Perimetro cyber, dopo l'Italia gli Usa. La rivoluzione targata Biden

Di Gabriele Carrer | 13/05/2021 -
James Bond

Dopo i casi SolarWinds, Microsoft e Colonial Pipeline, ecco il provvedimento per rafforzare le difese cyber degli Usa. Primo punto: rafforzare la condivisione di informazioni tra pubblico e privato. L'avvocato Stefano Mele (Gianni&Origoni) spiega le similitudini con il Perimetro di sicurezza nazionale cibernetica italiano e dice: "Occasione per rafforzare l'alleanza strategica"

Nelle ore in cui la rete di oleodotto Colonial Pipeline riprendeva le sue attività dopo aver, come rivelato da Bloomberg, pagato i 5 milioni di dollari di riscatto richiesto dagli hacker (probabilmente russi) che la scorsa settimana avevano portato a termine un attacco, il presidente **Joe Biden** firmava l'atteso executive order pensato per rafforzare la sicurezza cibernetica degli Stati Uniti. Una rete che negli ultimi mesi è stata messa sotto forte pressione dall'esterno: in particolare dalla Russia (si pensi al caso SolarWinds) e dalla Cina (con gli attacchi contro Ivanti e Microsoft Exchange). Offesive che, come quella contro Colonial Pipeline, hanno dimostrato l'insufficienza delle difese cibernetiche del Paese, ha spiegato la Casa Bianca.

Per questo, l'amministrazione ha deciso di creare una serie di standard di sicurezza digitale per le agenzie federali e i loro fornitori di software. Tra questi, l'autenticazione a più fattori, come accade come vogliamo utilizzare il nostro home banking, e un approccio zero-trust nei confronti dei fornitori di software, che dovranno autocertificare la loro affidabilità ma saranno responsabili delle eventuali vulnerabilità che porterebbero a un divieto di vendita al governo federale, che inevitabilmente avrebbe pensanti ripercussioni anche sul mercato per i consumatori.

L'executive order si compone di sette passaggi cruciali. Primo: rimuovere gli ostacoli alla condivisione delle informazioni sulle minacce tra governo e settore privato per consentire difese più efficaci dei dipartimenti federali e per migliorare la sicurezza informatica della nazione nel suo complesso. Secondo: modernizzare e implementare standard di sicurezza informatica più rigorosi nel governo federale puntando su soluzione zero-trust e accelerando il passaggio ai servizi cloud sicuri. Terzo: rafforzare la sicurezza della supply chain del software. Quarto: istituire un Cyber Safety Review Board al dipartimento per la Sicurezza nazionale, che vede pubblico (Pentagono, Giustizia, Cisa, Nsa e Fbi) e privato riunirsi dopo attacchi significativi per analizzare l'accaduto e preparare le difese. Il comitato si ispira al National Transportation Safety Board, che viene consultato dopo i gravi incidenti aerei per esempio. Quinto: creare un manuale standard per rispondere agli incidenti che interesserà le agenzie federali ma possa anche rappresentare un modello per il settore privato. Sesto: migliorare le capacità di rilevare le minacce. Settimo: potenziare le capacità di indagine e risoluzione degli incidenti.

Il senatore **Mark Warner**, esponente di spicco del Partito democratico e presidente della commissione Intelligence, ha accolto con favore la mossa della Casa Bianca ma anche ha sottolineato che non basta, serve un'iniziativa del Congresso per proteggere gli Stati Uniti nel quinto dominio.

Ma la difesa non è l'unico strumento. Il presidente Biden ha già annunciato sanzioni contro la Russia per il caso SolarWinds, mentre il suo consigliere per la sicurezza nazionale, **Jake Sullivan**, ha parlato di conseguenze "invisibili". Parole che in un certo senso rievocano quelle pronunciate in un'intervista con Il Foglio dal prefetto **Franco Gabrielli**, scelto dal presidente del Consiglio italiano **Mario Draghi** come sottosegretario con delega ai servizi segreti: "Vi è senz'altro la volontà dello stato di rispondere, quando vi è la possibilità, agli attacchi cyber di matrice statuale".

Stefano Mele, partner dello studio legale Gianni & Origoni e presidente della commissione Sicurezza cibernetica del Comitato atlantico italiano, vede una "comunità d'intenti" tra il Perimetro di sicurezza nazionale cibernetica che sta prendendo forma in Italia sotto la regia del Dis e l'executive

order dell’amministrazione Biden. “I governi italiano e statunitense procedono sulla stessa strada, nell’ottica di fortificare l’organizzazione e la risposta alla minaccia cibernetica”, spiega l’avvocato a Formiche.net. “Gli Stati Uniti e l’Italia, come tutti gli altri Paesi occidentali, si trovano ad affrontare problemi simili e lo fanno, sia pur con diversi sensibilità e gradi di urgenza, seguendo una specifica direttrice: intensificare lo scambio di informazioni tra publico e privato, rafforzare la sicurezza della supply chain, elevare gli standard di sicurezza cibernetica all’interno delle aziende e della pubblica amministrazione per allinearli all’innalzamento del livello qualitativo degli attacchi cibernetica perpetrati dagli attori esterni”. Il Perimetro e il provvedimento rappresentano dunque “un’occasione per rafforzare ancor di più l’alleanza strategica tra Italia e Stati Uniti verso l’obiettivo di realizzare un’interconnessione d’intenti e di misure per la sicurezza internazionale nel cyber-spazio”, conclude Mele.

Formiche Online, 13 maggio 2021