www.ilfederalista.ch
Intervista curata da Beniamino Sani
Maggio 2021

Attacchi informatici: è silenziosa ma è guerra

Immaginate un blackout elettrico che si protrae per giorni -migliaia di persone senza luce, senza possibilità di cucinare, scaldarsi, comunicare- perché un gruppo di hackers ha preso il controllo della rete che gestisce la distribuzione. Immaginate che dietro all'attacco vi sia una potenza straniera, che intende mettere in difficoltà un Paese concorrente.

Sembrano scenari da film, ma qualcosa di analogo lo stanno sperimentando in questi giorni gli abitanti di alcuni Stati dell'Est americano, confrontati con la realtà di questa minaccia subdola ma decisamente concreta, a causa del blocco di uno dei più importanti oleodotti che porta i combustibili verso la costa orientale, andato in tilt a seguito di un attacco informatico.

Come sia potuto succedere non ancora è del tutto chiaro. La modalità più probabile potrebbe anche essere la più banale, come un impiegato che scarica un virus o apre un mail infetta. "In questo genere di attacchi c'è sempre una componente emotiva", ci dice **Alessandro Trivillini docente SUPSI e membro del gruppo Cyber Sicuro del Canton Ticino**, "perché l'email malandrina deve contenere normalmente qualcosa che riesca nel giro di pochi secondi a convincere il destinatario ad aprire un collegamento, un allegato o anche solo il messaggio stesso". Qualcosa che sia convincente, quindi, sul piano personale o di grande impatto sul piano aziendale.

Il tipo di programma utilizzato in questi casi è definito un ransomware, poiché finalizzato a un riscatto. Quando il programma decide di attivarsi, in assenza di protezioni sufficienti, renderà inaccessibili tutti i dati e i documenti presenti sul computer o sulla rete ad esso collegata fino a pagamento avvenuto.

Come si difende la Svizzera?

Quello delle grandi infrastrutture è certamente un capitolo che interessa il nostro Paese. Che la guerra cibernetica sia un pericolo reale lo ha esplicitato più volte il ministro della difesa **Viola Amherd negli ultimi mesi**. L'esercito si è dotato di una sua nuova strategia valida per il triennio 21-24, a conferma della gravità della minaccia per la sicurezza collettiva: la pirateria informatica è ormai considerato uno dei fronti "bellici" su quali bisogna tenere alta la guardia. In particolare **gli attacchi a scopo spionistico riguarderebbero soprattutto tre Paesi: Russia, Iran, Cina.**

Ma i bersagli non si riducono ai "segreti di Stato" ma possono mettere in gravi difficoltà le **strutture più sensibili della società**. In Svizzera sono già avvenuti attacchi notevoli per esempio contro **cliniche** private (come la Hirslanden la scorsa estate), le **università** -a più riprese- o anche **aziende** molto importanti per il Paese **come Swatch, Novartis o Stadler Rail.**

Le infrastrutture critiche non mancano, basti pensare alla **rete elettrica** che è sempre più interconnessa e digitalizzata: solo due anni fa la Commissione federale dell'energia elettrica (ElCom), esaminando la sicurezza informatica dei maggiori gestori di rete svizzeri, aveva individuato **importanti lacune nei sistemi difensivi.** Altre infrastrutture decisive che lavorano in rete sono, per dirne alcuni, le **ferrovie**, le **telecomunicazioni,** gli **ospedali**, etc.

Chi difende queste infrastrutture critiche per la vita collettiva? Ognuno per sé o esiste un cappello comune? "La sicurezza informatica, specialmente parlando di infrastrutture critiche, si misura sulla disponibilità all'aggiornamento costante", ci spiega Trivillini, poiché disporre tecnicamente di sistemi difensivi assolutamente impenetrabili non è altro che un miraggio. "La Svizzera è stata uno dei primi Stati europei ad istituire un delegato alla cibersicurezza, non una figura di governance, ma un tecnico con grande esperienza e competenza nel campo. Il luglio scorso poi è stato creato il Centro nazionale per la cibersicurezza (NCSC)".

Qual è il loro compito, dunque? "Quello di creare un quadro per far capire a chi si occupa di sicurezza informatica quale sia il grado di maturità del perimetro difensivo della sua azienda, permettendo anche il **costante aggiornamento sia del personale**, **che va sensibilizzato e alfabetizzato rispetto alle nuove minacce**, **sia degli apparati tecnici** (anti-virus e altri strumenti difensivi)".

La Svizzera si coordina a livello europeo", ci dice Trivillini, "perché la tendenza è uniformare l'approccio ai rischi che possono colpire molti Paesi contemporaneamente".

E a livello regionale, nel Canton Ticino, come opera gruppo Cyber Sicuro? "Il nostro scopo è di fare divulgazione scientifica autorevole". Il lavoro principale è quindi quello di rendere le imprese consapevoli: "**Agire da guida per le aziende**, offrendo un punto di riferimento che indichi cosa fare per tenersi aggiornati, dove riferirsi per avere informazioni autorevoli evitando le bufale, a quali partner affidabili rivolgersi". Poi **in caso di crisi maggiore**, **il gruppo sarebbe l'unità chiamata in causa dal Consiglio di Stato**, "poiché raccogliamo le competenze trasversali necessarie, dalla Polizia ai servizi informatici dell'amministrazione, alla perizia tecnica della SUPSI da me rappresentata".

Ma quanto è possibile che vi siano degli Stati dietro episodi come quello americano? "È impossibile dirlo; di certo non si tratta di sprovveduti" che sarebbero individuati subito, "essendo penetrati proprio nel Paese che è leader nel settore informatico". In questo caso sembra che la ragione principale sia stata la ricerca di un riscatto, tanto che il gruppo coinvolto (Darkside) ha pubblicato un comunicato per scusarsi dei disguidi causati alla vita delle persone comuni, tenendoci a sottolineare una propria **delirante "etica criminale".** "Ciò però non significa che dietro non vi possa essere una speculazione da parte di attori interessati a sfruttare la vulnerabilità politica in cui si trovano ora gli Stati Uniti", conclude Alessandro Trivillini.