando scoperto un fianco costituito dalla crescente interconnessione di tutte le infrastrutture sanitarie.

• **La P.A. italiana, insieme con aziende private e università partner, deve farsi trovare pronta per la sfida dei Competence Center e degli European Digital Innovation Hubs.** A partire dal programma nazionale Industria 4.0, avviato nel 2016, l'Italia ha lavorato alla costituzione dei cosiddetti Competence Center – network di università, centri di ricerca e importanti aziende private – per offrire alle imprese, soprattutto piccole e medie, la possibilità di sperimentare e testare progetti innovativi e di sviluppo tecnologico. Da qualche mese, per tali Competence Center, esiste la possibilità di candidarsi a diventare Digital Innovation Hubs di livello europeo. Il nostro Paese deve farsi trovare pronto a cogliere l'occasione con candidature all'altezza, senza disperdere gli sforzi in troppi rivoli. Lo sviluppo di competenze teoriche e partnership operative legate alla cybersecurity sarà uno degli obiettivi fondanti di questi futuri European Digital Innovation Hubs. La corsa a livello europeo è già partita. Non a caso il presidente francese Macron, sulla scorta dei recenti attacchi cyber subiti dal suo Paese, ha promosso con enfasi nuovi investimenti e progetti per rafforzare le difese di nuova generazione degli asset strategici. Da qui l'idea di dispiegare risorse, finanziarie e umane, per fondare un vero e proprio "Campus Cyber" alla Défense, quartiere alle porte di Parigi, dove far confluire grandi gruppi, start-up, centri di ricerca. Nemmeno troppo velatamente, un embrione di Digital Innovation Hub, per promuovere un approccio finalmente sistemico nell'opera di riforma della P.A., garantendo la funzionalità dell'amministrazione pubblica in un ecosistema in profondo cambiamento e a tutela dei suoi asset strategici.

Article printed from Luiss Open: <https://open.luiss.it>

URL to article: <https://open.luiss.it/2021/03/14/scudi-digitali-quali-sono-le-nuove-strategie-per-la-cybersecurity-e-perche-la-pubblica-amministrazione-deve-adottarle-al-piu-presto/>

Copyright © 2020 Luiss Open. All rights reserved.