# Rassegna stampa

Centro Studi C.N.I. 24 settembre 2017


Waypress
media monitoring

## CYBERSECURITY

**Emergenza sicurezza** | Trasformazione digitale | Consapevolezza

# La cybersecurity da minaccia a opportunità per il sistema

## Un ecosistema tra ricerca, pubblico e privato da creare: l'Italia non è all'anno zero

*di* **Roberto Baldoni**

La cybersecurity è la seconda emergenza in Europa, dopo il cambiamento climatico e prima dell'immigrazione. Lo ha detto Jean-Claude Juncker nel discorso sullo stato dell'Unione del 13 settembre scorso. In realtà da diversi anni le cancellerie di tutto il mondo mettono la cybersecurity ai primissimi posti delle loro agende. Blocco dell'operatività di aziende, controllo surrettizio di servizi di infrastrutture critiche, furto della proprietà intellettuale o di informazioni cruciali per la sopravvivenza di una azienda sono esempi delle maggiori minacce che un paese deve affrontare. Le recenti campagne di malware "Wannacry" e "Notpetya" sono stati gli eventi visibili di una sfilza impressionante di attacchi avvenuti negli ultimi mesi in ogni angolo del pianeta.

Impossibile garantire una sicurezza assoluta a causa delle numerose vulnerabilità presenti nei software che creano quel dedalo di tunnel utilizzati dai cybercriminali per entrare e uscire da sistemi sempre più interconnessi. Dobbiamo ridurle, ma questo è un processo lungo che ha bisogno di importanti passi in avanti nella verifica e nella scrittura automatica del codice.

Arrivare a una soluzione "politica" globale agli attacchi cyber in questo momento è arduo. Reperire informazioni e controllare sistemi di altri paesi da una superiorità strategica alla quale difficilmente rinuncerebbe.

Il futuro si preannuncia complesso. Le politiche di trasformazione digitale come Industria 4.0, necessarie per la competitività del nostro sistema industriale, faranno crescere a dismisura la superficie d'attacco di una azienda. Un paese che non metterà la cybersecurity al centro delle proprie politiche di trasformazione digitale, sarà un paese che metterà a serio rischio la propria prosperità economica. In Italia, interi settori di eccellenza come la meccanica, la cantieristica, il Made in Italy e i trasporti, potrebbero subire pesanti ridimensionamenti di fatturato a causa di attacchi perpetrati nello spazio cibernetico da stati sovrani o da competitor.

L'Italia non è all'anno zero nella cybersecurity. I governi che si sono succeduti negli ultimi cinque anni hanno perseguito e consolidato nel tempo un asset importante tra settore pubblico e ricerca nazionale, che non ha eguali in altri paesi. Sono state inoltre gettate le basi per una proficua collaborazione con il settore privato. Il recente Dpcm Gentiloni e il piano operativo propongono un ventaglio articolato e multidimensionale di azioni assolutamente all'avanguardia: il nucleo di sicurezza cibernetica, il centro di ricerca nazionale di cybersecurity, il laboratorio nazionale di crittografia, il cyber-range nazionale e il centro di valutazione e certifi-


**Dati creditizi a rischio.** L'attacco informatico a Equifax, negli Stati Uniti, è senza dubbio uno dei più gravi mai effettuati. L'intrusione nel colosso americano del controllo dell'affidabilità creditizia ha messo a rischio i dati di 143 milioni di cittadini americani e britannici, con tanto di numero di previdenza sociale e di carte di credito. L'agenzia sarebbe sotto attacco dalla scorsa primavera

cazione. Pezzi di un mosaico complesso che si deve comporre per supportare una politica nazionale cyber. Il lavoro è iniziato. Tuttavia, è importante che queste azioni si traducano al più presto in elementi concreti e si mettano a disposizione in programmi pluriennali le risorse che altri paesi hanno già stanziato da tempo. La cybersecurity, come il cambiamento climatico e l'immigrazione sono emergenze che ci accompagneranno per decenni.

Dobbiamo stimolare la nascita di quell'ecosistema cyber tra ricerca, pubblico e privato che consenta lo svilupparsi di un'economia fatta di idee, risultati della ricerca, startup e imprese. Un'economia in grado di fornire quelle soluzioni tecnologiche che rappresentano uno dei perni su cui basare la resilienza del sistema Italia rispetto agli attacchi. Un'economia che possa rappresentare un volano economico per il paese.

La cybersecurity è soprattutto lavorare sulle capacità umane: consapevolezza, organizzazione e formazione. La creazione di una workforce adeguata per il nostro paese è priorità assoluta: tecnici, ingegneri e talenti cyber. Questi ultimi rappresentano delle pepite d'oro che dobbiamo trovare e valorizzare.

Il rischio cyber deve diventare un rischio primario da gestire in ogni consiglio di amministrazione. Prendere sottogamba questo rischio significa mettere a repentaglio la sopravvivenza stessa dell'azienda. Si deve gestire questo rischio in modo efficiente attraverso l'adozione di un mix tra pratiche organizzative e tecnologia che rendono più costoso attaccare un obiettivo per un cybercriminale. Se il costo di un attacco diventasse troppo alto rispetto ai benefici, l'attaccante non troverebbe più conveniente penetrare quel sistema. L'equilibrio fra costo e benefici non è fisso, ma va perseguito in modo continuo perché la tecnologia, l'esposizione cyber di una azienda e le modalità di attacco cambiano nel tempo.



– Professore di Sistemi distribuiti all'Università La Sapienza di Roma