**Contro gli attacchi cyber serve un'azione coordinata tra Stato e aziende**

Di Laura Ciarti | 25/01/2022 -

*Se le grandi aziende sono all'avanguardia nell'affrontare le minacce tecnologiche, bisogna rafforzare l'azione congiunta con le istituzioni, e garantire anche la protezione delle piccole e medie imprese. Gli interventi di Volpi e Borghi (Copasir), Chittaro (Snam), Rapisarda (Eni), Iezzi (Swascan) nell'ambito dello Speciale I-Week*

Nell'ambito dello Speciale I-Week, promosso da Vento & Associati, il talk conclusivo "Intelligenza artificiale, Data economy e Cyber security" ha visto la partecipazione, tra gli altri, dei membri del Copasir **Raffaele Volpi** (Lega) ed Enrico Borghi (PD), del Senior vice president global security & cyber defense department di Snam, **Andrea Chittaro** (che è anche presidente dell'Associazione italiana professionisti della sicurezza aziendale – Aipsa), dell'Head of Group Security di Eni, **Alfio Rapisarda**, del Ceo di Swascan, **Pierguido Iezzi**, e dell'ambasciatore **Sergio Vento**, presidente di Vento & Associati.

L'intenso dibattito, moderato dal direttore di *Formiche.net* **Giorgio Rutelli**, è stato aperto dal senatore Volpi, che ha sottolineato quanto per affrontare le sfide alla sicurezza cibernetica occorra concentrarsi sul fattore umano, l'unico in grado di interpretare i dati, investendo su un processo di aggiornamento continuo sia sulle novità tecnologiche, quanto sulle mutevoli dinamiche di un contesto geopolitico sempre più incerto.

Da questo punto di vista la collaborazione tra le intelligence dei vari Paesi va ricercata senza pregiudicare l'autonomia nazionale. Nel contesto attuale gli alleati tendono nonostante tutto a essere rivali in ambito

economico. Una prospettiva matura – ha concluso Volpi – deve quindi raccogliere gli attori nazionali e solo in un secondo momento creare piattaforme di condivisione all'interno dell'Ue.

Borghi ha invece evidenziato quanto l'Italia sia costantemente sotto attacco nel dominio cibernetico, in alcuni casi con notevole gravità, e l'attuale pandemia sia stata un'opportunità per compiere attacchi più pericolosi e più numerosi. La recente creazione dell'Agenzia per la Cybersicurezza Nazionale (Acn) è solo il primo passo verso una soluzione più ampia e globale. Secondo Borghi, i fondi offerti dal Pnrr rappresentano un'opportunità per accorciare i tempi e dotare il paese di difese adeguate.

Il confronto è proseguito con l'intervento dell'avvocato Stefano Mele, partner di Gianni & Origoni, che ha ricordato l'urgenza di mettere in sicurezza le Pmi, prive di risorse e competenze sufficienti per proteggersi dalla minaccia cyber, attraverso un cloud nazionale che offra loro livelli di sicurezza elevati. E, riprendendo un suo intervento su queste pagine, ha ribadito la necessità di definire minacce alla sicurezza nazionale gli attacchi cyber contro servizi essenziali

Dal lato delle aziende, Andrea Chittaro di Snam ha evidenziato come i consigli di amministrazione debbano mettere in agenda la questione della sicurezza cibernetica, evitando di reagire in modo estemporaneo e perseguendo invece una visione di insieme capace di adeguarsi a minacce in continua evoluzione. La stessa Acn non è sufficiente senza un partenariato pubblico-privato che preveda la condivisione dei dati tra imprese e istituzioni, tramite opportuni strumenti legali.

Le aziende – ha concluso Chittaro – un tempo restie a condividere le proprie informazioni, sono ora maggiormente consapevoli della necessità di fare squadra per assicurare la vitalità del sistema-Paese.

La creazione di sinergie è stata auspicata anche da Alfio Rapisarda, Head of Group Security Eni, che ha evidenziato quanto le minacce cyber riguardino imprese, infrastrutture, istituzioni e anche persone singole, che quotidianamente usano la rete per le loro esigenze quotidiane. La difesa cibernetica non è un optional, ma un'esigenza primaria per il Paese, tanto più che tra gli obiettivi della pirateria informatica figurano le informazioni che orientano le decisioni dei poteri pubblici. Tutti gli stakeholder devono dunque cooperare, fare sistema per l'interesse nazionale, ha precisato Rapisarda.

Iezzi di Swascan ha raccontato, con un certo scoramento, quanto l'Italia sia un buon pagatore, destinata perciò a finire nel mirino degli hacker a caccia di riscatti. Serve dunque una legge per impedire il pagamento dei riscatti, un po' come avvenuto negli anni '70 per contrastare l'anonima sequestri. Gli attacchi più pericolosi – ha continuato Iezzi – sono però gli zero-day, raddoppiati nell'ultimo anno. Essi rappresentano una vera e propria arma, come mostra il suo uso nel conflitto russo-ucraino e in quello, meno noto, tra

Israele da una parte e Siria e Iran dall'altra. L'obiettivo che deve perseguire l'Italia non è limitarsi a difendersi dalle minacce, ma sviluppare le proprie capacità di reazione e contrattacco, dotandosi di competenze e possibilità offensive paragonabili a quelle dei maggior attori.

L'Italia ha già delle eccellenze mondiali nel settore cibernetico, ma è urgente dotare il paese degli strumenti necessari per svilupparle, attraverso un partenariato pubblico-privato che stimoli la ricerca e l'attività dei laboratori. Altrimenti – ha concluso Iezzi – il nostro Paese sarà destinato a essere escluso dal tavolo decisionale della "guerra fredda digitale" già in corso.

Concludendo il dibattito **Andrea Vento**, Ceo di V&A, ha ribadito l'importanza di disporre di risorse finanziarie adeguate per tenere il passo dell'evoluzione tecnologica e digitale. Le risorse messe a disposizione della sicurezza cibernetica in Italia sembrano infatti modeste, soprattutto se raffrontate a quelle su cui possono contare la NSA negli Stati Uniti e la sua corrispondente britannica Gchq. Unitamente a quanto hanno rilevato altri relatori sulla necessità di un partenariato pubblico – privato, anche a tutela delle numerose piccole e medie imprese, in ritardo nell'adeguamento delle difese cibernetiche.

Formiche.Net, 25 gennaio 2022