Cybersecurity Trends

Edizione italiana, N. 1 / 2017

Manifesto italiano di Coordinated Vulnerability Disclosure

INTERVISTA VIP:

Gian Carlo CASELLI

Carla LICCIARDELLO

Global Cyber Security Center

Speciale Italia: sicurezza nel mondo digitale

Global Cyber Security

La Fondazione GCSEC è un'organizzazione senza scopo di lucro, creata per promuovere la sicurezza informatica in Italia e nel resto del mondo. Il Centro, fondato e finanziato da Poste Italiane, ha sede a Roma e collabora con Istituzioni Italiane e Internazionali Governative, enti privati, istituti di ricerca e organismi internazionali.
La missione della Fondazione è quella di sviluppare e diffondere la conoscenza e la consapevolezza sulla sicurezza informatica, creando le condizioni per migliorare le capacità, le competenze, la cooperazione e la comunicazione tra i diversi attori coinvolti nell'uso e nella protezione di Internet.

Information Sharing
Creazione di modelli di information sharing pubblico - privato

Threat Intelligence
Analisi di modelli di attacco e delle tecnologie necessarie a velocizzare l'analisi stessa

Sensibilizzazione
Campagne di sensibilizzazione multi-livello

Formazione
Attività di formazione a corsi di specializzazione e master

Fondazione Global Cyber Security Center
Viale Europa, 175 – 00144 Roma
www.gcsec.org

GLOBAL CYBER SECURITY CENTER

autore: Nicola Sotira

BIO

Nicola Sotira è Direttore Generale della Fondazione Global Cyber Security Center GCSEC e responsabile della Sicurezza delle Informazioni in Poste Italiane divisione di Tutela Aziendale, con la responsabilità della Cyber Security e del CERT. Lavora nel settore della sicurezza informatica e delle reti da oltre venti anni con un'esperienza maturata in ambienti internazionali. Contesti nei quali si è occupato di crittografia e sicurezza di infrastrutture, lavorando anche in ambito mobile e reti 3G. Ha collaborato con diverse riviste nel settore informatico come giornalista contribuendo alla divulgazione di temi inerenti la sicurezza e aspetti tecnico legali. Docente dal 2005 presso il Master in Sicurezza delle reti dell'Università La Sapienza. Membro della Association for Computing Machinery (ACM) dal 2004 e promotore di innovazione tecnologica, collabora con diverse start-up in Italia e all'estero. Membro di Italia Startup nel 2014 dove con alcune società ha partecipato allo sviluppo e progetto di servizi in ambito mobile e collabora con Oracle Security Council.

Caro lettore,

Sono lieto di comunicarti che Cybersecurity Trends Italia è divenuto realtà! Abbiamo in mano uno strumento agile e innovativo con cui intendiamo contribuire a diffondere la cultura della sicurezza; siamo pronti ad affrontare questa sfida con passione ed entusiasmo che ci ha fatto lavorare sino a tardi, quello che ha spinto me e i miei collaboratori a credere in questo progetto sino a questo giorno in cui andiamo in stampa.

Con questa pubblicazione trimestrale vogliamo dare il nostro contributo alla formazione e consapevolezza in tema di *cybersecurity*, attività che la Fondazione Global Cyber Security Center (GCSEC) persegue orientando le sue iniziative in relazione ai compiti, ai ruoli e alle funzioni del personale aziendale oltre che agli utenti finali.

La trasformazione digitale in atto nel paese sta spingendo imprese e Pubblica Amministrazione a evolversi rapidamente, aumentando la competizione e l'efficienza del sistema paese.

La digitalizzazione fa leva sulla monetizzazione dei dati, informazioni raccolte da clienti, partner e backend aziendali che contribuiscono a creare nuovi flussi e modelli di business. Questo modello di business collega ciò che è digitale con il mondo fisico e tutto questo crea una maggiore influenza sui clienti, permette di cambiare processi e decisioni in tempo reale e può scalare in base alle esigenze.

Questo scenario viene definito da Yuval Harari, nel suo libro *Homo Deus: A brief history of Tomorrow, come Dataism*. Nel libro discute di come questa rivoluzione digitale, oltre a temi di sicurezza abbia anche delle implicazioni sociologiche.

Nel suo libro sostiene che oggi ci si aspetta che siano gli algoritmi a fornirci risposte, quali ad esempio dove vivere, come affrontare un problema economico ecc. spostando sempre più l'autorità verso le aziende che gestiscono questi dati, trasformando i big data in una "nuova religione".

La sua conclusione e che sarà molto difficile staccarsi da questa dipendenza in corso che porterà benefici tali per i quali le persone saranno disposte a rinunciare alla loro privacy in cambio dei vantaggi che potranno ottenere e, cita, quale esempio il progresso nel campo della medicina.

Ritengo che l'umanità, che ha più volte raccolto le sfide poste da nuove tecnologie senza finire in un olocausto nucleare, saprà sicuramente raccogliere i nuovi cambiamenti della trasformazione digitale, della sicurezza, dell'intelligenza artificiale per progredire, alleviare la fame, la malattia e la guerra. Questo *upgrade* ha sicuramente delle nuove sfide da affrontare che noi della Fondazione sapremo cogliere e raccontare. ■

Buona lettura…

Indice

Un esempio di "good practices": Cybersecurity Trends adottato e adattato in Italia

autore: **Marco Obiso,**

Coordinatore per la cyber security, International Telecommunications Union, Ginevra

La cyber security è senza dubbio la principale sfida del 21° secolo, perché ci riguarda tutti, dai più importanti Enti di Stato alle imprese – dalle multinazionali alle start-ups – ai singoli cittadini. Minacce e pericoli non sono mai stati così numerosi, diversi e globalizzati, mirando potenzialmente ognuno di noi e ovunque esso si trovi.

Come coordinatore per la cyber-security nel quadro dell'International Telecommunications Union (ITU), partecipai in settembre 2013 alla nascita di una piattaforma di dialogo pubblico-privato molto speciale "Cybersecurity in Romania", organizzata a Sibiu (Romania) dalla Swiss Webacademy, in partenariato col gruppo media Agora.

L'interesse generale raccolto da quest'iniziativa, che ha creato le fondamenta di un vero dialogo pubblico-privato di scala macro-regionale, ha motivato l'ITU a sostenere il progetto allocando assistenza tecnica, logistica e risorse permettendo a specialisti di fama mondiale di venire ad offrire le loro conoscenze a Sibiu.

Siccome il successo della piattaforma è cresciuto anno dopo anno, i principali partner istituzionali e privati del congresso si sono chiesti se non ci fosse un metodo non solo di rendere perenne questo dialogo, ma anche di renderlo accessibile al grande pubblico. Ed è così che gli stessi organizzatori vennero con l'idea di una rivista trimestrale basata sull'etica, la visione e la mission del congresso.

E' proprio così che è nata, nei primi mesi del 2015, la rivista Cybersecurity Trends, che porta regolarmente all'attenzione del pubblico rumeno punti di vista e preziose informazioni da parte delle principali autorità romene e moldave, ma anche degli specialisti internazionali tra i più qualificati, su un tema centrale di grande attualità, diverso in ogni numero. La versione di Cybersecurity Trends stampata, così quella online gratuita, può essere considerata uno strumento eccellente per aumentare la sensibilità e la presa di coscienza del grande pubblico, elementi fondamentali dal punto di vista dell'ITU, e di portare il lettore a proteggersi contro le minacce che fanno parte del mondo digitale nel quale viviamo.

Peraltro, i testi proposti hanno considerevolmente aiutato a far crescere la visibilità – e a diffondere i materiali – di Enti pubblici e delle ONG partner della rivista, siano essi nazionali che internazionali. All'ITU, abbiamo sin dal primo numero considerato Cybersecurity Trends come un esempio di "good practices" e speravamo in una sua rapida adozione in altri paesi, portandola verso nuove comunità linguistiche. Dopo il CLUSIS (Associazione svizzera della sicurezza dell'informazione), che da gennaio ha portato al pubblico una variante essenzialmente in lingua francese per la Svizzera, la Fondazione GCSEC pubblica la versione dedicata al lettore italiano.

Le nostre speranze iniziali sono state realizzate poiché la rivista è oggi arricchita da un cospicuo numero di articoli di specialisti proposti da queste due ONG, e quindi ne cresce sia il dinamismo che il valore dello scambio di idee di professionisti con orizzonti sempre più diversi.

In questo senso, ringraziando la Fondazione GCSEC per la pregevole iniziativa, l'ITU non può che augurare "lunga vita" a questa iniziativa. Soprattutto, auguriamo ai lettori divenuti ormai internazionali, una piacevole quanto istruttiva lettura. ■

Intervista a Carla Licciardello, Child Protection Online Focus Point, ITU (International Telecommunication Union)

** questo materiale é stato gentilmente messo a disposizione dall'UNICEF*

Carla Licciardello,
ITU Child Online Protection Focal Point

BIO

Carla Licciardello è Focal Point del programma Child Online Protection presso l'ITU (International Telecommunication Union). Le sue responsabilità principali sono di coordinare le attività dell'ITU Child Online Protection e di sviluppare progetti per la protezione dei bambini online sia con gli Stati Membri dell'ITU che con altre organizzazioni internazionali. Lavora anche nel campo della cyber security e contribuisce a progetti multi-agenzie. Prima di entrare nell'ITU, Carla Licciardello ha lavorato, sempre a Ginevra, per la Missione Italiana presso le Nazioni Unite, e poi all'ONU presso il dipartimento del Disaster Risk Reduction. Ha lavorato al ripristino delle comunicazioni e agli aiuti umanitari per gli stati membri dell'ONU colpiti da calamità naturali.

Ci descriva per cortesia, il Suo campo principale di attività e il Suo più importante progetto legato all'uso delle tecnologie Internet per i giovani. Ciò che la soddisfa, la contraria e ciò a cui si deve il successo nel Suo lavoro.

Il potere di liberare tutto il potenziale delle tecnologie dell'informazione e delle comunicazioni (ICT) è oggi nelle mani dei bambini e dei giovani. Le tecnologie ICT sono un mezzo eccellente per lo sviluppo dei bambini, fornendo loro l'occasione di apprendere, di creare e di impegnarsi in modo innovativo nella soluzione di problemi. La 'democratizzazione' delle tecnologie ICT implica che il fenomeno assumerà sempre più importanza.

Malgrado i profondi vantaggi che le tecnologie ICT possono offrire, i bambini e i giovani si trovano a dover far fronte a rischi sia nuovi che significativi. I giovani possono essere esposti a contenuti o a contatti inopportuni, come per esempio a potenziali predatori sessuali. Possono subire danni di immagine attraverso la pubblicazione di informazioni personali sensibili, online o causati da fenomeni come il 'sexting', poiché essi fanno fatica a cogliere le implicazioni a lungo termine delle loro 'impronte' digitali. I giovani possono essere coinvolti in comportamenti rischiosi o inopportuni, che possono avere delle ripercussioni negative, sia a livello personale che a terzi. Per questa ragione, l'ITU ha reso questa tematica una sua priorità ed ha deciso di lanciare il programma COP (Child Online Protection) nel 2008.

L'iniziativa COP coinvolge partner di tutti i settori della comunità globale in un dialogo internazionale per affrontare la questione della sicurezza dei giovani online, con lo scopo di creare un'esperienza che permetta a tutti i minori della terra di beneficiare di una maggiore consapevolezza in rete.

La COP raduna i partner di tutti i gruppi di attori che sostengono uno sforzo globale per proteggere i minori online, attraverso forum, quale il Gruppo di lavoro sulla Protezione del Minore Online, beneficiando anche della portata mondiale che abbiamo in quanto Agenzia delle Nazioni Unite.

Insieme, abbiamo percorso un lungo viaggio: la sicurezza online del minore é ormai una priorità all'ordine del giorno dei politici in molti paesi ed é diventata

una priorità assoluta per una larga diversità di protagonisti, incluse le imprese e le istituzioni finanziarie.

Il nostro scopo globale comune, di assicurare la fiducia nello spazio virtuale, non può essere realizzato da paesi e da terzi che agiscano isolatamente: tutti dobbiamo lavorare insieme se vogliamo riuscire a colmare le lacune esistenti. In un mondo sempre più interconnesso, che non conosce alcuna frontiera, é estremamente importante che tutti questi sforzi differenti siano allineati verso uno scopo comune, ossia quello di costruire uno spazio virtuale sicuro e degno di fiducia.

Se si proiettasse, in questa stessa professione, fra 10 anni, quali differenze immaginerebbe?

Fra 10 anni, credo che Internet – che é ancora al suo debutto – andrà ancora ben più lontano. Le tendenze del mondo digitale indicano che oggi assistiamo sempre più a connessioni senza filo, a velocità esponenzialmente più rapide, così come al trasferimento di quantità di dati sempre maggiore. Questo implica che il lavoro che abbiamo realizzato sino ad oggi potrà essere rivisto, per assicurare che le nostre reti siano a prova di insuccesso e che le generazioni future di utenti possano usufruire dello spazio virtuale in un ambiente più sicuro.

Poiché noi continuiamo a lavorare per permettere l'uso dell'ICT sia in paesi in via di sviluppo che in paesi meno sviluppati, da cui proverrà l'ultimo miliardo dei futuri utenti di Internet, dobbiamo ridurre le differenze all'accesso e alla diffusione dell'ICT per permettere lo sviluppo sociale, la protezione dell'ambiente, produrre ricchezze, offrire servizi medici e un'istruzione di qualità ai minori del mondo intero.

Dobbiamo anche riconoscere che non potremo mai realizzare il pieno potenziale offerto dall'ICT, se i minori, ovunque essi vivano, non hanno fiducia nel loro utilizzo. Possiamo assicurare questa fiducia solo lavorando insieme con le parti beneficiarie di tutte le nazioni, soprattutto se si tiene conto che sorgeranno nuove sfide, e cioè che nuovi strumenti e meccanismi di coordinamento dovranno essere sviluppati e condivisi.

In che modo le imprese e gli altri attori protagonisti dovranno lavorare insieme per raccogliere le diverse sfide e opportunità riguardanti i minori e il mondo digitale?

Per ridurre i rischi della rivoluzione digitale permettendo a sempre più bambini e giovani di raccoglierne i vantaggi, i governi, la società civile, le comunità locali, le organizzazioni internazionali e il settore privato devono lavorare mano nella mano con uno scopo comune. L'industria tecnologica ha un ruolo vitale da svolgere nello stabilire le fondamenta per un uso più sicuro e più rassicurante dei servizi che hanno per base Internet e le altre tecnologie.

Per esempio, il partenariato tra pubblico e privato è una delle chiavi fondamentali per elaborare una risposta nazionale, regionale e internazionale, coordinata al problema degli abusi sessuali online sui minori e per assicurare la condivisione delle informazioni tra le diverse parti interessate. L'industria, gli enti responsabili dell'applicazione della legge, i governi e la società civile devono lavorare in stretta collaborazione gli uni con gli altri per assicurare la messa in opera degli ambiti legali adeguati, in conformità con le norme internazionali in vigore.

Tali strutture di lavoro dovrebbero criminalizzare tutte le forme di abuso sessuale su minori e lo sfruttamento degli stessi, ma anche proteggere i giovani che sono vittime di tali abusi o di sfruttamento e assicurare che tutti i processi di segnalazione, di indagine e di cancellazione di un contenuto siano trattati nel modo più efficace possibile.

Chi o quale organismo considera come il 'leader' atto a provocare un cambiamento ed una progressione dei diritti dell'infanzia nel mondo digitale e perché?

Le Nazioni Unite svolgono un ruolo importante nel mondo digitale come facilitatore per le diverse parti in causa, invitandole a discutere insieme, identificare, poi mettere in opera delle soluzioni che permettano la costruzione di un Internet universalmente disponibile, aperto, in sicurezza e degno di fiducia.

Quali applicazioni o programmi creativi o innovativi svilupperebbe per i minori e i genitori per quanto riguarda la partecipazione civica e/o la cittadinanza digitale?

Credo che noi dobbiamo stimolare la produzione di contenuto online creativo ed educativo per i minori, così come la promozione di esperienze online positive per i più giovani.

Delle misure tecniche possono costituire una parte importante per essere sicuri che i minori siano protetti da potenziali rischi ai quali si trovano di fronte online, ma, questi ultimi sono solamente un elemento dell'equazione. I mezzi di controllo parentali, la presa di coscienza e l'educazione sono componenti chiave che aiuteranno a formare e a informare i giovani di diversi gruppi di età, così come i loro genitori, il personale che se ne prende cura e gli educatori.

Le parti in causa possono sostenere in modo proattivo i diritti del minore contribuendo a chiudere il divario digitale. La partecipazione dei minori esige un'alfabetizzazione digitale, cioé la capacità di capire e di partecipare al mondo digitale.

Senza questa capacità, i cittadini non potranno partecipare a numerose funzioni sociali che sono diventate 'digitalizzate', come tra l'altro la dichiarazione per le tasse, il sostegno a candidati politici, le firme per petizioni online, la registrazione di una nascita, o semplicemente l'accesso al commercio, alla salute, alle informazioni educative o culturali.

Dunque, é cruciale sviluppare programmi che sostengano le iniziative multimedia per fornire ai minori particolarmente a coloro che vivono in zone rurali o mal servite, le competenze digitali. Affinché diventino cittadini fiduciosi, connessi e attivamente impegnati, permettendo loro di partecipare appieno e senza rischi al mondo digitale.

Noi dobbiamo anche sviluppare piattaforme online che promuovano il diritto ai minori di esprimersi. Bisogna facilitare la partecipazione alla vita pubblica, incoraggiare la collaborazione, la partecipazione imprenditoriale e civica.

Infine, é importante concepire dei programmi per collaborare con le società civili locali e i governi sulle priorità nazionali o locali per estendere l'accesso universale ed equo all'informazione e alle tecnologie della comunicazione, alle piattaforme ed ai dispositivi e, naturalmente, a tutta l'infrastruttura sottostante che ne é la base. ■

"Applicazione Whitelisting": la più efficace delle strategie anti-malware

autore: Cătălin Pătraşcu

Analizzando non solo i dati trattati dal CERT-RO durante questi ultimi anni, per quanto riguarda i diversi tipi di malware, ma anche le informazioni pubblicate da differenti organizzazioni attive nel campo della sicurezza informatica, si nota una tendenza evidente di diversificazione, di specializzazione e di crescita della complessità delle applicazioni malevole – che si tratti di APT *(Advanced Persistent Threats)*, di botnets, di malware destinati al settore finanziario *(banking botnets)* o di *ransomware*.

Fra le minacce informatiche, i *malware* sono uno dei tipi più frequenti e pericolosi, a causa, in primo luogo, dell'impatto negativo che possono avere su un sistema informatico una volta infettato.

Oggi, esiste una vasta gamma di nuove tecniche e di tecnologie per combattere questo tipo di minaccia, come gli antivirus, gli IDS, gli IPS, ecc. Queste risultano essere abbastanza efficaci, ma, secondo la nostra opinione, il concetto integrato di *Application Whitelisting* può avere un impatto rilevante nella lotta contro i malware.

L'applicazione *Whitelisting* implica la messa in campo di un meccanismo che garantisca, nel quadro di un sistema informatizzato, la funzionalità dei soli software autorizzati dal gestore del sistema. A prima vista, potrebbe sembrare un obiettivo idealista e forse per queste ragioni tale meccanismo non è ancora abbastanza diffuso, in particolare presso piccole organizzazioni e utenti individuali.

Il concetto stesso non è in sé innovativo, ma rappresenta praticamente un'estensione a livello TCP/IP di un'applicazione con un approccio di tipo *"default deny"* (interdizione in modo implicito), utilizzato da lungo tempo dalle tecnologie firewall.

La messa in opera corretta dell'applicazione Whitelisting implica:

- strumenti destinati a facilitare l'identificazione degli eseguibili e delle software library (come DLL in Windows) e che permettono di bloccare il loro funzionamento;
- metodi di identificazione degli eseguibili e delle software library che non siano basati su regole deboli, come il nome del file o la sua posizione nel repository. Il metodo più efficace consiste nell'identificare l'utilizzazione di tutti i programmi sulla base dei certificati digitali con i quali sono contrassegnati o, nel caso in cui non siano contrassegnati, sulla base delle impronte digitali di tipo *"hash"*;
- meccanismi di tipo ACL (Access Control List) che prevengono le modifiche da parte degli utenti dalla lista dei software consentiti.

Ad oggi, si considera l'applicazione *Whitelisting* come una delle strategie più importanti per combattere le minacce di tipo *malware*. Sono già disponibili una varietà di soluzioni tecniche grazie alle quali implementarla, ivi compreso da utenti individuali, ad esempio nel quadro del sistema di configurazione di Windows, dove la messa in opera di questa applicazione può essere realizzata utilizzando mezzi che sono già contenuti nei sistemi nativi di gestione dei programmi, come ad esempio:

- ***SRP (Software Restriction Policies)*** – nella dotazione *Group Policy* presente in tutte le generazioni successive a Windows XP.
- ***AppLocker*** – funzionalità raccomandata a partire dal sistema Windows 7, con la stessa finalità e dotata delle stesse facilità del SRP dell *Group Policy*.

Se si usa un sistema operativo Linux/Unix, l'implementazione dell'applicazione *Whitelisting* è un po' difficile, perchè non è supportata in modo nativo da *Kernel* e non esiste ancora, nella gamma dei prodotti dei più importanti distributori di Linux, uno strumento consacrato a questo lavoro.

Tuttavia, esistono soluzioni commerciali facili da installare a seconda della versione di Kernel utilizzata, tenendo in mente che potrebbero sorgere problemi durante gli aggiornamenti del sistema.

Altre varianti possibili sono ad esempio l'utilizzazione dei mezzi *SELINUX o AppArmor*, anche se essi non sono stati concepiti a questo fine, e implicano quindi l'uso di risorse importanti seguite da test.

In alcuni casi, la messa in opera dell'applicazione *Whitelisting* può rivelarsi ingombrante e richiedere molte risorse, ma i vantaggi, dal punto di vista della prevenzione di infezioni da *malware* sono considerevoli.

Per di più, si ottiene un alto livello di visibilità per quanto riguarda i file eseguibili e le software library presenti in un sistema informatico, un aspetto estremamente utile nel procedimento di investigazione di incidenti della sicurezza informatica.

In conclusione, mi permetterei di affermare che, benché non si possa considerare alcuna soluzione di sicurezza come una panacea, è probabile che l'applicazione *Whitelisting* sia il metodo più efficace per ridurre l'impatto generato da *malware* nell'ambito dei sistemi informatici utilizzati oggi. ■

BIO

Cătălin Pătraşcu è a capo del servizio di Sicurezza informatica e Monitoraggio al CERT-RO. In questa funzione, ha coordinato numerose attività di risposta a incidenti cyber, ma anche progetti tecnici nonché esercitazioni cyber.

Public-private Partnerships. Lo scambio di informazioni nel campo «cyber»: Il contesto europeo visto dalla Moldavia.

autore: Natalia Spinu

Al giorno d'oggi nessuno può permettersi il lusso di trascurare il ruolo di Internet. Esso facilita una comunicazione rapida e aumenta il rapporto costo-efficacia degli impiegati, fornendo nello stesso tempo innumerevoli opportunità per il mondo degli affari, per i cittadini, ma anche per i governi.

Tuttavia, Internet è diventato anche da tanto tempo un ambiente privilegiato per malfattori, le cui tipologie e scopi sono sempre più eterogenei: Scripts Kiddies, Hacktivisti, crimine organizzato, terrorismo e anche gruppi di attaccanti e di intrusione patrocinati da Stati con uno scopo ben preciso. Questo gruppo di protagonisti, tanto disparato quanto le minacce che indirizza alle società, comporta l'adozione di altrettanti metodi, capacità tecniche e umane specifiche al conseguimento di scopi precisi di ciascuno di essi.

Lo sviluppo rapido di nuove tecnologie offre ai malfattori molte occasioni tra le quali scegliere quella più appropriata e favorevole per effettuare le loro intrusioni. Le amministrazioni pubbliche, ma anche il settore privato, non hanno mai faticato tanto ad affrontare con efficacia questa sfida.

L'epoca in cui ogni organizzazione poteva resistere, isolatamente, alle pressioni degli attaccanti, è ormai passata. Gli incidenti sofisticati recenti che hanno avuto come vittima grandissime imprese, come Sony, eBay o ancora JP Morgan, ma anche istituzioni governativi come l'Ufficio di gestione del Personale governativo degli USA, ne sono la prova. Ora, trattandosi di entità che hanno investito milioni di dollari nella cyber security, si può facilmente realizzare quanto siano reali le minacce di intrusione. Che cosa dovremmo dire allora a riguardo di imprese più piccole, dalle capacità ben più ridotte per quel che riguarda la loro protezione, anche solo nel cuore dell'ecosistema delle loro attività?

Per questa ragione, la cooperazione e lo scambio di informazioni svolge un ruolo sempre più importante nel garantire la sicurezza del mondo digitale. I vantaggi di tale partenariato sono evidenti – lo scambio

BIO

Natalia Spinu dirige il Cyber Security Center (CERT-GOV-MD), un'istituzione che fa parte del Servizio di Telecomunicazioni Speciali della Cancelleria di Stato della Repubblica Moldova. Prima di assumere questo incarico, è stata a capo del dipartimento presso lo stesso Ente Speciale e coordinatrice di progetti al Centro di Informazione e Documentazione della NATO. Ha conseguito il master dell'Institute of European Studies dell'Università di Ginevra nonché dei CAS di Advanced Security Studies (Marshall Center) e di European Security Policy (Geneva Centre for Security Policy).

> *Lo scambio reciproco di informazioni dovrebbe essere una regola naturale di coesistenza nella prosperità ma, come abbiamo visto nella maggior parte dei paesi, molti interessi, sia privati che pubblici, ostacolano la realizzazione di partenariati realmente efficaci e proattivi.*

di informazioni permette di rafforzare le capacità di individuazione di tutti i membri che partecipano ad una rete, permette il trasferimento rapido di conoscenze nel campo delle nuove minacce e impedisce anche la propagazione delle minacce conosciute, riducendo gli sforzi di ogni membro evitando la replica delle medesime attività di analisi da parte di più soggetti e consentendo l'applicazione di contromisure idonee.

Tuttavia, la messa in opera delle componenti necessarie ad uno scambio di informazioni funzionale, nel contesto delle imprese o dei governi, non è di gran lunga così facile come potrebbe apparire a prima vista.

Ci sono molti problemi da risolvere, come anche certi blocchi, sia in seno alle istituzioni pubbliche che nelle compagnie private, e altrettante sfide da affrontare che impediscono il raggiungimento di uno scopo comune – essere più resistenti per difendersi meglio.

Senza voler pretendere di essere esaurienti, ne elenchiamo di seguito alcuni.

▸ **Iniziative.** Chi deve innescare e coordinare il processo? Il governo o il mondo degli affari? In generale il pubblico considera il mondo degli affari come il motore dello sviluppo delle tecnologie, le più progredite nella prevenzione degli attacchi cyber e, in qualche modo, la forza «che sa' meglio ciò che si deve fare e come farlo». A differenza del settore privato, il settore pubblico, che è tra l'altro un fornitore dei servizi, pensa spesso «che non è nel suo ruolo occuparsi di tutte le componenti della nazione».

▸ **Concorrenza del mercato.** Le società private dovrebbero comprendere che la conoscenza delle minacce rappresenta un vantaggio competitivo. D'altro canto, gli organismi di regolamentazione del commercio potrebbero riconoscere in un vero scambio di conoscenze un comportamento anti concorrenziale a discapito di chi paga per queste informazioni.

▸ **Reputazione.** «OK. Se rivelo le informazioni riguardanti una minaccia di cui sono stato oggetto e la rendo pubblica, chi avrà ancora fiducia nei servizi che propongo ai clienti?». La paura di danneggiare la propria reputazione rivelando tali informazioni sono spesso dovute al riflesso negativo che questa apertura potrebbe avere sui mass media avidi di scandalo più che di informazione.

▸ **Confidenzialità.** In molti paesi, la legislazione sulla protezione dei dati nazionali impone che il Protocollo Internet (indirizzo IP) ed altre informazioni digitali a carattere personale non possano in alcun modo essere condivise senza il consenso esplicito degli interessati.

▸ **Capacità.** Non è sufficiente solo far parte di una iniziativa di scambio di informazioni. Da un lato, l'organizzazione deve avere le capacità umane e tecniche necessarie per poter condividere con la community informazioni sulle minacce. Dall'altro, essa deve poter utilizzare le informazioni ricevute.

A questo proposito, è interessante osservare le differenze con cui i diversi Membri affrontano queste questioni. Uno studio recente[1], effettuato dall'ENISA (l'Agenzia Europea incaricata della sicurezza delle reti e dell'informazione), gli Stati Membri dell'Unione Europea, dello Spazio Economico Europeo (EEA), gli Stati Membri dell'Associazione Europea di libero scambio (AELE), ha esaminato i diversi modi di promuovere lo scambio di informazioni nel campo della cyber-sicurezza.

Gli aspetti di base sono: «legislazione di comando e di controllo», «regolamentazione per la cooperazione», e «autoregolazione».

L'approccio «legislazione di comando e di controllo» implica l'applicazione delle norme giuridiche comuni e obbligatorie nelle legislazioni nazionali, identificando le parti che devono distribuire le informazioni concernenti gli incidenti di cyber riguardanti certe entità.

Un buon esempio di applicazione di queste regole è la direttiva 2009/140/EC, per la quale la legge dell'Unione Europea è stata rinforzata da parecchi emendamenti riguardanti le comunicazioni elettroniche e anche i prestatori di servizi delle comunicazioni elettroniche disponibili per il pubblico. Questi ultimi «notificheranno agli organismi di regolamentazione competenti le violazioni di sicurezza o la perdita di integrità, che hanno avuto un impatto significativo sulle reti o i servizi»[2].

L'approccio basato sulle «regole basate sulla cooperazione» implica l'esistenza di un organismo di regolamentazione che faciliti in modo diretto la creazione di centri settoriali di analisi e di scambio di informazioni (ISACc), sotto la forma di partenariati Pubblico-Privato (PPP).

Si tratta di comunità chiuse, in certi casi, con un numero limitato di partecipanti, dove lo scambio di informazioni, in regola generale,

La Banca Mondiale incoraggia la creazione di PPP funzionali

è effettuata su una base volontaria durante una riunione plenaria, organizzata più volte l'anno e coordinata dalle istituzioni governative.

Un esempio di iniziativa basata sul quadro regolamentare della cooperazione è quella del Centro nazionale per la Cyber-Sicurezza (NCSC) dell'Olanda, che ha organizzato i centri settoriali, le analisi e lo scambio di informazioni in diversi settori quali l'acqua, l'energia, la finanza ed altri settori a rischio; ISACc simili sono stati organizzati dal Centro governativo per la protezione delle infrastrutture nazionali della Gran Bretagna, ma anche da altri Stati.

In definitiva, l'approccio basato sull' «autoregolazione» implica che le iniziative che promuovono e che sostengono lo scambio di informazioni debbano poi divulgare i risultati ottenuti ad un target specifico, conformemente al proprio statuto di ogni organizzazione in parte, indipendentemente che si tratti di entità governative o private, commerciali o a scopo non lucrativo, nazionali o internazionali.

In generale, una tale impostazione è utilizzata dalle istituzioni vicine alla sfera della cyber security, come i team di risposta agli incidenti legati alla Sicurezza Informatica (CSIRT), le imprese della sfera della sicurezza dell'informazione o le community di esperti di settore.

Tra le iniziative europee importanti di questo tipo, si può menzionare il «Centro Industriale di Cyber-sicurezza» (CCI) in Spagna, l'N6 (piattaforma di Scambio d'Incidenti della Sicurezza delle Reti) in Polonia, o ancora l'«Associazione degli Esperti in infrastrutture critiche» in Italia.

Esiste anche un'altra modalità per affrontare i problemi della condivisione di informazioni di cyber security. Per esempio, alcune compagnie rinforzano il loro livello di cyber security ottenendo informazioni sulle minacce sia da fonti a pagamento o da siti «open source».

Tuttavia, nel primo caso, l'impresa dovrebbe già possedere un budget significativo (a partire da – 250000 euro all'anno e più), nel secondo caso essa dovrebbe essere capace di trattare delle informazioni grezze al fine di eliminare i dati non affidabili, ingannevoli o incompleti e quelli non in ambito che resta quello di analizzare i pericoli pertinenti ed imminenti.

Nella Repubblica della Moldavia, lo scambio di informazioni in campo della cyber-security è ancora in fase di avviamento. Tuttavia, i primi passi sono stati compiuti dall'anno 2009, con l'adozione della legge sulla prevenzione e la lotta contro la criminalità informatica. Ad oggi, lo scambio di informazioni è organizzato ad hoc, in caso di attacchi cyber.

Paragonata ai paesi dell'Unione Europea, la Repubblica della Moldavia applica l'approccio basato sulla «legislazione di comando e di controllo» e quella sull' «autoregolazione» per trovare delle soluzioni che possano ovviare alle difficoltà di scambio di informazioni. La «Legislazione di comando e di controllo», a livello nazionale, si basa su una sola legge che inquadra i regolamenti per lo scambio di informazioni (Legge Non. 20 del 03.02.2009 sulla prevenzione e la lotta contro la criminalità informatica) e su tre risoluzioni governative (Risoluzione Governativa N. 735 dell'11.06. 2002 -per quanto riguarda i servizi di telecomunicazioni speciali della Repubblica della Moldavia - Risoluzione Governativa N. 857 del 31.10.2013 - sulla strategia

nazionale per lo sviluppo delle tecnologie della società dell'informazione «Moldavia Numerica 2020» - e infine sulla Decisione Governativa N. 811 -del 29.10.2015 che concerne il programma nazionale di cyber-sicurezza della Repubblica della Moldavia per gli anni 2016-2020).

Nel suo insieme, il corpus legislativo obbliga i fornitori di servizi elettronici (ESP) a riportare agli organismi nazionali competenti ogni incidente legato alla cyber-security e al cyber crime, permette alle Istituzioni di richiedere agli ISP e alle Autorità Pubbliche le informazioni necessarie per le indagini e stabilisce gli obiettivi e gli incentivi allo scambio informazioni sulla cyber-security con il settore pubblico e privato. Include, inoltre, il supporto allo sviluppo delle attività di cooperazione.

L'applicabilità dell'approccio basato sull' «autorità autoregolatrice» a livello nazionale è datata 2010, con la creazione del team di risposta agli incidenti informatici, il CERT-GOV-MD.

Senza entrare nei dettagli, alla sua fondazione, il CERT-GOV-MD, doveva limitarsi ad assicurare unicamente una risposta agli incidenti delle reti governative.

Rapidamente, il CERT ha rinforzato eccellenti relazioni con gli altri organismi competenti, sia nazionali (Servizi di Informazioni e Sicurezza, Ministero degli Affari Interni, Procuratore Generale, Centro speciale della lotta contro la cyber-criminalità, ecc.) che internazionali (OSCE, UNDP, IMPACT e ben altri ancora), divenendo membro della comunità CSIRT e ponendosi come attore privilegiato e punto di dialogo centrale per risolvere non solo i problemi chiave di scambio di informazione, ma anche per creare un sistema nazionale di prevenzione e di allerta in tempo reale per far fronte ai rischi connessi ad Internet.

Nel campo dello scambio informazioni, un ulteriore passo avanti è stato fatto nel 2015, quando il CERT-GOV-MD ha tentato di superare un «punto morto», quello dell'assenza dei PPP, convocando un congresso nazionale sull'argomento.

Malgrado la presenza, l'interesse e un'apertura per lo meno dichiarata, di tutti i principali attori privati del settore, rimane chiaro che le imprese rimangono prioritariamente interessate alla vendita delle loro soluzioni e dei loro prodotti, anche a discapito della ricerca di soluzioni multi stakeholder che aiutano a risolvere i problemi nazionali nel campo della cyber security.

Noi pensiamo che l'esempio della Moldavia può servire per una riflessione in numerosi paesi.

Considerando che anche le multinazionali con i livelli di sicurezza più elevati sono state vittime di attacchi cyber, è evidente che solo una conoscenza comune delle minacce e dei pericoli può permettere all'ecosistema nazionale di costituire uno scudo minimo indispensabile per proteggere cittadini, imprese e Stato. Ciò apporterà benefici a coloro che, pur non avendo grandi mezzi finanziari, potranno assicurare la propria difesa a costi accessibili.

Lo scambio reciproco di informazioni dovrebbe essere una regola naturale di coesistenza nella prosperità ma, come abbiamo visto nella maggior parte dei paesi, molti interessi, sia privati che pubblici, ostacolano la realizzazione di partenariati realmente efficaci e proattivi.

Alle difficoltà già menzionate si aggiunge la realizzazione tardiva da parte dei think-thank internazionali, che deve tener conto delle specificità di ogni paese. La diversità delle amministrazioni pubbliche e delle loro competenze, le caratteristiche del tessuto economico, il grado di educazione dei cittadini, la ricchezza del paese e la sua cultura devono essere tenuti in considerazione per adattare ad una nazione un concetto europeo e farlo diventare percorribile. Solo degli insiemi di leggi, di regolamenti, di CERT settoriali e di PPP realizzati per ogni paese nel quadro del *framework* dato dall'ENISA, potrà portare i suoi frutti.

Nella Repubblica della Moldavia, la lotta contro la cyber criminalità non è più nella sua fase iniziale grazie alla condivisione delle informazioni. L'esperienza acquisita nel tempo ha dimostrato che l'applicazione di un insieme di misure legislative e amministrative troppo diverse del quadro europeo e troppo individuali non produrrà, neanch'essa, il risultato desiderato. Nello stesso tempo, si osserva che il settore privato non sarà pronto a cooperare pienamente con il settore pubblico nello scambio di informazioni e di esperienze sulla cyber-security.

Tutto ciò ci porta a credere che l'«autoregolazione» è verosimilmente l'approccio più attuabile a livello nazionale moldavo. Parecchi passi avanti sono stati fatti in questa direzione dal team del CERT-GOV-MD, fra l'altro con solidi risultati presso le comunità locali e dei gruppi di lavoro internazionale come anche la messa a disposizione pubblica di numerose fonti che dettagliano le minacce attuali, ma il successo a medio e lungo termine degli obiettivi proposti è incerto, poiché le risorse del CERT-GOV-MD sono estremamente limitate.

Ma questo è un altro dibattito, relativo al finanziamento delle istituzioni pubbliche per le attività di collaborazione con i cittadini e privati a cui non spetta a noi dare una risposta. ■

Nota:

1 European Union Agency for Network and Information Security, Cyber Security Information Sharing : An Overview of Regulatory and Non-Regulatory Approaches (Heraclion : ENISA , 2015).

2 Official Journal of the European Union, Directive 2009/140/EC of the European Parliament and of the Council (Strasbourg: OJEU,2009).

Manifesto italiano di Coordinated Vulnerability Disclosure

autore: Elena Mena Agresti

Il fronte delle minacce cyber risulta essere sempre più organizzato e sofisticato. Su forum e blog nel deep web, quotidianamente gli attaccanti si scambio informazioni su nuove tecniche di attacco, vulnerabilità, strumenti per sfruttarle, sistemi vulnerabili da attaccare. In taluni casi sono forniti su richiesta veri e propri servizi di attacco.

Per rispondere a un tale scenario, le organizzazioni dovrebbero continuare ad alimentare le collaborazioni tra pubblico e privato ma iniziare anche a instaurare nuove forme di collaborazione con gli altri stakeholder della community della cyber security per usufruire della creatività e delle competenze collettive.

In tale ambito, la fondazione GCSEC promuove l'iniziativa del Manifesto italiano di Coordinated Vulnerabilty Disclosure, meccanismo di cooperazione tra le organizzazioni e la comunità della sicurezza informatica per la scoperta "coordinata" e "responsabile" delle vulnerabilità tecnologiche. Tramite quest'approccio, un esperto del settore, comunemente definito reporter, potrà responsabilmente (rispettando i termini e le condizioni condivise e definite) riportare alle organizzazioni firmatarie del manifesto le vulnerabilità scoperte dando la possibilità alle organizzazioni di identificare e mitigare le vulnerabilità prima che possano essere sfruttate da terzi riducendo il rischio di compromissione.

L'idea del manifesto italiano nasce dall'analoga iniziativa, avviata dalla multinazionale olandese Rabobank che offre servizi bancari e finanziari, e la piattaforma CIO, l'associazione indipendente dei CIO e responsabili IT delle organizzazioni pubbliche e private nei Paesi Bassi. Il Manifesto olandese il 12 maggio 2016 è stato sottoscritto da oltre trenta organizzazioni tra cui ABN AMRO, ENCS, Honeywell, ING, NS, NUON, NXP,

BIO

Laureata in Ingegneria Aerospaziale presso l'Università La Sapienza di Roma, opera per la Fondazione GCSEC e la struttura Tutela delle Informazioni di Poste Italiane.
Esperta di compliance, standard internazionali, governance dell'information security, gestione dei rischi, security audit, formazione e awareness, ha partecipato a tavoli tecnici internazionali dell'ISO e OCSE per la revisione e lo sviluppo di standard e linee guida di information security.
È stata responsabile scientifico di tre corsi di master in cyber security istituiti nel 2015-2016 con l'Università della Calabria e Poste Italiane e attualmente collabora con numerose università italiane in corsi di cyber security. Ha lavorato presso diverse società di consulenza, tra cui in Booz & Company nella practice Risk, Resilience and Assurance. Membro di Europrivacy e della Oracle Community for Security, è Lead Auditor ISO/IEC 27001:2013 e ISO 22301 e ha conseguito le certificazioni STAR Auditor e ISIPM Project Management.

> *La fondazione GCSEC promuove l'iniziativa del Manifesto italiano di Coordinated Vulnerabilty Disclosure.*

Palo Alto Networks, Philips, PostNL, SAAB, SNS Bank, Stedin, Surfnet, Tennet, TNO e Vodafone.

Tale meccanismo non è attivo solo in Olanda ma è già adottato da anni da organizzazioni internazionali come Facebook, Nokia, Apple e Tesla Motors rafforzando il loro livello di sicurezza informatica, aumentando la fiducia dei clienti, riducendo al minimo le opportunità per i cyber criminali di sfruttare le vulnerabilità e dando l'opportunità agli esperti del settore di ottenere premi.

La «segnalazione responsabile della vulnerabilità» riguarda solo le vulnerabilità tecniche di sicurezza. Il «servizio» non può essere utilizzato per segnalare reclami relativi a frodi, alla qualità o disponibilità dei servizi, a casi di phishing. I cosiddetti "reporter" possono testare le vulnerabilità esclusivamente rispettando le regole stabilite nella «politica di divulgazione coordinata delle vulnerabilità», pubblicato sul suo sito web dell'organizzazione, agendo in buona fede e impegnandosi a non causare alcun danno a dati, sistemi o servizi. Il reporter non sfrutta le vulnerabilità né divulga o condivide la scoperta con altri senza il consenso dell'organizzazione stessa (se gli viene concesso).

In cambio, l'organizzazione si impegna a non intraprendere azioni legali nei confronti del reporter, che ha scoperto e segnalato responsabilmente la vulnerabilità, e in taluni casi conferisce una ricompensa e/o il riconoscimento delle competenze. Il nome del reporter viene pubblicato sul cosiddetto "hall of fame" contenente la lista di tutti i reporter che si sono distinti con la relativa classifica. Il punteggio viene assegnato in base alla tipologia delle vulnerabilità scoperte, alla loro numerosità e alla percentuale di vulnerabilità confermate dalle analisi interne di cui l'organizzazione non era a conoscenza.

Solitamente, una volta identificata una nuova vulnerabilità, l'esperto invia all'organizzazione un report che include almeno la descrizione della vulnerabilità, le evidenze dell'avvenuto sfruttamento della stessa (es. screenshot, video, log e indirizzi IP, URL vulnerabili e parametri), le istruzioni per sfruttarla e le possibili remediation da implementare. Generalmente, le organizzazioni inviano un primo riscontro entro 2 o 3 giorni a seconda della complessità dell'analisi da effettuare. Alcune aziende, come GitHubSecurity, dichiarano di inviare una prima risposta entro le prime 24 ore. Il team di sicurezza dell'organizzazione convalida o meno la segnalazione ricevuta, invia al reporter l'accordo di riservatezza sulla vulnerabilità e risolve la vulnerabilità stessa. Se necessario, può chiedere al reporter di aggiornare l'analisi e di fornire ulteriori evidenze o informazioni.

Durante tutto l'iter, il reporter è costantemente informato dello stato di avanzamento delle indagini, sottoscrive l'accordo di riservatezza e pubblica le vulnerabilità solo se autorizzato dall'organizzazione stessa. In alcuni casi, quando la remediation della vulnerabilità è troppo costosa, difficile o impossibile da realizzare, l'organizzazione potrebbe vietare la divulgazione della vulnerabilità.

E' importante notare che il team di sicurezza dell'organizzazione o altri esperti potrebbero aver già individuato una serie di vulnerabilità. Per ottenere il premio, il reporter deve essere stato il primo a rilevarla rispettando le regole definite.

La tipologia e l'ammontare della ricompensa varia da caso a caso e dipende dal valore rappresentato dalla vulnerabilità scoperta per l'organizzazione. Ad esempio nel caso di Google, i premi per bug qualificati variano da $ 100 a $ 20.000 mentre per FCA da $ 150 a $ 1,500

Proprio FCA, Fiat-Chrysler Automotives, rappresenta un caso di recente adozione del modello - lo scorso luglio - ma che in breve tempo ha ottenuto grandi risultati. A oggi sulla pagina di Bugcrowd, piattaforma scelta da FCA, del "hall the fame" è pubblicata la lista dei 197 reporter che si sono distinti segnalando importanti problematiche di sicurezza dei veicoli connessi di FCA, inclusi i sistemi interni, i servizi e le applicazioni esterne che interagiscono con loro. A oggi, in pochi mesi, sono stati assegnati già 54 premi, dimostrazione della rilevanza delle vulnerabilità scoperte.

Bugcrowd (bugcrowd.com/fca), in particolare, è un portale, già utilizzato da molte altre realtà anche diverse tra loro (es. MasterCard, Aruba, Tesla Motors, Western Union, Sophos) sul quale i membri della community, esperti di sicurezza, possono segnalare le vulnerabilità riscontrate.

Forse la più famosa piattaforma di bug bounty è Hackerone, un portale che mette in contatto più di 550 organizzazioni con la community di esperti in cyber security. Sono presenti su Hackerone ad esempio Dropbox, General Motors, Adobe, Dipartimento della Difesa Americano, Yahoo!, Twitter e Uber.

La fondazione GCSEC promuove il Manifesto italiano, una dichiarazione d'intenti in cui le organizzazioni sostengono il principio di divulgazione coordinata delle vulnerabilità e dichiarano di impegnarsi ad attuare le best practice concordate; inoltre sta analizzando le best practice internazionali per la stesura del framework di riferimento e la definizione di linee guida come punto di partenza di discussione per le organizzazioni italiane interessate a partecipare all'iniziativa.

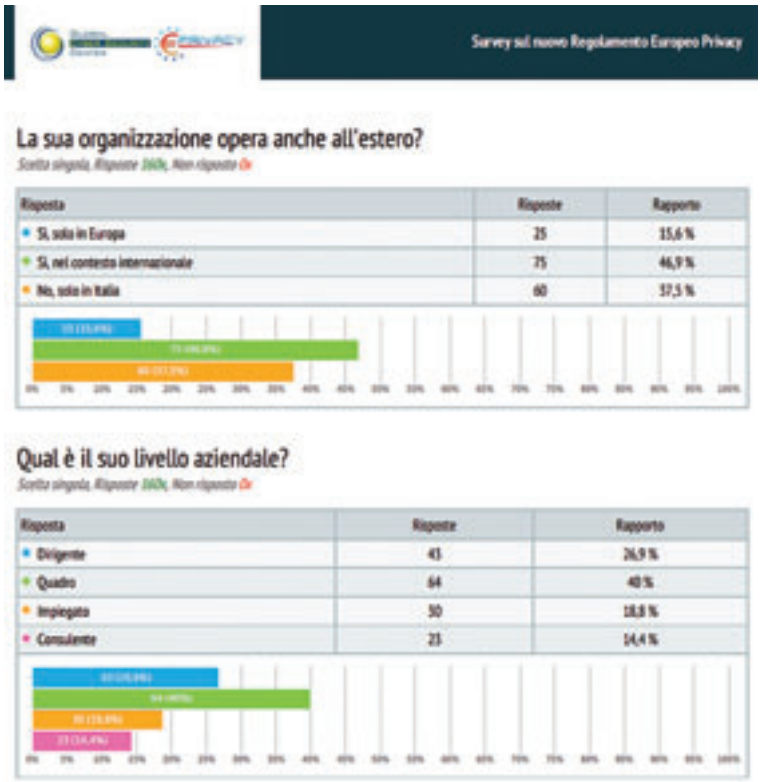
È stata già presentata l'iniziativa a una pletora di rappresentanti delle infrastrutture critiche italiane con cui verranno effettati gli approfondimenti sulla tematica cercando di includere anche la PA che sta definendo internamente una propria iniziativa. ■

La percezione delle aziende italiane del nuovo Regolamento europeo sulla data protection

autore: Elena Mena Agresti

Con l'emanazione del Regolamento Generale sulla Protezione dei Dati (GDPR), le organizzazioni europee e tutte le società che forniscono servizi o prodotti a cittadini dell'Unione, indipendentemente dalla loro posizione geografica, dovranno rispettare nuovi diritti, principi e approcci di gestione dei dati personali.

La fondazione GCSEC insieme all'osservatorio Europrivacy ha condotto una survey per valutare la conoscenza delle organizzazioni italiane del GDPR e la percezione degli impatti che la conformità al Regolamento potrebbe comportare. Alla survey hanno risposto 160 rappresentanti appartenenti nel 46,9% dei casi a grandi aziende che operano a livello internazionale.



BIO

Laureata in Ingegneria Aerospaziale presso l'Università La Sapienza di Roma, opera per la Fondazione GCSEC e la struttura Tutela delle Informazioni di Poste Italiane.
Esperta di compliance, standard internazionali, governance dell'information security, gestione dei rischi, security audit, formazione e awareness, ha partecipato a tavoli tecnici internazionali dell'ISO e OCSE per la revisione e lo sviluppo di standard e linee guida di information security.
È stata responsabile scientifico di tre corsi di master in cyber security istituiti nel 2015-2016 con l'Università della Calabria e Poste Italiane e attualmente collabora con numerose università italiane in corsi di cyber security. Ha lavorato presso diverse società di consulenza, tra cui in Booz & Company nella practice Risk, Resilience and Assurance. Membro di Europrivacy e della Oracle Community for Security, è Lead Auditor ISO/IEC 27001:2013 e ISO 22301 e ha conseguito le certificazioni STAR Auditor e ISIPM Project Management.

Dai risultati emerge che le organizzazioni italiane stanno muovendo i primi passi e pianificando, attraverso assessment interni, le azioni da intraprendere in vista della data di piena operatività fissata per il 25 maggio 2018.

La percezione unanime è che le organizzazioni si sentono ancora impreparate a rispondere ai nuovi obblighi e principi quali di notifica di violazione dei dati personali, la portabilità dei dati, privacy by design e by default. Tali cambiamenti comporteranno con alta probabilità impatti significativi in termini principalmente organizzativi e tecnologici. Una rivoluzione dei modelli organizzativi potrebbe essere causata anche dall'introduzione della figura del Data Protection Officer (o Responsabile della protezione dei dati) e dalla corresponsabilità dei Responsabili al trattamento con il Titolare nel caso di inosservanza del regolamento e sotto determinate condizioni. Dalla survey emerge, infatti, una resistenza da parte dei Responsabili al trattamento a mantenere tale ruolo. Ciò probabilmente porterà le aziende a rivalutare tale figura e ad aggiornare i propri modelli organizzativi interno e i contratti e le gare d'appalto con i fornitori e subfornitori.

Nonostante fosse un principio già implicitamente richiesto dall'attuale normativa, dal sondaggio emerge che ben il 41,9% delle aziende non considera gli aspetti da data protection fin dalle primissime fasi di ideazione e progettazione dei nuovi servizi e prodotti, dichiarando quindi implicitamente una attuale dubbia conformità alla normativa in essere.

Tale adempimento è uno dei più impegnativi poiché presuppone un radicale cambiamento nell'approccio alla data protection. Se da un lato, le organizzazioni dovranno con grande sforzo inziale a rivedere tutti i processi interni, dall'altro potranno avere una gestione completa della privacy. Il principio di privacy by design probabilmente indurrà l'istituzione nelle organizzazioni, anche se non richiesta dal GDPR, della figura del "privacy designer" già presente in numerose realtà extra europee. Inoltre, l'obbligo del rispetto dei principi di privacy by design e by default indurrà i fornitori a progettare i nuovi prodotti e servizi conformi alla normativa, per essere certi di avere mercato e aumentare la propria competitività.

Dal sondaggio emerge, inoltre, un aumento della "consapevolezza" delle organizzazioni sul tema privacy a causa delle possibili sanzioni pecuniarie previste in caso di mancato adempimento del Regolamento. Al contempo però, le organizzazioni sembrano non tenere in debita considerazione le altre tipologie di danni che potrebbero subire in caso di violazione. Indipendente dalla scelta dell'Autorità di Controllo di infliggere o meno una sanzione in base alle circostanze del singolo caso – ad esempio delle misure adottate per attenuare il danno, la gravità e la durata della violazione - le altre tipologie di impatti continuerebbero a sussistere quali ad esempio quelli legati ai rischi di class action, perdita di immagine, aumento del tasso di abbandono dei propri clienti e costi di comunicazione.

Una delle novità più discusse nelle aziende è la figura del Data Protection Officer (DPO), soggetto super partes deputato principalmente a sorvegliare l'osservanza del regolamento, a cooperare e fungere da punto di contatto con l'Autorità di controllo e supportare e consigliare il Titolare o il Responsabile al trattamento sugli obblighi derivanti dal regolamento e fornire pareri in merito alla valutazione di impatto. Non tutte le organizzazioni sono obbligate a istituire tale figura ma ne è incoraggiata l'adozione volontaria. In particolare, nelle proprie linee guida dei garanti europei (WP 29) viene suggerito alle organizzazioni di prendere tale decisione a fronte di un'analisi interna da documentare e lasciare agli atti.

E' bene, però, precisare che anche nei casi di designazione su base volontaria del DPO sussiste l'obbligo del rispetto di tutti i requisiti definiti dal GDPR.

Da Regolamento, il DPO è una figura obbligatoria per le autorità e gli enti pubblici (ad eccezione di quelli che svolgono funzioni giudiziarie) e per le organizzazioni che svolgono come attività principali il "monitoraggio regolare e sistematico" degli interessati "su larga scala" o che trattano categorie particolari di dati personali.

I garanti europei, tramite le linee guida, e il garante italiano, con le proprie faq, forniscono suggerimenti utili per comprendere quando un trattamento viene eseguito "su larga scala" e quando un monitoraggio è "regolare e sistematico" fornendo anche alcuni esempi. Le normali attività effettuate da una compagnia di assicurazioni / una banca, da fornitori di telefonia o di servizi Internet o dal trasporto pubblico di una città tramite tessera elettronica sono esempi di trattamento su larga scala.

Nonostante ciò, numerosi punti rimangono aperti. Dalla survey è emerso che quasi 1/4 delle organizzazioni italiane non sa stabilire se la propria organizzazione ricada o meno tra i soggetti obbligati a dotarsi del DPO mentre solo il 35% dei rispondenti ritiene che sia presente che nella propria organizzazione una figura equiparabile, che svolge ad oggi principalmente attività di coordinamento, vigilanza e controllo, supporto strategico e di rappresentanza verso il Garante.

Ma come scegliere il DPO e quali competenze dovrebbe avere? Deve essere un avvocato, un esperto di security, aver ottenuto specifiche certificazioni di settore o avere un certo inquadramento professionale?

È interessante notare come, per le organizzazioni italiane, il primo criterio di scelta di un DPO siano le certificazioni da questo possedute, anche se tale requisito non è espresso dalla norma o dalle linee guida euroepee sul DPO.

Il Regolamento indica che "può essere designato in base alle qualità professionali e, in particolare, alla conoscenza approfondita del diritto in materia di protezione dei dati nonché alla capacità di svolgere i propri compiti".

È bene precisare che non esiste a oggi una definizione univoca delle competenze e caratteristiche del DPO. A breve ci sarà di grande aiuto la norma tecnica "Profili professionali relativi

al trattamento e alla protezione dei dati personali – Requisiti di conoscenza abilità e competenza" che sta definendo l'UNI/UNINFO e la cui fase di consultazione pubblica si è conclusa il 25 marzo 2017. Tale norma definirà i profili, le competenze e le abilità del DPO e delle altre figure che lavorano nel contesto del trattamento e della protezione dei dati personali.

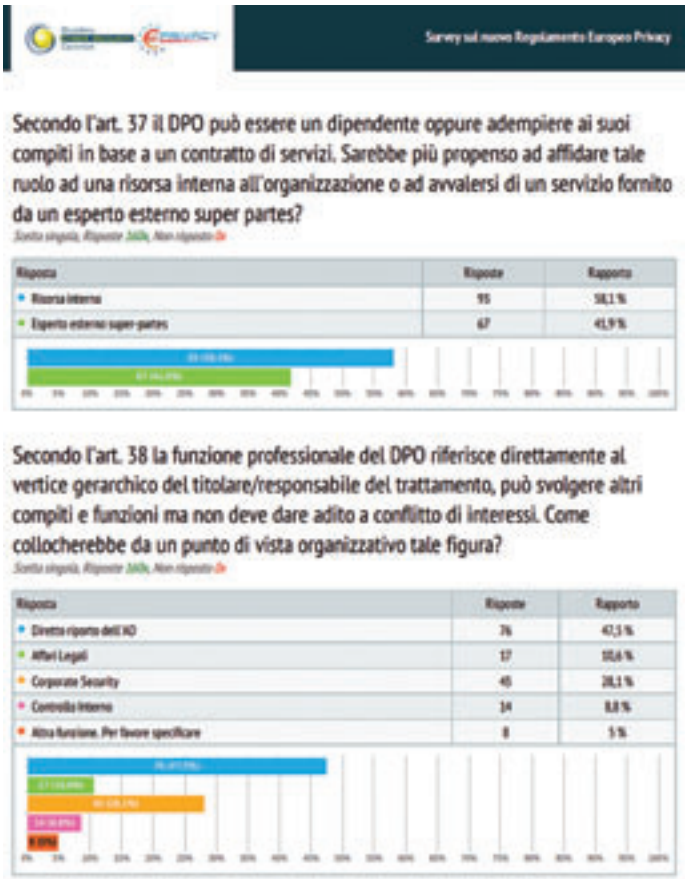
Da una prima lettura del "progetto di norma" pubblicato in fase di consultazione, emergono oltre alle competenze legali e di information security anche quelle relazionali, di comunicazione e di conoscenza del settore di riferimento, ritenute rilevanti per un corretto svolgimento del ruolo del DPO.

Con certezza, possiamo affermare, infatti, che il DPO per svolgere al meglio le proprie attività dovrà necessariamente avere una buona conoscenza della normativa privacy, della sicurezza delle informazioni ma anche del contesto e del settore di riferimento, per comprendere appieno la rischiosità dei trattamenti per i diritti e le libertà fondamentali.

Il livello di competenza richiesta per il DPO dovrà essere proporzionale al contesto di riferimento e alla complessità e sensibilità di dati trattati dall'organizzazione. Di conseguenza più l'organizzazione avrà grandi dimensioni, tratterrà grandi quantità di dati o dati sensibili, maggiori saranno le competenze richieste per il DPO.

Secondo le linea guida dei garanti europei, la capacità di svolgere il ruolo dipende anche dalla posizione attribuita all'interno dell'organizzazione del DPO che, da Regolamento, dovrebbe "riferire direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento". Dalla survey, emerge che quasi il 50% dei rispondenti inserirebbe il DPO a diretto riporto dell'AD, quindi ai più alti vertici aziendali.

Il GDPR, così come le linee guida dei garanti europei, sottolineano la netta separazione del ruolo e delle responsabilità del DPO, del titolare e del responsabile del trattamento secondo il principio di accountability. Il DPO non è responsabile personalmente in caso d'inosservanza del Regolamento. La responsabilità di garantire l'osservanza della normativa in materia di protezione dei dati ricade sempre sul titolare / responsabile del trattamento. Come definito



nell'articolo 24 (1) del GDPR la responsabilità del titolare è "attuare misure tecniche e organizzative adeguate per garantire, e per essere in grado di dimostrare, che il trattamento sia effettuato in conformità al Regolamento".

Dal sondaggio, infine, emerge una carenza formativa in materia di data protection. Le attività svolte sono riferibili principalmente a campagne interne di sensibilizzazione o di formazione e-learning per il personale coinvolto. È significato che quasi il 20% dichiara di effettuare autoformazione, nessuna formazione o di essere stato coinvolto in attività formative negli anni precedenti. ■

Una politica di sicurezza cibernetica più snella e integrata per l'Italia

autore: Alessandra Zaccaria

ABSTRACT: Nelle more del recepimento della direttiva europea NIS, è stato approvato dal CISR un nuovo programma di sicurezza cibernetica, che risponde alle esigenze di individuare un riferimento strategico della politica nazionale, di razionalizzare la catena di comando nella fase di gestione degli attacchi informatici e di agire sul fronte della prevenzione. In attesa del testo del nuovo DPCM che sostituirà il decreto Monti e dell'assegnazione delle risorse economiche individuate dalla ultima legge di stabilità, l'idea di un programma da sviluppare in più fasi lascia immaginare un impegno costante e corale in favore di quella che è considerata ormai parte integrante della sicurezza nazionale e presupposto imprescindibile della trasformazione digitale dell'Italia.

Lo scorso 17 febbraio, da una nota del DIS (Dipartimento delle Informazioni per la Sicurezza) si apprende la notizia dell'approvazione del CISR (Comitato Interministeriale per la Sicurezza della Repubblica) di un nuovo programma nazionale di sicurezza cibernetica e dell'adozione da parte del Presidente del Consiglio di un decreto che sostituirà quello del 24 gennaio 2013, varato dall'esecutivo Monti. A detta di diversi esperti, il decreto Monti presentava degli aspetti migliorabili, in termini di direzione politica, catena di comando e reazione, interlocuzione col settore privato e prevenzione.[1] Si tratta di criticità emerse nel Piano Nazionale di attuazione del decreto per il biennio 2014-2015, che hanno impresso la svolta nell'anno successivo e un ripensamento generalizzato che ha gettato le basi poi per lo sviluppo del nuovo Piano Nazionale 2016-2018, così come conferma il Documento di sicurezza nazionale, allegato alla Relazione del DIS sulla politica della sicurezza 2016:[2]

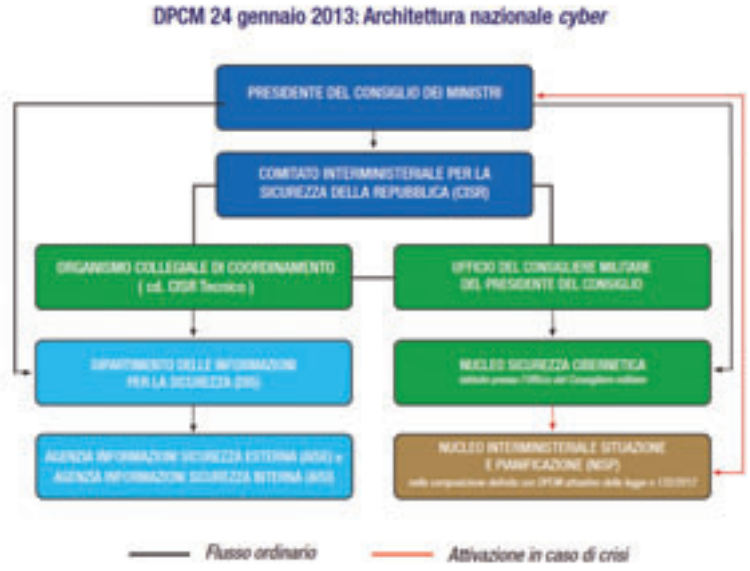
La svolta è stata impressa anche dalla entrata in vigore della direttiva europea NIS (Network and Information Security), che richiede una protezione cibernetica dell'Unione più efficace, a partire dall'obbligo di notifica degli incidenti significativi riportati dai fornitori di servizi digitali e dagli operatori dei servizi essenziali ad un'unica autorità nazionale, che dovrà gestirli tempestivamente, forte della condivisione delle informazioni con gli altri paesi membri.

BIO

Laureata in Scienze Internazionali e Diplomatiche all'Università Di Bologna, ha cominciato ad interessarsi di sicurezza cibernetica durante la ricerca finalizzata alla stesura della tesi magistrale, dal titolo "Cybersecurity e Infrastrutture Critiche". In ambito accademico, si è dedicata successivamente alla guerra cibernetica, come ulteriore dimensione delle Relazioni Internazionali ed ha svolto un tirocinio presso la Fondazione Global Cyber Security Center di Poste Italiane, dove si è cimentata nella valutazione degli investimenti nella sicurezza informatica in ottica di contrasto al cyber crime. Da ultimo, ha conseguito un Master di II livello in Homeland Security, presso l'Università Campus-Bio Medico di Roma, ampliando il suo ambito di competenza a Risk Analysis, Business Continuity e Crisis Management.

In tale ottica, il nuovo programma approvato dal CISR prevede le seguenti novità:

- il Nucleo per la Sicurezza Cibernetica (NSC), struttura operativa di supporto del CISR e del Presidente del Consiglio, è ricollocato all'interno del DIS con l'ulteriore compito di fornire una risposta coordinata in seguito alla notifica di eventi informatici rilevanti. Si rafforzano l'interazione del Nucleo con l'AgID (Agenzia per l'Italia Digitale) e il CERT (Computer Emergency Response Team) della Pubblica Amministrazione per la componente tecnica della gestione delle crisi, mentre resta invariato il sistema di raccordo con i ministeri del CISR;
- il direttore del DIS è incaricato di indicare le linee di azione per assicurare gli adeguati livelli di prevenzione e sicurezza delle reti strategiche, pubbliche e private, col coinvolgimento delle eccellenze del mondo accademico e della ricerca e del settore privato;
- il CISR, presieduto dal Presidente del Consiglio, di cui fanno parte il Ministro degli Affari Esteri, il Ministro dell'Interno, il Ministro della Difesa, il Ministro della Giustizia, il Ministro dell'Economia e delle Finanze ed il Ministro dello Sviluppo Economico, ed oggi integrato con la partecipazione del Ministro per la Semplificazione e la Pubblica Amministrazione, dovrà emanare le direttive recanti le indicazioni per nuovi livelli di allerta qualora si presenti la necessità, coadiuvato da DIS, AISE, AISI e dal consigliere militare (CISR tecnico).



Il testo del nuovo decreto non è ancora disponibile, ma dalla nota del DIS si possono cogliere alcuni propositi, in linea con le esigenze di rivedere la vecchia architettura istituzionale e nella prospettiva di recepire la sostanza della normativa NIS:

- razionalizzare e snellire il processo decisionale in caso di evento cibernetico significativo per la sicurezza nazionale, abolendo il NISP (Nucleo Interministeriale Situazione e Pianificazione), che il Nucleo Sicurezza Cibernetica aveva il compito di attivare affinchè comunicasse lo stato di allerta al Presidente del Consiglio, un passaggio poco funzionale alla gestione di un attacco cyber, che può risultare rapido, simultaneo e pervasivo. Inoltre, saldando il rapporto tra NSC e l'AgID, autorità competente per l'attuazione dell'agenda digitale europea, si lascia presupporre che il Nucleo si candidi al ruolo di autorità competente in materia NIS, considerando che già funge da bacino di confluenza delle notifiche degli eventi cibernetici e da punto di riferimento per i rapporti con NATO, ONU e UE;
- fare del DIS, in collaborazione con AISI e AISE, il cuore operativo dell'intera architettura, a dimostrazione di quanto sia vitale l'attività di condivisione, analisi e valorizzazione delle informazioni per le decisioni strategiche anche nell'ambito della sicurezza cibernetica. In aggiunta, il trasferimento del Nucleo di Sicurezza Cibernetica all'interno del DIS, oltre ad assolvere ad esigenze pratiche, simboleggia quanto la cybersecurity sia parte integrante della sicurezza nazionale;
- riconoscere al CISR la capacità di indirizzo politico, nella sua forma collegiale, intento probabilmente già preannunciato da un intervento normativo del 2015 che gli attribuisce compiti di consulenza, proposta e delibera, in situazioni che incidono sulla sicurezza nazionale, su richiesta del Presidente del Consiglio.[3] Il CISR tecnico assorbe in sostanza il NISP e funge da canale di comunicazione diretta degli incidenti cibernetici al Presidente del Consiglio.

A sostegno di questo nuovo programma, il 21 febbraio Consiglio Nazionale delle Ricerche (CNR) e il Consorzio Interuniversitario per l'Informatica (CINI) hanno dato vita al Comitato nazionale per la ricerca in cybersecurity, mettendo a sistema il pubblico, il privato e l'accademia. Il comitato dovrà occuparsi di prevenzione attraverso la sensibilizzazione di cittadini e imprese riguardo ai rischi cyber, di formazione del personale specializzato in materia e di resilienza delle infrastrutture critiche, attraverso la valorizzazione delle soluzioni *secure by design* del settore privato. In attesa dell'assegnazione dei fondi destinati dalla legge di stabilità, nello specifico 150 milioni di euro, la nascita del Comitato rappresenta un buon segnale verso la costituzione di un ecosistema sicuro e resiliente, essenziale allo sviluppo digitale dell'Italia. ■

Note:

1 Per una trattazione puntuale e completa, si consulti De Zan T., Criticità nell'architettura istituzionale a protezione dello spazio cibernetico nazionale, collana Osservatorio Politica Internazionale del Parlamento Italiano, Istituto Affari Internazionali, marzo 2016, reperibile al link seguente: http://www.iai.it/sites/default/files/pi_a_0117.pdf

2 Il Documento fornisce un aggiornamento annuale sullo stato dell'arte in materia di sicurezza cibernetica e viene allegato alla Relazione sulla politica di sicurezza del DIS, scaricabile dalla pagina seguente: http://www.sicurezzanazionale.gov.it/sisr.nsf/relazione-annuale/relazione-al-parlamento-2016.html

3 Si tratta del decreto legge 30 ottobre 2015, n.174, modificato dalla legge 11 dicembre 2015, n.198il cui art. 7-bis, comma 5 riconosce in capo al CISR i compiti descritti. Si veda Giustozzi C., "Giustozzi, così cambierà la cybersecurity nazionale: catena di comando più semplice ed efficace", Agenda Digitale, 1 marzo 2017, reperibile al link: https://www.agendadigitale.eu/infrastrutture/giustozzi-cosi-cambiera-la-cybersecurity-nazionale-catena-di-comando-piu-semplice-ed-efficace/

Dai campi al "cyberlaundering": le agromafie attentano alla sicurezza delle reti. A colloquio con Gian Carlo Caselli

autore: Massimiliano Cannata

«Le stime sul "fatturato" agromafioso, sono passate da circa 16 Miliardi, dato ufficiale reso noto nel 2016, a 21,8 miliardi. Si tratta di un numero approssimato per difetto che comunque segna un incremento di circa il 30%, e che dà l'idea della gravità del fenomeno. La criminalità ha abbandonano l'abito "militare" per vestire il "doppio petto" e il "colletto bianco", riuscendo così a gestire i vantaggi della globalizzazione e della finanza 3.0. Ciò che rende appetibile questo settore, oltre all'inadeguatezza delle leggi, che non riescono ad imporsi per rendere più difficile la pratica agromafiosa, è la capillarità delle sue diverse articolazioni».

Il procuratore Gian Carlo Caselli, Presidente del Comitato Scientifico dell'Osservatorio sulla criminalità nel settore agroalimentare può vantare una decennale esperienza nel campo della lotta alla criminalità organizzata e al terrorismo. In questa intervista affronta i temi caldi del Rapporto Agromafie, giunto alla quinta edizione, nato per iniziativa del Presidente dell'Eurispes Gian Maria Fara e realizzato in collaborazione con Coldiretti.

Massimiliano Cannata: Procuratore, quello dell'agroalimentare è un business in continua crescita per la criminalità. Cosa deve spaventarci di più?

Gian Carlo Caselli: Innanzi tutto il camaleontismo cioè la capacità di trasformazione di una mafia che ha cambiato pelle e che sarebbe fuorviante trattare secondo gli schemi che abbiamo seguito negli ultimi decenni. Nessuno vuole negare le origini storiche di un fenomeno peculiare dei nostri territori meridionali, che negli anni si è dimostrato capace di inserirsi nei gangli vitali delle grandi città del Centro e del Nord del nostro Paese. Ma oggi quella che fa più paura è la "mafia silente", che prolifera adottando modi di operare totalmente diversi dal passato. Basti pensare al fenomeno del cyberlaundering, ossia al riciclaggio del denaro sporco on line, per comprendere il processo di trasformazione in atto.

Massimiliano Cannata: Cosa significa in concreto?

Gian Carlo Caselli: Vuol dire che la "nuova" mafia non solo non taglieggia il proprietario del supermercato o dell'autosalone: piuttosto ne

diventa socia o ne rileva in toto l'attività procurandosi sempre nuovi canali "puliti" per il riciclaggio. La nuova criminalità sfrutta Internet che costituisce una sorta di acceleratore. Se un tempo le mafie traevano i propri proventi principalmente dallo sfruttamento di stampo gangsteristico e violento sul territorio, imponendo il "pizzo" in cambio della "protezione", oggi si è fatta essa stessa "imprenditrice", che porta a compimento una strategia di "normalizzazione". Una delinquenza che opera sulle rotte virtuali. Da sempre lo scopo del riciclaggio è quello di allontanare il denaro dalla sua provenienza attraverso una serie di operazioni che mirano ad ostacolare la tracciabilità delle origini dei proventi. Con Internet viene ampliata la distanza tra il riciclatore e il capitale, rendendo più complessa l'indagine sui soggetti sospettati.

Massimiliano Cannata: Quali sono le conseguenze di questo mutamento così radicale?

Gian Carlo Caselli: Sono evidenti: la concezione di mafia e di mafioso ha finito con l'allargarsi fino ad inglobare altri territori che richiedono un quadro normativo conseguente che deve essere messo al passo con la "nuova" criminalità che si nasconde dietro i consigli di amministrazione, le holding, i fondi internazionali, le società di consulenza, oltre che, come non di rado accade, dietro il paravento formale della politica e delle Istituzioni.

Dal *kalashnikov* alle reti virtuali

Massimiliano Cannata: Per che cosa si caratterizzano le strategie adottate dalle organizzazioni malavitose nel settore agroalimentare, che dimostrano questa straordinaria padronanza nel maneggiare le nuove tecnologie?

Gian Carlo Caselli: Sul versante agroalimentare, si sta per altro profilando un'economia parallela. Nell'ipotesi del *cyberlaundering* cui facevo prima riferimento, l'attività si riduce ad un'unica operazione virtuale e dematerializzata, in cui il fenomeno del riciclaggio di capitali illeciti può trovare le condizioni ideali per svilupparsi. La criminalità organizzata è così passata velocemente al mondo della tecnologia, passando così dai kalashnikov ad armi più sofisticate, come le botnet, reti che controllano anche decine di migliaia di computer e che possono essere utilizzate per aggredire aziende ed organizzazioni in Rete.

Massimiliano Cannata: Si tratta di operazioni delicate, che implicano la capacità di mettere insieme profili e competenze diverse. Siamo a un cambio generazionale, oltre che di metodi e strategie, a un "salto di qualità" della nuova delinquenza organizzata?

Gian Carlo Caselli: Occorre ribadire che Internet e la Rete stanno consentendo alla criminalità organizzata di ogni paese di allargare i confini della propria azione, offrendo opportunità e prospettive fino a poco tempo fa inimmaginabili. Questo ha determinato una trasformazione del profilo e dell'identità della "vecchia mafia". Va poi sottolineato che il web rappresenta una "zona franca" in grado di fornire garanzie di sicurezza ed anonimato, un'area "grigia" che presta il fianco alla possibilità di commettere varie tipologie di reati. La sicurezza delle reti nel nuovo contesto diventa dunque un mezzo importante anche per il contrasto di una strategia criminale che non ha frontiere e che sta diventando sempre più minacciosa.

BIO

Gian Carlo Caselli, nato ad Alessandria nel 1939, dopo la laurea in giurisprudenza è stato dal 1964 assistente volontario di Storia del Diritto italiano presso l'Università di Torino. Al 1967 risale il suo ingresso nella magistratura, con la nomina a Uditore giudiziario, alla quale seguì, nei primi anni '70, quella a Giudice Istruttore presso il Tribunale di Torino. Nell'assolvere a questo incarico, da lui mantenuto fino al 1986, Caselli istruì in particolare (dapprima come giudice singolo, poi in "pool" con altri magistrati) tutte le inchieste sull'attività terroristica delle Brigate Rosse e di Prima Linea di Torino, Genova e Milano.

Rientrato a Torino come Presidente della 1a Corte di Assise, nel 1992, dopo le stragi mafiose di Capaci e via d'Amelio, che costarono la vita ai giudici Giovanni Falcone e Paolo Borsellino, chiese di essere nominato Procuratore della Repubblica presso il Tribunale di Palermo, per mettere la propria esperienza nella lotta al crimine organizzato a servizio del Paese e della fondamentale missione di contrastare la mafia.

Completato il proprio periodo di incarico a Palermo, Caselli ha proseguito la carriera con la stessa passione e con altri ruoli prestigiosi, anche a livello internazionale: nel 1999 Direttore del Dipartimento di amministrazione penitenziaria, nel 2001 componente dell'unità di cooperazione giudiziaria europea "Pro-Eurojust", nel 2002 Procuratore Generale della Repubblica presso la Corte d'Appello di Torino.

L'impegno da magistrato è proseguito a Torino, dove è stato nominato, con voto unanime del Consiglio Superiore della Magistratura, Procuratore Capo in sostituzione del giudice Marcello Maddalena.

In continuità con il suo impegno nella diffusione della cultura della legalità, dal 2014, è Presidente del Comitato Scientifico della Fondazione di Coldiretti "Osservatorio sulla criminalità nell'agricoltura e sul sistema agroalimentare".

E' stato Presidente della Commissione per l'elaborazione di proposte di intervento sulla riforma dei reati in materia agroalimentare (D.M. 20.4.2015) voluta dal Ministro Andrea Orlando; - i lavori della Commissione si sono conclusi con la presentazione al ministro di un dossier con 49 articoli e relative linee guida del progetto di riforma.

Massimiliano Cannata: Una criminalità che si sta mettendo in evidenza anche per la capacità di penetrazione "commerciale" nei nuovi mercati. Anche questo è un fatto inedito non crede?

Gian Carlo Caselli: E' di fatto quello che sta avvenendo. Le mafie con un'insospettabile vocazione al marketing, dopo aver ceduto in appalto ai manovali l'onere di organizzare e gestire il caporalato e altre numerose forme di sfruttamento, oggi condizionano il mercato, stabilendo i prezzi dei raccolti, controllando i trasporti e lo smistamento di intere catene di supermercati, gestendo l'esportazione del nostro vero o falso *Made in Italy,* la creazione all'estero di centrali di produzione dell'*Italian sounding*, e la creazione ex novo di reti di smercio al minuto.

Gian Carlo Caselli

La sicurezza delle reti quale asset strategico di contrasto

Massimiliano Cannata: Si riferisce alla cosiddetta "mafia liquida"?

Gian Carlo Caselli: E' la definizione più appropriata per fotografare l'attitudine della malavita ad infilarsi dappertutto, proprio come l'acqua. I mafiosi adottando gli stratagemmi più svariati, fanno incetta di cospicui flussi dei finanziamenti europei. Basti pensare che nel solo 2016 la Guardia di Finanza ha confiscato 137 terreni e individuato 29.689 terreni nella disponibilità di soggetti appartenenti alla criminalità organizzata; ha, inoltre, sequestrato patrimoni per un valore di 150 milioni di euro e 35 milioni di euro di finanziamenti indebitamente percepiti.

Massimiliano Cannata: Le innovazioni non si fermano qui. L'High frequency trading è l'altro termine chiave con cui dovremmo fare i conti. Lo può tratteggiare in sintesi?

Gian Carlo Caselli: E' un ulteriore strumento a disposizione della criminalità organizzata, che consente gli scambi di Borsa ad altissima velocità, operati in modo automatico sulla base di algoritmi. Sono operazioni speculative realizzate mobilitando masse di denaro in grado di condizionare l'andamento dei titoli. Siamo di fronte a dispositivi ipertecnologici, i quali immettono in breve tempo sul mercato una frequenza elevatissima di ordini, che possono arrivare a superare i 5.000 al secondo. Una sorta di "insider trading automatico", i cui operatori sono, per gli inquirenti, difficili da individuare.

Massimiliano Cannata: Di fatto come operano i criminali?

Gian Carlo Caselli: Attraverso l'*High frequency trading*, banche e operatori finanziari agiscono contemporaneamente su diverse piattaforme regolamentate, come le Borse, o, cosa che accade ancor più spesso, prive di ogni controllo, come gli *Over the counter* (Otc), realizzando profitti di natura meramente speculativa. Grazie alla velocità di esecuzione delle operazioni, infatti, immettono, modificano e cancellano milioni di ordini al giorno, giocando sulle minime differenze di prezzo tra vendita e acquisto, e chiudendo tutte le posizioni entro fine giornata.

Massimiliano Cannata: Rapidità e controllo delle reti sono ancora una volta alla base di questa azioni illecite?

Gian Carlo Caselli: Il punto focale è proprio la velocità: algoritmi, sempre più complessi, "vedono" gli ordini di un titolo, effettuati dai concorrenti nei diversi mercati, e in quel brevissimo lasso di tempo tra l'istante in cui l'ordine viene immesso e quello in cui compare nel cosiddetto book di negoziazione di ogni mercato, cioè nel prospetto telematico che contiene le proposte di vendita e acquisto, con quantità, prezzo e operatore, inondano i mercati di ordini, ricercando su altre piattaforme lo stesso titolo, e riuscendo così a chiudere la negoziazione a un prezzo più conveniente. Queste migliaia di ordini hanno quindi l'unico scopo di alzare o abbassare la quotazione del titolo e vengono poi cancellati, a negoziazione conclusa, in altrettante frazioni di secondo. La rapidità è tale che gli organi di controllo dei diversi paesi stimano che appena il 10% degli ordini effettuati con l'*High frequency trading* venga portato a termine; il rimanente 90% viene cancellato.

Massimiliano Cannata: Quali iniziative vanno intraprese per contrastare fenomeni così sofisticati e articolati?

Gian Carlo Caselli: La complessità della rete dei fenomeni criminali ha raggiunto livelli molto elevati. Il nostro sforzo in questa fase è concentrato nell'attività di mappatura della penetrazione delle attività criminali nella filiera agroalimentare, al fine di individuare un "Indice di Permeabilità" che ci possa aiutare a comprendere meglio i punti di fragilità del nostro territorio per avviare un'attività di prevenzione e tutela sempre più efficace e al passo con i tempi. Siamo ormai di fronte a un problema transnazionale, mentre le Autorità di vigilanza sono a carattere nazionale, per cui nessuna di esse può avere una visione completa delle attività degli operatori Hft. Appare dunque evidente la necessità di orchestrare strategie investigative di prevenzione del rischio e delle vulnerabilità, fondate su un'intelligence di respiro transnazionale, che deve contemplare efficaci strategie di cyber security. Dalla centralità della lotta alle mafie, potrà discendere un orizzonte di libertà per il nostro Paese. Siamo di fronte a una partita che non possiamo permetterci di perdere. ■

Identità digitale e diritto all'oblio

autore: Michele Gallante

Il costante e spasmodico utilizzo di applicazioni ed oggetti connessi ad una rete informatica, sta influenzando irrimediabilmente il modo di comportarsi delle persone, che condividono in un batter d'occhio informazioni personali, senza pensare alle conseguenze e alla loro difficile cancellazione dal mondo virtuale: infatti, una volta caricato un file nel web diventa quasi impossibile rimuoverlo totalmente.

BIO

Michele Gallante è un praticante Avvocato iscritto all'ordine di Roma. Laureato in Giurisprudenza presso l'Università degli Studi Roma Tre, ha svolto la ricerca tesi con titolo "Dilemmi giuridici sull'utilizzo dei Droni nei Conflitti Armati" alla University of Washington, School of Law, Seattle, US. Dopo gli studi ha ottenuto un Master in "Homeland Security" presso l'Università Campus Bio-Medico di Roma, dove ha approfondito argomenti riguardanti la Security, Data Protection e Privacy. Ha svolto attività di ricerca presso la fondazione Global Cyber Security Center di Poste Italiane in merito a problematiche giuridiche riguardanti la sicurezza informatica. Attualmente è Security Consultant presso una società di Soluzioni Informatiche e Consulenza Integrata.

Il *mare magnum* di informazioni e dati personali che circolano costantemente nel web ha permesso all'identità digitale di essere sempre meno sotto controllo, e, allo stesso tempo, di causare ripercussioni determinanti nella vita reale di tutti i giorni.

Per difendere i diritti connessi alla diffusione impropria di questi dati nella rete informatica e garantire la privacy di ogni cittadino si è formato il c.d. "Diritto all'Oblio" ossia il diritto di un individuo di essere dimenticato e non essere più ricordato per fatti che lo riguardano. Nella pratica, questo diritto, viene posto a garanzia di coloro che non vogliono restare esposti a tempo indeterminato alle conseguenze dannose che possano influenzare negativamente la reputazione per fatti accaduti in passato (specialmente in un epoca digitale come la nostra, dove la maggior parte delle notizie circola online). Come affermava il filosofo Friedrich Nietzsche "l'oblio è una facoltà attiva" che nel mondo moderno va esercitata con delle procedure ben precise.

Ad esempio, vediamo com'è possibile richiedere la deindicizzazione web per un motore di ricerca importante come Google[1]: si compila l'apposito modulo messo a disposizione online, si forniscono le specificazioni dei motivi, e si esibisce copia obbligatoria di un documento d'identità del richiedente. L'effettiva rimozione non è né immediata né tantomeno automatica, e, ovviamente, non comporta la cancellazione anche da altri motori di ricerca diversi da Google.

> *Per difendere i diritti connessi alla diffusione impropria di questi dati nel web e garantire la privacy di ogni cittadino si è formato il c.d. "Diritto all'Oblio".*

Nella valutazione delle ragioni portate dal richiedente, il motore di ricerca, può anche decidere di considerare la richiesta illegittima e negare la cancellazione del contenuto. A quel punto l'utente può fare ricorso al Garante per la Privacy con una spesa di 150 euro e un'attesa massima di sessanta giorni. Infine, se neanche in questo caso il soggetto ritiene di essere soddisfatto, può rivolgersi a un giudice civile per ricorrere contro il Garante, ma ciò, ovviamente, richiede tempo e somme di denaro più elevate.

L'iter procedurale sembra facile ma Google dal 2014 ha accolto poco più del 30% di 36.000 richieste, perché non adeguatamente compilate o per mancanza di motivazioni sufficienti. Il consiglio delle Autorità è di farsi affiancare da consulenti esperti del settore per non incappare in cavilli burocratici e non veder riconosciuto un proprio diritto. Tuttavia, anche in questi casi, spesso, un'informazione pubblica è difficile da eliminare: infatti, nel caso di una notizia divenuta virale, la procedura descritta non sarebbe sufficiente per una completa cancellazione.

Il diritto alla riservatezza e la reputazione dei soggetti coinvolti che si vuole garantire, si contrappone però con il diritto di cronaca, e solo un perfetto bilanciamento degli interessi in gioco permetterà una decisione appropriata. Come detto da Rodotà "Il diritto all'oblio può pericolosamente inclinare verso la falsificazione della realtà e divenire strumento per limitare il diritto all'informazione" e per queste ragioni serve una disciplina chiara e trasparente.

Recentemente il Regolamento Europeo 679/2016 ha creato una prima forma di disciplina. Infatti, l'articolo 17 del testo sancisce che ogni interessato ha diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo. Tale diritto, tuttavia, viene meno quando la diffusione di determinate informazioni sia necessaria per l'esercizio del diritto alla libertà di espressione e di informazione, per l'adempimento di un obbligo legale o per l'esecuzione di un compito svolto nel pubblico interesse o nell'esercizio di pubblici poteri, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Nel nostro ordinamento non esiste un'espressa regolamentazione, ma resta esclusivamente di matrice giurisprudenziale. Il 3 Dicembre 2015 il Tribunale di Roma con Sent. N. 23771 ha ribadito che il diritto all'oblio non è altro che una peculiare espressione del diritto alla riservatezza (espresso anche a livello europeo negli articoli 7 e 8 della Carta dei Diritti Fondamentali). Le conclusioni derivanti da questa sentenza chiariscono che il fatto che si intende dimenticare non debba essere recente, e che lo stesso abbia uno scarso interesse pubblico.

Nel bilanciamento degli interessi sottesi al diritto in esame, in assenza di una peculiare normativa italiana, va rilevato come l'interesse pubblico giochi un ruolo fondamentale nella decisione. Infatti, anche nel Testo unico dei doveri del giornalista (3 febbraio 2016), è raccomandato agli scrittori il dovere di evitare di far riferimento a particolari del passato, a meno che essi non risultino essenziali per la completezza dell'informazione.

"L'oblio è una forma di libertà" (Khalil Gibran) e per questo in una società evoluta come la nostra deve essere disciplinato in modo chiaro e trasparente, garantendo una protezione adeguata della nostra identità con particolare attenzione alla nuova realtà digitale. L'armonizzazione europea resa dal nuovo regolamento in materia di trattamento dei dati personali, definitivamente vincolante a partire dal 25 Maggio 2018, è solo l'inizio di una condivisione di intenti volti al rispetto di un diritto riconosciuto come fondamentale. ■

Nota:

1 Link: https://support.google.com/legal/contact/lr_eudpa?product=websearch.

Cosa dobbiamo aspettarci dalla comunità dei CERT?

autore: Eduard Bisceanu

Negli ultimi anni, abbiamo assistito a un'accelerazione dello sviluppo di entità destinate a combattere le minacce cibernetiche e a gestire gli incidenti di sicurezza cyber – note sotto l'acronimo di CERT – ma anche a una crescita, quantomeno a livello statistico, del numero di esperti in questo campo.

In modo evidente, questo fenomeno è la risposta delle nostre società a quanto avviene mediamente online, sia tenendo conto della crescita dell'uso delle tecnologie in tutte le attività della vita, sia nell'intento di frenare le evoluzioni spettacolari degli attacchi cibernetici registrati a livello planetare.

In modo prevalente nel settore statale, ma anche nel privato, la creazione di strutture di tipo CERT e l'ingaggio di personale altamente specializzato nelle discipline connesse al campo della sicurezza cibernetica dovrebbe fornire una risposta adeguata ai più sofisticati attacchi cibernetici che possono essere generati da qualsivoglia tipo di attore, indifferentemente dalle motivazioni e dalle risorse che quest'ultimo ha a sua disposizione.

Ma tutte queste strutture e la loro pleiade di esperti, presenti nello spazio pubblico, hanno davvero le capacità di fornire i risultati attesi?

Se ci atteniamo ai messaggi proposti in quasi tutte le ricerche, articoli o conferenze di settore dell'ultimo periodo, personalmente considero che siano in maggioranza mancanti di proporzionalità rispetto al reale livello di rischio: sovente troppo allarmanti e quasi sempre sprovvisti di soluzioni adatte al grande pubblico oppure alle nicchie di pubblico alle quali sono indirizzati.

Secondo la mia esperienza, posso affermare che il livello di pericolo generato oggi dagli attacchi cibernetici è ancora ben al di sotto del livello critico che potrebbe generare effetti devastanti, mentre è proprio con questo ultimo vocabolo che spesso ci viene presentato il quadro d'insieme della sicurezza della rete e delle tecnologie in generale.

Per sostenere la mia tesi, mi rapporto semplicemente alla crescita evidente e sempre più rapida dei diversi servizi online proposti, sia da parte dei governi, sia dal mondo degli affari. Ora, semplicemente, se i rischi fossero davvero più grandi delle opportunità, gli investimenti di sviluppo di nuovi servizi online sarebbero completamente inefficienti.

Nello stesso tempo, l'evoluzione costante delle complessità degli attacchi cibernetici, così come dei risultati ottenuti dagli attaccanti, pongono seri problemi alle comunità specializzate nel campo della sicurezza cibernetica, sia dal punto di vista della tutela della sicurezza del cittadino utilizzatore di tecnologie e di servizi online, sia dal punto di vista dei governi che devono assicurare le condizioni necessarie al funzionamento delle infrastrutture critiche in condizioni di sicurezza, senza dimenticare il punto di vista delle compagnie private fornitrici di tecnologie o di servizi in questo campo.

Non è mia intenzione in questa sede sostenere le mie affermazioni riproponendo dati statistici o descrizioni di attacchi cibernetici estremamente distruttivi degli ultimi mesi, perché vi sono sufficienti risorse online specializzate in questo campo al quale il lettore può fare riferimento. In cambio vorrei cercare di sintetizzare quelle che considero le gravi mancanze di oggi al livello globale, per continuare a far prevalere un'attitudine di sicurezza e di trust nelle tecnologie sulle minacce di qualsivoglia natura e soprattutto sul panico generale che si avverte ogni volta che avviene un fatto pericoloso online, spesso senza essere stato previsto da nessuno.

Non sostengo qui una visione messianica su quello che dovrebbe essere messo in atto nel campo della sicurezza cibernetica, bensì tento di mettere in evidenza il fatto

BIO

Eduard Bisceanu è un esperto riconosciuto a livello nazionale nel campo della cyber-security. Le sue competenze spaziano dal management della sicurezza informatica all'investigazione di attacchi cibernetici complessi – ivi compresi i casi di frodi che usano gli strumenti di pagamento elettronico – all'analisi, valutazione e risposta alle minacce cibernetiche. Nel quadro della sua carriera di 16 anni al servizio del SRI (Servizio Romeno di Intelligence), è stato distaccato per compiere le funzioni di direttore esecutivo del CERT-RO. In questo quadro, è stato tra i primissimi specialisti del suo paese a studiare il campo delle minacce cibernetiche di livello nazionale. Eduard occupa oggi la funzione di CSO presso la UniCredit Bank Romania.

che, pur facendo passi avanti in questa direzione come l'adozione di regolamentazioni, la costituzione di strutture specializzate ecc., i risultati reali si lasciano ancora aspettare mentre il potenziale che un'Armaggedon cibernetico possa manifestarsi in un contesto generale di crisi globale diventa sempre più probabile.

In questo testo, vorrei soffermarmi sulle strutture di tipo CERT e sulle ragioni per le quali considero che, in generale, non abbiano raggiunto un grado di maturità necessario per rispondere alla situazione reale con la quale essi si confrontano online.

E qui parliamo sia di entità di tipo CERT governativi, sia private, tutte create con un singolo obiettivo generico: elevare il grado di resilienza delle infrastrutture ed assicurare la sicurezza delle informazioni veicolate dalle stesse, includendo anche le funzionalità vitali assicurate tramite le tecnologie nel quadro delle infrastrutture critiche.

Questo tipo di entità ha una presenza sempre più visibile sul piano globale, specialmente nel contesto europeo, dove le pagine web di queste strutture abbondano di informazioni utili a tutti. Purtroppo, spesso, le attività di queste strutture è prevalentemente costituita da una componente reattivo-difensiva, pregiudicando la componente preventiva che invece è molto più importante dal punto di vista dei bisogni di sicurezza della rete.

La mia affermazione è ovviamente contestabile, pur se prevista tra le molteplici attività quotidiane che svolgo in qualità di direttore di sicurezza presso una istituzione di tipo finanziario-bancaria, ovvero la ricerca di informazioni valide su nuovi tipi di attacchi cibernetici (indicatori di compromissione, indicatori di attacchi, analisi di malware, valutazioni specializzate e tentativi di attribuzione di determinati attacchi complessi ecc.), nello scopo di adattare i sistemi tecnici e procedurali dell'organizzazione, dalla quale sono stato assunto, per proteggerla contro le più recenti categorie di minacce.

Le procedure, le politiche e i consigli utili – specialmente quelli che riguardano l'adeguatezza della risposta a un attacco cibernetico che ha già prodotto effetti – le pagine web ed i feeds di sicurezza sono generati da diversi organismi di tipo CERT e considerate di valore (Es: https://first.org/, http://cert.org/, https://www.cert.pl/en/, https://cert.europa.eu/cert/plainedition/en/cert_about.html, https://www.ncsc.gov.uk/, https://cert.ro/).

Invece, se cerco informazioni sulle azioni (con utilità immediata) relative ad attacchi nuovi, complessi, sofisticati e che generano un impatto significativo sulle infrastrutture target, devo andarle a cercare quasi sempre sulle risorse messe a disposizione (in modo pubblico o a pagamento) dalle compagnie specializzate nel campo della sicurezza cibernetica.

Per alcuni, ciò potrebbe sembrare normale, perché queste compagnie sono state fondate proprio per questo scopo … tuttavia se analizziamo gli obiettivi e le ingenti risorse finanziarie investite da governi e settori privati in strutture di tipo CERT, capiamo bene che qualcosa non gira per il verso giusto…

Tenterò di presentare alcune azioni che considero come priorità di grado zero per la comunità, facendo sì che la funzione di prevenzione di una struttura di tipo CERT prevalga sulla reattività manifestata in presente, quali:

- il paradigma del partenariato pubblico-privato deve essere cambiato con azioni concrete e non per forza tramite legislazione. Anche se può sembrare un'affermazione azzardata, non esiste una legislazione che proibisca la cooperazione reale tra il settore pubblico e quello privato, esistono soltanto dei decisori poco convinti (da ambo le parti) che non capiscono i benefici delle diverse forme di cooperazione;

- ad affiancare sia le campagne pubbliche di informazione sui pericoli online, che spesso sono peraltro indirizzate ad un pubblico già consapevole, sia la ricerca permanente delle responsabilità di chi deve occuparsi dell'educazione del cittadino, una vera e propria azione reale deve ormai consistere nell'elaborazione di materiali educativi semplici, facili da capire e personalizzati, da mettere a disposizione delle diverse categorie di pubblico, ed infine l'introduzione rapida di questi materiali nel quadro dell'insegnamento scolastico obbligatorio, in tutte le classi di età;

- svolgere campagne di educazione destinate ai manager del settore privato e ai dirigenti del settore pubblico. Tra queste élites, una persona scorrettamente informata è destinata a prendere continuamente decisioni contro-produttive o tantomeno a non prendere le decisioni giuste;

- elaborazione di curricula per formare nuove competenze nel quadro della risposta degli incidenti di sicurezza cibernetica – accessibili sia dal punto di vista dei costi ma anche dal punto di vista dell'attualizzazione del contenuto ogni volta che nuovi elementi della realtà lo rendono necessario – questo accanto alle certificazioni di valore (costose ed inaccessibili alla grande maggioranza) che propongono le diverse entità private e il mondo accademico. Questi nuovi programmi risponderebbero perfettamente al bisogno reale di expertise richiesta dal mercato;

- effettuare scambi di informazioni in tempo reale – non esistono scuse e motivazioni reali per non mettere a disposizione, in tempo reale, indicatori di attacco o di compromissione, nel caso di un attacco cibernetico con impatto significativo.

Una standardizzazione più rapida del formato degli scambi al livello della comunità condurrebbe velocemente a far scadere il tempo di risposta nonché la crescita della compatibilità dei sistemi tecnologici utilizzati dalle diverse entità di tipo CERT;

- creazione di strutture adatte alla detenzione, alla risposta e all'analisi degli attacchi cibernetici efficienti, tramite l'adozione di buone pratiche utilizzate dalle compagnie private (selezione dei manager e degli esperti tramite criteri di competenza, stipendi adatti all'importanza ed alla criticità delle attività svolte, accesso continuo a informazioni di rilievo ed all'uso di strumenti tecnologici competitivi, ecc.);

- assumersi il ruolo di arbitro tra le diverse entità statali e i vari settori economici che sinora non scambiano informazioni per motivi che appartengono a strategie concorrenziali;

- assumersi il ruolo di fornitori di fiducia attraverso la validazione di diverse tecnologie fornite dal mercato specializzato;

- assumersi gli errori e valorizzare in modo più attivo le lezioni tratte da questi;

- fornire periodicamente dei prodotti del tipo Cyber Threat Intelligence, che dovrebbero contenere, accanto alla componente tecnica d'azione (sulla quale sono orientate la maggioranza delle piattaforme e dei fornitori privati attuali), analisi e valutazioni professionali riguardanti l'evoluzione della prospettiva della sicurezza online al fine di consolidare le componenti di prevenzione e di sostegno informazionale nell'atto decisionale (e questo a favore sia del settore pubblico, sia di quello privato).

Senza avere la presunzione di aver coperto tutti i problemi delle comunità di tipo CERT, e nemmeno di aver proposto delle soluzioni speciali, ho la certezza che gli aspetti presentati creeranno non poche controversie.

Ma dalla mia esperienza, è quasi sempre dalle contraddizioni e dalle critiche costruttive che viene generata un'evoluzione. ■

Automobile e Internet degli Oggetti: relazioni pericolose

autore: Yannick Harrel

Se gli attacchi DDoS *(Distributed Denial of Service)* avevano la tendenza negli ultimi anni a diventare degli episodi nocivi informatici di minore impatto, all'occorrenza irritanti, molti casi specifici recenti hanno dimostrato che stanno ritornando con forza. Uno di questi casi, particolarmente grave, è accaduto in Francia nel settembre del 2016 dove una grande società francese di web hosting, la OVH, ha dovuto affrontare, in un tentativo criminale di paralisi della sua rete, degli attacchi che hanno raggiunto un *Terabit* al Secondo.

Se la densità del flusso di saturazione della banda è ragguardevole, la sua alimentazione é ancor più preoccupante. Dopo l'inchiesta, sono stati gli stessi dispositivi di sorveglianza degli IP della società, poco o non protetti, che avrebbero servito da trasmettitori per questo attacco. Ora, c'è chi dice siano state le telecamere di sorveglianza con indirizzo IP, chi afferma Internet degli Oggetti *(Internet of Things)* in generale.

La problematica dell'Internet degli Oggetti, per quanto riguarda la sicurezza informatica, si divide in due rami: il primo concerne la loro esplosione demografica, che dopo aver passato nel 2010 la soglia degli 8 miliardi di oggetti attivi, si avvia verso 80 miliardi di oggetti previsti all'orizzonte del 2020 (secondo lo Studio IDATE); il secondo concerne la loro messa in sicurezza. I due rami sono correlati: come rendere sicuro in modo efficace un fenomeno in piena espansione e in fase di cambiamento? Ed è proprio in questo contesto che avviene anche la nascita delle automobili del futuro.

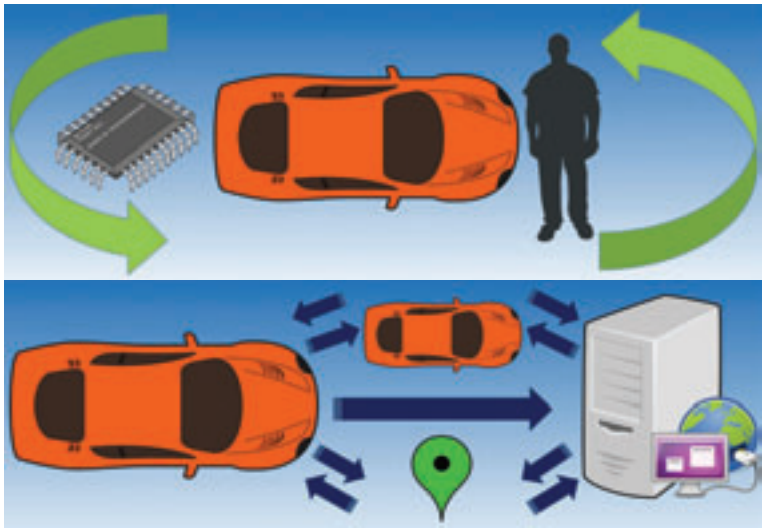
I costruttori di lunga data, come i giganti del digitale, pensano ormai seriamente alla vettura del futuro come a una vettura autonoma, cioè pilotata dall'intelligenza artificiale. Ora, chi parla di intelligenza artificiale intende, prima una delega parziale, poi totale della guida.

Questo può accadere solo se il veicolo può garantire il rispetto di un itinerario selezionato, il più fidato possibile, e affinché questo sia conforme con l'ordine di partenza, è necessario che il veicolo sia connesso permanentemente con l'ambiente circostante e con gli apparecchi trasmettitori di comunicazione.

Se i veicoli degli anni 2000-2015 disponevano di una base di dati preinseriti e integrati nello schermo di controllo, permettendo al conducente umano di orientarsi, d'ora in poi la preoccupazione dei costruttori è di fornire una base di dati auto-evolutiva e aggiornata che possa rispondere alle tante domande specifiche, quali una modifica del percorso a causa di un ingorgo temporaneo o la ricerca di una stazione di servizio con le tariffe più vantaggiose in un raggio stabilito di chilometri. È questa la prima tappa verso la guida autonoma dinamica (1).

Questa guida necessiterà di un flusso di informazioni aggiornate, in uno scenario che va dal passatempo (esempio: indicazione di un festival che si svolge nelle vicinanze del passaggio del veicolo) alla sicurezza (esempio: strada temporaneamente inaccessibile perché inondata). Possiamo raggruppare queste informazioni in cinque categorie:

- L'info-divertimento (indicazione di punti di interesse turistico nei dintorni della posizione della vettura o software di divertimento integrati nello schermo di controllo).
- L'interazione con il veicolo (indicatore del livello di consumo delle batterie o chiamata al centro di riparazioni del costruttore).
- La gestione della guida (eco-guida o pianificazione dell'itinerario).
- La sicurezza propria del veicolo (direzione assistita, velocità, freni in funzione del luogo e delle condizioni metereologiche locali, indicazione delle distanze fra veicoli o su lavori in corso sulla strada).
- I servizi annessi (pagamento a distanza del posto di parcheggio o servizio di geo-localizzazione per recuperare un veicolo di noleggio).



BIO

Esperto e Professore associato in Cyberstrategy presso la Business & Finance School di Strasbourg, membro fondatore del think-tank strategico Echo RadaR e noto tramite il suo blog personale «Cyberstrategy East-West», Yannick Harrel è autore di numerose pubblicazioni nei campi della strategia cibernetica e della geopolitica, frutto di ricerche fatte su domanda di diverse istituzioni e riviste di settore. Nel 2011, ha ricevuto il premio nazionale «Amiral Marcel Duval», conferitogli dalla rivista French National Defense. Dopo essere stato impiegato in una impresa pionieristica specializzata nell'implementazione della fibra ottica in Francia, ha partecipato alla nascita del master di difesa cibernetica presso l'Alta Scuola Militare di Saint-Cyr; sull'invito del Consiglio dell'Europa, ha partecipato alle prime due edizioni del Forum Mondiale per la Democrazia, nel panel dei temi digitali d'attualità. Nel 2013, ha pubblicato il primo libro in lingua francese dedicato alla strategia cibernetica della Federazione Russa, mentre il suo ultimo volume, uscito di stampa nel 2016, "Automobile 3.0" è focalizzato sull'impatto delle nuove tecnologie di comunicazione e controllo inserite nelle automobili.

Tuttavia, qual è la connessione fra i veicoli di cui sopra e i dispositivi IP accennati all'inizio? Semplicemente perché seguono le stesse logiche e ci pongono gli stessi interrogativi: il loro numero aumenterà in modo esponenziale nei prossimi anni e, come dimostrato in alcuni casi, il livello di sicurezza non è attualmente comprovato.

Citiamo appunto un esempio che ha fatto molto rumore nella stampa specializzata: due ricercatori in informatica, Charlie Miller e Chris Valasek, sono riusciti ad interagire a distanza con una Jeep Cherokee (2). Essi hanno disposto a piacere di tutti gli elementi a bordo di questo 4x4: dalla climatizzazione ai freni, alla direzione, il tutto a qualche decina di miglia di distanza dal veicolo (cioè 16 kilometri). Il gruppo Fiat-Chrysler ha preso molto sul serio questa dimostrazione e ha disposto la correzione delle falle di sicurezza informatica, chiudendo le vulnerabilità. Questa presa di controllo può anche essere fra le più insidiose come gli stessi ricercatori hanno dimostrato, modificando sostanzialmente l'itinerario scelto sul piano della navigazione digitale.

Messo in causa, il sistema UConnect è un insieme di strumenti che permettono sia di navigare che di ascoltare musica o di rispondere a una chiamata telefonica. Questo coltello svizzero elettronico, che si ritrova più o meno nelle funzioni di veicoli prodotti da altri gruppi del settore, è una porta d'entrata per qualsiasi individuo malintenzionato.

Parecchi punti di entrata/uscita sono altrettante falle potenziali sui veicoli moderni:

- Port OBD *(On Board Diagnostic)*
- Modem 4G / LTE *(Long Term Evolution)*
- Bluetooth
- CAN *(Controller Area Network)*; Bus / VAN *(Vehicle Area Network)*; Bus
- "Chip card" RFID *(Radio Frequency Identification)*
- Lettore CD/DVD

Queste falle non sono sempre dovute ad inattenzioni o a un rifiuto della messa in sicurezza da parte dei fabbricanti o degli appaltatori. Molte brecce informatiche sono in realtà sconosciute, ovvero vittime potenziali di attacchi nuovi *(Zero Day)*, e sono oggetto di correttivi solo una volta scoperte. Purtroppo, la creatività dei criminali e la moltiplicazione dei punti di accesso ai veicoli moderni complicano seriamente il compito del personale che si dedica all'estirpazione delle fragilità natie. Inoltre, la domanda, diventata abitudine, dei consumatori di poter disporre di un insieme di funzioni all'interno dell'abitacolo, rende impossibile la loro limitazione tecnica, come è anche impossibile disattivare gli aiuti elettronici che servono a stabilizzare il veicolo in ogni situazione.

In queste condizioni, il mercato in espansione dei veicoli connessi, va assimilato senza dubbio all'Internet degli Oggetti, poiché questi comunicheranno e interagiranno in funzione dell'occupante e dei punti di connessione statici o mobili ai quali sono legati. La differenza tra il pirataggio di una telecamera IP e quello di un'automobile connessa sta nel fatto che in quest'ultimo caso la presa di controllo a distanza fa correre un rischio letale altamente elevato sia per il conduttore e i suoi passeggeri sia per terzi.

Si tratta di un pericolo reale che ha suscitato non solo l'attenzione di numerosi costruttori e fornitori di attrezzature che intendono portare il problema fino a una soglia prossima al rischio zero, ma è giunto al punto, ad esempio, di richiedere la creazione di gruppi di lavoro in collaborazione con specialisti di diverse specialità del mondo digitale nonché di ricercatori in sicurezza informatica o di società produttrici di antivirus e di firewall (è il caso per esempio dell'Auto-ISAC *(Information Sharing and Analysis Center)* o dell'EVITA *(E-safety Vehicle Intrusion Protected Applications)*. Una necessità dovuta dalla dimensione potenziale del problema: si stima che quasi 100 milioni di linee di codice sono contenute in un veicolo connesso, rispetto ai "soli" 8 milioni di linee che servono ad un moderno aereo da caccia.

Questi scambi tra i differenti attori del settore dovrebbero permettere non solo di elevare il livello di sicurezza ma anche di proteggere i segreti tecnologici dei componenti cruciali a bordo. Se la presa a distanza del veicolo è un rischio maggiore, quello di un furto dei dati contenuti dai sistemi del veicolo non è da escludere, poiché questi ultimi vanno dai dati personali del conduttore ai dettagli elettro-meccanici del suo mezzo di trasporto.

Per concludere, non dobbiamo mai dimenticare che il primo scudo in materia di sicurezza informatica rimane l'utente che si deve preoccupare della preservazione dei suoi beni… e della sua vita. ■

Andy Geenberg, *Hackers remotely kill a jeep on the highway- with me in it*, Wired , 21 luglio 2015 - https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway
Auto-ISA - https://www.automotiveisac.com/
EVITA Project - http://www.evita-project.org/

(1) Un veicolo autonomo non è obbligatoriamente connesso: può per esempio servirsi di differenti sensori e telecamere integrate ai mezzi di locomozione – come il LIDAR *(Light Detection and Ranging)* – al fine di orientarsi nel suo spazio. Tuttavia la sua efficacia è solo dentro un certo limite geografico e per una attività di guida pura. Per di più, il veicolo non comunica con ciò che circola intorno a lui: riceve informazioni senza emetterne. La guida autonoma dinamica, invece, consta in uno scambio di dati in tempo reale. Nello stesso modo, un veicolo connesso non è obbligatoriamente un veicolo autonomo, sia che l'opzione della delega di guida non sia stata selezionata, si che essa non sia disponibile sul modello scelto.
(2) Nel 2013, una Toyota Prius e una Ford Espace erano state anch'esse piratate, tuttavia la procedura aveva richiesto la presenza nell'abitacolo di due specialisti, di conseguenza con intrusione fisica nel sistema per immettervi dei dati. Nel 2015, la dimostrazione è stata interamente operata a distanza.

Sicurezza, ma anche comunicazione, comprensione della tecnologia e possibili trends nel mondo corporate e nelle organizzazioni internazionali. Un'intervista esclusiva con Luca Tenzi

Luca Tenzi

autore: Laurent Chrzanovski

Laurent Chrzanovski: In quanto specialista della sicurezza a 360° che ha lavorato e lavora sia per grandi gruppi multinazionali sia per organizzazioni internazionali, come può descriverci l'ambiente di sicurezza che vi regna? Come spiega, ad esempio, la nostra comune "risatina" quando recentemente, al giorno del smartphone-pay, delle NFC, non siamo riusciti a pagare i nostri caffè al bar di una grande Istituzione specializzata dell'ONU Ginevra se non frugandoci le tasche per trovare franchi svizzeri in contanti mentre la stessa Istituzione usa esclusivamente il net per le gare d'appalto, i concorsi per i posti di lavoro, etc.? Per Lei, è' un gigantesco "bazar" che bisognerà prima o poi ricominciare da zero oppure ci sono ancora possibilità di armonizzare sistemi e garantirne una sicurezza di qualità?

Luca Tenzi: Ritengo che bisogna dividere i problemi. All'interno di ogni azienda, ormai, ci sono diversi players, ognuno con la propria concezione della tecnologia e della sicurezza. Tutti vanno dal CTO o il CIO per chiedere e far validare l'acquisto dei prodotti di cui avrebbero bisogno. Sono queste le figure che ormai dovrebbero coordinare, vedere le sincronie dei progetti principali e mettere in azione un piano di sviluppo.

Purtroppo, in molte aziende, piccole, medie o grandi, questo non avviene, perché la domanda viene dal business o da una *facility* e nella *facility*, come ad esempio la necessità di un POS/NFC per la caffetteria. Ora, questa *facility* non comunica né con le risorse umane, né con il CIO.

La grande sfida è di coordinare meglio i progetti tecnologici, un'azione che purtroppo non sta avvenendo. Bisogna cominciare a parlare di tutti i progetti, assolutamente tutti, come "progetti tecnologici" che dovrebbero quindi essere trattati come tali, sotto una piattaforma unica di gestione. Non esistendo ad oggi una tale struttura, c'è una cacofonia dei mezzi tecnologici nel seno della stessa azienda o organizzazione.

Se non iniziamo, con il coordinamento di questo "ufficio di gestione", a fare "cantare" il coro tecnologico dei diversi servizi e bisogni allo stesso diapason, continueremo ad avere questa cacofonia, vettore evidentemente di problemi di sicurezza.

Laurent Chrzanovski: Sulle disfunzionalità dell'ultra-coordinamento troviamo invece, tipicamente, i siti degli enti pubblici (ad esempio il portale unico della Confederazione svizzera o quello del cantone di Ginevra) che sono stati voluti omogenei e non permettono a nessuna struttura (ministeri, unità) di sviluppare nemmeno a livello di identità grafica il proprio contenuto… Come evolveranno questi portali di stato verso una gestione unica?

Luca Tenzi: E' un esempio classico di siti, ideati quando dietro al portale web c'era, come in una piccola rivista, una coperta (la homepage) e qualche pagina (le pagine web). Ormai, nel web 3.0 e 4.0, questo non sarà più possibile. La *digital portability* esige pagine dinamiche adattative.

Ad esempio, ho assistito ieri allo smarrimento di una cassiera di una grande libreria di Ginevra, di fronte ad un cliente che voleva pagare con lo *smartphone*. Questa tecnica, adottata dalla libreria, non era stata ben spiegata al personale ed il cliente ha dovuto aiutare la cassiera a svolgere l'operazione.

Questo fa ben vedere che i portali devono essere integrati; non comunicano più solo la *corporate identity* ed il messaggio che l'azienda o l'ente vuole fare passare ma ricevono messaggi: devono essere connessi ai social media, ad esempio.

Un ente o una multinazionale che non ha profili social media profilati in maniera giusta, oramai è come se non comunicasse. Ancora una vota, come per la libreria, il privato da il tono. Il miglior esempio recente è l'ultimo single di Adele, *"Hello"*, che è ufficialmente uscito due settimane dopo essere stato reso disponibile su *YouTube*. E' diventato subito una hit, anche perché rinviava come un *"joke"* ad una vecchia melodia di Lionel Richie. Il risultato è che quando il pezzo è andato in onda sulle radio e televisioni, è diventato subito numero uno senza che un centesimo di pubblicità aggiuntiva o campagna promozionale sia stato fatto dalla star o dalla casa discografica.

Le aziende devono diventare molto dinamiche, specialmente con le giovani generazioni, che sono nate col multimedia. La difficoltà è che il top management, delle istituzioni e aziende, deve fare un salto enorme e non ne hanno coscienza. Non ho potuto trattenere un sorriso quando, l'altro giorno, all'eccesso opposto ho visto l'MI5 che cercava proprio sulle reti social i profili di professionisti per migliorare la sua dinamica di comunicazione e ricezione verso e dal cittadino. È uno degli estremi che mostra a che punto convivono pacificamente quelli che rimangono al web 1.0 e quelli che, quasi esageratamente, vorrebbero velocemente fare un salto quantico.

Laurent Chrzanovski: Ed in termini di security? Verso che tendenze ci orientiamo? Uno spaccamento definitivo tra la parte di visibilità e di dialogo e quella di lavoro oppure altro?

Luca Tenzi: Si andrà verso delle pagine uniche. Un "cosmo" di soluzioni. Ad esempio, presso molti Enti internazionali e aziende moderne, è possibile già sottoporre una candidatura di lavoro tramite il proprio profilo pubblico di Linkedin. Ma il problema subentra poi, durante la fase di trattamento della candidatura quando il candidato viene assunto, con l'obbligo per il datore di lavoro di trattare questi miei dati personali come confidenziali, trasferendoli in un altro database. E' esattamente quello che succede con le gare d'appalto.

Nei prossimi anni, ineluttabilmente, si dovrà a tutti i livelli fare pulizia e separare bene i quattro assi fondamentali: pubblico, privato, professionale e divertimento. Questi saranno i vettori fondamentali per costruire il web 4.0. In questo senso, oggi assistiamo ancora ad una confusione totale dei generi; ad esempio mi fa sempre sorridere quando vedo nella pubblicità di una marca di pasta o di frutta *"seguiteci su Facebook"*: sono ovviamente imperativi commerciali delle ditte, per mandare delle offerte, ma capiti male perché non vedo il senso di fare sapere a tutti che oggi ho mangiato una banana di tale marca dopo gli spaghetti della ditta tal dei tali.

Nel futuro, le stesse società capiranno che questo tipo di link non è più necessario. Parimenti, non credo che in certe organizzazioni la mentalità sia già pronta per questo salto e ci dovremo aspettare un salto generazionale nell'area dirigente per osservarlo.

Leggevo in un libro di management che nel 2020 avremo 4 generazioni completamente diverse che collaboreranno negli stessi ambienti di lavoro, per cui l'arrivo degli *"indigeni del web"* farà fare un grosso salto qualitativo sulle piattaforme. In più, tutto quello che è *quality data* (e non *big data*) farà si che ci saranno sempre più scenari previsibili e quindi una facilitazione per trovare le giuste soluzioni tecnologiche.

Laurent Chrzanovski: Ho l'impressione, condivisa da tanti esperti, che c'è ormai un fossato sempre più grande tra chi si occupa o interessa di security e la massa dei cittadini, che non ha ricevuto la minima educazione sull'uso delle tecnologie, inclusi i responsabili IT che non hanno avuto una cultura di security. Non andiamo da qualche parte "nel muro" tra esplosione di nuove tecnologie ogni giorno e (quasi) inesistenza di un minimo awareness?

Luca Tenzi: Credo che la contraddizione del business model attuale verrà sempre più soggetta a contestazione. Oggi ancora, dei giovani talentati possono adunare centinaia di migliaia e talvolta milioni di dollari tramite il *crowdfunding* per elaborare una *app*, e nel giro di 2 anni hanno una società che può interessare una grande multinazionale.

C'è una sovrapproduzione di applicazioni e sono sicuro che andiamo verso una saturazione di queste *apps*. La tecnologia ci obbliga a fare abbonamenti dappertutto, attivare la geo-localizzazione per avere le "notizie" in modo tempestivo etc. Si va verso una saturazione del pubblico e tra non molto vedremo una divisione netta tra chi è visibile e chi, invece, deciderà di "non esistere" sul web oppure giocherà sul numero di profili, alias, indirizzi.

Le società inizieranno a riflettere, e a rifiutare nuovi prodotti col semplice ragionamento di "ma questo non ne ho bisogno, ho vissuto benissimo senza".

Laurent Chrzanovski: La sicurezza degli IoT sembra sfuggire ad una stragrande maggioranza di direttori di ditte e di governanti, e pure negli stati asiatici come Taiwan o Singapore, dove i consumatori hanno cominciato a scartare IoT che non portavano più valuta alla loro vita, essi non l'hanno fatto per motivi di sicurezza. Come spiegare questa "beata incoscienza"?

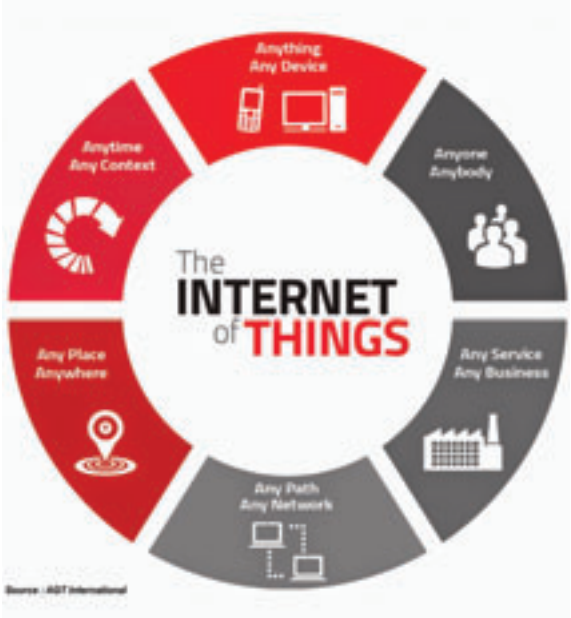
Luca Tenzi: L'incoerenza delle conoscenze sulla sicurezza è enorme, e l'asimmetricità tra miglioramento tecnologico e numero di minacce aggiuntive diviene gigantesca. Ogni volta che si sviluppa un'applicazione che non fa che un qualcosa in più di quella precedente, questo qualcosina in più moltiplica esponenzialmente il numero dei rischi aggiuntivi. Negli IoT vediamo, in Asia, un *push-back*.

Certi sviluppi sono di nicchia e prettamente inutili, se non nell'ottica del consumerismo ad oltranza; leggevo di un'*app* sviluppata per una ditta che produce sci per sportivi, e che permette di leggere la temperatura della neve, la direzione delle curve della pista. Come ottimo sciatore, posso dire che questa applicazione mi sembra assolutamente superflua.

Il problema delle applicazioni e della spinta commerciale fa sì che molti giovani si lanciano nello sviluppo di tecnologie che non integrano in nessun modo un minimo di sicurezza perché non sono capite da questi giovani. Se guardiamo le numerose applicazioni che permettono di vedere che ristoranti ci sono, o che cinema, dove mi trovo, si vede

BIO

Luca Tenzi – Vice president CLUSIS Svizzera - esperto di sicurezza aziendale con quasi 20 anni di esperienza in aziende quotate in borsa - ha condotto operazioni di sicurezza in ambienti diversi. La sua esperienza si estende su più settori, tra cui, manifatturiero, farmaceutico, tecnologie dell›informazione e della comunicazione, istituti finanziari tutte aziende Fortune 100 e 500. Completata da esperienze in agenzie specializzate delle Nazioni Unite, tra cui l'agenzia leader delle tecnologie dell›informazione e della comunicazione. Forte sostenitore per la convergenza della sicurezza fisica e sicurezza ICT. Innovativo pensatore strategico, con una comprovata esperienza di cooperazione, attualmente si occupata di progetti di convergenza e integrazione tecnologica. Ha pubblicato articoli in materia di sicurezza fisica, organizzazione e ICT, ed è stato invitato a presentare osservazioni in riviste di settore o di geopolitica e seminari internazionali presentando i rischi emergenti o latenti per la sicurezza delle attività di business esponendo le nuove minacce asimmetriche.
Ha conseguito un Post Graduate in gestione della sicurezza e le emergenze presso l'Università Bocconi, un Master in Criminalità e gestione del rischio alla Leicester University, e un DAS in gestione dei Rischi Aziendali presso l'HEG-SO (Geneve). Presente come lectuer in diverse scuole specialistiche tra cui HEG-SO Ginevra.



bene che chi le ha ideate non aveva idea che queste sarebbero state usate non per la loro utilità dal consumatore, ma come una vera e propria spia per raccogliere sempre più dati su di lui, volutamente o tramite *malware*.

Gli attacchi sulle automobili spente e chiuse fanno ben vedere che l'aggiunta di tecnologie ha solo portato ad un'insicurezza maggiore.

Un dubbio atavico dell'uso delle nuove applicazioni è quello della sicurezza. Recentemente, in un congresso internazionale, uno dei massimi esperti di IoT paragonava i prodotti sul mercato con un'auto che noi compreremmo accettando che le portiere posteriori verranno montate tra due mesi, con la versione 2.1, le ruote tra sei mesi con la versione 2.4, il freno verrà tra un anno con la versione 2.6, e così via, ovvero che accettiamo dei prodotti non finiti nell'ambito della tecnologia nello stesso tempo che non accetteremo mai questo tipo di rischi nei nostri acquisti fisici.

Laurent Chrzanovski: Se osserviamo la Svizzera e i paesi vicini, e se studiamo i codici, gli obblighi e le misure di evacuazioni in caso di incendio, nonché i vari tipi di estintori obbligatori, vediamo che essi sono stati spesso aggiornati negli anni. Nello stesso tempo, non si è vista ancora la minima proposta, anche minimalista, di regolazione sulla sicurezza IT degli uffici. Come mai?

Luca Tenzi: Innanzitutto le ICT sono effimere. A differenza dell'estintore che è un'oggetto fisico, omologato, per delle condizioni estreme (incendio) che si producono in luoghi che non sono poi tanto cambiati col tempo, un "estintore" ICT valido oggi non lo sarebbe già più domani.

Il secondo punto di questa mancanza di regolamenti risiede nell'internazionalità dei vari prodotti, servizi, software ed applicazioni utilizzati, facendo in modo che un regolamento nazionale non avrebbe successo. Anche se sono svizzero, lavoro in Svizzera per una firma svizzera, ma uso regolamentare un hosting e dei siti, per non parlare dei codici fonte, che sono "domiciliati" altrove.

Ci sono invece grandi attività da parte di organizzazioni internazionali e ditte di peso per tentare di allinearsi su di un minimo di sicurezza, ma si torna troppo spesso alla mancanza di una visione chiara e comunemente accettata di che cosa entra o meno nel mondo "cyber". Nell'ambito ancora più piccolo della sicurezza, non c'è ad esempio una linea chiara di divisione tra le azioni di attacco e gli errori. La difficoltà comunicativa quindi viene a rafforzare i paesi che possiedono tecnologie e che hanno una volontà geopolitica non solo di controllarli ma anche di espanderne l'uso.

Laurent Chrzanovski: Proprio su questo, si sentono sempre più voci nell'Unione europea che vorrebbero imitare il sistema americano, con uno stato presente per aiutare le ditte e la società a livello di raccomandazioni ma con la responsabilità reale in caso di danni lasciata alla vittima ed all'assicurazione. Come europeo, cioè vivendo in sistemi dove il cittadino accetta di pagare un certo numero di tasse ed imposte per far si che lo stato lo tuteli, questa tendenza non la preoccupa?

Luca Tenzi: E' il trend. In Svizzera un tale sistema non farebbe dibattere perché siamo abituati a pagare assicurazioni private su tutto, sentivo proprio l'altro giorno che dovremo pure pagare una nuova polizza per coprire eventuali danni a terzi imputabili ai nostri animali domestici…

Però, a parte questa battuta, la volontà di passare ad un sistema assicurativo senza altri attori nel mondo della cyber-security è molto pericoloso. In primis, un danno "cyber" non ha limiti nel tempo (immagine, perdita di dati, etc.) e quindi non può essere valutato in termini di costi reali e nemmeno realistici dopo un attacco.

Poi, rischiamo di ritrovarci, ed è lì che subentra la componente europea, con delle assicurazioni che rifiuteranno il rischio se un'incidente avviene od è legato agli Stati Uniti d'America, dove le multe sono esorbitanti e non ci sono limiti per i danni morali. Basti guardare le clausole delle assicurazioni malattia svizzere: siamo coperti dovunque nel mondo tranne negli Stati Uniti, dov'è fissato un massimo quantificato di rimborso.

Con un po' di fortuna geopolitica, si arriverà a un consenso almeno europeo, speriamo globale *ad minima* però con dei criteri omogenei di che cosa deve fare una ditta, in materia di sicurezza, per beneficiare di questa copertura. Ma siamo ben lontani, ragion parlando, da questo momento. ■

Parlare al business

autore: Massimo Cappelli

I responsabili dei dipartimenti di Information Security (CISO) hanno un problema di fondo: farsi comprendere dal business. Ogni fine anno, per utilizzare una metafora pubblicitaria, c'è un CISO che si alza con l'obiettivo di stilare la lista degli investimenti e delle esigenze per il prossimo anno per proteggere l'azienda. Ogni fine anno, dall'altra parte, c'è un responsabile amministrativo-finanziario (CFO) che si alza e si rende conto che dovrà battagliare con un CISO per comprendere a quale scopo siano necessari nuovi investimenti o risorse per la funzione di Information Security.

E questa è solo una delle battaglie che un CISO deve affrontare durante l'anno. Al di là dei problemi quotidiani che possono derivare da informazioni da proteggere, vulnerabilità da far rientrare, minacce da presidiare, il CISO, sempre che sia invitato ai tavoli, deve anche combattere con i responsabili delle linee di business per includere nelle nuove progettualità un budget per gli aspetti di sicurezza. Accade di frequente che il budget stilato per lo sviluppo di un nuovo servizio digitale non tenga in considerazione il costo delle contromisure necessarie alla sua protezione per le ragioni più disparate ma sostanzialmente per l'urgenza del business di decollare con nuovi servizi e il timore che la "Security" possa in qualche modo rallentare o bloccare alcune delle funzionalità sviluppate.

L'incomprensione fra i due mondi spesso è dettata dall'utilizzo di linguaggi diversi: quello del CFO e dei responsabili di business legato ad ottiche economiche di costi-benefici, di risparmi, di ritorno degli investimenti, mentre quello del CISO legato a ottiche più tecniche: firewall, protocolli di sicurezza, anti-virus, intrusion detection system, SIEM e così via. Ed ecco che ogni fine anno, le richieste di investimento del CISO vengono tagliate in quanto ritenute un costo a cui non si riesce ad associare un reale beneficio.

C'è un punto di incontro fra i due mondi? Potenzialmente il punto di incontro per facilitare il processo di autorizzazione all'investimento potrebbe essere il Return on Security Investment (ROSI). Il ROSI è una formula che può essere semplificata come:

ROSI = (Riduzione della perdita monetaria – Costo della soluzione)/Costo della soluzione

La formula di per sé è semplice e lineare. Se ci si addentra però un attimo sulle 2 sole voci che la compongono, si aprono dei vasi di pandora da cui escono filosofeggianti interpretazioni su cosa debbano contenere e come stimarli, lasciando in questo caso basiti sia i CISO sia i CFO. Non sarà questo articolo a infondere la scienza esatta riguardo il ROSI e le voci che devono comporlo, l'intenzione è semplicemente di arrivare ad un "so what" tanto caro alla consulenza quanto ai decisori.

Il "so what" è determinato dai dati e non dalle dichiarazioni. Pertanto, durante il progetto europeo Ecrime, la Fondazione si è interrogata su quali potessero essere i dati da considerare nel costo della soluzione. Per affrontare l'argomento si è partiti dall'analisi di alcuni scenari di attacco. E' stata presa una potenziale tipologia di attacco ad un'azienda (es. ransomware). L'attacco è stato suddiviso in fasi, seguendo a grandi linee il modello della cyber kill chain. Una volta identificate le fasi, sono state considerate tutte le contromisure che avrebbero potuto contrastare l'attacco in ogni singola fase. Esempio per evitare l'apertura di un' email di spear phishing (singola fase di un attacco), le contromisure da mettere in campo possono essere:

1. Campagna di sensibilizzazione dei dipendenti
2. Policy aziendale sulla gestione delle email
3. Aggiornamento dei software a protezione dell'end point
4. Utilizzo di software contro il phishing

Probabilmente ci sono anche altre contromisure ma questo è un semplice esempio. Identificate le contromisure, la Fondazione si è interrogata su quali

BIO

Massimo Cappelli è operations planning manager presso la Fondazione GCSEC. Da gennaio ricopre anche il ruolo di responsabile del CERT e della cyber security di Poste Italiane all'interno della funzione Tutela delle Informazioni. Nella sua passata esperienza ha lavorato come consulente in Booz Allen Hamilton e Booz & Company nella practice Risk, Resilience and Assurance.

potessero essere i costi associati alle soluzioni stesse. Pertanto prendendo ad esempio, la contromisura "Campagna di sensibilizzazione dei dipendenti", i costi da imputare a tale contromisura sono il risultato della sommatoria delle seguenti voci:

a. Percentuale del tempo annuo delle risorse impiegate a preparare il programma di valutazione e formazione per la sensibilizzazione dei dipendenti moltiplicato per il costo delle risorse (comprensivo di contributi previdenziali versati dalla azienda);

b. Percentuale del tempo annuo impiegato dalle risorse ad effettuare il test per la valutazione del proprio livello di sensibilizzazione e a seguire i corsi preparati moltiplicato per il costo delle risorse;

c. Ammortamento della quota parte dell'applicativo utilizzato per le attività di e-learning o in aula

d. Costo del materiale necessario per l'attività di formazione e sensibilizzazione (es. brochure, linee guida,..)

e. Costo di eventuali formatori esterni.

Questo esempio ci fa comprendere come sia complesso anche per un CISO tenere traccia di tutti i costi associati ad una contromisura. Inoltre, molte delle informazioni qui sopra rappresentate non sono di diretta gestione del CISO stesso. Ecco che è necessario quindi un lavoro trasversale in cui si devono reperire i dati e associare le giuste percentuali in base alle attività svolte. Il costo per l'utilizzo di uno strumento non deriva solo dal costo di ammortamento ma anche dalle persone che impiegano il tool. Ovviamente i più attenti noteranno che alcuni costi non sono stati rappresentati ma possono essere imputati come costi generali.

Prendiamo il caso della email di spear phishing, come faremo a valutare se l'utilizzo delle campagne di sensibilizzazione hanno portato ad un risultato positivo o negativo? In teoria nel momento in cui, email di spear phishing vengono segnalate dai propri dipendenti all'ufficio competente, è già un primo indice di successo ma non ci rappresenta quantitativamente il valore in termini economici.

Una possibilità è definire quale potesse essere lo scenario nel caso in cui quelle email di spear phishing fossero state aperte. Qui di fatto entra in gioco la capacità del CISO di dettagliare lo scenario di impatto derivante dall'esecuzione dell'attacco stesso. A chi era rivolta l'email, quali informazioni gestisce la persona a cui era rivolta, di quali credenziali o privilegi era in possesso, etc. etc. Inoltre da un'analisi anche dei link contenuti nell'email e di quanto possa essere raccolto si può determinare anche lo scopo e risalire a casistiche similari o identiche e pertanto formulare delle ipotesi di mancato impatto in termini di informazioni preservate, disservizi evitati, reputazione mantenuta.

La Fondazione ha effettuato un passo ancora in più e ha cercato di fornire una classificazione delle contromisure inserendole in un modello internazionale. Il modello scelto è stato il cyber security framework del NIST, ultimamente diffuso con qualche modifica anche in Italia. Il modello prevede 5 macro "Funzioni" al cui interno vengono identificate delle categorie di attività. Prendendo il nostro esempio, la contromisura "Campagna di Sensibilizzazione dei dipendenti" rientra nella Funzione "Protect" (PR) dentro la categoria Awareness & Training (AT). Pertanto le voci di costo relative all'iniziativa sensibilizzazione vengono classificate con il codice "PR.AT". In questo modo, tutte le attività di Information Security vengono rendicontate, categorizzate analiticamente e possono essere richiamate per varie tipologie di reportistica.

Alla fine dell'anno, prendendo sempre il caso dello spear phishing, il CISO, se avrà fatto bene il suo lavoro di rendicontazione, avrà in mano tutte le casistiche di spear phishing che hanno impattato l'azienda a cui dovrà attribuire un valore di impatto avvenuto, nel caso l'attacco sia andato a buon termine ed evitato nel caso in cui le varie contromisure abbiano avuto successo. Il beneficio ovviamente viene calcolato sull'impatto evitato mentre quello accaduto purtroppo produrrà delle perdite per l'azienda che si andranno ad ammontare nella bilancia dei costi e benefici ai costi sostenuti dall'azienda.

"Perché servono risorse e investimenti per le campagne di spear phishing? Perché dallo storico si evidenzia che a fronte di un costo sostenuto pari a X abbiamo evitato un impatto pari a Y, dove X<Y pertanto l'azienda ci ha guadagnato per un danno potenziale evitato". Stessa cosa varrebbe se la fase di attacco fosse stata fermata in un'altra fase dell'attacco, magari quando il C&C era già stato installato. In questo caso il CISO valuterà anche il peso delle singole contromisure messe in piedi e verificherà qual è il giusto bilanciamento. Ovviamente la matrice di impatto deve essere concordata con le funzioni di business e con il top management generale. Questa, come già espresso in precedenza, non è scienza esatta ma vuole gettare le basi per iniziare a ragionare in ottica di business anche per strutture che vengono definite di puro costo. Non abbiamo trattato l'argomento della metodologia di calcolo dell'impatto, ma sicuramente sarà un argomento che verrà trattato prossimamente. Alla base di tutto c'è sempre un dato. E' come lo raccogliamo, analizziamo, classifichiamo e aggreghiamo che fa la differenza. Prima di iniziare molti aspettano di avere in mente il quadro completo, ma spesso il quadro completo viene realizzato iniziando a dipingere e si raggiunge la perfezione solo attraverso dei tentativi revisionati. ■

IE2S, un convegno fuori dal comune

In esclusiva gli atti del convegno

autore: Laurent Chrzanovski

Mescolando atelier di lavoro, momenti di formazione e la conferenza plenaria, il Sommet IE2S di Chamonix crea un'atmosfera di lavoro unica, propizia alla fertilità e alla libertà degli scambi, nel cuore del prestigioso scrigno del Monte Bianco. Lontano dall'agitazione dei centri di decisione delle grandi capitali e secondo un programma propizio alla discussione, i partecipanti si focalizzano con serenità sui loro scambi. Il Sommet IE2S di Chamonix procura così ai partecipanti l'opportunità unica di apprendere gli uni dagli altri, di condividere delle idee e di iniziare insieme la messa in opera di nuove soluzioni in una cornice molto privilegiata. Il Sommet è patrocinato dall'Istituto degli Alti Studi per la Difesa Nazionale (IHEDN - Institut des Hautes Études de Défense Nationale).

BIO

Professore Universitario di archeologia, storia e sociologia, Laurent Chrzanovski dirige ricerche nel quadro della Scuola dottorale e post-dottorale dell'Università di Sibiu. Regolarmente invitato a tenere corsi nelle maggiori università europee, è autore/editore di 18 libri e più di un centinaio di articoli scientifici, ai quali vanno aggiunti innumerevoli articoli destinati al grande pubblico. Nel campo della cyber-security, si è specializzato nello studio antropologico dei comportamenti individuali nell'uso delle nuove tecnologie; è membro e consulente contrattuale del "Roster of Experts" dell ITU e di numerosi gruppi di lavoro in Romania ed in Svizzera. Ha fondato e dirige il congresso annuale "Cybersecurity in Romania. A macro-regional public-private dialogue platform", dal quale è nata l'idea della rivista Cybersecurity Trends, nel quadro della quale svolge il ruolo di redattore capo.

Queste giornate di seminario molto esclusivo sono riservate a venticinque dirigenti d'impresa che dialogano con un numero equivalente di esperti dell'alta Amministrazione e dei Servizi dello Stato, delle Forze Armate, della Gendarmeria, della Polizia, del Ministero dell'Economia, delle Finanze e del Digitale.

Due giorni di seminario a porte chiuse offrono anche il vantaggio di riunire una cerchia ristretta di esperti e di professionisti in un vero Chatham House dove le persone imparano a conoscersi, a darsi fiducia e quindi a dibattere realmente sul fondo delle problematiche che stanno al centro delle loro preoccupazioni. Una conferenza aperta al pubblico, agli insegnanti, alle PME e alla stampa chiude questo evento.

L'intelligenza economica nell'era del digitale:

L'intero concetto è stato recentemente rivisto nel cuore stesso dello Stato Francese, con la creazione del Servizio di Informazione Strategica e della Sicurezza Economica (SISSE), presso il Ministero dell'Economia e dell'Industria, con a capo il Commissario Jean-Baptiste Carpentier, recentemente nominato dal Governo.

Questa funzione regia, era prima occupata dalla D2IE, Delezione Interministeriale all'Intelligenza Economica, che è stata sostituita da

Jean-Baptiste Carpentier Commissario nazionale all'informazione strategica e alla sicurezza economica.

questo commissariato dipendente da un solo ministero, dunque con una più grande rapidità nella gestione delle informazioni poiché centralizzata in un vero servizio. Questo va di pari passo con la riforma, nel 2015, dell'ANSSI, l'Agenzia Nazionale della Sicurezza dei Sistemi d'Informazione, che è passata dal suo ruolo originale di organo, essenzialmente consultivo, validando la conformità di un certo numero di tecnologie e software, a un ruolo centrale dotato di poteri coercitivi, che gli permettono di gestire la situazione, di monitorizzare l'applicazione delle normative e di sanzionare le imprese che non vi si adatterebbero.

Il nuovo approccio presentato da questa nuova autorità ci è apparso audace, ma in simbiosi con le realtà d'oltre-Atlantico. Esso parte dalla constatazione che lo stato, nel campo digitale, non può assumere contemporaneamente sia i costi delle negligenze delle imprese private che quelli di tutti i tipi di reati commessi sul net. Lo scopo è quello di fare abbassare drasticamente la curva del rischio, così come valutato in molti campi, cioè un diagramma semplice costituito dal dato «impatto» e dal dato «probabilità».

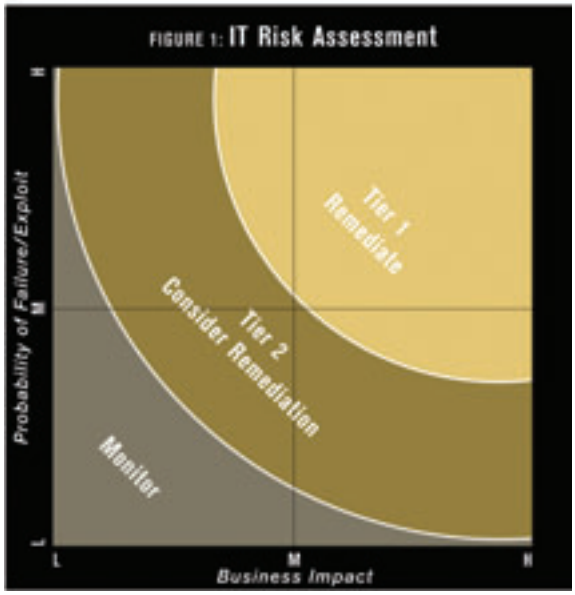


Grafico: © Bruce Jones, Report Security and Risk Metrics in a Business-Friendly Way, (Information Security 10.2009)

In questo diagramma, se l'insieme della curva si abbassa grazie ai regolamenti e al supporto dello Stato presso le imprese per ciò che riguarda la prevenzione e la messa in campo di un insieme di misure di previdenza, allora lo Stato potrà coprire le perdite dovute agli avvenimenti a forte probabilità ma con debole impatto o ancora agli imprevisti indipendenti dalla buona conformità delle imprese, mentre sarà responsabilità delle imprese assumersi i propri errori (se sono dovuti ad una non-conformità alle norme) o ancora alle assicurazioni di assumere i costi causati da attacchi devastanti con molto debole probabilità.

L'analisi, molto pertinente, del Commissario Carpentier ha puntato il dito su un assioma quasi schizofrenico, consistente, da una parte, da certi imprenditori che vedono nel mondo «cyber» delle opportunità, mentre, dall'altra parte, da imprese specializzate e certi responsabili dello Stato che vedono in questo stesso mondo un vespaio di pericoli e minacce. L'evoluzione della cultura imprenditoriale e istituzionale deve portare a una presa di coscienza che il mondo digitale è fatto sia di pericoli che di opportunità e che lo Stato deve tenere il ruolo di un attore saldo e discreto permettendo alle imprese diventate coscienti di acquisire un forte valore-aggiunto, difensivo e offensivo, calcolabile in termine di benefici.

Il concetto stesso di sicurezza è fortemente esteso nel suo perimetro in rapporto a ciò che abbiamo avuto l'occasione di intendere in forum simili a quello di Chamonix : per l'atelier diretto dal nuovo capo del SISSE, la direzione di un'impresa proattiva deve, in termini di comprensione dell'insieme del sistema, avere una strategia basata su una combinazione (non esaustiva) dei seguenti fattori: un sistema provato di vigilanza a tutti i livelli, ivi compreso l'antiterrorismo, la sicurezza sul lavoro, una solida conformità («*compliance*») di fronte a dei rischi ben conosciuti, per esempio quelli che sono legati all'ecologia, alla corruzione o ancora alla criminalità, un dominio eccellente dell'informazione detenuta o acquisita e infine una strategia adattativa di cyber-sicurezza completa messa in campo ad ogni livello.

Cyber –sicurezza

Colonello Xavier Guimard Sotto-direttore dell'anticipazione e della coordinazione del servizio delle tecnologie e dei sistemi d'informazione

La grande questione risiede sempre nel fatto di trattare o meno la gestione del rischio digitale in un modo simile a quello degli altri rischi. Secondo gli esperti presenti, è chiaro che la risposta è, logicamente, negativa, poichè se si può applicare lo schema *security/safety* (nel caso presente, *security* = trattamento dei rischi accidentali; *safety* = trattamento dei rischi legati alla malevolenza), l'insieme delle azioni condotte nel mondo digitale sfugge allo schema tradizionale di prevenzione-azione-reazione dal punto di vista giuridico o di polizia.

In effetti, l'equilibrio è molto differente. Se si parte dalla filosofia del criminale, quest'ultimo aveva di fronte tradizionalmente una situazione data, la speranza di un guadagno, una difficoltà a perpetrare il suo misfatto (tecnica, logistica, tradizionalmente un fattore di cui ogni impresa deve prendersi carico) e un rischio corso (la pena di giustizia, campo riservato alle istituzioni dello Stato).

Ora, nel mondo digitale, lo schema è veramente rovesciato. Contrariamente all'ambiente puramente fisico, l'ultima componente, quella del rischio, non esiste praticamente più.

Il delinquente determinato sa beneficiare di tutte le carte della extraterritorialità giocando sul piano internazionale, rendendo quasi nulla la possibilità che venga arrestato, giudicato e condannato per i suoi atti. La sola arma rimane dunque quella di rinforzare al massimo le difficoltà poste all'attaccante. Questo campo dipende dagli investimenti delle imprese e lo Stato è, a priori, assente.

Il ruolo dello Stato, forte della sua esperienza, è da situare nel campo cruciale della prevenzione, cioè di condividere con le imprese i rischi che esse incorrono, il potenziale che hanno di essere attaccate e le perdite economiche che un attacco riuscito comporterebbe sul loro bilancio e sull'immagine.

Terrorismo e lezioni da trarre su altri piani

Dopo gli attentati del 13 dicembre 2015, si sono imposte numerose riflessioni, dirette in più direzioni, in *primis* quelle che sono legate alla prevenzione e alla difesa della maggioranza delle persone. La prima costatazione, la battaglia più lunga da condurre, è quella di trasformare i riflessi «culturali» e di adattare la mentalità collettiva alle nuove minacce.

Una professoressa armata in una scuola israeliana

Per esempio, è stato sottolineato che, in Francia, un bagaglio o un pacco abbandonato rimanda ancora, nel subconscio collettivo, di una semplice dimenticanza e non di un atto intenzionale di deporre un artefatto devastatore, un riflesso agli antipodi di quello di un cittadino israeliano, per il quale ogni oggetto lasciato in luogo pubblico è associato a una minaccia imminente, che richiede un intervento immediato.

Mappa degli attentati di Parigi: dalle 21h20 – 0h20, i terroristi seminano la morte a Saint-Denis e nell'Est parigino © Le Monde

Uno degli esempi più sorprendenti e certamente di più triste memoria, è quello dei terroristi che hanno condotto il massacro del Bataclan: durante tre ore, i criminali sono rimasti nella loro automobile nelle vicinanze del luogo dello spettacolo.

Quattro chiamate telefoniche hanno indicato questo atteggiamento sospetto alla Polizia, che non le ha considerate rilevanti, sottostimando il grado di rischio potenziale portato a loro conoscenza dai cittadini inquieti durante le loro chiamate: questo è un segnale d'allarme che dimostra a che punto, e anche a che livello, lo Stato non crede ancora (culturalmente) a un pericolo imminente.

Per educazione, nessuno pensa male a priori, ciò che rende la missione educativa dello Stato urgente e necessaria, rendendo ogni persona un attore della responsabilità della difesa collettiva, senza peraltro sviluppare una paranoia.

Gli scenari possibili di attacchi ancora ben più devastanti di quelli del 22 dicembre, sono diventati l'oggetto di gruppi di lavoro e di simulazioni di crisi. Ciò che mette in luce la volontà delle Istituzioni Francesi di cambiare sia il dogma che l'equazione della sicurezza.

Ad esempio, non esiste nessuna misura reale contro il terrorismo nelle scuole, poichè i dispositivi ed i procedimenti da seguire in caso di attacco armato sono gli stessi di qualsiasi altro pericolo (sismico, meteorologico, ecc.), regolamentati tal quali da vari decenni. Questo darebbe ai criminali, che non hanno niente da perdere, tutto il tempo necessario per compiere azioni mirate prima che le forze dell'ordine possano intervenire.

Un altro aspetto vitale da rinforzare al più presto, è quello dell'aiuto alle vittime attraverso le altre vittime. L'esempio del Bataclan dimostra che se la popolazione avesse avuto le basi pratiche tipiche dei volontari del pronto soccorso (i «gesti che salvano», come la respirazione bocca-a-bocca, la stimolazione cardiaca, la messa in posizione dei feriti) parecchie vite avrebbero potuto essere salvate prima dell'intervento massiccio delle ambulanze e dei medici professionisti.

Gli attentati sono serviti a condurre una revisione in profondità dell'analisi proattiva e in «live» dei «segnali deboli». Il vantaggio di questo approccio, destinato prima di tutto alla messa in sicurezza dello spazio pubblico fisico, può essere applicata con successo sia alla sicurezza cyber che all'intelligenza economica.

Anche qui, la mancanza di una cultura del pericolo imminente, la mancanza di mezzi o ancora le barriere giuridiche riguardanti la vita privata sono altri temi che devono essere imperiosamente rivisti al più presto.

Nelle scuole, per esempio, si tratta di formare un certo numero di professori e di genitori a riconoscere le attitudini non abituali e sospette e a rapportarle al più presto ai referenti designati e con i quali saranno in contatto permanente.

Nello spazio pubblico, lo Stato dovrebbe dotarsi di mezzi per analizzare in diretta il flusso delle informazioni delle videocamere e di scoprirvi comportamenti, presenze, gesti non abituali o sospetti, sapendo sempre e ugualmente stabilire delle priorità nei differenti tipi di segnali deboli.

Di fronte all'immenso numero di dati raccolti, bisogna investire su quei segnali che presentano criteri tali da giustificare un investimento umano e un'analisi approfondita, poichè hanno un'alta possibilità di essere precursori di attività criminali di grande impatto.

Le segnalazioni di comportamenti sospetti da parte di cittadini volontari, ognuno nel suo quartiere, simile al sistema messo a punto dalla gendarmeria, avrebbe anche il suo peso, poichè il volontario potrà indicare tutto ciò che gli sembrerà sospetto e saranno in seguito gli esperti a valutare ogni situazione, rilevando da un lato le piste interessanti e scartando, dall'altro, i comportamenti individuali privi di pericolo.

L'applicazione della buona comprensione dei «segnali deboli», nel campo cyber, deve effettuarsi attraverso una combinazione di analisi automatiche, e in seguito umane, delle anomalie all'interno del sistema così come verso il sistema, che si tratti di una istituzione o di un'impresa.

Geopolitica e sfide future

La rottura del nostro ambiente circostante attuale con il passato, è sempre più marcata.

Gli eventi terroristici, le crisi, si riavvicinano con delle cadenze mai raggiunte prima, e la vecchia strategia di attaccare da lontano, per esempio in Afghanistan, per difendere la patria, non è più di attualità in un paese che ha subito attentati e che deve tenere in conto della presenza di elementi ostili sul suo territorio.

Cambiamenti, disseminazione e la moltiplicazione di pressioni esterne sono tre fonti ormai allineate all'interno di una stessa Nazione; questa nuova realtà esige mutamenti profondi dei mezzi e delle strategie da mettere in campo.

In materia di informazione bisogna, idealmente, portare nuove risposte per quanto concerne lo *jihadismo*. I mass-media hanno sparso opinioni spesso rinforzate da elementi del mondo politico, che danno a questa dipendenza sia una legittimità «religiosa» che uno statuto di combattente, poichè secondo la retorica convenzionale, il fatto, per l'Europa, di dichiararsi in guerra, implica di essere militarmente di fronte a un nemico, che si riconosce come tale, e non di dover reprimere in modo poliziesco dei criminali.

Tra l'altro, risulta che un elemento che non è stato considerato nel suo giusto valore negli anni 2000 è quello della identificazione a rango di eroe del «nuovo terrorista». Prima del 2000, nessuno voleva veramente diventare un terrorista, le cui incarnazioni (Mesrine, Carlos) erano personaggi singolari, nemici pubblici a vita con lo statuto di delinquenti, mentre oggi, il terrorista è glorificato: è un resistente che offre la sua vita per una causa.

Questo fenomeno, forse «consacrato» dalla dichiarazione di guerra di George W. Bush in seguito agli attentati del 2001, genera continuamente dei nuovi "candidati"; è diventato una sorta di avventura proposta ai giovani grazie ad un discorso di manipolazione, accattivante e molto ben strutturato, continuamente adattato alla situazione quotidiana e contrariamente a degli stereotipi spesso veicolati dalla stampa.

Lo *jihadismo* è una espressione moderna in risposta al mondo occidentale, che utilizza sia i codici della comunicazione moderna che le tecniche migliori di manipolazione mentale. La cassa di risonanza, che sono i mass-media, favorisce in un certo modo la considerazione di questo movimento in un'ottica religiosa e di guerra, a spese di una realtà composta di individui manipolati che diventano assassini sulla base di un ideale prima di tutto politico.

Di fatto, ci troviamo assolutamente di fronte a un «management» estremamente sofisticato, sia che si tratti di quello relativo ai grandi attentati condotti da Al Qaeda negli anni 2000, sia a quello del «macello organizzato» gestito dallo Stato Islamico nei territori che occupa e, in Occidente con i giovani indottrinati e addestrati ad azioni di forza che ritornano nel proprio paese.

I mezzi di prevenzione e di educazione da mettere in opera sono enormi, poiché il caso francese dello *jihadismo* è anche un rivelatore delle coesioni sociali attuali, e anche se gli spot televisivi e i portali multimediali «*stop-jihadismo*» sono stati giudicati «deboli» come risposta – l'account Twitter «*stop-jihadismo*» fa una pallida figura di fronte ai più di 30.000 account pro-jihadisti francofoni – si incominciano a vedere i loro frutti poiché il loro unico scopo è di far sapere a tutti che esistono delle risposte, che esistono delle cellule specializzate di ascolto alle famiglie e, soprattutto, che esiste un momento in cui, l'individuo caduto in preda ai messaggi radicali, può essere salvato e reintegrato.

Olivier Kempf
Ricercatore associato all'Istituto delle Relazioni Internazionali e Strategiche (IRIS) e direttore del foglio strategico La Vigie.

È in questo momento preciso che tutti gli sforzi devono essere dispiegati, poiché è semplice da identificare: ogni manipolazione mentale riuscita passa da un momento di seduzione (i siti internet) ma non diventa effettiva se non dopo la presa in mano dell'individuo, nel mondo reale, da parte di esperti in indottrinamento, seguita dal viaggio in zone di combattimento.

Così, è prima di una di queste due tappe e, soprattutto a monte del primo incontro fisico fra il giovane ed il suo «mentore», che bisogna, da parte dei congiunti e delle famiglie, avvertire lo Stato affinché possa avere più possibilità di portare a buon fine la sua azione di prevenzione.

Il fatto che una buona parte dei futuri *jihadisti* europei siano partiti per il Medio Oriente convinti di andare a effettuare aiuti umanitari prima di ritrovarsi, sul posto, con un'arma in mano per l'ultimo stadio della manipolazione, dimostra bene che il sistema di comando dell'individuo manipolato passa attraverso due tappe di indottrinamento.

Il problema da risolvere è anche quello della definizione del ruolo dello Stato, la cui presenza deve essere sia più visibile che meno burocratica, ma deve anche trasformarsi in il maggiore attore che stimola pratiche di sicurezza da parte dei cittadini e delle imprese senza esserne l'unico ed inaggirabile motore. Lo Stato deve suscitare delle iniziative civiche, ispirarle senza per forza condurle.

Le soluzioni centralizzate di un tempo, basate sulle azioni dello Stato, non sono più efficaci in un quadro così complesso, dove il volume dei dati «pro-jihadisti» è ancora oggi nettamente superiore a quello dei dati e dei siti di prevenzione, nella guerra dell'informazione che si svolge attualmente sul net.

Tra l'altro gli attentati di Parigi non nascondono ma al contrario permettono delle proiezioni future ben lontane dallo Stato Islamico.

In effetti, il modello di Stato totalizzante quale quello dello Stato Islamico offre una coerenza ideologica, dà una spiegazione a tutto, attirando ogni persona recettiva a questa retorica. Questo metodo, di fronte ad un individuo divenuto consumatore prima di essere cittadino, incomincia in effetti a raggiungere ben altri ambienti alter-mondialisti.

Due elementi interessanti sono stati evidenziati. È stato sottolineato che nella mancanza di punti di riferimento delle società di «consumo» nelle quali viviamo, il problema che pone il terrorismo è che, da un lato gli individui si abituano alla nuova situazione e che, dall'altro non c'è un fenomeno di causa ed effetto sulle imprese.

Per gli individui, questo riflesso ci ricorda l'epoca dei bombardamenti effettuati dagli Alleati sulla Germania: invece di suscitare la rivolta della popolazione contro il regime nazista, queste distruzioni quotidiane sono state talmente massicce che gli abitanti delle grandi città si sono poco a poco abituati. Per le imprese, se si prende l'esempio di una compagnia di trasporto il cui veicolo ha subito un attentato, ci sarà certo una perdita del giro d'affari nei giorni successivi, ma non a lungo termine.

La problematica del futuro è di iniziare d'ora in avanti a lavorare in profondità su questo fondo di rassegnazione e di adattamento della società. La resilienza dell'individuo, nel mondo fisico ma anche virtuale, deve essere mantenuta ed educata, poichè si osservano già i segnali inquietanti della strutturazione di movimenti diversi.

Tutti uniti nel rigetto della società come si presenta oggi, questi potrebbero attaccare non dei civili ma bensì delle reti nevralgiche, delle centrali nucleari, dei treni a grande velocità, o ancora a dei capi d'impresa, esattamente secondo il modello delle Brigate Rosse e della Rote Armee Fraktion degli anni 1960.

Dresda nel 1945

Il caso di Notre-Dame-des-Landes – la rivolta massiccia contro il progetto di costruzione del Grande Aeroporto di Parigi e le azioni di sabotaggio – può sbocciare alla fine su dei cyber -attacchi di punta o ancora su assassini mirati. Secondo il contesto, queste movenze ed i loro atti potrebbero rapidamente passare, da epifenomeni a tendenze di successo del terrorismo di domani, che sarebbe ancora più internazionale e più frequente degli attentati jihadisti attuali, puntiformi e mirati ad un dato paese.

Manifestanti opposti alla costruzione del Grande Aeroporto di Parigi sul sito di Notre-Dame-des-Landes

In questo caso sarebbero le imprese ad essere toccate in pieno, ed è per questa ragione che la sensibilizzazione e la preparazione dell'amministrazione delle imprese è più che mai all'ordine del giorno. Secondo gli specialisti, questa forma di terrorismo, studiata da 15 anni, inizia a prendere ampiezza e a superare la sua forma di «fenomeno emergente».

Una delle conclusioni maggiori dei dibattiti è che l'insieme delle direzioni studiate costituisce in un certo modo - salvo per gli specialisti - dei «*campi informi*» (cyber, mondializzazione, intelligenza economica, terrorismo) per i quali è vitale creare, in seno allo Stato, delle cellule flessibili, adattative e trasversali, in comunicazione costante con la società e le imprese.

È solo con una maggiore comprensione di questi aspetti, che sono paradossalmente strettamente legati gli uni agli altri, che individui ed attori pubblici e privati potranno imparare ad adattarsi e a difendersi per evolvere in essi.

La nuova sfida per la Francia, risiede nel creare delle Istituzioni che permettano alla società e al mondo economico di diventare attori maggiori nella creazione e l'applicazione delle misure da mettere in campo e non il contrario. ■

Intervista VIP a Christophe Réville, Presidente e fondatore del Summit nazionale IE2S "Intelligence économique et sécurité/sûreté".

Christophe Réville

autore : Laurent Chrzanovski

Laurent Chrzanovski: Signor Réville, Lei è uno dei principali artefici del 2° Summit sull'Intelligenza Economica e la Security/Safety, IE2S. Come è arrivato, così rapidamente, a passare dall'idea alla realizzazione di un momento di confronto che riunisce tanti partecipanti di prestigio su temi così diversi come quelli che sono stati trattati?

Christophe Réville: Auditor dell'Istituto degli Alti Studi per la Difesa Nazionale (IHEDN), formato all'intelligenza economica da numerosi anni, e peraltro sensibile alle problematiche della sicurezza, attraverso la mia agenzia francese di contro-spionaggio economico partecipo da lungo tempo a congressi, forum, conferenze e altri simposi, che trattano questi temi. Con il mio collega Jean -Pierre Troadec, anch'egli auditor dell'IHEDN e specialista di intelligenza economica, abbiamo constatato che questi eventi, certamente istruttivi ed interessanti, non permettevano di creare veri contatti con i partecipanti di alto livello e nemmeno di assistere ad un vero scambio di idee e di conoscenze.

Questo progetto del Summit sull'intelligenza economica e sulla security/safety è nato parecchi anni fa e ha preso corpo con la prima edizione nel 2015.

La nostra idea – copiare una formula ben conosciuta nel mondo anglosassone come ad esempio il forum di Davos – consisteva nel creare un evento nel quale limitare allo stretto necessario il tempo dedicato ai tavoli di lavoro per sviluppare maggiormente il networking e la comunicazione tra i partecipanti. Il principio base è stato di aprire la partecipazione ad un numero ristretto di soggetti al fine di garantire una reale conoscenza e scambio di opinioni tra loro.

Abbiamo cosi riunito una cinquantina di partecipanti, per metà, rappresentanti dello Stato e delle grandi agenzie governative e l'altra metà di imprese importanti, che hanno potuto così conversare in maniera approfondita sulle realtà della vita economica – nell'ambito delle tematiche che trattano, in tutta libertà e riservatezza. Il patrocinio dell'Istituto degli Alti Studi di Difesa Nazionale ci ha permesso un accesso alla «rete delle reti» e di avere un approccio diretto alle più alte autorità dello Stato. E' stato così facile, nel 2014-2015, creare in qualche mese questo evento e dar vita quest'anno alla sua seconda edizione.

Laurent Chrzanovski: L'apertura ad una rosa scelta di invitati, che tra l'altro dà la possibilità ad alcuni studenti e rappresentanti dei mass-media di raccogliere i principali frutti degli atelier di lavoro, è una decisione che

merita di essere indicata. Come è stata accolta dai rappresentanti dei settori più "confidenziali " del vostro summit?

Christophe Réville: Il numero dei posti al Summit è stato volontariamente limitato al fine di privilegiare la qualità dei lavori piuttosto che la quantità. Tuttavia è importante presentare al mondo esterno l'output dei lavori che hanno avuto luogo durante i seminari privati- o perlomeno ciò che può esserne divulgato. La nostra missione all'Istituto degli Alti Studi di Difesa Nazionale è di diffondere lo spirito di Difesa nazionale e di sicurezza nella società civile. L'interesse degli studenti per questi temi è sempre maggiore ed è nostro dovere accoglierli nel maggior numero possibile, per cui sono invitati a nostre spese. Anche i rappresentanti delle PMI ma di gruppi industriali invitati si fanno portavoce degli insegnamenti del Summit nella loro cerchia professionale.

Nonostante l'aspetto un po' "elitista" del seminario privato in cui non tutti possono essere ammessi, questa iniziativa è molto acclamata da parte dei partecipanti.

Laurent Chrzanovski: Nel momento in cui solo le multinazionali più in vista e le organizzazioni internazionali interessate incominciano a balbettare il termine di "sicurezza logica", il summit è stata la dimostrazione eclatante che tutti i vari «campi» compresi in questo termine sono ben collegati: sicurezza fisica, video, cyber, intelligenza economica, safety, resilienza e difesa.

Christophe Réville: Da sempre, la sicurezza dei sistemi di informazione fa parte del concetto di intelligenza economica. Ma, contrariamente a certi professionisti, noi crediamo che non si debba associare la gestione dell'informazione alla sua sola protezione. Tra l'altro, questo è un concetto a doppio senso. La protezione dell'informazione altrui è un dato che fa pienamente parte della vigilanza e della colletta di informazioni custodita sia da parte di un'azienda, sia da parte dello Stato.

La protezione dell'impresa e del suo capitale di informazioni copre uno spettro molto largo che va dalla sicurezza fisica quotidiana del personale e delle infrastrutture alla sicurezza che è possibile mettere in campo in caso di minacce identificate o ipotetiche. In questo campo, il fattore umano è preponderante.

È pure in questo campo che le «porte di accesso» per i criminali sono le più evidenti ed in pieno sviluppo – benché siano quelle che richiedono risorse umane qualificatissime – e che le tecniche di emulazione, di ingegneria sociale, di atti delittuosi (minacce, estorsioni, ricatto, ecc.).

C›è quindi il bisogno urgente, al di là dei tradizionali mezzi e tecniche di protezione, di condurre un lavoro molto importante di educazione, di sensibilizzazione, di formazione da effettuare presso l'insieme del personale dell'organizzazione, nessuno escluso.

Questo ha ovviamente delle ripercussioni sulle risorse umane (contratti di lavoro e regolamenti interni), che sono legalmente obbligate di raccogliere l'assentimento delle persone interessate per potere intervenire nelle loro sfere di social media.

BIO

Co-fondatore e supervisore del Summit IE2S Chamonix Mont-Blanc 2015, Christophe Réville è esperto in management, comunicazione e fattori umani in intelligenza economica, presso l'Istituto degli Alti Studi per la Difesa Nazionale (IHEDN - Institut des Hautes Études de Défense Nationale), Région Lyonnaise. Co-iniziatore del Summit IES Chamonix Mont-Blanc 2015, Christophe REVILLE dirige una società di consulenza e di formazione in strategie d'impresa e comunicazione. Diplomato all'EM Lyon, dopo quindici anni in qualità di dirigente di impresa e di comunicazione, si è dedicato alla formazione per le imprese. Diplomato in Programmazione Neuro Linguistica, formato all'Analisi Transazionale e alla Gestalt, ha sviluppato programmi di management del cambiamento e gestione dei fattori umani relativi alle problematiche della sicurezza e dell'intelligenza economica. Professionista della comunicazione interpersonale, si è specializzato nel contro-spionaggio economico dal punto di vista delle risorse e dei fattori umani. Auditor dell'IHEDN (178e sessione in regione IHEDN, 2009), Christophe Réville è riservista della gendarmeria (capo squadra RC) e membro della rete di cyber-difesa della riserva civile, collegata allo stato maggiore delle armate.

E'quindi un lavoro importante e di lunga scadenza che si deve mettere in cantiere, soprattutto nelle organizzazioni importanti: la base stessa dell'organizzazione deve essere ripensata, rifondata con l'accordo di tutto il personale.

Ora, pur se le imprese sono pronte a investire (tra l'altro con cifre relativamente modeste) nel sistema di protezione, non manifestano un grande entusiasmo nell'adozione di politiche di regolamentazione, di sensibilizzazione e di motivazione del proprio personale.

Niente può essere fatto sui temi della sicurezza senza un coinvolgimento diretto di tutti attori dell'impresa

Laurent Chrzanovski: Come avete identificato i partecipanti che, oltre a essere fra i più riconosciuti nel settore di appartenenza, sono stati soprattutto capaci ad approcciare ad una delle più vaste iniziative transdisciplinari che abbiamo avuto modo di osservare recentemente?

Christophe Réville: Gli esperti (e le esperte) presenti al Summit dell'intelligenza economica e della security-safety sono tutte e tutti molto impegnati. Confortati dall'adozione della regola di «Chatham house», che vuole che ogni fonte di informazione rimanga totalmente riservata, essi nutrono fiducia e non esitano a scambiarsi informazioni di prima mano.

La nostra modesta organizzazione è composta da personalità di altissimo livello che desiderano partecipare al Summit in qualità di esperti. Talvolta siamo obbligati a fare scelte drastiche. In effetti, l'aspetto pluridisciplinare fa anch'esso parte delle grandi originalità del Summit: il nostro scopo è di far comunicare due mondi che non si parlano abitualmente: il mondo dell'intelligenza economica – spesso considerata come molto universitaria – e il mondo della sicurezza, spesso ricondotta all'immagine caricaturale di «guardiano di parcheggio».

Infine, esiste chiaramente una distinzione che si produce nel piccolo mondo dell'intelligenza economica/sicurezza

fra coloro «che sono stati al Summit» (2015 o 2016), cioè che fanno parte del Circolo IE2S, e gli altri. Il prezzo per farne parte è elevato: impegno, disponibilità (tre giorni, sono molto lunghi per delle personalità di spicco impegnatissime), libertà di tono e di parola rare.

Laurent Chrzanovski: Si è spesso parlato di semantica, ma, né le definizioni delle parole, né il significato presente e passato di termini tecnici, hanno creato problemi di comprensione, anche quando essi erano utilizzati in modo molto differente da parte degli attori del Summit. Come si spiegano oggi le grandi incomprensioni "linguistiche" spesso esistenti fra i vari team di una stessa azienda di grandi dimensioni?

Christophe Réville: A partire da un certo livello, gli specialisti di alto livello conoscono il contesto e le sfumature riferibili ad un termine o ad un altro. Noi ci rivolgiamo ben al di là dei direttori di sicurezza o dei responsabili di sorveglianza: il nostro pubblico è costituito da amministratori di società o da dirigenti che hanno una visione strategica multidimensionale e spesso multiculturale e che quindi conoscono queste parole. Anche se la nostra vocazione è essenzialmente francese o in ogni caso francofona, parliamo di strategie mondiali che sono state evocate prendendo spunto dalle migliori pratiche conosciute in certi paesi stranieri per poi adattarle alle specificità francesi, sia culturali che sociologiche, le quali sono molto particolari – e questo non è sempre una qualità. E' interessante ricordare le differenze di definizione fra i termini sécurité (security) e sûreté (safety) secondo l'ambiente professionale dell'interessato. Eppure, alla fine, tutti si capiscono.

Laurent Chrzanovski: Durante la maggior parte degli incontri del 2016 in Europa, la forte plusvalenza in termini di risultati ottenuti merita una divulgazione verso il top management del settore privato e pubblico. Come pensate di valorizzare gli output del Summit negli ambiti politici, economici e civili?

Christophe Réville: È stata pubblicata una sintesi del Summit sull'intelligenza economica e la security/safety 2016 naturalmente. Tuttavia, al di là della diffusione numerica, noi lavoriamo essenzialmente sull'influenza diretta sul top management che orienterà le proprie strategie e politiche nella direzione comune definita durante il Summit. Il buon esito dei lavori sarà certo poco diffuso tramite i media, e senza dubbio poco «glorioso», ma noi puntiamo a una efficacia operativa piuttosto che ad una riconoscenza del pubblico. Detto questo, non c'é nessuna condiscendenza nè disprezzo del pubblico, solamente la preoccupazione di una efficacia massima, la più rapida possibile, attraverso azioni concrete, nel rispetto della Legge e dell'interesse generale.

Laurent Chrzanovski: Quali sono le vostre impressioni "a caldo"? Qual è secondo voi il più grande successo del 2° Summit e quali sono gli aspetti che vorreste migliorare?

Christophe Réville: In primis, la nostra soddisfazione è che questo secondo Summit abbia prima di tutto avuto luogo, e si sia svolto in seguito in buone condizioni. Sarà, in effetti, una sfida ripetere questo evento, al quale auspichiamo una lunga vita con il patrocinio dell'IHEDN.

La formula può certamente essere ancora migliorata, come già avvenuto a seguito dei rinvii dopo la prima edizione. Possono essere migliorati numerosi dettagli logistici e organizzativi, ma l'essenziale è che il contenuto e il format siano stati apprezzati dai partecipanti, che hanno manifestato il desiderio di ritornare il prossimo anno. Noi conserviamo il nostro credo: «prendere altitudine - il Summit si tiene a 2000 metri n.d.r. - per mettere in sicurezza il mondo di domani».

Laurent Chrzanovski: Di primo acchito, dopo solamente due edizioni, avete già un'idea dei miglioramenti o delle nuove tematiche che vorreste affrontare al Summit?

Christophe Réville: Nel 2016, il programma è stato influenzato da avvenimenti drammatici avvenuti in quest'ultimo anno nel nostro paese. Sono state condotte delle riflessioni, concrete ma sottili, sugli aspetti della lotta antiterroristica nelle imprese, la resilienza, e la difesa dei nostri interessi di fronte alle minacce emergenti. Questo è tra l'altro il tema ripreso nel prossimo colloquio annuale del Club dei Direttori della Sicurezza delle Imprese che si è tenuto il 15 dicembre; il CDSE è uno dei nostri partner etici e scientifici.

Non c'è dubbio che nel 2017, gli eventi di attualità alimenteranno le nostre riflessioni.

Tuttavia, gli spunti di riflessione e di azione sul tema dell'intelligenza economica e della security/safety sono molti e daranno luogo a nuovi lavori. Bisogna essere non solamente reattivi ma anche proattivi e anticipare le minacce emergenti.

E' un po' prematuro identificare un tema, il nostro comitato non si è ancora riunito per determinare le tematiche da affrontare per il 2017, parleremo senza alcun dubbio dei rischi i cui segnali deboli sono stati registrati, come ad esempio il rischio insurrezionale sul territorio – un avvenimento la cui probabilità è debole (ma al quale l'armata svizzera si è già interessata più di quattro anni fa). I nostri organi pubblici si sono preparati ad un tale disastro, ma niente traspare sul terreno economico concreto, che rimane il nostro campo d' azione essenziale. Il contesto elettorale nazionale della Francia nel primo

semestre 2017 mobilizzerà anche l'attenzione. Ci sarà del movimento nelle agenzie nazionali; è indispensabile esercitare la nostra influenza etica e positiva sulle politiche pubbliche future, facendo sentire le preoccupazioni dei dirigenti d'impresa. ■

XGen, è arrivata la sicurezza di nuova generazione

autore: Gastone Nencini,
Country Manager Trend Micro Italia

Trend Micro è la prima azienda di security a proporre il machine learning ad alta fedeltà in una strategia di protezione. Inizialmente applicata agli endpoint questa tecnologia è stata estesa a tutte le soluzioni, rendendo ancora più efficace la protezione server di Deep Security e la difesa delle reti con TippingPoint.

BIO

Gastone Nencini vanta una carriera significativa nel settore IT, iniziata oltre 25 anni fa con un'esperienza come programmatore presso Elsi Informatica e proseguita in Genesys come Technical Manager.
Nel 1998 Nencini approda in Trend Micro Italia dove viene nominato Senior Sales Engineer per il Centro e Sud Italia, per passare successivamente a un ruolo di maggiore responsabilità e prestigio, diventando prima Technical Manager Developing BU (Italia, Benelux e Paesi Scandinavi) per poi focalizzarsi sul mercato Italiano con l'incarico di Senior Technical Manager Italy. Nel 2012 Gastone diventa Technical Director Southern Europe e a Gennaio 2015 è ufficialmente nominato anche Country Manager Italia.
Durante questi anni in Trend Micro, Gastone Nencini ha gestito e supervisionato una serie di importanti progetti di sicurezza per i maggiori clienti, fra cui, a livello italiano, si possono citare: Telecom, Fiat, Poste, Vodafone, Ferrari, Banca Nazionale del Lavoro, Banca Intesa San Paolo.
Nencini ha, inoltre, introdotto servizi innovativi di assistenza e supporto per i clienti Enterprise e per il canale di rivenditori.

Trend Micro, leader globale nelle soluzioni di sicurezza informatica, ha reso disponibile **XGen Security**, una nuova e innovativa tecnologia per contrastare le minacce informatiche. Questa tecnologia ha fatto il suo debutto a ottobre 2016 focalizzandosi sulla protezione endpoint, con il nome appunto di XGen™ endpoint security. Il fulcro di questa nuova soluzione è un insieme intergenerazionale di tecniche di difesa dalle minacce che applicano in maniera intelligente la giusta tecnologia nel momento corretto. Il risultato è una protezione più efficace ed efficiente contro le minacce. Questo approccio di Trend Micro è unico, utilizza metodi comprovati per identificare velocemente i dati benigni e le minacce conosciute, mentre attiva le sue tecniche avanzate come il controllo delle applicazioni, la prevenzione degli exploit, le analisi comportamentali e il machine learning, per identificare più velocemente e in maniera accurata le minacce sconosciute. Trend Micro è stata la prima azienda di security a includere il machine learning ad "alta fedeltà" nel suo approccio, questo permette di analizzare i file sia prima della loro esecuzione che durante e utilizza funzioni di controllo e whitelisting per ridurre i falsi positivi.

A febbraio Trend Micro ha compiuto un ulteriore passo avanti ed esteso le capacità di **XGen a tutte le soluzioni**. Questo è un approccio intelligente alla sicurezza che viene incontro anche ai consumi, utilizzando tecniche come la prevenzione delle intrusioni, web e file reputation e il controllo delle applicazioni per gestire efficacemente il volume di minacce conosciute. Le tecniche più avanzate come l'analisi comportamentale, il machine learning e l'analisi sandbox sono utilizzate invece per gestire in maniera più veloce e accurata le minacce sconosciute più difficili da rilevare. Tutte queste capacità sono

alimentate dalla piattaforma di intelligence Smart Protection Network, che grazie alla massima protezione ed efficienza assicura una sicurezza veloce ai clienti in tutto il mondo.

Estendo le capacità di XGen a tutte le soluzioni, TippingPoint è diventato così il primo vendor NGIPS (Next-Generation Intrusion Prevention System) a rilevare e bloccare gli attacchi in tempo reale utilizzando il machine learning. **TippingPoint NGIPS** è parte delle soluzioni Trend Micro per la difesa delle reti e combinandosi con una protezione dalle minacce avanzata è ottimizzata per prevenire gli attacchi mirati, le minacce avanzate e i malware. Trend Micro TippingPoint NGIPS applica i modelli statistici del machine learning per caratterizzare i vettori estratti dai dati di rete e decidere in tempo reale se il traffico di rete è dannoso o benigno. Questa evoluzione aiuta a rilevare meglio i malware avanzati e le comunicazioni invisibili ai normali standard. TippingPoint NGIPS applica anche le tecniche di machine learning, per rilevare e bloccare le famiglie di malware che utilizzano algoritmi per la generazione di domini (DGAs).

TippingPoint è anche leader nel **Magic Quadrant di Gartner** dedicato ai sistemi di rilevamento e prevenzione delle intrusioni. TippingPoint NGIPS è sostenuta dai TippingPoint Digital Vaccine® Labs (DVLabs) e dal programma Zero Day Initiative e permette una prevenzione accurata e preventiva delle minacce in tempo reale e senza danneggiare le prestazioni di rete. Rispetto agli anni passati ha significativamente migliorato il suo posizionamento nel quadrante, nella "completezza di visione" e nella "abilità di eseguire".

La tecnologia XGen è stata estesa ovviamente anche a Deep Security, che arrivata alla sua decima versione è la soluzione ammiraglia Trend Micro per la protezione dei server e si estende ora anche ai container. **Deep Security** continua a essere la soluzione leader nella protezione dei server fisici, virtuali e cloud negli ambienti più utilizzati come quelli VMware, Amazon Web Services (AWS) e Microsoft Azure, aggiungendo nuove caratteristiche ottimizzate per ottenere la massima prestazione, l'efficienza operativa e la risposta alle ultime minacce. Deep Security include un insieme intelligente di tecniche intergenerazionali di difesa dalle minacce per proteggere i server, che comprende funzioni anti-malware e di prevenzione dalle minacce (IPS) per rilevare e fermare gli attacchi sofisticati. Come parte della strategia di sicurezza XGen, Deep Security 10 aggiunge nuove caratteristiche inclusa la prevenzione dei cambi di software non autorizzati grazie al controllo delle applicazioni. La nuova funzione di controllo applicazioni è stata pensata per il cloud ibrido e protegge i server da attacchi sofisticati come quelli ransomware, perfino quando le applicazioni cambiano costantemente e i carichi di lavoro elastici sono distribuiti negli ambienti virtuali e cloud. Deep Security 10 si focalizza sul migliorare ulteriormente l'abilità nel rilevare le minacce sconosciute e supporta l'integrazione con la sandbox di Trend Micro Deep Discovery. Presto si completerà anche con il machine learning. Deep Security è ottimizzata per VMware, AWS e Microsoft Azure e fornisce una visibilità completa che permette la protezione automatica dei server. Questa nuova release aggiunge dei miglioramenti nella gestione e nell'integrazione, come una connessione più veloce per i carichi di lavoro AWS e Azure, insieme al supporto per l'ultima versione dell'account Azure e Azure Resource Manager v2 (ARM). La soluzione va oltre i carichi server e protegge i container Docker con funzioni anti-malware, IPS e controllo delle applicazioni. ■

> *TippingPoint è leader nel Magic Quadrant di Gartner (sistemi di rilevamento e prevenzione delle intrusioni), mentre Deep Security è leader nella protezione dei server fisici, virtuali e cloud.*

Il 2016 è stato l'anno delle estorsioni

Il 2016 è stato, come previsto da Trend Micro, l'anno delle estorsioni online. Il numero di famiglie ransomware in circolazione ha registrato una crescita del 752%, passando da 29 a 247 e il numero di ransomware che si è abbattuto su utenti, aziende e organizzazioni in tutto il mondo è stato di oltre 1 miliardo, generando perdite colossali.

Ecco cosa è successo in Italia nel 2016:

- **L'Italia è stata raggiunta dal 2,40% di ransomware di tutto il mondo. A livello EMEA è la più colpita**
- **Il numero totale di malware intercettati è di 22.104.954**
- **Il numero di app maligne scaricate è 2.646.804, l'Italia è tra i Paesi con il numero maggiore di app maligne scaricate**
- **Le comunicazioni spam inviate dall'Italia sono state 22.550.991**
- **Le visite a siti maligni sono state 21.790.390**
- **4.686 i malware di online banking intercettati**

Cresce il numero degli attacchi e i costi per le aziende

autore: Morten Lehn,
General Manager Italy, Kaspersky Lab

La sicurezza informatica diventa sempre più strategica per il management.

Gli investimenti nella sicurezza IT sono in crescita stimolati anche dal fatto che le perdite finanziarie stanno aumentando in modo significativo: in media oggi un solo incidente di cyber-security costa 861.000 dollari alle grandi aziende e 86.500 dollari alle piccole e medie imprese. Ancora più allarmante è che il costo delle attività di ripristino cresce significativamente in base a quando viene scoperto l'incidente. Le piccole e medie imprese tendono a pagare il 44% in più per riprendersi da un attacco scoperto una settimana o più dopo la violazione iniziale, rispetto agli attacchi individuati in un giorno. Le grandi imprese, nelle stesse circostanze, pagano il 27% in più. Questi sono i principali risultati emersi dal report di Kaspersky Lab "Misurare l'impatto finanziario della sicurezza IT sulle imprese", basato sull'indagine Corporate IT Security Risks[1] del 2016.

Per questo motivo le conversazioni sulla sicurezza informatica non riguardano più solo le divisioni IT ma anche il top management, questo significa che chi è responsabile di evitare i cyber attacchi può chiedere budget maggiori con la possibilità di ottenerli.

In base alla ricerca svolta da Kaspersky Lab, in Italia il 70% delle aziende prevede una crescita nei prossimi tre anni dei propri budget per la sicurezza IT. La disponibilità di budget più alti può portare ad un aumento nel numero di addetti alla sicurezza in azienda, maggiori investimenti in tecnologia, opportunità di sviluppo professionale e la revisione dei sistemi legacy, e sempre più questo significa anche superiori investimenti in servizi come formazione, forensic, intelligence o altro.

In alcuni casi, si tratta di una mossa forzata dovuta ai nuovi requisiti normativi o forse a causa della rapida espansione del business, ma sempre più perché la sicurezza informatica è ora considerata in modo diverso dal top management. Dal momento che il costo di una violazione è così alto e la frequenza degli attacchi maggiore, le difese per la cyber sicurezza sono viste come ormai un vantaggio competitivo.

In Italia, la principale ragione dell'incremento dei budget destinati alla sicurezza informatica è stata quella di rispondere alle esigenze normative (36%). Altre aziende hanno dichiarato che la scelta è stata guidata dal top management e dalla volontà di migliorare le difese dell'azienda (31%), solo il 13% ha invece affermato che il fattore determinante è stato la consulenza esterna. ■

BIO

Norvegese di nascita, Morten Lehn a luglio 2014 è stato nominato General Manager Italy di Kaspersky Lab, diventando il punto di riferimento dell'azienda per il mercato italiano.
Prima di ricoprire questa carica è stato Sales Director sempre in Kaspersky Lab, occupandosi delle attività di tutto il sales team dell'azienda, per il segmento B2B Corporate ed Enterprise, B2C Consumer e per le vendite online.
Prima di approdare in Kaspersky Lab nel 2013, ha lavorato presso il distributore di informatica Bludis, in qualità di Sales Manager dal 2002 al 2009 e in seguito di Sales Director, rispondendo direttamente al CEO dell'azienda. In precedenza Lehn è stato Business Development Manager in Unified Messaging Systems AS, dove ha gestito la start up della filiale italiana dell'azienda, e Sales Manager in Euroline AS.

Nota:

1 Corporate IT Security Risks l'indagine annuale condotta da Kaspersky Lab in collaborazione con B2B International. Nel 2016 è stato chiesto a oltre 4000 rappresentanti di piccole, medie e grandi imprese di 25 diversi Paesi quali fossero le opinioni riguardo la sicurezza IT e quali incidenti avessero dovuto affrontare.

EURISPES: Rapporto Italia 2017

La cyber security in Italia: maggiore consapevolezza da parte delle imprese ma budget limitato

autore: Massimiliano Cannata

"A circa centosessanta anni dall'Unità non siamo ancora riusciti ad amalgamare economicamente, socialmente i nove stati dai quali è nata l'Italia moderna. Il risultato è che abbiamo un paese frammentato in tante realtà che non comunicano tra loro. Alcune regioni del Nord possono vantare standard produttivi e livelli medi di vita paragonabili alle regioni più sviluppate del Centro Europa, di contro le regioni esposte a Mezzogiorno continuano da troppi anni a segnare il passo, restando lontane dai bagliori dello sviluppo. Le rappresentanze politiche per tutta risposta risultano sempre più autoreferenziali, disinteressate al dialogo e al confronto, hanno perso di vista il destino dei territori e delle comunità di cui sarebbe loro dovere preoccuparsi".

E' un' "Italia polimorfe" quella che è emerge dal Rapporto Italia 2017 dell'Eurispes, presentato a Roma nella prestigiosa cornice della Biblioteca Nazionale di Castro Pretorio. Una nazione angosciata- spiega il Presidente Gian Maria Fara - da livelli di povertà crescente (un italiano su quattro pensa di esserlo soprattutto a causa della perdita del lavoro) che vede la metà delle famiglie in difficoltà ad arrivare alla fine del mese e tantissimi giovani (circa il 13%) "costretti" a una retromarcia verso casa in mancanza di un'occupazione possibile".

Il presidente dell'Eurispes, Gian Maria Fara

Come ogni anno tante le fenomenologie sociali ed economiche oggetto di analisi e di studio. L'innovazione e il mondo dell'ICT è uno dei grandi temi al centro della trattazione.

Il cyberspace: un asset da tutelare

Come rivela puntualmente il Rapporto nella società digitale la sicurezza del cyberspace è diventata una priorità, per gli stati che devono difendere l'interesse generale, la vita dei cittadini e le infrastrutture critiche e per le imprese impegnate a proteggere i propri asset strategici. Secondo le previsioni del Report Global Risks 2014 del World Economic Forum nel 2020 le perdite economiche causate da attacchi cyber potrebbero arrivare fino a tremila miliardi di dollari. Non basta certo l'iniziativa dei singoli per affrontare una emergenza così grave, occorrono piani strategici di ampio respiro che coinvolgono pubblico, privato e ricerca, per effettuare un'efficace *governance del rischio informatico.*

Gli attacchi informatici causano alle sole imprese italiane danni per 9 miliardi di euro l'anno. Potenza e fragilità si toccano della dimensione della "infosfera", area preziosa che contiene dati riservati e informazioni sensibili, come sa bene il cyber crime, che si conferma come la prima causa di attacchi gravi a livello globale, attestandosi al 68% dei casi nel 2015 (era il 60% nel 2014). I crimini informatici nei primi sei mesi del 2015 sono aumentati del 30% rispetto al 2014, arrivando a costituire la causa del 66% degli attacchi informatici gravi. Sempre più spesso le azioni dei criminali hanno come obiettivo le infrastrutture critiche, come, ad esempio, le reti di distribuzione dell'energia e quelle di telecomunicazione: mentre nel secondo semestre 2014, su scala globale, si

BIO

Massimiliano Cannata (Palermo, 1968), Filosofo, giornalista Professionista, autore televisivo, svolge attività di consulenza nell'ambito della comunicazione d'impresa. Membro del Comitato scientifico di "Anfione e Zeto", collabora con "Technology Review", "L'impresa", "IlGiornale di Sicilia", "Centonove Press". E' autore di numerosisaggisuitemidella social innovation, della formazione, dello sviluppo organizzativo e manageriale.

sono verificati solo due attacchi, nella prima metà del 2015 se ne sono registrati 20, con un aumento del 900% (Fonte: Elaborazione Eurispes su dati Clusit, 2016).

Tra le potenziali vittime di attacchi informatici rientrano sia le Istituzioni pubbliche sia le imprese. Le imprese di piccole e medie dimensioni sono le più vulnerabili perché la cybersecurity comporta costi, legati alla dotazione di un efficace sistema di protezione, che non sempre queste hanno la capacità di affrontare. Inoltre, non sono da sottovalutare i danni economici e reputazionali con i quali le imprese sottoposte ad attacchi informatici si trovano spesso a fare.

Le diverse tipologie di attacco

Nel nostro Paese, sempre secondo le rilevazioni del Rapporto Clusit i settori maggiormente colpiti da attacchi informatici sono stati: *informazione e gioco:* media online, piattaforme di blogging e gaming nel 2015 hanno subìto un incremento degli attacchi pari al 79% rispetto al 2014; *automotive:* gli attacchi nel 2015 sono stati circa il 67% in più rispetto all'anno precedente; *ricerca ed educazione:* settore in cui si è registrato un incremento degli attacchi pari al 50%, per lo più con finalità di spionaggio; *ospitalità, alberghi, ristoranti, residence e collettività:* il comparto viene registrato per la prima volta nel Rapporto Clusit. A ben vedere, in questi casi gli attacchi sono finalizzati a colpire gli utenti. Ogni mese, un attacco su tre va a buon fine e viene scoperto in ritardo. Nel 66% dei casi la presenza di un attacco viene spesso scoperta dopo mesi (la media globale è del 51%), nel 7% dei casi (come la media globale) le violazioni vengono individuate dopo giorni e nel 16% dei casi dopo settimane (la media globale è del 22% - Fonte Elaborazione Eurispes, su dati Accenture, "High Performance Security Report, 2016). Secondo una ricerca Accenture, HfS emerge, inoltre, che le organizzazioni soffrono la carenza di budget da investire nell'assunzione di dipendenti opportunamente formati per difendersi dagli attacchi informatici. Per il 42% degli intervistati, infatti, è necessario un aumento di fondi per l'assunzione di professionisti di cyber security così come per la formazione delle risorse umane attualmente disponibili in azienda che, per oltre la metà dei rispondenti (54%), non sono sufficientemente formate per prevenire il verificarsi di violazioni della sicurezza. Interessanti anche i rilevamenti della quarta indagine internazionale di Zurich sul rischio di attacchi informatici che mettono in luce, gli effetti di attacchi informatici più temuti dalle piccole e medie imprese: furti di dati dei clienti (20%), reputazione aziendale (17%), furti di denaro (11,5%), furti di identità (7,5%) e furti di dati dei dipendenti (6,5%).

Il 29° Rapporto Italia dell'Eurispes

L'impegno sulla sicurezza

A dispetto della gravità di un fenomeno in espansione bisogna dire che soltanto il 19% delle grandi imprese ha maturato una consapevolezza tale da avere una visione di lungo periodo sulla sicurezza e da sviluppare piani concreti con approcci tecnologici e ruoli organizzativi definiti, mentre il 48% si trova ad uno stadio iniziale del percorso di cyber security. Le minacce più diffuse negli ultimi due anni sono state: malware (80%), phishing (70%), spam (58%), attacchi ransomware (37%) e frodi (37%). Le principali vulnerabilità sono: la consapevolezza dei collaboratori su policy e buone pratiche di comportamento (79%), la distrazione (56%), l'accesso in mobilità alle informazioni aziendali (45%), la presenza di dispositivi mobili personali (33%). Le imprese hanno sviluppato, in particolare, la necessità di porre al proprio interno responsabili manageriali per le strategie di cyber security. Tuttavia, oggi, meno della metà delle grandi imprese (42%) ha al proprio interno una figura di Chief Information Security Officer (CISO), il professionista incaricato di definire la visione strategica, implementare programmi a protezione degli asset informativi e mitigare i rischi, mentre nel 10% dei casi è prevista l'introduzione nei prossimi 12 mesi. (Fonte: Osservatorio Information Security & Privacy della School of Management del Politecnico di Milano).

Nel 36% dei casi l'Information security è affidata ad altri ruoli in azienda, come il responsabile della sicurezza. Il 12% delle imprese non ha una figura dedicata e non ne ha in programma l'introduzione nel breve periodo. L'aumento dei dati e l'eterogeneità delle fonti informative rendono, dunque, necessarie anche figure professionali per la gestione dei problemi della privacy. Il nuovo Regolamento europeo sulla protezione dei dati personali introduce la figura del Data Protection Officer (DPO), la cui presenza è prevista come obbligatoria per gli enti pubblici e le Pubbliche amministrazioni e in altri specifici casi previsti dalla nuova normativa dell'Unione. Il DPO è il professionista con competenze giuridiche, informatiche, di gestione del rischio e di analisi dei processi aziendali che mette in atto la politica di gestione del trattamento dei dati personali per adempiere alle normative di riferimento.

I maggiori ostacoli

I principali limiti con cui oggi le imprese italiane devono fare i conti per far fronte efficacemente agli attacchi cibernetici rimangono comunque: *Le competenze professionali:* le imprese denunciano la scarsità di fondi da investire nella formazione e nell'assunzione di figure professionali specializzate laddove la formazione e la sensibilizzazione culturale sono elementi fondamentali per proteggersi dal cyber crime; il *budget:* la cyber security richiede investimenti in formazione delle risorse umane, ma anche in tecnologia (applicazioni riguardanti cognitive computing e intelligenza artificiale e piattaforme per la cifratura dei dati); la qualità del *management:* spesso l'executive management considera la cyber security una spesa superflua mentre occorrerebbe definire una vera e propria strategia di cyber security, che tenga conto delle priorità del business, tra cui la tutela della propria reputazione aziendale e della protezione del dato. ■

autore: **Laurent Chrzanovski,**
Fondatore e co-redattore di
Cybersecurity Trends

Un onore seguito da grandi responsabilità

E' doveroso iniziare la postfazione del primo numero in lingua italiana lodando il coraggio, la lungimiranza e la professionalità della Fondazione GCSEC di Poste Italiane.

Dopo l'iniziativa di Poste Italiane e della Fondazione GCSEC di offrire al pubblico italiano la mostra "Eroi e Vittime dei Social Media, dai geroglifici a Facebook", ormai in esposizione permanente presso il Distretto Cyber Security di Cosenza, GCSEC oggi lancia il primo numero dell'edizione italiana di Cybersecurity Trends, l'unica rivista europea di spessore destinata a informare gratuitamente i cittadini e i dipendenti delle organizzazioni pubbliche e private sui rischi e i pericoli del mondo digitale nel quale viviamo.

Oltre alla lungimiranza della Fondazione, è doveroso evidenziare l'importanza di questa iniziativa per tre motivi ben precisi:

Il primo ha ispirato l'idea e poi la nascita, poco più di due anni fa, di Cybersecurity Trends. Tra gli esperti del gruppo dell'ITU, da anni ci rendevamo ben conto che in materia di awareness tutti i grandi paesi d'Europa, senza eccezione, stavano - e continuano - *"reinventando la ruota"*, elaborando all'interno di vari enti o gruppi di lavoro temi con scopi identici a quelli sviluppati contemporaneamente da altri gruppi, in altri paesi o addirittura nella stessa Nazione.

Questo fenomeno porta il cittadino europeo, che è il vero destinatario di queste iniziative, a non saper più scegliere il sito o la rivista che gli possa dare le informazioni più utili in base alla ricchezza e qualità dei contenuti offerti. Ancora peggio, tale fenomeno riduce le probabilità che il cittadino possa accedere a materiali di qualità superiori alla media.

Il secondo motivo è meramente culturale: un'educazione basica di awareness indirizzata agli adulti deve essere fornita con chiarezza nella propria lingua natia e non può essere proposta al cittadino in *"globish"*, la lingua inglese globale non-oxfordiana usata a livello internazionale. Per queste ragioni, spesso, importanti riviste, report e libri non sono letti o, peggio ancora, non compresi da chi non ha una buona conoscenza della lingua inglese.

L'ultimo motivo, e forse il più importante, è la decisione di rivolgersi al cittadino adulto. Fino a pochi anni fa, per motivi soprattutto sociali, ma anche di ricadute positive di immagine per il mondo politico, iniziative europee di awareness sono state dedicate quasi esclusivamente alla protezione on line dei bambini e degli adolescenti o sono state rivolte ai loro professori e genitori. Un motivo in più per cui questa iniziativa, in Europa, rimane vitale.

La Fondazione GCSEC di Poste Italiane, a dispetto della mediocre proattività tipica del nostro vecchio continente, ha precorso i tempi permettendo ai suoi lettori di essere preparati quanto i cittadini dei paesi asiatici. In effetti, dai risultati dei più recenti studi effettuati da vari Paesi sul fenomeno del rischio cibernetico e delle sue conseguenze, emerge che nei paesi più avanzati (Giappone, Taiwan, Singapore, Corea del Sud) le nuove generazioni, già dai primi anni di scuola, imparano a conoscere i pericoli della rete.

In questo contesto, anche il mondo adulto è un bersaglio facile perchè redditizio per la criminalità. Indifeso, nato con la macchina da scrivere o con il Commodore 64, inconscio delle fragilità delle nuove tecnologie e del mondo virtuale, espone la propria vita professionale, sociale e privata, a volte anche nei suoi aspetti più intimi, a nuovi rischi.

Inoltre emerge sempre più la necessità di portare awareness, cultura, educazione ai dipendenti delle organizzazioni statali e delle aziende. Tenendo conto dell'ampiezza che può avere un attacco SCADA come quello alla rete elettrica della regione di Ivano-Frankivvsk (Ucraina, 23 dicembre 2015), ci si rende ben conto che l'adozione delle soluzioni tecniche più avanzate, affiancate ai migliori esperti di cyber security non bastano più per far fronte attivamente alle minacce se gran parte di esse sfruttano la mancanza di sensibilizzazione e preparazione dei dipendenti sulla sicurezza informatica.

La fiducia accordataci da qualche mese dal CLUSIS, con il quale pubblichiamo in Svizzera la versione francese, e ora anche dalla Fondazione GCSEC di Poste Italiane, comporta molte responsabilità, *in primis* quella di portarLe caro lettore italiano, contenuti sempre più utili ed in linea con quanto avviene in tutta Europa. Con la nascita delle edizioni in lingua inglese (a giugno) e tedesca (a settembre), gli articoli provenienti da aree geografiche e da ambiti professionali diversi ci permetterà di offrire ai natii di ben 5 lingue diverse i punti di vista dei migliori esperti europei, nel vostro caso scelti, tradotti e integrati dalla Fondazione GCSEC. ■

Una pubblicazione

AGORA get to know! e

web for business swiss webacademy

A cura del GLOBAL CYBER SECURITY CENTER

Redazione:
Laurent Chrzanovski e Romulus Maier
(tutte le edizioni)
Per l'edizione del GCSEC:
Nicola Sotira, Elena Agresti

ISSN 2559 - 1797
ISSN-L 2559 - 1797

Indirizzi:
Bd. Dimitrie Cantemir nr. 12-14,
sc. D, et. 2, ap. 10, settore 4,
040234 Bucarest, Romania
Tel: 021-3309282
Fax 021-3309285

Viale Europa 175 00144 Roma, Italia
Tel: 06 59582272
info@gcsec.org

www.gcsec.org
www.cybersecuritytrends.ro
www.agora.ro
www.swissacademy.eu

Proteggere i bambini on-line è una sfida globale che richiede un approccio globale. Mentre molti sforzi per migliorare la protezione online dei bambini sono già in corso, la loro portata finora è stata più di carattere nazionale che globale. L'ITU (Unione Internazionale delle Telecomunicazioni) ha avviato l'iniziativa Child Online Protection (COP) per creare una rete di collaborazione internazionale e promuovere la sicurezza online dei bambini in tutto il mondo. COP è stato presentato al Consiglio ITU nel 2008 e approvato dal Segretario generale dell'ONU e da capi di Stato, Ministri e capi di organizzazioni internazionali provenienti da tutto il mondo.
Poste Italiane, insieme alla propria Fondazione GCSEC e alla Polizia Postale e delle Comunicazioni ha prodotto la Versione italiana delle linee guida ITU, guida per la protezione dei bambini nell'uso di Internet e guida per genitori, Tutori ed insegnanti per la protezione dei bambini nell'uso di Internet.

Scaricatele su: www.distrettocybersecurity.it/linee-guida-itu

www.itu.int/cop

web for your business
swiss webacademy

together with:

NEW STRATEGY CENTER

ANSSI

AGORA

Presents:

CYBERSECURITY IN ROMANIA CONGRESS
5th Edition

European Public-Private Dialogue Platform

September 14-15, 2017, Sibiu, Romania

https://cybersecurity-romania.ro

Under the aegis and with the support of:

ITU

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ambassade de Suisse en Roumanie

ANCOM
Autoritatea Națională pentru Administrare și Reglementare în Comunicații

SRI
Pazim și privim

CYBERINT

IGPR
POLIȚIA ROMÂNĂ

REPUBLIQUE ET CANTON DE GENEVE

POLICE GENEVE

CTS
Centrul de telecomunicații speciale

CSC
Centrul pentru Securitatea Cibernetică

RÉGION-IHEDN FRANCHE-COMTÉ

SIBIU
COUNTY COUNCIL

UNIVERSITÉ DE GENÈVE
OBSERVATOIRE UNIVERSITAIRE DE LA SÉCURITÉ

Romanian Association
for Information Security Assurance

ANIS
employers' association of the software and services industry

ULBS
Universitatea "Lucian Blaga" din Sibiu

GLOBAL CYBER SECURITY CENTER