Attacchi cibernetici: la risposta dell’Europa

Autore: Fabio Di Nunno

Gli attacchi informatici aumentano e diventano sempre più pericolosi: l’Unione europea istituisce una nuova unità dedicata.

I recenti attacchi cibernetici ai sistemi informatici della Regione Lazio, dei quali si stanno interessando anche l’Fbi e l’Europol assieme alla Polizia Postale, **riaprono il dibattito sulla necessità di garantire a tutti i livelli la sicurezza informatica**. Diversi Stati membri dell’Unione europea (UE) stanno subendo degli attacchi informatici, ma anche diverse istituzioni europee, tra cui la Commissione europea, l'Agenzia europea per i medicinali e l'Autorità bancaria europea, sono state oggetto di attacchi informatici. Secondo i dati diffusi dalla Commissione europea, **nel 2020 ci sono stati 949 attacchi informatici significativi nell'UE**, con un aumento del 72% rispetto al 2019, di cui 742 hanno preso di mira i cosiddetti settori critici (quali energia, trasporti, acqua, salute, infrastrutture digitali e settore finanziario). Il costo annuale della criminalità informatica per l'economia globale nel 2020 è stato stimato in **5,5 trilioni di euro**. Inoltre, sotto il profilo economico, nell'UE esistono più di 60.000 società di sicurezza informatica e 660 centri di competenza in materia di sicurezza informatica, con un valore di mercato stimato in oltre 130 miliardi di euro. Inutile dire che anche le opportunità di lavoro in questo settore sono notevoli. **Si stima che entro il 2022 ci saranno circa 350.000 posti vacanti in Europa** nel settore della sicurezza informatica laddove, attualmente, le donne rappresentano solo il 7% della forza lavoro. Pertanto, la Commissione europea ha proposto di **istituire una nuova task force** per rispondere al numero crescente di attacchi informatici in Europa, alla quale gli organismi nazionali responsabili della sicurezza informatica potranno chiedere assistenza ad altri Stati membri per affrontare e riprendersi da tali attacchi su larga scala. L’Unità cibernetica congiunta coordinerà le operazioni tra le istituzioni e le agenzie dell'UE e le iniziative delle autorità nazionali in tutto il blocco, scambiando informazioni in tempo reale sulle minacce per prevenire, scoraggiare e rispondere agli attacchi informatici. Inoltre, **l'Unità cibernetica congiunta rafforzerà la cooperazione** non solo tra i paesi, ma anche con tutte le parti interessate: comunità di sicurezza informatica, comprese le comunità civili, forze dell'ordine, comunità diplomatiche e di difesa informatica e aziende del settore privato. Sarà sia una piattaforma fisica, in cui gli esperti di sicurezza informatica possono riunirsi, sia una piattaforma virtuale per la condivisione delle informazioni e le capacità di rilevamento. L'Unità cibernetica congiunta dovrebbe essere operativa entro la metà del 2022 e completamente istituita entro la metà del 2023. Secondo **Thierry Breton**, Commissario al Mercato interno, «gli attacchi informatici fanno parte della nostra realtà. Proprio come facciamo nel mondo fisico, dobbiamo proteggere le nostre istituzioni democratiche, i nostri servizi pubblici, i nostri ospedali e la nostra industria». Infatti, «le minacce informatiche si evolvono rapidamente, sono sempre più complesse e adattabili». Pertanto, «per garantire che i nostri cittadini e le nostre infrastrutture siano protetti, dobbiamo pensare a diversi passi avanti, lo scudo per la sicurezza informatica resiliente e autonomo dell'Europa ci consentirà di utilizzare le nostre competenze e conoscenze per rilevare e reagire più velocemente, limitare i potenziali danni e aumentare la nostra resilienza». È chiaro che «investire nella sicurezza informatica significa investire nel futuro sano dei nostri ambienti online e nella nostra autonomia strategica». La strategia dell'UE per la cibersicurezza, presentata sul finire dello scorso anno, **intende rafforzare la resilienza collettiva dell'UE contro le minacce informatiche** e contribuirà a garantire che tutti i cittadini e tutte le imprese possano beneficiare appieno di servizi e strumenti digitali affidabili. Nello specifico, a prescindere da quali siano i dispositivi connessi, le reti elettriche, i servizi bancari o i trasporti aerei che i cittadini europei utilizzano o le amministrazioni pubbliche o le strutture ospedaliere che frequentano, essi devono potervi accedere con la sicurezza di essere protetti dalle minacce informatiche. Inoltre, la strategia dell’UE per la cibersicurezza potrebbe consentire all'UE di rafforzare le norme e gli standard

internazionali nel ciberspazio e **di intensificare la collaborazione con i partner in tutto il mondo** al fine di promuovere un ciberspazio globale, aperto, stabile e sicuro, fondato sullo Stato di diritto, sui diritti umani, sulle libertà fondamentali e sui valori della democrazia.