ISPI DOSSIER Agosto 2019

LA GESTIONE DEI RISCHI NELLO SPAZIO CIBERNETICO

a cura di **Fabio Rugge, Samuele Dominioni**

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
Agosto 2019

COS'È IL "RISCHIO CYBER" E PERCHÉ CE NE DOBBIAMO PREOCCUPARE

Corrado Giustozzi
AGID, Enisa

Il rischio cibernetico è comparso solo di recente nell'elenco delle grandi minacce per la nostra società, ma è già saldamente attestato ai vertici della classifica. Ad esempio, nella lista dei primi dieci grandi rischi globali pubblicata dal World Economic Forum[1] l'attacco cibernetico su larga scala si trova attualmente al quinto posto fra quelli a maggiore probabilità di accadimento (al primo vi sono gli eventi meteorologici catastrofici) ed al settimo fra quelli a maggiore impatto (al primo vi sono le armi di distruzione di massa).

Ma cosa si intende per "rischio cibernetico"? Perché è balzato all'attenzione generale solo adesso? E che tipo di minacce porta effettivamente con sé?

Il concetto di rischio cibernetico è strettamente associato a quello di "spazio cibernetico" o cyberspace[2], un termine nato nella fantascienza degli anni Ottanta dello scorso secolo e poi sdoganato dapprima in ambito militare e quindi in termini generali. Esso indica il dominio globale risultante dall'interconnessione di tutte quelle reti, eterogenee ed interdipendenti, fatte di sistemi di elaborazione delle informazioni e di infrastrutture di comunicazione. A questo dominio, ancorché comunemente percepito come una sorta di dimensione immateriale, viene oramai unanimemente riconosciuto uno status di realtà oggettiva e concreta, soggetta addirittura alla legittima sovranità degli stati, pur se tuttora in assenza di specifiche normative o accordi internazionali e perfino di una definizione condivisa della sua stessa natura.

Non vi sono dubbi tuttavia che il ciberspazio, comunque lo si voglia intendere, sia oramai divenuto un elemento cruciale per il funzionamento e la stessa sopravvivenza della nostra società: dai sistemi di

Corrado GIUSTOZZI, Cybersecurity expert at Agenzia per l'Italia Digitale for the development of the governmental CERT for the Public Administration (CERT-PA). Member of the Permanent Stakeholders' Group at ENISA.

elaborazione e trasmissione delle informazioni dipendono infatti tutti i servizi essenziali per la vita quotidiana dei cittadini e delle imprese, per lo sviluppo ed il sostegno dei sistemi economici e finanziari, per il funzionamento della cosa pubblica e addirittura per l'esercizio stesso della democrazia. Sono dunque naturali e fondate le preoccupazioni riguardanti i possibili impatti che eventuali interruzioni e malfunzionamenti all'interno del dominio cibernetico potrebbero avere sulla società.

Purtroppo il dominio cibernetico è caratterizzato da debolezze tecniche e strutturali intrinseche che lo rendono particolarmente vulnerabile nei confronti di azioni malevole, deliberatamente indirizzate ad alterarne il funzionamento a scopo doloso. Ciò è conseguenza sia di un antico retaggio storico che caratterizza la progettazione stessa delle sue componenti più fondamentali, sia della ben più recente tendenza alla forsennata e spesso dissennata interconnessione di tutto con tutto.

Il primo fattore risale alla genesi stessa del cyberspace, ossia ad ARPAnet: la sperimentazione, voluta dall'ente militare statunitense per la ricerca avanzata (DARPA) ma condotta da un pugno di università californiane, grazie alla quale, fra la fine degli anni Sessanta e inizio anni Settanta, vennero sviluppati i protocolli e le tecnologie su cui si fonda internet ancora oggi. Da quella iniziativa nacque il modello di una rete aperta, inclusiva, democratica, paritetica, universale: una rete illuminista e ottimista, che avrebbe consentito ai partecipanti (principalmente, se non esclusivamente, scienziati) di condividere liberamente e facilmente idee, informazioni, dati, servizi, a beneficio della comunità. Forse uno specchio dei tempi, in particolare della controcultura hippie imperante in quel periodo e in quelle località, ma questo era la rete nella mente di coloro che l'hanno immaginata e plasmata: uno strumento cooperativo senza limitazioni imposte artificialmente. Basti pensare che la maggior parte dei protocolli tecnici fu deliberatamente progettata escludendo i concetti di autenticazione o autorizzazione: chiunque poteva connettersi a qualsiasi server altrui ed ottenere anonimamente informazioni tecniche o di servizio (dall'ora esatta alla lista di utenti presenti e/o attivi sul sistema), ma anche usarlo per inviare email senza bisogno di autenticarsi[3], perché anche la spedizione della posta era considerata un servizio della e per la comunità. Questa filosofia di progettazione, che al giorno d'oggi definiremmo quantomeno naïf, ha fatto sì che internet sia nato e si sia sviluppato senza alcun meccanismo intrinseco di sicurezza e autoprotezione, cosa che scontiamo tutt'ora. Di fatto ogni moderno sistema di sicurezza relativo ad internet non è altro che un retrofit il quale cerca di colmare le carenze progettuali inserite ab origine nelle fondamenta tecniche che regolano il funzionamento della Rete.

Il secondo fattore è assai più recente, e deriva da quella sorta di "effetto valanga" per cui la massa critica di oggetti collegati in rete ha preso ad aumentare esponenzialmente grazie alla diffusione stessa della rete, in una sorta di circolo vizioso che si autoalimenta a velocità sempre crescente. Così oggetti che non erano stati progettati per essere connessi, quali ad esempio i sistemi di controllo industriale (ICS/SCADA), dal giorno alla notte sono stati messi in rete: spesso per esigenze di riduzione dei costi nella gestione degli impianti[4], un po' per semplice moda,

raramente per reali esigenze tecniche; e quasi mai ciò è stato fatto nel rispetto di misure anche minime di sicurezza[5]. Questo scenario si sta purtroppo aggravando con l'arrivo dell'internet delle cose e della nuova generazione di dispositivi elettronici consumer cosiddetti "smart": un'infinità di oggetti economici, dotati di grande capacità di calcolo, sempre connessi alla rete, e caratterizzati da un livello bassissimo di sicurezza intrinseca, che sta popolando le nostre città e le nostre case.

La concomitanza di tutti questi fattori fa sì che oggi il cyberspace sia sempre più facilmente e frequentemente oggetto di attacchi organizzati, provenienti da varie tipologie di attori (criminalità, terrorismo, governi) e caratterizzati da varie finalità (sabotaggio, spionaggio, truffa, estorsione ecc.), a danno sia di privati cittadini che di organizzazioni e addirittura stati. Non a caso la recente dottrina militare è concorde nel conferire al cyberspace il ruolo di vero e proprio teatro di operazioni, definendolo come "quinto dominio" della conflittualità[6] dopo terra, acqua, cielo e spazio.

La minaccia cibernetica è inoltre particolarmente subdola in quanto gli "attacchi" non sono quasi mai tali, ossia palesi: nella maggior parte dei casi si tratta invece di infiltrazioni silenti realizzate mediante malware che, inoculati nelle reti e nei sistemi della vittima, vi permangono per mesi o anni. La preoccupazione è dunque che le infrastrutture critiche di un paese possano essere minate da "bombe logiche" latenti, che attendono solo il momento giusto per attivarsi e colpire. E, grazie all'interconnessione globale, gli obiettivi potrebbero non essere solo logici ma anche fisici: centrali di generazione e sistemi di dispacciamento dell'energia, infrastrutture di trasporto ferroviario o aereo, dighe e impianti industriali, e così via. In ultima analisi, un attacco cibernetico potrebbe oramai anche causare perdite umane dirette se condotto verso i cosiddetti sistemi ciber-fisici che sempre più sono presenti nello scenario socio-industriale contemporaneo.

Il rischio cyber dunque non può più essere sottovalutato. L'Europa sin dal 2013 ha attivato una serie di iniziative coordinate che, partendo dalla definizione di una cyberstrategy comune, ha portato alla creazione di centri nazionali di prevenzione e risposta agli incidenti (CERT e CSIRT) ed all'emissione di una normativa coordinata per la protezione cibernetica dei servizi essenziali (Direttiva NIS). Ma molto rimane ancora da fare. La gestione del rischio cibernetico richiede infatti una risposta coordinata che si snodi non solo sul piano tecnico ma anche su quello legale, del fattore umano, socio-economico e politico: in particolare è cruciale un'efficace cooperazione internazionale, perché la minaccia è intrinsecamente transnazionale.

La recente istituzione di una vera e propria agenzia permanente europea per la cybersecurity, avvenuta affidando ad ENISA – l'agenzia dell'UE per la sicurezza informatica – un mandato più ampio e maggiori risorse, è un altro passo fondamentale per razionalizzare e centralizzare le iniziative di prevenzione e contrasto della minaccia cibernetica nell'Unione. In questo suo nuovo ruolo ENISA potrà infatti ulteriormente rafforzare le già attive cooperazioni con Eurojust, CEPOL ed Europol/EC3 al fine di intensificare l'azione europea anche sul piano dei risvolti giuridici e delle attività di *law enforcement.*

L'Europa insomma sta facendo la sua parte con ammirevole sforzo e unitarietà d'intenti, ma la partita è complessa e si gioca su molti tavoli, nazionali ed internazionali. I portatori di interessi sono molteplici, nel pubblico e nel privato, ed ognuno dovrà contribuire all'azione complessiva perché solo con la collaborazione di tutti si otterranno i risultati auspicati.

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
Agosto 2019

SPAZIO CIBERNETICO: LE MINACCE, I RISCHI E LE OPPORTUNITÀ PER L'ITALIA

Luigi Martino
Scuola Superiore Sant'Anna di Pisa

Il Documento di Sicurezza Nazionale del 2018 – allegato alla relazione annuale che i Servizi di Intelligence italiani presentano al parlamento – rappresenta un'ottima fonte primaria dalla quale attingere per riuscire a comprendere l'entità delle minacce cyber in Italia. Nel documento infatti si sottolinea, in modo incontrovertibile, come la minaccia cyber rappresenti un serio rischio per gli interessi economici, scientifici e militari del nostro paese. Infatti, dall'analisi dei dati contenuti nel Documento affiora chiaramente che le azioni malevoli protratte dal cyberspazio hanno avuto un incremento esponenziale nell'ultimo anno. Infatti, il documento del 2018 recita:

Emerge un numero complessivo di azioni ostili più che quintuplicato rispetto al 2017, prevalentemente in danno dei sistemi informatici di pubbliche amministrazioni centrali e locali (72%). Un'analisi più approfondita degli eventi che hanno interessato i soggetti pubblici attesta un incremento pari a oltre sei volte (+561%) rispetto all'anno precedente. È stato rilevato, in particolare, un sensibile aumento di attacchi contro reti ministeriali (24% delle azioni ostili, in aumento di 306 punti percentuali) e contro infrastrutture IT riconducibili ad enti locali (39% del totale del periodo in esame, con una crescita in termini assoluti pari a circa 15 volte).[1]

L'allarme lanciato dai Servizi di Intelligence italiani evidenzia, allo stesso tempo, un ulteriore dato allarmante, ovvero che le minacce provenienti dal mondo cyber hanno raggiunto livelli di sofisticatezza tali per cui ad essere in pericolo non sono più "esclusivamente" i meno avvezzi ai rischi provenienti dal cyberspazio, ma l'intero apparato della pubblica

„Luigi MARTINO, Phd student 'Human rights and global politics' all'Istituto Dirpolis della Scuola Superiore Sant'Anna di Pisa,"

amministrazione centrale e locale.[2]

Si evidenzia altresì come l'Italia sia sempre più a rischio di minacce "sistemiche", ovvero attività malevole condotte "per procura" ed effettuate da attori non statali i quali, attraverso attacchi informatici mirati contro attori pubblici (pubblica amministrazione o funzionari pubblici) e attori privati (che gestiscono o possiedono infrastrutture critiche) prediligono target strategici, attraverso soprattutto l'esfiltrazione di informazioni sensibili e riservate.[3]

Alla luce di quanto detto sopra, le priorità relative alla protezione della competitività, della sicurezza nazionale e della stessa sovranità statale assumono quindi elevata rilevanza strategica (e quindi politica), visto che la minaccia di tipo cibernetico ha assunto contorni sofisticati, così come sempre più spesso le azioni cyber vengono strumentalizzate a fini di competizioni intra e inter nazionale.

Nello specifico, le sfide provenienti dal mondo cyber hanno caratteristiche eterogenee, di provenienza esogena ed endogena. Per quanto concerne le prime è del tutto evidente che, come si evince da recenti riscontri, nella "quinta dimensione della conflittualità"[4] siano sempre più labili i confini tra amico e nemico, alleato e avversario.

L'Italia, in questo senso, si trova a dover fronteggiare una crescente perniciosità delle azioni cyber le quali, grazie alla plausible deniability, riescono a garantire un elevato livello di anonimato con relativa immunità rispetto all'attribuzione della responsabilità. Non a caso da varie ricerche è emerso come vi sia un interesse sempre maggiore nei confronti del know-how italiano, il quale viene minacciato da crescenti campagne di spionaggio informatico dedito anche alla sottrazione di segreti industriali e brevetti innovativi.

La crescita poi delle minacce esogene che interessano l'Italia va messa in correlazione con lo sviluppo innovativo e tecnologico che pone sfide di natura "sistemica", ovvero relative alla capacità di sviluppare competenze di difesa di un perimetro che di fronte alla diffusione dell'intelligenza artificiale, del 5G e dell'Internet of Things (IoT), diventa sempre più ampio, interconnesso e interdipendente. Basti pensare alla sfida relativa al 5G (sfida non solo politico-commerciale ma anche tecnica), nella quale possono emergere problemi rispetto al Regolamento Europeo per la Protezione dei Dati (GDPR), qualora tali dati venissero gestiti da infrastrutture che fanno capo a paesi terzi, i quali non hanno nessun obbligo nei confronti del menzionato regolamento. E ancora la minaccia relativa al 5G rispetto alla sempre maggiore labilità esistente tra settore civile e militare e quindi rispetto alle capacità di difendere il perimetro vitale della riservatezza delle informazioni.

In quest'ottica si inseriscono le sfide endogene, fra cui la questione "culturale" della cyber security che, ancora oggi, stenta ad affermarsi in Italia. Come già sottolineato, l'Italia dovrebbe affrontare i rischi cyber attraverso un'elevata capacità di governare le minacce tramutandole in opportunità per incrementare la propria competitività sul piano internazionale.[5]

Tuttavia, la bassa diffusione della cultura della cyber security in Italia mette in serio pericolo la tenuta del sistema paese.

Lo dimostrano i dati del Rapporto Clusit, i quali mettono in evidenza come gli attacchi cyber (soprattutto di tipo criminale) abbiano subito un salto "quantico" e un trade-off negativo fra azioni criminali e consapevolezza degli utenti.[6]

Un'altra sfida endogena per l'Italia è rappresentata dalla capacità dei decisori politici e istituzionali di tramutare la cyber security da minaccia a opportunità economica, culturale e industriale per il sistema paese.

Nel tentativo di fronteggiare le minacce esogene ed endogene, l'Italia ha messo in pratica le indicazioni contenute nel Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico e gli obiettivi operativi previsti dal "Piano Nazionale", avviando così una serie di azioni concrete sui rischi provenienti dall'arena digitale con il prezioso contributo del comparto intelligence e, in particolare, del Nucleo per la Sicurezza Cibernetica (coordinato dal Vice Direttore del DIS con delega alla cyber security). Tra le azioni, vi sono:

La realizzazione di un "perimetro di sicurezza nazionale cibernetica", volto ad elevare i livelli di sicurezza degli assetti vitali del paese;

La costituzione di un ulteriore gruppo di lavoro, volto ad individuare linee guida per un procurement "sicuro" di prodotti e servizi ICT per la PA, coordinato dall'Agenzia per l'Italia Digitale (AgID), al quale hanno aderito, oltre ai componenti NSC, anche Consip;

L'avvio di una collaborazione con il MiSE per la creazione – in conformità alle normative italiane ed europee – del Centro di Valutazione e Certificazione Nazionale (CVCN) per la verifica delle condizioni di sicurezza delle soluzioni ICT destinate al funzionamento di reti, servizi delle infrastrutture critiche, nonché di ogni altro operatore per cui sussista un interesse nazionale.[7]

Affinché queste azioni di contrasto dei rischi e mitigazione delle minacce possano realizzarsi è necessario, oltre alla creazione di un quadro di politiche create ad hoc, anche la capacità di comprendere che, rispetto alle minacce provenienti dal cyberspazio, deve vigere una situazione "win-win" tra enti pubblici, aziende e società civile laddove tutti gli attori in campo ricevano il beneficio dalla collaborazione sotto forma di partnership attraverso un approccio di sicurezza partecipata.

1. Cfr. Presidenza del Consiglio dei Ministri, Sistema di Informazione per la Sicurezza della Repubblica, "Documento di Sicurezza Nazionale", in Relazione sulla politica dell'informazione per la sicurezza 2018.

2. Ibidem

3. Ibidem

4. Luigi Martino, La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale, in Politica & Società, Fascicolo 1, gennaio-aprile 2018.

5. Cfr. Luca Zorloni, Sicurezza informatica, la strategia dell'Italia contro gli attacchi hacker, in Wired

6. Cfr, Associazione Italiana per la Sicurezza Informatica, Rapporto Clusit 2019.

7. Cfr. Presidenza del Consiglio dei Ministri, op. cit.

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
Agosto 2019

L'ARCHITETTURA ITALIANA DI CYBERSECURITY

Samuele Dominioni
ISPI

La capacità dello stato di gestire i rischi cibernetici sta diventando una delle priorità strategiche per le amministrazioni pubbliche al fine di assicurare il giovamento e il beneficio dei vantaggi e delle opportunità derivanti da uno spazio cibernetico sicuro ai cittadini e alle imprese. Infatti, alla luce delle attuali rivoluzioni digitali in corso (ad es. industria 4.0, smart cities) la tutela e la protezione cibernetica è essenziale per la prosperità della nostra economia. Tuttavia, gestire e garantire la sicurezza dello spazio cibernetico non è come proteggere il paese in un qualsiasi altro dominio strategico (come terra, mare o cielo). Infatti, esso si contraddistingue per una serie di caratteristiche che lo rendono unico rispetto agli altri terreni di difesa. Esso è un dominio completamente costruito dall'uomo, estremamente complesso e interconnesso, dove le tradizionali categorie di spazio e tempo non trovano applicabilità e dove la minaccia è asimmetrica, rendendolo un terreno particolarmente pericoloso e arduo da difendere. Come descritto da Luigi Martino, le minacce che riguardano il nostro paese sono sempre più sofisticate. Per far fronte a ciò, l'Italia ha sviluppato nel corso degli anni documenti programmatici e operativi al fine di erigere un sistema in grado di gestire e rispondere alle minacce derivanti da questo particolare dominio.

La struttura italiana di cybersecurity è relativamente recente. Tutto è cominciato meno di dieci anni fa, dall'approvazione nel 2010 di una relazione del COPASIR (il Comitato parlamentare che controlla i servizi di informazione) sulla necessità di proteggere anche a livello cibernetico le infrastrutture critiche. Da ciò è seguito il primo essenziale tassello, la

Samuele DOMINIONI is a Research Fellow at the ISPI Centre on Cybersecurity, in partnership with Leonardo.

legge 133 del 2012 nella quale si menzionava il necessario rafforzamento della sicurezza informatica nazionale al fine di fronteggiare efficacemente i pericoli della minaccia cibernetica e assegnava al Dipartimento Informazioni per la Sicurezza (DIS) il coordinamento delle attività informative indirizzate alla protezione delle infrastrutture critiche e dello spazio cibernetico del paese. Successivamente, il DPCM Monti del gennaio 2013 ha definito l'architettura nazionale di sicurezza cibernetica. Al decreto è seguito il Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico e il Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica pubblicati dalla Presidenza del Consiglio dei Ministri nel dicembre dello stesso anno. In questi documenti, che costituivano le prime fondamenta della cybersecurity nazionale, si identificava nella Presidenza del Consiglio dei Ministri l'apice dell'architettura nazionale dove veniva incardinato nell'Ufficio del Consigliere Militare (UCM) il Nucleo per la Sicurezza Cibernetica (NSC), si definivano i ruoli degli altri soggetti pubblici (tra cui quello del Ministero degli Affari Esteri che ha un Coordinatore per la sicurezza cibernetica, dove da poco si è insediata la ministra plenipotenziaria Laura Carpini) permettendo all'Italia di sopperire ad una grave carenza istituzionale in materia. Tuttavia, a seguito della necessità di razionalizzare e rendere più agevole il processo decisionale all'interno dell'organigramma istituzionale e in previsione di trasporre le indicazioni derivanti dalla direttiva europea sulla sicurezza dei network (NIS – Network Information Security), nel febbraio del 2017 il governo Gentiloni ha emanato un nuovo decreto volto alla riorganizzazione dell'architettura nazionale di cybersecurity a cui seguì il Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica del marzo 2017.

Al centro della governance per la cybersecurity il decreto ha posizionato il Dipartimento Informazioni per la Sicurezza che è l'organo per assicurare unitarietà nella programmazione della ricerca informativa, nell'analisi e nelle attività operative delle agenzie intelligence AISE e AISI. Il DIS è il focal point unico per quanto concerne l'armonizzazione richiesta dalla direttiva NIS con gli altri paesi europei e presiede il Nucleo Sicurezza Cibernetica (traferito dall'UCM). Quest'ultimo è un board intergovernativo che svolge funzioni di gestione delle crisi cibernetiche e di raccordo tra le diverse componenti dell'architettura istituzionale. Con il decreto del 2017 il vice direttore del DIS, oltre ad avere incarico di coordinamento interministeriale, presiede il NSC che è composto anche dal consigliere militare e da un rappresentante rispettivamente del DIS, dell'AISE, dell'AISI, del Ministero degli affari esteri, del Ministero dell'interno, del Ministero della difesa, del Ministero della giustizia, del Ministero dello sviluppo economico, del Ministero dell'economia e delle finanze, del Dipartimento della protezione civile e dell'Agenzia per l'Italia digitale.

Nel campo della prevenzione e della preparazione ad eventuali situazioni di crisi cibernetica, il Nucleo: a) promuove la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte delle amministrazioni e degli operatori privati interessati e l'elaborazione delle necessarie procedure di coordinamento interministeriale, in raccordo con le pianificazioni

di difesa civile e di protezione civile; b) mantiene attiva, 24 ore su 24, 7 giorni su 7, l'unità per l'allertamento e la risposta a situazioni di crisi cibernetica; c) valuta e promuove, in raccordo con le amministrazioni competenti per specifici profili della sicurezza cibernetica, procedure di condivisione delle informazioni, anche con gli operatori privati interessati, ai fini della diffusione di allarmi relativi ad eventi cibernetici e per la gestione delle crisi; d) acquisisce le comunicazioni circa i casi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrità significativi ai fini del corretto funzionamento delle reti e dei servizi dal Ministero dello sviluppo economico, dagli organismi di informazione per la sicurezza, dalle forze di polizia e, in particolare, dal Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) nell'esercizio dei servizi di protezione informatica delle infrastrutture critiche. Infine, il decreto Gentiloni ha introdotto la necessità della certificazione nazionale per quanto riguarda la valutazione "delle componenti ICT destinate ad essere impiegate nei sistemi di soggetti titolari di funzioni critiche o strategiche", che ha poi trovato realizzazione nell'istituzione del Centro di valutazione e certificazione nazionale (CVCN) avvenuta nel marzo del 2019.

L'architettura nazionale di cybersecurity è stata inoltre coinvolta dal recepimento della Direttiva NIS avvenuto nel 2018. L'Unione europea riconobbe la disomogeneità delle normative riguardanti la sicurezza cibernetica nei diversi paesi membri e decise pertanto di delineare delle minime disposizioni in materia di pianificazione, scambio di informazioni, cooperazione e obblighi comuni di sicurezza con particolare riferimento agli operatori di servizi essenziali e ai fornitori di servizi digitali. L'Italia, come gli altri paesi membri, fu chiamata ad indicare quali fossero gli operatori di servizi essenziali e digitali dai quali dipende la società e l'economia del paese (ad esempio quelli del settore energetico, dei trasporti, ma anche di quello finanziario e sanitario). Inoltre, la direttiva rese obbligatorio l'istituzione di un unico Computer Security Incident Response Team, detto CSIRT, in ogni paese membro, al quale vennero affidati compiti di natura tecnica nella prevenzione e risposta ad incidenti informatici da svolgere in cooperazione con gli altri CSIRT europei. Lo CSIRT italiano è stato già formalmente costituito presso la Presidenza del Consiglio dei Ministri e andrà a sostituire i Computer Emergency Response Team (CERT) operanti presso l'Agenzia per l'Italia Digitale e il Ministero dello Sviluppo Economico.

Infine, pochi giorni è stato pubblicato in Gazzetta ufficiale il decreto legge in materia di perimetro di sicurezza nazionale cibernetica. Esso si riferisce in particolare a tutti quei servizi e operatori sia pubblici che privati che svolgono un ruolo cruciale per gli interessi dello Stato. In tal senso, vi possono essere delle sovrapposizioni con alcuni degli operatori dei servizi essenziali già soggetti alla Direttiva NIS ed in tal caso essi dovranno continuare ad ottemperare alle disposizioni previste da essa, aggiungendovi on top eventuali disposizioni previste dal perimetro di sicurezza nazionale cibernetica. La responsabilità di attuazione e vigilanza per quanto riguarda il perimetro sono condivise dal Ministero per lo Sviluppo Economico (per quanto riguarda le attività

che coinvolgono attori privati) e dalla Presidenza del Consiglio (per quanto riguarda le attività che coinvolgono il settore pubblico). La realizzazione del perimetro di sicurezza nazionale cibernetica necessiterà di ulteriori passaggi legislativi, e si prevede che sarà completato entro un anno dall'entrata in vigore del disegno di legge.

A ciò si affianca anche l'estensione del Golden Power per garantire la sicurezza delle nuove infrastrutture di telecomunicazione, in particolare quelle 5G. Stando al nuovo decreto gli attori pubblici e privati saranno soggetti anche a controlli sulle apparecchiature adottate dalle telco. I poteri speciali sono esercitati nella forma di imposizione di specifiche prescrizioni o condizioni ogniqualvolta ciò sia sufficiente ad assicurare la tutela degli interessi essenziali della difesa e della sicurezza nazionale. Per essere efficace il testo pubblicato in Gazzetta ufficiale il 21 settembre 2019, dovrà essere convertito in legge dal Parlamento entro 60 giorni.

Nel giro di pochi anni l'architettura nazionale per la sicurezza cibernetica si è sviluppata attorno a due aspetti cardine: la difesa della società e la protezione dello stato stesso. Proprio su quest'ultimo aspetto, peculiare rispetto ad altri casi, si riscontra la centralità di un attore, lo stato appunto, in un ambiente dove per molto tempo è rimasto marginale e con strumenti inadeguati per far fronte alle crescenti minacce cibernetiche.

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
Agosto 2019

L'ESPERIENZA DI LEONARDO NELLE PARTNERSHIP PUBBLICO-PRIVATO E PRIVATO-PRIVATO

Stefano Bordi
Leonardo
Eleonora Cordaro
Leonardo

Questo contributo intende presentare una serie di esempi di cooperazioni tra diversi tipi di organizzazioni, prendendo spunto, in particolare, dalle esperienze sviluppate da Leonardo, con l'obiettivo di mostrare come sia possibile trovare molteplici ambiti in cui definire collaborazioni utili alla protezione cyber di enti ed organizzazioni. Da ormai molti anni Leonardo opera infatti nel settore della cyber security concentrandosi non solo su attività di mercato, ma anche sullo sviluppo di relazioni di partnership sia in ambito pubblico-privato, sia privato-privato, collaborando, cioè, con modalità propositive ed inclusive, con organizzazioni governative e con aziende strategiche, siano esse clienti, fornitori, business partner o una combinazione di questi.

Leonardo è tra le prime dieci società operanti a livello globale e la prima a livello nazionale nell'Aerospazio, Difesa e Sicurezza (ADS), in Italia rappresenta inoltre il primo gruppo nel settore manifatturiero ad alta tecnologia con 30mila dipendenti (oltre 46mila nel mondo). I prodotti, le soluzioni e i servizi di Leonardo sono utilizzati in più di 150 Paesi nel mondo ed il gruppo investe per l'evoluzione del proprio portafoglio di tecnologie e prodotti circa il 12% dei ricavi, pari a 1,4 miliardi di Euro nel 2018.

I numeri sopra indicati ben rappresentano la sfida di un contesto globale, che presenta molteplici interlocutori con esigenze ed aspettative differenti, dalle agenzie governative, alle infrastrutture critiche. Un contesto caratterizzato dalla continua evoluzione dovuta sia all'introduzione ed all'integrazione di nuove tecnologie sia ad una sempre più marcata

Stefano BORDI is Senior Vice President Cyber & Information Security, Leonardo.
Eleonora CORDARO is Head of Marketing - Cyber Security Division, Leonardo.

domanda di nuovi modelli di business, con relativa trasformazione dei processi aziendali e delle relazioni con la catena di fornitura e con i business partner.

Per un'azienda che opera in questo particolare contesto, la messa in comune di informazioni, processi, modalità operative ed organizzative, così da poter condividere, a vari livelli, iniziative e progetti che sfruttino la collaborazione ed un mutuo scambio di esperienze e competenze è di fondamentale importanza ai fini della sicurezza interna. Ma Leonardo partecipa, in questo modo, anche alla creazione di valore per il sistema Italia, contribuendo a creare e supportare molti dei meccanismi messi in campo da istituzioni, associazioni, gruppi di interesse, think-tank, ecc. per arricchire il paese in termini sia di tecnologia che di cultura della protezione cibernetica.

LEONARDO E LE "PUBLIC-PRIVATE PARTNERSHIP"

Nell'ultimo decennio il ruolo del settore pubblico è cambiato e si è evoluto, soprattutto grazie alla rivoluzione digitale. Dal punto di vista normativo questa richiede ad amministrazioni ed agenzie uno sforzo consistente. La digitalizzazione ha fatto decadere il modello pubblico prevalente: centrale, pensante, esclusivamente pianificatore e separato dal campo, e lo ha di fatto riavvicinato ai soggetti pubblici sul territorio, ai soggetti privati e alla cittadinanza. Al fine di attivare questo nuovo modello integrato, interoperabile ed incentrato sull'utente, serve l'implementazione di strumenti innovativi di trasformazione digitale che consentano l'evoluzione tecnologica della pubblica amministrazione per offrire servizi evoluti e, al contempo, fertilizzare il territorio permettendone così la crescita e la trasformazione. Le convenzioni attivate dall'Agenzia per l'Italia Digitale (Agid) per l'implementazione delle linee guida della trasformazione digitale sicura del sistema paese ne rappresentano un esempio che oggi tende a crescere e che trova a livello internazionale applicazioni paragonabili e altrettanto convincenti.

Leonardo affianca ormai da molti anni la pubblica amministrazione per attività di mercato – ad esempio, l'erogazione di servizi di sicurezza infrastrutturale ed applicativa o la co-creazione di sistemi innovativi ed evoluti per la sicurezza cibernetica nazionale – ma anche per attività di sicurezza interna, con scambi informativi ed attività di ricerca e sviluppo riguardanti argomenti di Cyber Defence (threat intelligence, big data, digital forensics, etc.).

Dal punto di vista dei servizi, Leonardo ha contribuito negli anni alla costruzione della cyber security dell'amministrazione, dalla strategia alla governance, dalla protezione degli asset all'implementazione di sistemi e applicazioni intrinsecamente sicuri, funzionali all'erogazione dei servizi essenziali ai cittadini.

Al dominio della co-creazione appartiene invece, ad esempio, la realizzazione della Piattaforma di Esercitazione/Gaming e Cyber Training per il Centro Interforze Operativo Cibernetico della Difesa Italiana (CIOC). Si tratta di un ambiente per la verifica e la validazione di strumenti avanzati di cyber security e per la creazione di teatri realistici evoluti per esercitazioni, in cui collaborano realtà industriali e università. La piattaforma consente di simulare, in ambito nazionale, ma anche internazionale, la conduzione di operazioni cibernetiche multi-dominio integrate con attività di difesa tradizionali, anche a supporto dell'evoluzione delle dottrine militari.

Meccanismi similari di collaborazione sono stati sperimentati anche nei partenariati pubblico-privato, secondo il modello dei centri di competenza promossi dal ministero per lo Sviluppo Economico a supporto di Industria 4.0. Ad esempio, il Competence Center START 4.0 coinvolge numerose realtà del tessuto economico imprenditoriale ligur, sui temi della cyber security, della safety e della security: conservazione, protezione, e condivisione dei dati nel processo di progressiva digitalizzazione del paese e del suo sistema industriale, sicurezza del trasporto delle merci e delle infrastrutture, movimentazione di persone.

Nell'ambito della sicurezza interna, Leonardo ha promosso e promuove molte collaborazioni di natura istituzionale. Tra queste possiamo citare ad esempio il Dipartimento Informazioni per la Sicurezza (DIS), nell'ambito di una partnership pubblico-privato tra governo, industria e università per il laboratorio di Malware Analysis attivo presso il Polo Tecnologico del DIS. La pluriennale cooperazione ha consentito di sviluppare un prototipo tecnologico dedicato al servizio di cyber threat intelligence del Computer Emergency Response Team (CERT) aziendale il cui personale ha partecipato ai corsi organizzati dalla Scuola di Formazione del DIS con università e ricercatori accademici del settore. Altro esempio è il "Tavolo Tecnico Imprese", istituito sempre presso il DIS, con l'obiettivo di favorire lo scambio informativo relativo alla minaccia cibernetica, una preziosa collaborazione che ha consentito negli ultimi due anni di aumentare le capacità di rilevazione delle minacce grazie alla qualità degli indicatori di compromissione scambiati.

A livello internazionale, Leonardo ha attivato dal 2017 uno scambio di informazioni e indicatori mirati ai servizi di Cyber Security sulla base dell'Industry Partnership Agreement con la NCIA (NATO Communication and Information Agency) della NATO e partecipa a molteplici iniziative di partnership pubblico-privato relative alla creazione di network quali, ad esempio:

- ECSO - European Cyber Security Organization, di cui è membro fondatore, che rappresenta la controparte per l'Unione Europea per l'implementazione della "contractual PPP" per la Cyber Security ed include numerosi stakeholder tra cui grandi industrie, piccole e medie imprese, startup, centri di ricerca, università, utenti finali, e amministrazioni locali, regionali e nazionali degli stati membri dell'Unione Europea.
- SPARTA - Special Projects for Advanced Research and Technology in Europe, un progetto supportato dal programma Horizon 2020 con l'obiettivo di sperimentare le modalità di collaborazione dei centri di ricerca e delle eccellenze dei vari stati nazionali, nell'ottica di implementare una rete di centri di competenza
- ECCSA, European Center for Cyber Security in Aviation, organizzazione promossa da EASA, Agenzia europea per la sicurezza dell'aviazione, per definire gli impatti che le esigenze cyber avranno sulle normative del settore

LEONARDO E LE "PRIVATE – PRIVATE PARTNERSHIP"

Una partnership tra organizzazioni private in ambito cyber security può avere un impatto sulle capacità operative dei partner, sfruttando i punti forti di un'organizzazione e condividendoli tra

tutti gli interlocutori, ma può anche contribuire al miglioramento delle capabilities, attraverso un mutuo scambio di competenze ed esperienze.

Un esempio evidente è quello della condivisione degli indicatori di compromissione di un attacco che è stato rilevato: i partner avranno infatti la possibilità di prevenire e/o rispondere a tale attacco con cognizione di causa ed un immediato ed evidente vantaggio operativo, ma anche in assenza di un attacco diretto l'esperienza indiretta fornisce sempre interessanti spunti formativi e di conoscenza della minaccia.

Nell'ambito delle partnership privato–privato, Leonardo è attiva, in particolare, nello scambio di informazioni sulle minacce cibernetiche e sulla loro gestione e valutazione, con gruppi di lavoro sia nazionali – con partecipanti da diversi ambiti (es. istituzionale e governativo, aerospazio e difesa, telecomunicazioni, bancario/finanziario, etc.) – sia europei, ad es. MISP, THE HIVE. Questi Gruppi di Lavoro sono mirati alla condivisione di esperienze e competenze tra i vari partecipanti, così da poter incrementare e migliorare le proprie tecnologie, i propri processi e modelli organizzativi.

Leonardo inoltre coordina un importante gruppo di lavoro sulla tassonomia degli indicatori di compromissione, al quale partecipano esponenti di realtà industriali e governative, il cui obiettivo è la definizione della nomenclatura da attribuire agli indicatori della minaccia cyber. L'esigenza deriva dalla necessità di condividere in maniera responsabile tali informazioni in una rete (constituency) attraverso una piattaforma di scambio delle informazioni che abbia uniformità di linguaggio, coerenza nel riconoscimento ed identificazione delle caratteristiche di un indice di compromissione relativo alla minaccia cibernetica.

Per finire, Leonardo ha organizzato negli ultimi due anni un'esercitazione Cyber, denominata "CyberShield", a cui hanno preso parte, oltre alle strutture interessate di Leonardo stessa, molte realtà sia nazionali che internazionali, che si sono cimentate nei vari scenari proposti. L'iniziativa ha portato ad una consistente attività di networking con tutte le entità che vi hanno preso parte, ed è stata utile a testare le capacità di Incident and Threat Analysis dei team coinvolti. È stata anche un'importante vetrina per confermare come Leonardo sia un player di riferimento sulle tematiche di Cyber Security. A fronte di un interesse generale e del buon successo delle precedenti edizioni, è già in preparazione una terza edizione per il prossimo anno.

Da quanto sopra evidenziato risulta chiaro come per un'azienda del settore ADS, che svolge anche il ruolo di partner istituzionale per una serie di tematiche afferenti a difesa e sicurezza cyber, le collaborazioni con entità sia pubbliche che private rivestano un ruolo fondamentale. Risulta peraltro anche evidente che tutte le aziende strategiche o essenziali, soggette allo stesso livello di rischio delle istituzioni e potenzialmente altrettanto critiche nel loro impatto sulla vita nazionale, possono trarre beneficio da una stretta collaborazione a prevenzione della minaccia cyber.

Come spesso ripetuto, la cyber security è un dominio di conflitto asimmetrico e la collaborazione tra organizzazioni e tra organizzazioni ed istituzioni è una delle modalità con cui è possibile far sì che il piatto della bilancia penda un po' meno nella direzione degli attaccanti.

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
Agosto 2019

CYBER SECURITY: LE POLITICHE A SOSTEGNO DELLA LEADERSHIP AZIENDALE

Federica Maria Rita Livelli
GCSC Initiative and Secretariat

Una sempre maggiore tendenza alla digitalizzazione ed alla connettività e la diffusione delle soluzioni IoT (Internet ofThings), intelligenza artificiale e Machine Learning tra le organizzazioni comporta diversi rischi e diversi punti di vulnerabilità in termini di cyber security. Numerosi fatti di cronaca dimostrano come sia facile entrare nei sistemi di un'organizzazione, modificarne dati, rubarli e venderli, chiedere un riscatto, o sabotare l'organizzazione stessa.

La cyber security non risiede solo nell'adozione di un software specifico. Essa necessita di un insieme di approcci e processi che – unitamente all'implementazione di standard di principi di continuità operativa, risk management e resilienza – permettono ad ogni azienda di fronteggiare le nuove minacce degli attacchi informatici.

La strategia di cyber security deve diventare parte integrante della strategia dell'organizzazione. Per questo, è fondamentale avere una chiara consapevolezza di sé e delle attività svolte, capire come raggiungere gli obiettivi di sicurezza e stabilire le priorità. Una strategia chiara, ben documentata e di facile comprensione che, pur essendo basata sulla situazione contingente, possa essere modulata/ modificata in previsione di esigenze future.

La cyber security non può limitarsi alla gestione del rischio o essere affidata alla funzione informatica. È necessario un approccio olistico che permetta di rispondere prontamente quando un incidente si verifica e salvaguardare ogni realtà organizzativa che oggi, di fatto – per via dell'impiego sempre più massivo della tecnologia e la sua caratteristica "liquida" – si regge sulla cyber security.

Federica Maria Rita LIVELLI, Board Member BCI ITALY FORUM

La cultura della cyber security deve diventare parte dell'organizzazione quale competenza chiave, fino a diventare una modalità di differenziazione rispetto alla concorrenza: l'organizzazione deve dimostrare di essere un partner affidabile, in grado di salvaguardare i dati e le informazioni strategiche, sia proprie sia quelle dei propri clienti, evitando in questo modo di essere bersaglio di attacchi ed esercitare piani di cyber security, per reagire prontamente ed efficacemente

Sarà necessario sviluppare e mantenere una cultura di cyber security attraverso un'attività di training – continuo e ad hoc – utilizzando strumenti che permettano di testare regolarmente il grado di consapevolezza, misurare i risultati e tenere traccia dei progressi raggiunti. Esistono software sul mercato che sono in grado di effettuare simulazioni di attacco da cui scaturisce un'analisi delle aree deboli che richiedono un miglioramento in termini di protezione. Il personale può essere sottoposto a training per misurare il proprio grado di capacità di identificazione di attività di phishing (i.e. pharming, malware-based, tabnapping,ecc..), attraverso tipologie di software di phishing simulationattack. In questo modo sarà possibile aiutare il personale ad aumentare la propria conoscenza e consapevolezza della sicurezza informatica.

Il coinvolgimento del Top Management nel processo di diffusione della cultura della cyber security è comunque fondamentale per migliorare la sicurezza dei processi automatizzati e dei dati relativi alle aziende ed alle persone. Senza il committment e la sponsorship del livello apicale delle organizzazioni è difficile estendere la cultura della cyber security all'interno delle stesse e fare sì che tutto il personale venga coinvolto. Solo lavorando insieme si potranno ottimizzare gli sforzi per contrastare gli hacker, innalzare la soglia dell'attenzione e aumentare la consapevolezza dei vari attori che risulteranno maggiormente preparati a gestire i cyber attack.

Sarà necessario attuare policy atte a ridurre l'esposizione dei rischi informatici e stabilire modalità per rilevare rischi, per rispondere ad essi e per recuperare dopo attacchi o interruzioni; garantire, sempre ed ovunque, lo scambio sicuro di informazioni tra utenti autorizzati; essere conformi alle normative vigenti; stabilire la sicurezza della struttura informatica e modalità di controllo su tutte le connessioni ad internet; verificare che tutti i dipendenti siano debitamente formati sulle best practice in termini di cyber security, in modo da contrastare il rischio del "fattore umano".

Ne consegue che le organizzazioni, per diventare sempre più resilienti e pronte ad affrontare i rischi cyber e garantire quindi la propria continuità operativa, dovranno conoscere bene i propri obiettivi di business. Sarà necessario identificare sia le informazioni e i dati che risultano critici, sia gli asset da salvaguardare, oltre ad effettuare valutazioni di impatto a fronte di attacchi cyber per misurare gli impatti finanziari, normativi, reputazionali ed organizzativi. Si potranno impiegare sistemi di Vulnerability Assessment, Penetration Test, Human Factor Risk Assessment, Cyber health check, ecc. per identificare le vulnerabilità della propria organizzazione e del proprio network rivolgendosi ad aziende specializzate presenti sul mercato.

Ne deriva che, con l'implementazione di un Sistema

di Gestione di Continuità Operativa (Business Continuity Management System – BCMS), si sarà in grado di identificare i rischi associati ai servizi informatici ed implementare un programma di gestione di risposta all'incidente.

L'adozione di una serie di misure e procedure atte a ridurre o mitigare i rischi (i.e. piani di disaster recovery, comunicazione interna ed esterna, piani di supply chain e logistica, ecc...) contribuirà a garantire la continuità operativa dell'organizzazione. Ma non dimentichiamoci che sarà comunque necessario organizzare regolari sessioni di consapevolezza e sensibilizzazione a tutti i livelli aziendali; bisognerà altresì verificare attraverso test ed esercitazioni il livello organizzativo interno e quello esterno dei propri fornitori, il grado di preparazione e di resilienza delle stesse organizzazioni in caso di cyber attack. Si dovranno aggiornare gli antivirus ed i sistemi operativi, eseguire periodicamente i backup dei dati da ripristinare in caso di attacco, dedicarsi alle evoluzioni dei rischi cibernetici, identificare e colmare lacune e trarre insegnamento dalle lezioni apprese. In questo modo sarà più facile evitare o ridurre il rischio ed aumentare la resilienza degli attori coinvolti.

Concludendo, la diffusione della cultura di cyber security è fondamentale se si vuole garantire la resilienza delle organizzazioni e ridurre le conseguenze di un attacco cyber in termini di danni ai prodotti, perdita di fiducia da parte dei clienti, perdita di opportunità commerciali, danni ambientali e cali di produzione in uno o più stabilimenti. Inoltre, una maggiore diffusione di cultura della cyber security contribuirà ad innalzare la sicurezza di reti e sistemi e garantire una maggiore resilienza a livello di sistema paese.

ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
Agosto 2018

CYBER-POLIZZE A MISURA DI IMPRESA

Fabio Martinelli
Institute of Informatics and Telematics (CNR)
Albina Orlando
CNR Istituto per le applicazionil del calcolo "Mauro Picone" IAC- Napoli
Artsiom Yautsiukhin
Information Security Group, Institute of Informatics and Telematics (CNR)

In base al rapporto Allianz Risk Barometer 2019 realizzato da Allianz Global Corporate & Speciality (AGCS)[1], per la prima volta i rischi informatici affiancano quello da interruzione di attività in cima alla classifica dei rischi più temuti dalle aziende di tutto il mondo. La criminalità informatica costa circa 600 miliardi di dollari all'anno, rispetto ai 445 del 2014. Un costo triplo di quello dovuto a catastrofi naturali, che è di 200 miliardi di dollari.

In questo scenario la Cyber Insurance riveste un ruolo fondamentale, in quanto è finalizzata a proteggere il patrimonio aziendale dal cyber risk. Oltre ad essere uno strumento per trasferire parte del rischio cibernetico e attenuarne l'impatto finanziario, la Cyber Insurance rappresenta uno stimolo affinché le aziende incrementino gli investimenti in cyber security. Ciò è dovuto innanzitutto al fatto che adeguati investimenti in sicurezza possono talvolta incidere sull'ammontare del premio. Inoltre, per poter accedere ad alcune offerte assicurative, spesso le aziende sono tenute all'aggiornamento dei sistemi IT nonché all'adozione di soluzioni di sicurezza adeguate.

Il primo mercato mondiale per la Cyber Insurance è quello degli Stati Uniti seguito dall'Europa e dall'Asia, che è in forte crescita. In Europa, i principali acquirenti di polizze cyber sono le grandi aziende e, in particolare, quelle che operano nel settore sanitario, in quello dell'educazione e nei settori delle telecomunicazioni e media. La ragione risiede nel fatto che si tratta di aziende che gestiscono una grande quantità di dati sensibili. Le Pmi (piccole e medie imprese) mostrano un interesse sempre maggiore nei confronti di questa tipologia di polizze.

Fabio MARTINELLI is a senior researcher of Institute of Informatics and Telematics (IIT) of the Italian National Research Council (CNR)
Albina ORLANDO is a Researcher at the CNR Istituto per le applicazioni del calcolo "Mauro Picone" IAC Napoli.
Artsiom YAUTSIUKHIN is a researcher at CNR Information Security Group

Si evidenzia, però, che la scarsa conoscenza e/o la sottovalutazione delle proprie esposizioni, la scarsa comprensione delle coperture dovuta a un basso livello di standardizzazione delle polizze e talvolta all'impreparazione degli intermediari assicurativi e, infine, i costi elevati, rappresentano certamente un ostacolo alla "conversione" del sopracitato interesse in acquisto vero e proprio della polizza. Una quota emergente di mercato è quella relativa ai singoli individui e alle famiglie, sempre più esposti a truffe informatiche e furti di identità. Un segmento, questo, ritenuto molto interessante e sul quale in Europa hanno iniziato a entrare diversi operatori del settore.

Per quanto riguarda l'offerta, le coperture cyber prevedono due modalità: come altre polizze tradizionali, tipicamente polizze RC Professionali e polizze multirischio per le PMI; o con contratti stand-alone. Esse coprono danni subìti dall'assicurato (danni derivanti da interruzione del network, cyber estorsioni, furto dati, ripristino dei dati), danni a terzi (danni dovuti a violazione dei dati e ad interruzione di network, danni da responsabilità civile, violazione diritti d'autore). Sono offerti, inoltre, altri benefit quali: risposta all'evento (assistenza legale, investigazioni forensi, supporto di esperti IT), gestione dell'evento cyber (servizi per tutelare l'immagine aziendale, investigazioni tecniche forensi), e fondo per il pagamento di informazioni.

Un forte stimolo agli investimenti in sicurezza e alla crescente domanda di protezione verso i rischi cyber è certamente stata l'entrata in vigore del GDPR (General Data Protection Regulation) che ha introdotto, a partire dal maggio 2018, importanti novità riguardo la violazione informatica dei dati nei paesi dell'Unione Europea cambiando radicalmente l'impostazione dell'apparato sanzionatorio.

Nel 2018 l'European Insurance and Occupational Pensions Authority ha pubblicato un rapporto basato su un sondaggio cui hanno partecipato 13 imprese (assicuratrici e riassicuratrici) con sede in Italia, Germania, Regno Unito e Svizzera. Le principali criticità evidenziate dalle compagnie di assicurazione hanno un nucleo centrale rappresentato dal bisogno diffuso di una più profonda comprensione del cyber risk. I maggiori ostacoli, in tal senso, sono sia esogeni (mancanza di dati sufficienti per le stime, natura sistemica dei potenziali eventi dannosi) che intrinsechi al problema (scarsa informazione sui rischi e carenza di assicuratori specializzati). Da ciò derivano la difficoltà di quantificare opportunamente i rischi con la conseguente sottostima del premio, la mancanza di adeguate coperture riassicurative e il pericolo di sottovalutare i silent risks. Questi ultimi sono relativi alla possibilità che un assicuratore si ritrovi a indennizzare dei sinistri derivanti da cyber risks su una polizza non pensata per quello scopo.

Per concludere, citiamo un'indagine realizzata da Office Automation che ha analizzato l'offerta di dieci compagnie assicuratrici operanti sul mercato italiano: AIG, Cattolica Assicurazioni, Groupama, HDI Global, Helvetia, ITAS Assicurazioni, Reale Mutua, Sara, Unipol e Zurich Insurance. Anche se mancano all'appello grandi compagnie come Generali, Axa, Allianz che offrono coperture assicurative per il cyber risk, il rapporto restituisce una fotografia esaustiva dell'offerta di Cyber Insurance in Italia.

Fino ad ora, le polizze erano rivolte soprattutto a grandi aziende. La tendenza, oggi, è quella di

soddisfare anche le necessità delle Pmi, che rappresentano la vera anima del tessuto industriale italiano. L'offerta è rivolta anche a studi professionali di piccole dimensioni e, talvolta, alla Pubblica amministrazione. I settori interessati vanno dal manifatturiero all'alberghiero. I danni per i quali si offre copertura sono sia quelli da interruzione di attività dovuta al blocco dei sistemi informatici, che quelli cagionati a terzi, come la perdita di dati e informazioni e la violazione della privacy.

Una considerazione fondamentale che emerge, è la necessità che Cyber Insurance e sicurezza informatica operino in sinergia, onde evitare che il ricorso all'assicurazione sia soltanto un palliativo.

1. Allianz Risk Barometer. Top business risks for 2019. Allianz Global Corporate & Speciality (AGCS), Gennaio 2019.