Strategie cybersecurity e cyberthreat: concretezza o 'chiac-chiere e distintivo'?

Elisabetta ZUANELLI

In questa riflessione, richiamo subito una distinzione fondamentale nel *cybercrime* che ricomprende un'economia estesa di finalità, attori, gruppi, 'aziende' che operano criminosamente nel cyberspazio: da un lato attacchi e minacce *cyber* ovvero "azioni forzose identificate, dirette verso l'accesso, l'esfiltrazione, la manipolazione o la compromissione dell' integrità , della riservatezza, della sicurezza o la disponibilità di dati, di un'applicazione o di un sistema…, senza l'autorizzazione necessaria "; dall'altro attività criminose quali il traffico di denaro sporco, la pedo pornografia, il traffico di stupefacenti, le attività terroristiche, il traffico di persone, ecc. espletate usando la rete. Ci occupiamo, qui, del primo tema ovvero di sicurezza, minacce e attacchi *cyber*. E, dunque, qual è lo stato della *cybersecurity* oggi?

I dati di tendenza

Secondo il Rapporto Symantec 2015 i dati registrati indicano un aumento dello spionaggio *cyber*, la crescita della sofisticatezza e professionalità del *malware*, la targetizzazione degli attacchi contro sistemi industriali, ambasciate e altri settori sensibili, l'aumento degli attacchi *spearphishing* (8%) e il ritardo considerevole da parte delle vittime nel riconoscimento del *malware* (talora oltre i 200 giorni). Negli ultimi quindici anni, lo sviluppo geometrico dei rischi, delle minacce e degli attacchi al cyberspazio conduce a tre inevitabili constatazioni.

La prima pone in diretta correlazione lo sviluppo straordinario delle interazioni in Rete connesso al potenziamento delle Reti stesse e alle tipologie di servizi *online* con la crescita esponenziale degli attacchi *cyber*. Le piattaforme di *e-commerce* e quelle di ricerca e *marketing online*, i servizi *cloud* e i *social network*, settori quali l'*ebanking*, l'*e-finance*, l'*egov*, l'*ehealth*, il turismo, i giochi, i servizi immobiliari e di intermediazione finanziaria *on line* e, più di recente, il settore dello IoT sono l'oggetto di crescenti attacchi mirati nei quali vengono sottratti dati, compiute frodi telematiche, criptati file, creati blocchi o interruzioni delle attività aziendali, imbrattati i siti. La situazione è drasticamente favorita nelle piattaforme e nei servizi *mobile* che ampliando le modalità e la quantità delle interazioni in Rete hanno aperto un mercato della *cyber security* e del *cybercrime* fino a qualche tempo fa impensabile.

Il secondo dato ha a che vedere con la crescente specializzazione e finalizzazione degli attacchi per i quali la storica sicurezza *in house*, *firewall*, *antivirus*, ecc. è superata: il *malware* utilizzato e i diversi attacchi avvengono attraverso la Rete e sulla Rete. Ad oggi nessuna soluzione tecnologica di sicurezza può essere garantita. Ciò tenendo conto che la tecnologia del *cybercrime* è fortemente sostenuta da investimenti anche istituzionali e appare talora più avanzata delle tecnologie ICT presenti, come dimostrano i rapporti provenienti da fonti diverse, nazionali e internazionali (Kaspersky, Symantec e via dicendo; in

Italia l'ottimo Rapporto annuale CLUSIT su dati nazionali e internazionali). In altri termini, l'innovazione tecnologica del *cybercrime* che emerge dalle tipologie degli attacchi segnala che una parte consistente di questi non è tecnologicamente riconosciuta e nota.

Il terzo dato riguarda il rischio e la minaccia *cyber* in ambito istituzionale, internazionale governativo, cresciuti considerevolmente lo scorso anno, con la prospettiva paventata di attacchi alle infrastrutture critiche: energia, acqua, nucleare, chimica, viabilità, trasporti, ecc. La minaccia è considerata dagli esperti statunitensi un'arma specialistica di governi contro governi, non ancora del terrorismo contro i governi nemici, in una *cyberwarfare* di crescente preoccupazione.

Il Dipartimento della *homeland security* statunitense così tratta oggi il tema della minaccia alle infrastrutture critiche. "L'abilità operativa necessaria per impiegare efficacemente la tecnologia e gli strumenti rimane un importante fattore limitante, soprattutto contro obiettivi più difficili come reti classificate o infrastrutture critiche. Per i prossimi 5/10 anni, solo gli stati nazionali sembrano avere disciplina, impegno e risorse per sviluppare appieno le capacità di attacco alle infrastrutture critiche. Il loro obiettivo è quello di indebolire, perturbare o distruggere gli Stati Uniti. I loro sotto-obiettivi includono lo spionaggio a fini di attacco; lo spionaggio per le tecnologie avanzate; interruzioni delle infrastrutture per attaccare l'economia americana; attacco su larga scala delle infrastrutture quando sono attaccati dagli Stati Uniti per danneggiare la capacità degli Stati Uniti di proseguire i suoi attacchi." (www.dhs.gov, sito ufficiale del Dipartimento della *homeland security*).

Se allo hackeraggio civile si aggiungono, dunque, la minaccia alle infrastrutture critiche e lo spionaggio governativo, politico e industriale che costituiscono bacini strategici d'azione per il *cybercrime* si comprenderà come sicurezza, minacce, attacchi e vittime siano stati configurati concettualmente come veri e propri ambiti di implicazione bellica militare.

Il mercato della *cybersecurity*

Ma a chi giova il mercato della *cybersecurity*? La dimensione globale del mercato *cybersecurity* è stimato crescere da 106,32 miliardi di dollari nel 2015 a 170,21 miliardi di dollari entro il 2020, a un tasso di crescita annuale composto (CAGR) del 9,8%. Chi sono i portatori di interesse e quali le offerte di servizi?

Secondo una recente ricerca sul mercato e le aspettative degli operatori aziendali in materia di sicurezza i portatori di interesse sono almeno i seguenti: venditori di sicurezza *cyber*, fornitori di soluzioni di Rete, venditori indipendenti di software, fornitori di software, integratori di sistemi, rivenditori a valore aggiunto, fornitori e distributori di servizi, organizzazioni di ricerca, agenzie di sicurezza IT, società di consulenza *cloud* e *business intelligence* (BI), fornitori di infrastrutture *cloud*, investitori e *venture capitalist*. E l'elenco potrebbe continuare con la recente accelerazione del settore assicurativo. Tra le attività del mercato possiamo annoverare la consulenza, la progettazione e l'integrazione, l'*assessment* del rischio e della minaccia, i servizi gestiti di sicurezza, l'addestramento e la formazione.

All'elenco dei fornitori di sicurezza *cyber* va tuttavia affiancato quello dei creatori della minaccia e degli attacchi. Come ho

a suo tempo segnalato, gli hacktivisti operano sia come singole entità, gruppi, aziende di criminalità informatica che ottengono denaro e potere direttamente dagli attacchi *cyber* sia vendendo attacchi e dati ad altri *player* nel mercato. I *player* sono industrie, intermediari finanziari, aziende che possono trarre vantaggio dall'attività criminosa svolta per proprio conto dalla filiera criminale. L'analisi di mercato, dunque, dovrebbe includere gli interessi, le quote di mercato non solo sul lato dell'offerta, ma anche dal lato della domanda. In altri termini occorre chiedersi chi sono gli acquirenti, non solo i venditori, di servizi di criminalità informatica e quanto vale il crimine informatico. Il tema, come si intende, è complesso e si affronta oggi in maniera parziale.

Venendo alle soluzioni di mercato, personalmente ritengo che tra gli ambiti di sviluppo e l'offerta di servizi di *cybersecurity* si debba collocare in via prioritaria il *big data analyzing*, un'*intelligence* innovativa con modalità predittive, non solo preventive o di risposta ad allarmi, per tempestivi che siano. Ne consegue, in ogni caso, che questo mercato esplosivo è un'area di *business* sulla quale si cimentano ormai realtà aziendali aggressive e molto competitive verso utenti/clienti non sufficientemente attrezzati.

Le risposte istituzionali

Ma veniamo a un secondo ordine di considerazioni che tocca la risposta di sistema, nazionale e internazionale ai temi della sicurezza e delle minacce *cyber*.

Negli anni più recenti, si sono consolidate nella UE due linee d'azione: la regolazione normativa e gli standard che comportano necessariamente il tema della protezione dei dati e della *privacy*, rispetto alle quali è in discussione il *business* stesso dei servizi *online* e la gestione istituzionale della sicurezza.

Circa la regolazione sulla protezione dei dati, il quesito concerne la soglia di responsabilità dei gestori dei servizi stessi nella tutela da attacchi informatici esterni da un lato, dall'altro nell'uso dei dati acquisiti e conservati, con localizzazioni extraeuropee, in assenza di norme condivise e valide e, dunque, di giurisdizione. Il tema della protezione dei dati, come si intende, va al di là del diritto alla privatezza e riservatezza dei dati personali, oggetto della sentenza della Corte di giustizia europea e della conseguente sospensione del *Safe Harbour*. Il quesito va inoltre oltre, ovviamente, gli attacchi e le minacce *cyber*; nella questione sono in gioco interessi potenti inerenti l'uso dei dati di cui sono in possesso, in particolare, i giganti GAFTAM (Google, Amazon, Facebook, Twitter, Apple, Microsoft): concerne la profilazione mondiale delle società e degli individui nelle scelte di lavoro e di vita, nelle tendenze religiose, sessuali, politiche e del tempo libero, un controllo esistenzialmente conturbante. Concerne le masse di dati acquisite di natura politica, tecnologica, industriale, commerciale e l'uso lecito o illecito che di esse si può fare. Su questo aspetto la UE si è impegnata ad approfondimenti entro il 2016 nella prospettiva del Mercato unico europeo.

Venendo alla gestione istituzionale delle minacce e degli attacchi informatici stretti, i colossi europeo e statunitense si sono mossi con orientamenti tendenzialmente convergenti. Dal 2011 e nel 2013 sono proliferate in Unione Europea le strategie nazionali, i piani operativi e l'istituzione di organismi, enti, soggetti vari preposti alla

cybersecurity, sulla scorta delle linee guida dei paesi più avanzati. Oltre all''ENISA e ad Europol si è creata una pletora di centri, istituti, organismi pubblici e privati e sono stati lanciati piani d'azione sulla sicurezza e la protezione dei dati. Al di là della difficolta di conciliare gli interessi delle industrie ICT con i temi della protezione e *privacy* evocati, va detto che le regole poco possono. Infatti, su compromissioni di interessi statuali governativi, aziendali o personali a poco valgono gli steccati quando i buoi sono fuggiti. Come immaginare una rivalsa economica, istituzionale o personale contro i giganti dei dati qualora si potesse dimostrare che i dati sono stati usati con intenti maligni, nella concorrenza o nell' immagine? O come assegnare la responsabilità degli attacchi informatici esterni e di danni economici conseguenti al gestore dei dati stessi nei settori *cloud* o *ecommerce*? E, in ogni caso, come quantificare e qualificare specifici danni?

La soluzione delle regole, in ogni caso necessarie, è un utile paravento di carta rispetto ai temi globali in discussione. E' una risposta in parole da parte delle istituzioni di governo nazionale e internazionale a minacce crescenti di livello diverso dalle quali, fortunatamente, le masse non sembrano minimamente toccate. Si pensi solo allo sfoggio esibizionistico e voyeuristico dei dati personali e relazionali nelle piattaforme *social* e nell'uso selvaggio delle transazioni *mobile*, addirittura di tipo economico.

Gli Stati Uniti dispongono di vari strumenti di intervento e informazione sulle minacce *cyber*: dallo storico NIST (*National Institute of Standards and Technology*) al *National Vulnerability Database* (NVD) sponsorizzato dal *Department of Homeland Security* (DHS), il *National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team (US-CERT)*. Apprezzabile l'intento pratico verso I cittadini, responsabili inconsapevoli spesso delle falle informatiche create da loro stessi a vantaggio degli *hacker* informatici.

Il quesito di fondo rimane tuttavia lo stesso: quali azioni servono per tamponare e contrastare questo fenomeno preoccupante che riguarda da un lato la protezione interna e i flussi di dati digitalizzati e dall'altro la difesa contro le diverse tipologie di attacchi informatici per non ridurre il tema a chiacchiere e distintivo? A due recenti seminari cui ho partecipato al CASD del Ministero della difesa, rivolti a personale NATO e ad operatori nazionali, ho sottoposto all'attenzione gli spunti seguenti.

Priorità e concretezza

Evitare l'inutile sovrapposizione e moltiplicazione disordinata di organismi, responsabilità, attori nella *cybersecurity* e coordinarne le azioni è un passo strategico da considerare nelle singole realtà nazionali e nel contesto UE. La Rete e la sicurezza informatica sono per definizione sovralocali, come dimostrano i tentativi di correlazione delle attività di *intelligence* in materia di terrorismo. E le attività 'meta' costano. L'illusione che la verbosità istituzionale locale ed europea corrisponda a soluzioni effettive va contrastata mentre vanno alimentate logiche di *cyberdiplomazia*, in parte avviate in ambito NATO. Le minacce non solo alle infrastrutture critiche ma anche all'informazione e ai dati economici e finanziari qualora passasse una visione iperliberistica dei flussi di dati sono

reali. Pertanto, la proliferazione di azioni 'meta', che riflettono sulla sicurezza ma non agiscono concretamente per la stessa, vanno rimeditate a favore di altri interventi di sistema: qualificazione e riqualificazione formativa operativa, per filiera e utenti, in materia di comportamenti prosicurezza; incentivazione dello R&D specifico; condivisione istituzionale obbligatoria dei dati d'attacco da parte delle 'vittime'; incentivazione economica per gli investimenti privati e pubblici in materia; nuove modalità di analisi e *intelligence*. Riassunte in *item* specifici: servono interventi globali di cyberdiplomazia, soluzioni manageriali/organizzative, training e formazione, R&D applicato, integrazione di tecnologie della sicurezza. Forse meno chiacchiere e più fatti.

Elisabetta Zuanelli

Professore ordinario, cattedra di I fascia, Glottodidattica/Comunicazione digitale presso l'Università di Roma, "Tor Vergata", Dipartimento di Studi di Impresa, Governo, Filosofia.

Responsabile innovazione tecnologica Facoltà di Lettere e Filosofia dell'Università di Roma "Tor Vergata".

Presidente del Centro di Ricerca e sviluppo sull'E-Content dell'Università di Roma "Tor Vergata".

Consigliere alla PCM su Comunicazione pubblica e istituzionale dal 1987al 1992.

Capo Dipartimento delle discipline organizzativo-informatiche e delle scienze internazionalistico-comunitarie e comunicazionali presso la Scuola Superiore dell'Economia e delle Finanze (SSEF), Ministero dell'Economia e delle Finanze dal 1993 al 2004.

Già professore ordinario di Comunicazione istituzionale e linguaggio della P.A. presso la Scuola Superiore dell'Economia e delle Finanze (SSEF), Ministero dell'Economia e delle Finanze dal 1993.

dal 2005 Esperto dell'Unione Europea nel Programma econtent plus and security/Valutatore dei progetti 2005-2006.

dal 2010 Membro del Comitato scientifico di redazione e Referee internazionale di IEEE/MEEM (Institute of Electrical and Electronic Engineers, Multidisciplinary Engineering Education Magazine).

dal 2012 Esperto MIUR Ricerca industriale (Decreto MIUR n. 30/Ric. del 2 febbraio 2012).

2012 direttore scientifico del progetto di piattaforma www.moltiplicalavita.it per il Ministero della salute (il Presidente della Repubblica Giorgio Napolitano ha conferito al progetto Moltiplica la vita e al premio una propria medaglia di rappresentanza).