CYBERSECURITY:

un quadro d'insieme per affrontare consapevolmente il problema

confetra
Confederazione Generale Italiana
dei Trasporti e della Logistica

L'utilizzo di internet ha raggiunto una dimensione globale, la rete è l'infrastruttura su cui viaggiano i nostri dati personali, i dati delle aziende per cui lavoriamo, le nostre idee e i nostri interessi. Tuttavia la digitalizzazione della nostra vita porta con sé sia opportunità che minacce. Le campagne di *ramsonware*, come *wannacry* e *notpetya*, il *phishing,* le *fake news* sono la punta emersa di un iceberg che include tutte le minacce portate dalla trasformazione digitale. La parte sommersa dell'iceberg è costituita da migliaia di attacchi giornalieri, che hanno come obiettivo le infrastrutture critiche nazionali, le aziende, le organizzazioni governative e i cittadini, al fine di sottrarre dati, monitorare comportamenti, controllare funzionamenti e truffare.
Molte ricerche di istituti importanti e terzi, quali le Banche Centrali Nazionali, hanno mostrato come la sicurezza nel dominio cibernetico non possa più essere considerata un costo certo di fronte a un danno incerto. L'aumento esponenziale degli attacchi, sempre più intelligenti e complessi, continuerà senza sosta nel prossimo futuro. Le organizzazioni che non prenderanno le opportune contromisure alimentando una cultura della sicurezza al loro interno, vedranno accrescere il rischio di essere oggetto di attacchi.
Gli attacchi cyber avvengono sfruttando una combinazione di vulnerabilità umane e tecnologiche. I cyber-criminali non attaccano soltanto banche e grandi multinazionali: gran parte del loro fatturato è infatti realizzato attaccando decine di migliaia di medie, piccole e micro imprese completamente impreparate ad affrontare efficacemente la minaccia. I criminali bloccano l'operatività di queste imprese per poi chiedere un riscatto, rubano i loro *asset*, i loro dati o spiano le loro strategie di *business*. Questo mette a rischio la sopravvivenza stessa dell'impresa. Le recenti campagne di *malware wannacry* e *notpetya* rappresentano gli eventi visibili, il primo ha messo in ginocchio 200mila computer in tutto il mondo, colpendo 74 Paesi e centinaia di aziende mentre il secondo ha colpito diverse centinaia di aziende tra le quali la AP Moller-Maersk, azienda danese di trasporti navali, e l'azienda di logistica TNT dove il *malware* ha fatto saltare il sistema di tracciamento delle spedizioni. Quello di TNT è l'esempio lampante di quanto possa essere devastante un attacco informatico dal punto di vista del *business*: al di là degli affari, è il danno di immagine a pesare notevolmente[1]. Non è un caso che la stragrande maggioranza delle aziende che subiscono un attacco informatico tendano a pagare il riscatto (nel caso di attacco *ransomware*) e a non far trapelare nulla all'esterno. Mossa impossibile per un'azienda come TNT, dato che di mezzo ci sono migliaia di clienti in attesa delle loro spedizioni.
Durante il convegno svoltosi a Genova "Le rotte digitali del trasporto IoT e big data: opportunità e rischi della digital transformation" è stata fatta una simulazione di cyber attacco. Sono bastati solo 10 minuti, un pc portatile e una connessione ad internet affinchè Gianni Cuozzo, Amministratore delegato della società Aspisec, specializzata in consulenza sul cyber-risk, potesse accedere e prendere, potenzialmente, il controllo del sistema informatico di una nave in piena attività[2].

"Un paese che non metta la cybersecurity al centro delle proprie politiche di trasformazione digitale è un paese che mette a serio rischio la propria prosperità economica e la propria indipendenza."[3]

Lo scenario normativo

Gli strumenti giuridici con cui la Commissione Europea ha aggiornato e rafforzato la propria strategia in tema di cybersecurity sono: una raccomandazione, due comunicazioni, una proposta di regolamento e una proposta di direttiva.
L'iniziativa, preannunciata dal Presidente Juncker ha un obiettivo chiaro: aumentare la resilienza dell'Unione Europea nei confronti degli attacchi cyber e creare un'effettiva deterrenza per proteggere il nascente mercato unico della cybersecurity con interventi concreti. La direttiva NIS[4] – *Network and Information Security* – costituisce la pietra miliare della strategia europea in tema di cybersecurity, si occupa soprattutto di tre aspetti: (i) rafforzare le capacità di gestione

[1] Il Sole 24 Ore, "TNT e le altre: così un attacco hacker mette in ginocchio un'azienda per giorni" Simonetta Biagio, 07 luglio 2017
[2] Il Sole 24 Ore, "Attacco hacker in corso, coinvolte Chernobyl, Moller-Maersk e Saint Gobain" 27 giugno 2017
[3] Il nuovo libro bianco:"Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici", CINI – Consorzio Interuniversitario Nazionale per l'Informatica
[4] Recepita in Italia con D.Lgs 18 maggio 2018 n.65

della cybersecurity in ogni Stato dell'UE; (ii) incrementare il livello di collaborazione tra gli Stati dell'UE; (iii) potenziare le strategie di gestione dei rischi e segnalazione di incidenti di cybersecurity. Questa impone di designare a livello nazionale un'autorità competente per la sicurezza informatica e un *Computer Security Incident Response Team* (CSIRT) nazionale per la gestione dei rischi.
Nasce dalla necessità per ogni Stato membro di mettere in sicurezza le proprie infrastrutture e di garantirne il funzionamento secondo regole e requisiti comuni. Ciò impedirà alle imprese europee di operare in un ambiente frammentato e consentirà di facilitare e migliorare i loro sforzi di conformità alle predette regole.
L'entrata in vigore della direttiva NIS ha imposto, a livello italiano, una revisione del cosiddetto *DPCM Monti* del 24 gennaio 2013 che si è espletato nel *DPCM Gentiloni* del 17 febbraio 2017 finalizzato a ottimizzare la gestione delle crisi e a centralizzare le responsabilità. A tal fine è stato rafforzato il ruolo del *Dipartimento delle informazioni per la sicurezza* (DIS). Il DIS ospita il *Nucleo di Sicurezza Cibernetica* (NSC), un organismo operativo interagenzie e intergovernativo per la sicurezza informatica. Le competenze dell'NSC in materia di prevenzione, preparazione e gestione delle crisi cibernetiche, hanno rafforzato il ruolo del DIS, ponendolo al centro dell'architettura nazionale di cybersecurity.
Il tuo nemico può essere in ogni luogo, a non più di un centinaio di millisecondi da te e un singolo nemico, con una capacità cyber nella media, può effettuare nello stesso tempo attacchi verso migliaia di *asset* strategici di un Paese. Per questo occorre un piano operativo di coordinamento che sia flessibile, adattabile e con una catena di comando molto corta. Il settore con difese non adeguate diventa, infatti, l'anello debole dell'intero sistema Paese. Ai cittadini si richiede di mantenere un'adeguata forma di cyber-hygiene.
Il nuovo libro bianco sulla cybersecurity nasce con l'obiettivo di delineare un insieme di ambiti progettuali e di azioni trasversali che la comunità nazionale della ricerca ritiene essenziali a complemento e a supporto di quelli previsti nel DPCM Gentiloni.
La realizzazione dei progetti, data la diversità degli obiettivi e delle competenze necessarie, richiederà una particolare sinergia tra il mondo della ricerca, quello governativo e quello dell'industria, anche attraverso opportuni meccanismi di partnership pubblico-privato.
Le stime di queste grandezze non sono quasi mai fondate su metodi di rilevazione scientifici. Esistono alcune eccezioni. Nel Regno Unito il governo conduce un'indagine campionaria che abbraccia l'intero settore privato: essa mostra che poco meno di metà delle imprese britanniche è stata vittima di almeno un tentativo di attacco nell'ultimo anno. Nel nostro paese, la Banca d'Italia ha stimato che, tra settembre 2015 e settembre 2016, il 45% delle aziende nazionali è stata colpita da una qualche tipologia di attacco. I soggetti più a rischio sono le grandi imprese, gli esportatori e chi lavora in un settore ad alta intensità tecnologica.
Nello stesso universo di riferimento, nel 2016 la spesa in sicurezza informatica era modesta: l'impresa mediana destinava alla prevenzione degli attacchi appena 4.530 euro, ovvero il 15% della retribuzione lorda annuale di un lavoratore. I danni provocati dagli attacchi nella maggior parte dei casi determinano un impatto monetario diretto limitato; in Italia i costi di ripristino dei sistemi colpiti e le perdite superano i 50.000 euro solo in un caso su cento. La distribuzione dei costi è però fortemente asimmetrica: pochi grandi incidenti sembrano responsabili di una quota molto elevata dei danni economici complessivi.
Il rapporto dello studio legale Jones Walker Llp di New Orleans[5] mostra come gli attacchi informatici rappresentino un rischio per l'industria dello *shipping* a causa dell'impreparazione delle imprese. A fronte di un alto numero di attacchi è stato riscontrato fra gli operatori un falso senso di preparazione. La ricerca, fatta intervistando un campione di aziende degli Stati Uniti, ha messo in luce come l'80% delle grandi compagnie con oltre 400 dipendenti sia stata presa di mira nell'ultimo anno da un attacco informatico. Se si osserva l'intero campione senza considerare la dimensione, l'incidenza scende al 38%, con un 10% di attacchi riusciti. Questo significa che un'impresa dello *shipping* su dieci ha avuto danni da un cyberattacco nell'ultimo anno. A fronte di questo, il 69% del campione ha espresso fiducia nel fatto che l'industria marittima sia pronta a respingere gli attacchi informatici, cosa che, secondo lo studio legale, è un falso senso di sicurezza. Quello che preoccupa è che gli stessi operatori nel 64% dei casi, ammettano che la propria azienda non sia preparata a gestire le conseguenze commerciali, finanziarie, normative e relative alle pubbliche relazioni derivanti da un attacco informatico. Le

[5] "Maritime Cybersecurity Survey", Jones Walker LLP 2018

imprese medio-piccole sono quelle meno preparate, rispettivamente il 6% e il 19% delle piccole e medie imprese si dichiarano pronte ad un attacco. Queste mancherebbero delle protezioni fondamentali e sarebbero esposte ad enorme perdite. Il 92% delle piccole società e il 69% di quelle medie hanno affermato di non essere coperte da una polizza assicurativa contro il crimine informatico[6].

Non è ancora chiaro a tutti quanto siano diffuse le tecniche di attacco indiretto, che fanno leva sulla vulnerabilità di un soggetto per colpirne un altro. La presenza di migliaia di anelli deboli nella catena del valore si ripercuote sulla sicurezza del cyberspace nel suo complesso e pone le condizioni per il proliferare di incidenti su larga scala.

Il *Framework* Nazionale per la Cybersecurity[7] può essere adattato ai diversi contesti eterogenei presenti nel panorama nazionale tramite la creazione di apposite contestualizzazioni. Aziende di settori merceologici diversi hanno infatti, in ambito cyber, requisiti e criticità diverse e peculiari. Questo documento propone 15 controlli essenziali di cybersecurity, misure minime di sicurezza spiegate in modo semplice e facilmente attuabili, che possono essere adottati ed implementati da medie, piccole o micro imprese per ridurre il numero di vulnerabilità presenti nei loro sistemi e per aumentare la consapevolezza del personale interno.

L'innalzamento dei livelli di sicurezza delle piccole e micro imprese è un passaggio fondamentale per la messa in sicurezza delle filiere produttive. Un numero sempre maggiore di attacchi a grandi imprese capo-filiera viene infatti realizzato grazie a vulnerabilità presenti proprio nelle imprese parte delle loro filiere.

[6] The Meditelegraph, "Cybercrime in crescita, imprese poco preparate", Alberto Ghiara 31 ottobre 2018

[7] "Controlli Essenziali di Cybersecurity", CINI – Consorzio Interuniversitario Nazionale per l'Informatica, Marzo 2017