Cyber Security ed Intelligence Economica

Alla base della Cyber Security vi è la protezione degli utenti del cyberspace da eventi occasionali o accidentali, come il furto, il trasferimento di dati, la loro modifica, la distruzione degli stessi o il blocco dei sistemi.

di Massimo Franchi
Advisor, analista e docente è Direttore responsabile della rivista di cultura aziendale Capitale Intellettuale. Subject Matter Expert in Tecniche di Negoziazione presso NRDC-ITA. Membro della delegazione italiana presso la Gaminger Initiative, è laureato in Scienze Politiche e diplomato nei Master in Governance Politica e Geopolitica.

Il ruolo della Cyber Security è divenuto oggi di fondamentale importanza per le imprese di ogni dimensione, in quanto il benessere e la pace sociale di una nazione dipendono anche dalla protezione contro le minacce derivanti dal Cyberspace, un dominio materiale ed immateriale senza confini, nel quale si è sviluppato un nuovo modello sociale, informativo e relazionale, grazie all'uso di sistemi hardware, software, network di comunicazione, device mobili, ecc. Avere una policy per la Cyber Security significa proteggere il Cyberspace da qualsiasi tipo di minaccia che può colpire la privacy del singolo cittadino/consumatore come i dati sensibili delle imprese, di ogni dimensione e le infrastrutture critiche. In questi anni ogni paese evoluto ha messo in pratica azioni per la protezione delle infrastrutture critiche che però hanno assunto sfumature diverse. Per gli Usa si tratta di *sistemi e asset, sia fisici che virtuali,* così vitali che "l'incapacità o la distruzione degli stessi potrebbe avere un debilitante impatto sulla sicurezza, sulla sicurezza nazionale economica, sulla salute pubblica nazionale, sull'antinfortunistica e sulla combinazione di queste tematiche"[1], mentre per l'Unione Europea oltre agli *"asset e sistemi essenziali per il mantenimento delle vitali funzioni sociali"* viene evidenziato il *"benessere delle persone"* con un impatto della minaccia che si considera tale solo se presente in almeno due Stati membri.[2]

Alla base della Cyber Security vi è il *come proteggere* gli utenti da eventi occasionali o accidentali, come il furto ed il trasferimento di dati, la loro modifica, la distruzione degli stessi o il blocco dei sistemi. Tutto questo rappresenta una minaccia, ma anche un'opportunità per le aziende che operano in questo comparto e che vedranno una crescita esponenziale negli anni futuri, sia in termini di fatturato che di personale impiegato. Infatti, se da una parte gli utenti, privati o pubblici che siano, dovranno investire miliardi di euro per la loro protezione, sicuramente le imprese specializzate in questo settore strategico potranno fare affari d'oro.

Per l'Unione Europea i settori critici e da proteggere sono il food, l'acqua, l'industria nucleare, lo spazio, l'industria chimica, la sanità, l'industria finanziaria, i trasporti, l'energia, i centri di ricerca e l'ICT. Gli Usa hanno un concetto ancora più estensivo ed aggiungono l'industria del sistema difesa, i complessi commerciali e governativi ed i sistemi produttivi critici. Un tipico attacco, magari nel settore finanziario (il più grande segmento al mondo per la Cyber Security), è normalmente attuato per paralizzare le infrastrutture critiche oppure rubare informazioni con differenti scopi: criminali, terroristici o di spionaggio.

---

[1] US Public law 107-56 (October 26, 2001) "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act".

[2] European Union Directive 2008/114/EC.