Hacktivism e cyberspionaggio preoccupano l'Italia

Non solo la lotta al terrorismo e il contrasto all'immigrazione clandestina, ma anche tanta cybersecurity nella ***Relazione sulla politica dell'informazione per la sicurezza 2018***, curata dal **Comparto Intelligence**, presentata il 28 febbraio dal presidente del Consiglio dei ministri **Giuseppe Conte.**

Il documento redatto dagli 007 italiani riporta le principali informazioni nel settore della cybersecurity nazionale e cerca di rispondere ad alcune delle principali domande che emergono oggi relativamente alla situazione della sicurezza cibernetica in Italia.

Cybersecurity: le principali minacce

La Relazione evidenzia come **l'hacktivism** sia stata la minaccia più consistente nel 2018, almeno in termini numerici, responsabile del 66% degli attacchi monitorati. Il dato è in crescita rispetto al 2017, quando gli attacchi da parte di questi attori erano il 50% di quelli osservati.

Tra i gruppi più attivi in questo ambito svettano **Anonymous Italia**, **LtùzSec ITA** ed **AntiSec ITA**, questi gruppi hanno portato a termine operazioni di esfiltrazione di dati come la *#OpBlackWeek* che ha colpito diverse istituzioni che operano nel settore dell'Istruzione, del Lavoro, della Sanità, dei Sindacati, delle Forze Armate e delle amministrazioni centrali e locali. Gli attacchi al settore pubblico sono più che quintuplicati rispetto al 2017.

Boom degli attacchi alla PA italiana



Al secondo posto in termini di numero di attacchi vi sono quelli effettuati da attori legati al cyberspionaggio (statale), responsabili del 20% degli attacchi. Anche in questo caso si è verificato un aumento rispetto al 2017, quando gli attacchi di cyberspionaggio (statale) erano il 14%.

Le attività di contrasto al cyberspionaggio sono quelle che hanno impegnato maggiormente il Comparto intelligence italiano, che nella relazione annuale sottolinea come le minacce siano il più delle volte rappresentate da tratta di gruppi strutturati, indirizzati e finanziati da apparati governativi stranieri. Solo il 5% degli attacchi monitorati sono riconducibili a individui/gruppi impegnati in cybe-terrorismo.



Il ruolo dell'Italia, come si sta preparando il nostro Paese

L'allegato alla Relazione evidenzia come proprio nel corso del 2018 si siano potenziate le capacità cibernetiche nazionali tra cui l'avvio operativo del NSC. Quest'organo che si riunisce con cadenza mensile ha già verificato lo stato di attuazione delle misure di coordinamento interministeriale, raccolto e analizzato dati su violazioni di sicurezza e compromissioni di reti e sistemi, promosso e coordinato la partecipazione nazionale ad esercitazioni cyber internazionali (specie in ambito dell'Unione europea e della **NATO**).

Altri passi importanti sono stati fatti nell'implementazione degli indirizzi strategici e operativi previsti dal *"Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico*" (del 2013) e dal susseguente "*Piano Nazionale per*

la protezione cibernetica e la sicurezza informatica" (del 2017). Tra i vari impulsi vi è stata la realizzazione di un perimetro di sicurezza nazionale cibernetica per aumentare il livello di sicurezza del Paese, la creazione in collaborazione con il Ministero per lo Sviluppo Economico di un centro di Valutazione e Certificazione Nazionale per la sicurezza delle infrastrutture critiche e degli operatori dei servizi essenziali, lo sviluppo di sinergie tra attori pubblici e privati (come DIS AgID e Confindustria) finalizzate ad attuare l'iniziativa europea per la digitalizzazione dell'industria (Digitising European Industry).

L'italia e le regole europee

La relazione mette in evidenza anche i progressi compiuti dall'Italia nell'ambito del recepimento e attuazione delle diverse disposizioni europee in ambito di cybersecurity. Il 2018 ha visto la trasposizione nazionale della **Direttiva NIS** (Network and Information Security Directive) e la prima fase della sua implementazione.

La NIS è il perno della strategia europea di cybersecurity ed è finalizzata ad aumentare la sicurezza cibernetica dei Paesi membri e ad accrescere le capacità di cooperazione e di scambio di informazioni tra di essi. Il decreto legislativo per recepire le disposizioni della direttiva è stato redatto con il contributo attivo del DIS che ha assunto anche il ruolo di Punto di Contatto unico NIS per l'Italia. Sempre nel 2018, come prima fase di implementazione della Direttiva, era necessario identificare e stilare una lista dei cosiddetti Operatori dei Servizi Essenziali, che si è conclusa per tempo con l'individuazione di 465 soggetti (la cui identità però rimane segretata).

Un altro dossier europeo che ha suscitato particolare interesse in Italia nel corso del 2018 è stata la "Proposta di Regolamento relativo all'European Network and Information Security Agency (ENISA) e alla certificazione della

cybersicurezza delle tecnologie ICT", meglio conosciuto come Cybersecurity Act. Il regolamento, che sarà votato in via definitiva a marzo 2019, introduce due importanti novità volte ad aumentare la resilienza, la deterrenza e la difesa del cyberspazio europeo. La prima riguarda il rafforzamento dell'ENISA, rendendola permanente e affidandole il ruolo di guida per quanto riguarda le certificazioni europee in ambito ICT; la seconda, per l'appunto, introducendo un framework di cooperazione europeo per le soluzioni ICT.

Per consultare e scaricare la relazione *"Relazione sulla Politica dell'Informazione per la Sicurezza 2018"* completa clicca qui.

https://www.key4biz.it/hacktivism-e-cyberspionaggio-preoccupano-litalia/246626/