12/03/2021

Relazione sulla politica dell'informazione per la sicurezza: minaccia cibernetica e minaccia ibrida

Di Francesca Romana Tubili

La relazione annuale del Dipartimento delle informazioni per la sicurezza (DIS), destinata al Parlamento, pone l'attenzione sullo scenario internazionale e si sofferma sulle principali minacce al Sistema Paese in ambito economico-finanziario, cibernetico, terroristico-jihadista e della criminalità organizzata. L'emergenza pandemica ha reso più complesso il quadro della minaccia, riversandosi sull'economia, modificando sviluppi geopolitici e relazioni internazionali, inasprendo le competizioni soprattutto in ambito tecnlogico, aumentando in questo modo le ostilità. La relazione si sofferma in particolar modo sul fronte della minaccia cibernetica, condizionato dall'emergenza Covid. Il DIS sostiene che l'anno della pandemia ha generato un avanzamento tecnlogico con la diffusione di nuove tecnlogie della comunicazione remota a supporto del lavoro agile, senza però avere una sicurezza ed una consapevolezza nell'uso degli strumenti e della rete stessa. Esso sottolinea l'atteggiamento di alcuni attori ostili, i quali hanno sfruttato il massiccio ricorso allo smart working e l'accessibilità da internet, per accedere a risorse digitali di Ministeri, aziende di profilo strategico e infrastrutture critiche, divenuti bersaglio di campagne criminali o hacktiviste. L'obiettivo della Sicurezza Nazionale è stato quello di proteggere le strutture ospedaliere e i centri di ricerca nazionali, ma anche quelle realtà nate per lo sviluppo e la sperimentazione dei vaccini contro il Covid-19. I dati riportano l'esistenza di attori statuali che hanno approfittato della situazione per porre in atto attacchi sofisticati mirati ad ottenere informazioni sensibili sullo stato della ricerca e delle terapie. Inoltre c'è stato il tentativo di violare alcuni portali web e registrare domini malevoli con lo scopo di ingannare gli utenti. Gli attacchi hanno riguardato in particolar modo gli enti, gli operatori sanitari e della ricerca; i dicasteri e altre amministrazioni dello Stato, nei cui confronti si è registrata una intensa campagna di diffusione di

malware. Il Comparto dell'Intelligence ha attuato un monitoraggio preventivo a tutela di infrastrutture critiche e assetti strategici, per individuare vulnerabilità informatiche. Il complesso dei dati raccolti dall'Intelligence ha fatto emergere un generale incremento delle aggressioni (+20%), che per quanto riguarda la tipologia dei target hanno riguardato sistemi IT di soggetti pubblici, come ad esempio le Amministrazioni locali con il 48% in più rispetto al 2019. Le azioni digitali ostili nei confronti dei privati hanno interessanto il settore bancario con l'11% in più, rispetto allo scorso anno, il settore farmaceutico e sanitario con un aumento del 7% e alcuni servizi IT con l'11%. Per quanto riguarda gli attori ostili, il lavoro svolto dall'Intelligence ci spiega come sia difficile reperire le loro attività, a causa delle caratteristiche del dominio cibernetico e del sofisticato livello tecnologico raggiunto da alcune campagne cibernetiche. Il complesso degli attacchi cibernetici rilevati nel 2020 ha confermato l'hacktivismo come matrice più ricorrente (il 71%); ma i dati raccolti nel corso del 2020 non si discostano molto da quelli del 2019, considerando il numero di azioni condotte dal collettivo Anonymous Italia. Le attività di Anonymous consistono in attacchi collettivi o individuali su alcuni blog o profili Twitter, i quali poi vengono rilanciati sui siti ufficiali del collettivo. Tra le attività attribuite all'hacktivismo abbiamo, inoltre, proteste nei confronti di alcuni soggetti privati, come ad esempio le numerose incursioni digitali nei confronti di concerie campane, le quali sono state prese di mira poichè ritenute responsabili dell'inquinamento ambientale, in particolare del fiume Sarno. E' stato registrato un incremento di episodi dalla matrice non identificabile, dato importante che ci fa capire la capacità che hanno di rimuovere le tracce digitali, per nascondere il loro operato. Per quanto riguarda le tipologie di attacco, i dati raccolti hanno confermato l'utilizzo delle tecniche di SQL Injection per violare le infrastrutture informatiche delle vittime e la presenza di attacchi ransomware che hanno coinvolto soggetti di rilievo nazionale, sia del settore sanitario che dell'industria del Made in Italy, sfruttando per l'infezione nuove modalità di collegamento attivate per lo smartworking. Il 2020, quindi, ha registrato la preminenza di azioni prodromiche (il 53%) a potenziali attacchi e ha evidenziato un deciso incremento delle incursioni digitali, le quali hanno avuto come obiettivo quello di minare la credibilità dei target, come conseguenza della dichiarata ostilità da parte dei gruppi, come ad esempio Anonymous, nei confronti di aziende e istituti sanitari coinvolti nello studio di cure e di vaccini contro il Covid. In ultima analisi il Comparto pone l'attenzione sulle campagne che hanno finalità di spionaggio. Queste ultime sono le più insidiose per il Sistema Paese, poichè sono di difficile individuazione. Importanti sono state le campagne contro i Ministeri e i primari fornitori nazionali di servizi di comunicazione elettronica. L'attività dell'Intelligence si è soffermata non solo sulla minaccia cibernetica ma anche sulla cosiddetta minaccia ibrida, la quale è stata caratterizzata da attività di disinfomazione. Per questo motivo è stata registrata una elevatissima produzione di fake news e narrazioni allarmistiche, di difficile

comprensione da parte dei cittadini. Oltre al fenomeno della disinformazione online, sono state analizzate le logiche e gli algoritimi che sono alla base del funzionamento dei social media, i quali polarizzano l'informazione disponibile, alimentandone la parzialità. Questo fa sì che i principali attori ostili fondino attacchi cibernitici e campagne disinformative per sfruttare la crisi sociale ed economica che la pandemia ha creato. In tale ambito, anche l'Unione europea ha espresso un suo giudizio nei confronti del fenomeno della disinfomazione riguardo il Covid-19. L'impegno delle Istituzioni comunitarie si è tradotto nella pubblicazione, a giugno, di una comunicazione della Commissione e dell'Alto Rappresentante dell'Unione per gli affari esteri e la politica di sicurezza dal titolo "Tackling Covid-19 disinformation: getting the facts right." L'intervento dell‘ UE proponeva di rafforzare le capacità di comunicazione strategica, insieme ad un potenziamento della cooperazione tra Stati Membri e UE e tra questi e i partner internazionali; una maggiore trasparenza da parte delle piattaforme online e la tutela della libertà di espressione. Infine la relazione si è soffermata sulla "procedura di listing", una proposta formulata da alcuni Stati membri, finalizzata ad introdurre misure restrittive nei confronti di soggetti accusati di aver supportato o partecipato ad attacchi cyber. Il soggetto può essere sottoposto a queste misure restrittive nel caso in cui la minaccia esterna abbia avuto effetti significativi; provenga da un paese o da un soggetto stesso esterno dall'UE; impieghi infrastrutture esterne e che lo stesso attacco informatico sia compiuto da una persona fisica o giuridica, da un'entità o da un organismo stabile od operante al di fuori dell'UE, oppure siano commessi con il sostegno di questi ultimi. Le misure restrittive possono comprendere divieti di circolazione per le persone fisiche verso l'UE e il congelamento di beni sia di individui che entità.

Per ulteriori approfondimenti:

https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2021/02/RELAZIONE-ANNUALE-2020.pdf