Partecipazione pubblico-privato per una cybersecurity più efficace: le indicazioni della Polizia di Stato

intervista al Prefetto Roberto Sgalla, Direttore Centrale per la Polizia Stradale, Ferroviaria, delle Comunicazioni e per i Reparti Speciali della Polizia di Stato
a cura di Raffaello Juvara

La diffusione dei dispositivi in rete (IoT) sia ad uso privato che inseriti in sistemi complessi ad uso professionale, comporta nuovi rischi per i quali non sempre gli utilizzatori sono consapevoli. Quali linee sta seguendo l'Amministrazione per sensibilizzare gli utenti a questo riguardo?

La sensibilizzazione dei cittadini circa i rischi connessi all'utilizzo dei dispositivi in rete passa attraverso due momenti fondamentali: il momento della educazione alla cultura della prevenzione ed il momento della repressione di condotte criminali, laddove esse si siano verificate. Entrambi gli aspetti costituiscono gli obiettivi strategici dell'azione delle Istituzioni e, in particolare, della Polizia di Stato, la quale, attraverso la Specialità Polizia Postale e delle Comunicazioni, da molti anni affianca al suo tradizionale impegno nella repressione dei reati on line, un considerevole sforzo in termini di prevenzione.

Il panorama dei canali virtuali approntati dalla Polizia di Stato per raggiungere più agevolmente larghe fasce della popolazion e e diffondere, così, il proprio messaggio informativo e di prevenzione, si giova in primo luogo dei canali ufficiali, presenti sui maggiori siti e social network (basti pensare alle pagina Facebook "Polizia di Stato" e "Una vita da social", agli account ufficiali su Twitter, al canale youtube "Agente Lisa") che, negli anni, sono stati capaci di aggregare attorno a sé una Community virtuale che oggi ammonta a più di 80 mila contatti.

In questo senso, tuttavia, il presidio di massima prossimità al cittadino è senz'altro rappresentato dall'istituzione del Commissariato di P.S. on-line (www.commissariatodips.it), eccellenza italiana premiata non solo in ambito nazionale e prima esperienza in Europa nel suo genere.

Inserito all'interno del Servizio della Polizia Postale e delle Comunicazioni, il Commissariato di P.S. on-line nasce proprio allo scopo di mettere a disposizione del cittadino, in maniera semplice e fruibile, risorse che consentano di interagire con la Polizia, di informarsi con utili consigli per prevenire rischi legati all'utilizzo di dispositivi connessi in rete e, persino, di inoltrare dirette segnalazioni relative a fenomeni criminosi in atto.

Gli attacchi cibernetici, a matrice prevalentemente criminale, colpiscono oggi non soltanto le grandi imprese erogatrici di servizi pubblici essenziali, ma soprattutto le realtà delle piccole e medie imprese ed i singoli cittadini. Inoltre, molti degli attacchi più devastanti per le grandi aziende (le cd. capo-filiera) partono spesso dalla violazione di sistemi IT di realtà

imprenditoriali più piccole, attestate su livelli di sicurezza inferiori ma dotate di accessi privilegiati a dati ed infrastrutture delle società-madre. Quale strategia sta attuando l'Amministrazione per contrastare questo insidioso fenomeno?

È certamente vero come oggi, per le realtà produttive, il rischio più grande e concreto sia rappresentato proprio dal cyber crime. Pertanto, la necessità di aumentare il livello di sicurezza delle medie, piccole e micro imprese per limitare le vulnerabilità presenti nei loro sistemi informatici e aumentare la consapevolezza del personale interno, si impone quale esigenza imprescindibile. Considerando poi che la cybersecurity è un settore in cui non esistono (né esisteranno in futuro) soluzioni onnicomprensive in grado di azzerare il rischio, è fondamentale che la cultura della sicurezza informatica entri a far parte del DNA aziendale, in modo che tutti siano preparati ad affrontare la minaccia. Le piccole imprese sono spesso l'anello debole nella difesa dagli attacchi cibernetici, essendo molti degli attacchi più devastanti per le grandi aziende (capo-filiera) partiti proprio da piccole realtà imprenditoriali aventi livelli di sicurezza inferiori ma dotate di accessi privilegiati a dati e infrastrutture delle società capo-filiera.

È quindi fondamentale che le imprese inizino a pensare a se stesse non come degli elementi disgiunti, solitari, ma come parte di una rete fortemente interconnessa. Considerata la centralità del ruolo svolto dalle piccole e medie imprese all'interno del tessuto produttivo del Paese, la Polizia Postale ha allargato a tali soggetti la rete di protezione tradizionalmente approntata per le grandi Infrastrutture critiche, che vede il CNAIPIC (Centro Nazionale Anticrimine Informatico per le Infrastrutture Critiche) avvalersi, nella veste di Organo centrale, dei Nuclei operativi di sicurezza cibernetica presenti presso ogni Compartimento regionale di Polizia Postale Viene prevista, per la singola impresa, la possibilità di stipulare apposite convenzioni volte ad instaurare un rapporto diretto e quotidiano di interscambio di informazioni per ogni attività di prevenzione, necessità di intervento o richiesta di assistenza che si rendesse volta per volta necessaria.

I soggetti stipulanti entrano così a far parte di un unico sistema integrato di protezione che accresce notevolmente le capacità di resilienza di fronte ad attacchi informatici.

La direttiva NIS ha ridisegnato in chiave europea i pilastri del sistema di sicurezza cyber, confermando la bontà di un approccio multilivello, che veda i diversi attori pubblici interloquire con gli attori dell'industria e dell'imprenditoria nazionale. Gli stessi operatori privati del resto, considerata la tentacolare pervasività che caratterizza i moderni attacchi informatici, sono chiamati a metter in campo adeguati investimenti in sicurezza IT, che consentano alle imprese di qualunque dimensione di approntare idonei livelli di difesa. Come giudica questo tipo di approccio integrato al problema della cybersecurity?

La Direttiva NIS (Network Information Security) non ha certo trovato impreparato il nostro ordinamento, tra i primi nel panorama internazionale ad aver manifestato una particolare sensibilità verso le tematiche della cybersecurity.

Già nel 2005, il decreto Pisanu aveva previsto l'istituzione del CNAIPIC presso il Servizio Polizia Postale, quale Centro dedicato alla protezione delle infrastrutture critiche nella loro dimensione logica e non materiale, mentre il successivo DCPM 24 gennaio 2013 e, da ultimo, il decreto Gentiloni del 17 febbraio 2017, ha individuato una complessa architettura istituzionale in materia di Cyber Sicurezza Nazionale in grado di fotografare la minaccia e predisporre un'adeguata, sinergica risposta.

Anche qui, la chiave di volta risiede nella capacità di "fare sistema", mettendo a fattor comune le migliori risorse dei comparti dei Servizi di Informazione, della Polizia e della Difesa, oltreché i CERT nazionali (Computer Emergency Response Team) sotto un'unica organizzazione, capace di reagire con la necessaria prontezza alle emergenze conseguenti alla commissione di attacchi informatici, nonché di investire con altrettanta tempestività il decisore politico, per l'assunzione delle decisioni strategiche più opportune.

In questo quadro, gli operatori privati, parte della "rete" di protezione tesa dalle istituzioni pubbliche, sono chiamati ad un cambio di prospettiva, che induca a considerare le spese in cybersecurity come necessario investimento, anziché mero costo. Gli obiettivi sono rappresentati sia dall'innalzamento, dal punto di vista tecnologico, delle dotazioni aziendali di sicurezza, sia dallo sviluppo di un'adeguata *awareness* aziendale, che si traduce nella formazione degli operatori sul corretto utilizzo delle reti e dei sistemi aziendali e sul corretto comportamento da mantenere per evitare rischi.