Il Sole 24 ORE

diffusione:105722
tiratura:156556

Politica

Reti e software

Strategie a lungo termine

L'urgenza di un ecosistema cyber nazionale

Il nostro paese non è pronto per affrontare attacchi sofisticati. Serve un piano

di **Roberto Baldoni**

Tutta l'economia di un paese sviluppato poggia sul cyberspace. I programmi di trasformazione digitale, irrinunciabili, come il piano industria 4.0 non faranno che aumentare questa dipendenza. Il cyberspace è la cosa più complessa e articolata che l'uomo abbia mai concepito, unione di migliaia di reti dati e di stratificazioni di software che interconnettono uomini e cose in giro per il mondo. Tuttavia, questa complessità, non avendo come fulcro la sicurezza, è generatrice di vulnerabilità nelle reti e nei programmi software e nelle loro interazioni. I cyber-criminali cercano di sfruttare queste vulnerabilità, molto spesso anche umane, per penetrare i nostri computer e trafugare dati o bloccare i nostri sistemi. La ricerca, i governi e l'industria studiano soluzioni per rendere sempre più difficile e costoso questo accesso indebito per l'attaccante. In questo gioco tra "guardia" e "ladri" la capacità di fare sistema tra le varie componenti di un paese è condizione primaria per una risposta efficace.

In Italia non siamo all'anno zero nella cybersecirity. Dopo il Dpcm Monti, che ha strutturato l'architettura cyber Nazionale, alcuni passi sono stati fatti, la sinergia sistemica tra ricerca e governo ne è un esempio. Troppo poco. I fatti di questi giorni mostrano che siamo impreparati ad affrontare attacchi con un minimo di sofisticatezza, non certo comparabili ad esempio a quelli portati da APT28, gli hacker russi che hanno attaccato Italia e Nato. In un mondo che corre, i governi dei paesi più industrializzati pongono la cybersecurity in cima alle proprie agende investendo imponenti risorse in programmi (almeno) quinquennali. Il nostro Paese si sta muovendo troppo lentamente e praticamente senza risorse.

Cosa fare. L'estate scorsa abbiamo atteso invano una rivisitazione del Dpcm Monti con l'attivazione di una "Unità di Missione" all'interno della Presidenza del Consiglio dei Ministri che prendesse in mano le redini del problema. Benché la nascita di una struttura che centralizzi competenze sia auspicabile, non sarà questa struttura da sola a risolvere il problema! Abbiamo bisogno di creare un "ecosistema cyber nazionale", composto da alcune organizzazioni di dimensioni adeguate, in termini di personale e competenze, inserite sia nel settore pubblico che in quello privato. Queste strutture devono abilitare una fitta rete di collaborazioni e devono essere in grado di impostare "operations" sia a livello internazionale che tra settore pubblico e settore privato nazionale. Squadra per la risposta ad emergenze informatiche, certificazione di dispositivi (hardware/software/firmware), ricerca, supporto alle industrie nazionali, cybercrime, cyber-intelligence e cyberwarfare sono esempi di aree che richiedono strutture da realizzare o da ampliare appropriatamente. Se l'Italia non sarà in grado, come altre nazioni, di far partire questi centri sarà sempre più tagliata fuori da operazioni internazionali riservate a una élite di nazioni "cyber-dotate" e regredirà sempre più come sistema paese.

L'ecosistema richiede di attivare un percorso virtuoso di trasferimento tecnologico tra università e impresa con un supporto strategico governativo, per consentire che le miriadi di prototipi, proof of concept, algoritmi innovativi che vengono elaborati dalla ricerca italiana, spesso lasciati in un cassetto, abbiano la possibilità di trasformarsi in opportunità di business. Inoltre nell'ecosistema si devono fare crescere e proteggere le startup che producono tecnologia di interesse strategico nazionale. In questo gli Stati Uniti e Israele sono esempi virtuosi, seppure diversi tra loro. Ci si potrebbe domandare: perché questo modello di trasferimento tecnologico dovrebbe attivarsi nella cybersecurity e non in altri settori dell'informatica? Perché la cybersecurity italiana è una comunità coesa nella quale tutti comprendono da tempo i rischi e la portata della minaccia e l'importanza della stretta collaborazione tra pubblico-privato-ricerca.

Competenze. Per implementare l'ecosistema abbiamo bisogno di competenze. Non ne abbiamo molte in Italia. Quindi, in una prima fase, dobbiamo concentrare le competenze. Parallelamente, dobbiamo crearne altre attraverso un programma specifico che recluti docenti universitari allo scopo di creare nuovi corsi di laurea sul territorio nazionale per aumentare la "workforce" agendo in sequenza anche sulle scuole di dottorato e sui licei.

La cybersecurity è un tema tecnico, benchè multidisciplinare, quindi c'è bisogno di ricercatori e ingegneri per trattarla in maniera adeguata e di persone con altri profili ma con anni d'esperienza nel settore. L'incompetenza metterebbe a rischio l'intero ecosistema. Abbiamo bisogno da parte del Governo di un piano forte per la cyber sicurezza nazionale, di investimenti e di un programma pluriennale con obiettivi precisi. È la condizione necessaria per rimanere agganciati al treno dei paesi sviluppati, senza che le nostre aziende e amministrazioni o i nostri cittadini rimangano ostaggi non di APT28, ma di un qualsiasi ragazzino "sufficientemente smart".


Il paradosso italiano tra digitale e sicurezza