Cybersecurity, la Difesa investe poco: solo 500 milioni in 16 anni contro 1,4 miliardi della Francia nel 2018

"La sicurezza cyber costituisce un settore strategico nevralgico per la protezione delle infrastrutture critiche istituzionali di un'amministrazione che opera a garanzia degli interessi nazionali del Paese", si legge nel Documento programmatico pluriennale (**Dpp**) della Difesa, relativo al triennio 2019-2021*. "Il crescente livello della minaccia cibernetica, impone, quindi, di proseguire con il programma di potenziamento dei livelli di sicurezza",* è scritto nel documento governativo. Peccato che a questa strategia non corrisponda un'adeguato investimento economico.

Nel Dpp, pubblicato di recente dal Ministero della Difesa, si nota che il Governo per rafforzare la cybersecurity ha aggiunto soltanto un milione di euro per ciascuno dei tre anni, come previsto da un emendamento della legge di Bilancio 2019. Per un totale di 500 milioni di euro fino al 2033. Quanti sono, pochi o molti soldi investiti per tenere al sicuro le infrastrutture critiche dell'Italia? Per capirlo basta confrontare la cifra con quanto stanziato dagli altri Stati, a partire da quelli europei.

1,4 miliardi per la cybersecurity stanziati in Francia solo nel 2018

La Francia nel gennaio 2018 hanno inserito nella Finanziaria 4,8 miliardi per la Ricerca e Sviluppo, di cui 1,4 miliardi

per quella relativa alla cybersecurity. Nella legge di programmazione militare 2019-2025 si prevede una spesa complessiva di 78 miliardi per la costituzione di una cyber-armata di 6mila addetti. La strategia francese si distingue in Europa per proattività perché si pone in chiave non solo difensiva, ma anche offensiva, laddove si individuino possibili pericoli per la sicurezza nazionale. Quanto alla Gran Bretagna, ha un National Cyber Security Programme con una dotazione di circa 1,5 miliardo di euro.

L'altro parametro di riferimento per capire il valore dei fondi stanziati dall'Italia per la cybersecurity il documento redatto ogni anno dall'agenzia **Onu** per le telecomunicazioni, il *Global Cybersecurity Index*, che misura il grado di sicurezza informatica di 175 Paesi. L'Italia si posiziona nel 2018 al 25esimo posto. In miglioramento dal 31esimo del 2017, ma dietro tutti i Paesi europei avanzati e alle spalle di emergenti come Lituania, Georgia e Croazia.

L'esigua cifra investita dall'Italia stride un po' con quanto dichiarato dal ministro della Difesa, **Elisabetta Trenta**, quando a luglio scorso nell'illustrare in Parlamento le linee programmatiche del Dicastero, ha posto grande attenzione alla cybersecurity: *"La minaccia cyber è un imprescindibile fattore di rischio per il Paese. È necessario continuare ad investire in tecnologia per contrastare in maniera efficace la cyber guerra".*

https://www.key4biz.it/cybersecurity-la-difesa-investe-poco-solo-500-milioni-in-16-anni-contro-14-miliardi-della-francia-nel-2018/265445/

Cybercrime, scoperta vulnerabilità sull'infrastruttura Huawei

Gli esperti **Swascan** hanno identificato una serie di criticità sull'infrastruttura e sulle web app **Huawei**.

Secondo quanto riporta l'azienda – la prima piattaforma cloudbased
di Cybersecurity Testing italiana – dal *Responsible Vulnerability Disclosure* sono emerse alcune vulnerabilità di livello critical che, se sfruttate da Hacker criminali, avrebbero potuto impattare la Business continuity, la sicurezza di dati e informazioni degli utenti e la regolare attività dei servizi.

La società italiana, che grazie al suo Team era già stata in grado di svelare, tra le altre, le vulnerabilità di **Adobe**, **Microsoft** e **Lenovo** ha contattato i corrispettivi **Huawei** per informarli delle vulnerabilità identificate e per impostare una collaborazione volta all'attività di remediation di queste falle.

"*Nel mondo della Cyber security si sta affermando finalmente il principio della collaborazione. I rischi aumentano di n volte di anno in anno e a fronte di questo si è reso necessario un Paradigm Shift culturale oltre che tecnologico. La nostra esperienza con Huawei dimostra che se recepiti correttamente questi valori possono essere un'ulteriore colonna portante per creare un Cyber Security Framework efficace ed efficiente*", ha dichiarato **Pierguido Iezzi**, Co-Founder di Swascan.

In dettaglio le vulnerabilità appartenevano alle seguenti categorie CWE:

• **CWE-119** (Improper Restriction of Operations within the Bounds of a Memory Buffer): Il software esegue operazioni su un buffer di memoria, ma può leggere o scrivere in una posizione di memoria che si trova al di fuori del confine previsto del buffer. Se la memoria accessibile dall'attaccante può essere efficacemente controllata, può essere possibile eseguire codice arbitrario, come nel caso di un buffer overflow standard. Se l'attaccante può sovrascrivere la memoria di un puntatore (di solito 32 o 64 bit), sarà in grado di reindirizzare un puntatore di funzione al proprio codice dannoso. Anche quando l'attaccante può modificare solo un singolo byte, l'esecuzione arbitraria del codice è possibile. A volte questo è dovuto al fatto che lo stesso problema può essere sfruttato ripetutamente con lo stesso effetto. Altre volte è perché l'aggressore può sovrascrivere dati critici per la sicurezza specifici di un'applicazione – come un flag che indica se l'utente è un amministratore.

• **CWE-125** (Out-of-bounds Read): Il software legge i dati oltre la fine, o prima dell'inizio, del buffer previsto. In genere, questo può consentire agli aggressori di leggere informazioni sensibili da altre posizioni di memoria o causare un crash.

• **CWE-78** (OS Command Injection): Il software costruisce tutto o parte di un comando OS utilizzando input influenzati dall'esterno da un componente upstream, ma non neutralizza o neutralizza in modo errato elementi speciali che potrebbero modificare il comando OS previsto quando viene inviato a un componente a valle.

Gli aggressori potrebbero eseguire comandi non autorizzati, che potrebbero essere utilizzati per disabilitare il software o per leggere e modificare dati per i quali l'aggressore non ha il permesso di accedere direttamente.

Poiché l’applicazione mirata esegue direttamente i comandi al posto dell’aggressore, qualsiasi attività dannosa può sembrare che provenga dall’applicazione o dal proprietario dell’applicazione.

L’esperienza di cooperazione tra Swascan e Huawei riafferma quanto sottolineato da Pierguido Iezzi: per far fronte alle emergenti minacce dei Criminal hacker c’è bisogno di una doppia azione: lato azienda è necessaria un’infrastruttura informatica sicura e un personale qualificato, unita però alle competenze e agli strumenti che solo gli esperti di Cyber Security possono dare

https://www.key4biz.it/cybercrime-scoperta-vulnerabilita-sulli nfrastruttura-huawei/264347/

Direttiva Nis, l’Italia presenta le linee guida per la gestione dei rischi cyber

Ancora progressi sul fronte della cybersecurity. L’Italia ha appena dato seguito ad un altro punto chiave previsto dalla cosiddetta **Direttiva europea Nis** (Network and information security) sul rafforzamento delle risposte da parte degli Stati membri ad un attacco cibernetico.

A livello nazionale, le **Autorità competenti** all’attuazione della normativa Ue (i Ministeri dello sviluppo economico, delle infrastrutture e dei trasporti, dell’economia e delle finanze, della salute, dell’ambiente e della tutela del territorio e del mare, in collaborazione con Regioni e Province autonome di Trento e di Bolzano), **hanno elaborato le**

linee guida per la gestione dei rischi e la prevenzione e mitigazione degli incidenti che hanno un impatto rilevante sulla continuità e sulla fornitura dei servizi essenziali.

Le linee guida, basate sul framework nazionale per la cybersecurity saranno condivise nel mese di luglio con i 465 **Operatori di servizi essenziali** (Ose) individuati nel dicembre 2018: ossia organizzazioni pubbliche e private che garantiscono i servizi indispensabili nei settori energia, trasporti, bancario, infrastrutture dei mercati finanziari, sanitario, fornitura e distribuzione di acqua potabile.

Si tratta di un decisivo passo in avanti sul fronte della sicurezza cibernetica e della protezione dei dati, in quanto vengono indicati in concreto agli Operatori di servizi essenziali gli strumenti e le procedure necessari per innalzare la sicurezza di reti e sistemi, e garantire, quindi, la resilienza dell'intero Sistema-Paese.

L'approvazione delle linee guida è stata frutto di un ampio lavoro coordinato dal Dipartimento delle informazioni per la sicurezza (Dis) con tutti gli "attori Nis" italiani.

I prossimi passi. Una volta partita la comunicazione formale, gli Ose avranno tra i quattro ed i dodici mesi di tempo per uniformarsi alle linee guida, a seconda delle specificità settoriali. Le Autorità competenti, dal canto loro, sono pronte ad assistere gli Operatori per facilitare l'applicazione delle misure di gestione, prevenzione e mitigazione del rischio cyber. Un parametro, quello della compliance, che guiderà poi le stesse Autorità Nis nello svolgimento delle attività ispettive loro affidate dal decreto legislativo che ha recepito la Direttiva Nis nel nostro ordinamento.

L'Italia continua dunque a strutturarsi per essere più pronta

ed efficace rispetto alle minacce che già oggi insidiano la sicurezza e la crescita del Paese. Minacce che si ritiene siano destinate a crescere di pari passo con l'innovazione e lo sviluppo tecnologico. E', quindi, ancor più necessario dare concreto seguito ad un'architettura di cybersecurity europea fondata su alcuni principi cardine cui è da tempo ispirata la stessa strategia italiana di sicurezza cibernetica: approccio coordinato, aumento della consapevolezza e partnership pubblico-privato.

https://www.key4biz.it/direttiva-nis-litalia-presenta-le-linee-guida-per-la-gestione-dei-rischi-cyber/263874/

New Spelevo Exploit Kit Spreads via B2B Website

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/0_WOAOZPoRY/new-spelevo-exploit-kit-spreads-b2b-website

---

Baltimore Approves $10M in Funding for Cyber Attack Relief

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/StF6wP6

_b0U/baltimore-approves-10m-funding-cyber-attack-relief

Russian Tech Giant Yandex Targeted With ‘Regin’ Malware: Report

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/7qRDSbmzsdw/russian-tech-giant-yandex-targeted-regin-malware-report

---

Former Equifax Executive Gets 4 Months for Insider Trading

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/VSbfUtFt2jg/former-equifax-executive-gets-4-months-insider-trading

---

Iranian Cyberspies Update

Infrastructure Following Recent Report

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/kZlE3dJ93HQ/iranian-cyberspies-update-infrastructure-following-recent-report

---

Hackers Steal Millions from Cryptocurrency Exchange Bitrue

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/LjmPZUDm_e0/hackers-steal-millions-cryptocurrency-exchange-bitrue

---

Six Arrested in $27 Million Cryptocurrency Theft

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/zSLmIAU_E8Q/six-arrested-27-million-cryptocurrency-theft