Consapevolezza, conoscenza, condivisione: le tre parole chiave per proteggersi dai rischi della rete

intervista al Prefetto Domenico Vulpiani, già responsabile per il Ministero dell'Interno della transizione alla modalità operativa digitale | a cura di Raffaello Juvara

Possiamo fare un punto in generale sulle nuove minacce provenienti dalla rete?

A cinquant'anni dalla nascita di Internet, cioè dalla prima trasmissione di un pacchetto di dati tra due computer, assistiamo oggi ad una diffusione pervasiva di apparati mobili interconnessi che, unita all'avvento di nuovi oggetti tecnologici anch'essi collegati alla rete (c.d. *Internet of Things*), ha ridimensionato il concetto di *cybersecurity* e ampliato il perimetro da difendere. Si è passati cioè, dalla necessità di proteggere un sistema di elaborazione dati "fisico" e le sue connessioni di rete, ad un sistema di informazioni e, quindi, di vulnerabilità "diffuse". Se poi riflettiamo sul fatto che, al centro di questo sistema, c'è sempre l'individuo con la sua ineffabile imperfezione e con in mano il suo inseparabile *device*, comprendiamo i molteplici rischi per la sicurezza.

Quali sono i "nuovi" crimini più diffusi e quali le categorie più esposte?

In questo "ecosistema digitale", quattro quinti degli attacchi effettuati (il 79%) sono finalizzati ad ottenere denaro o a sottrarre informazioni per monetizzarle successivamente, così come riportato nel rapporto Clusit 2019.

Alle tradizionali tecniche di cyber-attacco già note, vanno ad aggiungersi nuove tipologie di minacce orientate in primo luogo alle informazioni presenti nei sistemi più diffusi tra gli utenti, cioè alle applicazioni di *social network* e alle piattaforme per apparati mobili. Inoltre, si è assistito ad un'intensificazione delle attività di spionaggio e sabotaggio

(queste ultime soprattutto attraverso *fake news*), sia a livello aziendale che istituzionale, a scapito delle preziose conoscenze e competenze di cui sono in possesso agli attori del contesto produttivo e mettendo a rischio la possibile tenuta del sistema democratico nazionale. In ultimo, ma non per ultimo, troviamo le nuove vulnerabilità connesse ai paradigmi dell'*Intelligenza Artificiale* e dell'automazione industriale avanzata (c.d. Industria 4.0). Da un lato, infatti, l'impiego di tali tecnologie potrebbe consentire la realizzazione di cyber-attacchi sempre più efficaci e meno costosi, mentre dall'altro tali sistemi potrebbero essere silenziosamente alterati e indotti in errore oltre che, più banalmente, attaccati e compromessi con tecniche tradizionali.

In che modo si è dovuto adeguare il metodo investigativo per contrastare la criminalità cibernetica?

Da anni, per contrastare le minacce provenienti dal cyber-spazio, gli attori (istituzionali e non) sono attivi, ciascuno nell'ambito delle proprie competenze, con strumenti tecnologici, investigativi, normativi ed informativi impiegati per "rincorrere" le sempre più sofisticate tecniche di attacco. In particolare, per quanto riguarda la difesa del perimetro cibernetico della propria azienda o istituzione, si è passati da una difesa tradizionale basata fondamentalmente sul monitoraggio del perimetro "logico" attraverso *firewall, antivirus, IDS/IPS*… ad una difesa "condivisa" fondata sull'*information sharing* (SOC, CERT,…). Ovviamente, le nuove frontiere della minaccia obbligano gli addetti del settore ad escogitare tecniche di contrasto sempre più sofisticate, che si spingono fino ad anticipare il possibile attacco attraverso il tracciamento, la ricerca e l'analisi degli avversari fuori dal perimetro: in sostanza, prima che questi costituiscano un pericolo attuale. Queste tecniche, definite di *cyber threat intelligence*, rappresentano una forma di analisi "prognostica" della minaccia, che consentono di neutralizzare o, quantomeno, di mitigare le azioni di malintenzionati nei confronti di un sistema informatico.

Quali sono i livelli di consapevolezza dei rischi della rete, in particolare da parte dei giovani?

Nessuna tecnologia, da sola, può rendere immuni da attacchi ostili o da eventi disastrosi poiché, torno a ricordare, al centro di qualunque sistema digitalizzato c'è sempre l'essere umano con le sue vulnerabilità e imperfezioni. Per tale ragione, è fondamentale diffondere la cultura della *cybersecurity* ad ogni livello di competenza, dall'utilizzatore di uno *smartphone* all'amministratore di una rete aziendale complessa. Tale esigenza di propagazione culturale può essere sintetizzata in tre parole: *consapevolezza, conoscenza e condivisione*, che sono relative ai rischi della rete e alle soluzioni adottate per difendersi. I giovani che si affacciano al mondo del cyber-spazio non possono prescindere da questi concetti, se vogliono uscirne indenni. Quelli che, invece, intendono approcciarsi ad attività lavorative legate alle tecnologie digitali, potranno sfruttarne le potenzialità se sapranno anticipare le esigenze dei cyber-consumatori con prodotti e servizi evoluti nei settori maggiormente deficitari come, ad esempio, semplificazione amministrativa, sanità, ecologia, supporto alle disabilità.