Cybersecurity Trends

Edizione italiana, N. 2 / 2017

Il nuovo Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica

INTERVISTA VIP:

Pierre-Louis GIRARD

Luciano VIOLANTE

GLOBAL CYBER SECURITY CENTER

Speciale PSD2

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 di Tutela 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.

Cari lettori,

In questi giorni, in cui esce il nostro secondo numero, i giornali sono pieni di notizie riguardanti attacchi massivi in ogni parte del mondo e diretti alle infrastrutture digitali. Per ben due volte in questi mesi *armi digitali* della National Security Agency (NSA) sono state trafugate e utilizzate contro di noi.

Questa tesi è presente su moltissimi siti dove si dibatte dei recenti attacchi cibernetici, in particolare nell'autorevole blog di Bruce Schneier, le prime pagine dei principali giornali americani trai i quali il NYT e Wired. Dal canto suo l'NSA disconosce il suo ruolo nello sviluppo di queste armi e i funzionari della Casa Bianca sostengono che l'attenzione deve concentrarsi sugli attaccanti e non su chi ha prodotto queste armi. Sempre in questo periodo ho terminato l'interessante lettura del libro scritto dell'ex consigliere per l'Innovazione del Segretario di stato di Clinton; Alec Ross "Il nostro futuro". Qui sostiene che la creazione di lavoro e di ricchezza nei prossimi vent'anni sarà guidata dall'innovazione e il digitale occupa una buona parte del libro. L'autore arriva a sostenere che "la terra è stata la materia prima dell'era dell'agricoltura. Il ferro la materia prima dell'era industriale e i dati sono la materia prima dell'era dell'informazione". Se poi analizziamo l'infografica *"Data Never Sleep"* della società Domo (www.domo.com) scopriamo che il minuto Internet viene scandito dall'invio di 204 milioni di mail, 2,4 milioni di post su Facebook, su YouTube sono caricate 72 ore di video e Instagram riceve 216.000 foto. Nel 2015 tutto questo corrispondeva 5,6 zettabyte, uno zettabyte corrisponde a un sestilione di byte o in alternativa a un trilione di gygabyte.

Ross descrive uno scenario di trasformazione digitale e di innovazione nel campo scientifico che ci permetterà di vivere meglio e più a lungo. Però, in uno dei suoi passaggi si trova anche un cenno alla *"Weaponization of Code"*, dove affronta il tema del codice applicato alle grandi sfide di politica internazionale, sostenendo che da un lato creerà nuove opportunità, dall'altro potrà essere usato come arma, portando nuove sfide e nuove emergenze nel campo bellico e della sicurezza dei cittadini.

Trasformazione digitale e resilienza delle informazioni sono pertanto temi sempre più strategici e fondamentali in questo nuovo scenario di business dove i dati sono diventati parte fondamentale ed elemento di competizione. Scenario che viene messo in evidenza anche dalla direttiva Europea PSD2 sui pagamenti digitali alla quale abbiamo dedicato una sezione speciale in questo numero.

La PSD2 cambierà le regole del gioco per le banche rompendo il monopolio che oggi le banche detengono sui servizi di pagamento, aprendo alla concorrenza di aziende interessate e di fatto lasciando ai clienti la possibilità di decidere quando e se consentire l'accesso al proprio conto a terze parti secondo un modello di banca aperta. La direttiva impone, inoltre, una standardizzazione nella protezione delle modalità di esecuzione dei pagamenti digitali rendendo di fatto più sicure le transazioni. Digitale e sicurezza un connubio imprescindibile per i nuovi scenari di competizione delle aziende on-line; chi riuscirà a essere più innovativo beneficerà del nuovo ecosistema che vede sempre più dati e digitale, ecosistema che deve garantire sicurezza e resilienza per prosperare. ■

Buona lettura….

Indice

1	**Editoriale** Autore: Nicola Sotira
3	**ITU: Sviluppare le proprie capacità per vivere in un mondo digitale più sicuro.** Autore: Marco Obiso
4	**Intervista VIP con l'Ambasciatore em. Pierre-Louis Girard: L'Organizzazione Mondiale delCommercio (WTO) e il mondo digitale** Autore: Laurent Chrzanovski
6	**La nuova dottrina di sicurezza della Federazione Russa del dicembre 2016** Autore: Yannick Harrel
9	**Buongiorno Charlotte! Un esempio di ingegneria sociale su LinkedIn** Autore: Battista Cagnoni
12	**Internet, terrorismo e opportunità** Autore: Alessandro Trivilini
14	**A chi appartiene veramente un'automobile autonoma?** Autore: Mika Lauhde
16	**IntervistaVIP a Luciano Violante: Università e impresa devono allearsi per generare crescita e sviluppo** Autore: Massimiliano Cannata
18	**La strada verso la resilienza** Autore: Luigi Brusamolino
22	**Il nuovo Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica** Autore: Massimo Cappelli
25	**Privacy e intelligenza artificiale** Autore: Giancarlo Butti
28	**PSD2, cambiano le regole del gioco.** Autore: Nicola Sotira
30	**PSD2, un nuovo challenge? Piccola guida di valutazione.** Autore: Mihai Scemtovici
32	**PSD2 e gli impatti sui processi antifrode** Autore: Teo Santaguida
34	**PSD2 e sicurezza** Autore: Veronica Borgogna
36	**Cyber Authentication: regolamentazione per un'autenticazione veloce e sicura** Autore: Michele Gallante
40	**Numero e complessità degli attacchi informatici in crescita, nuove minacce ogni giorno: come difendersi?** Autore: Elena Agresti
42	**Intervista VIP con Marianna Cicchiello, Distretto Cyber Security Cosenza, referente della mostra permanente "Eroi e vittime dei social media"** Autore: Laurent Chrzanovski
44	**Security, vita privata, fiducia e ... il cloud** Autore: Eduard Bisceanu
46	**Evoluzione degli APT. Gli ultimi trend negli attacchi avanzati** Autore: Giampaolo Dedola
47	**Sicurezza IT, in Italia la paura è il cyberspionaggio** Autore: Carla Targa
50	**Recensioni bibliografiche**
54	**Dalla redazione: Un pò di cyber-cultura in un mondo di cyber-intox** Autore: Laurent Chrzanovski

autore: **Marco Obiso,**

Coordinatore per la cyber security, International Telecommunications Union, Ginevra

Caro lettore,

In questi ultimi anni più che mai, la cyber security è stata una delle nostre principali preoccupazioni.

Non farò qui alcun tipo di riferimento alle *"breaking news"* degli ultimi mesi; al contrario, vorrei soffermarmi su diverse regolamentazioni dell'Unione Europea, che avranno presto un impatto positivo sia sull'economia che sulle nostre vite private.

Che si tratti della Regolamentazione NIS, o della Direttiva GDPR, le loro implementazioni avranno effetti su un'area ben più estesa di quella dei soli Stati membri dell'UE. Tutti e due i regolamenti sono stati elaborati per garantire una migliore sicurezza per lo Stato, le aziende e i cittadini. Questi ultimi e la loro privacy sono chiaramente diventati una priorità, come dimostrato anche dal testo della GDPR.

Nel frattempo, abbiamo recentemente assistito alla presentazione editoriale del "Tallinn Manual 2.0", un'opera che riassume l'enorme lavoro condotto da un think-tank di autori prestigiosi per offrire a tutti i policy maker una migliore comprensione delle operazioni "cyber" e dei loro contesti legali.

Da molti anni ormai, anche l'ITU conduce un lavoro simile, incentrato sullo sviluppo e la condivisione delle conoscenze, attraverso la definizione di buone pratiche e di programmi di assistenza nel quadro della Global Cybersecurity Agenda, coprendo quindi aree chiave in ordine di priorità, come quelle delle misure legali, tecniche e procedurali, il miglioramento del livello di capacità ed infine la collaborazione internazionale.

Se parafrasassimo i titoli di due delle pubblicazioni dell'ITU destinate al grande pubblico, potremmo dire che ogni stato desidera vedere il suo ecosistema digitale con meno timori di essere attaccato, e quindi è in *"quest for cyber peace"* [1], mentre i cittadini sono in *"quest for cyber confidence"* [2], ovvero alla ricerca della fiducia nei servizi digitali migliorando la loro conoscenza e la loro consapevolezza sul loro corretto utilizzo.

Lo sviluppo delle proprie capacità, in tutti i campi, inizia proprio mantenendosi informati sullo stadio attuale delle minacce, delle possibili soluzioni per limitarne i danni e per risolverle. Così avviene pure nella grande arena della cyber security: i cyber pericoli possono essere contrastati con una maggiore conoscenza dell'ecosistema e dell'uso adeguato degli strumenti a nostra disposizione. In questo campo, la prevenzione destinata agli adulti, oggetto di questa rivista, è ormai un *challenge* prioritario, non meno importante della prevenzione dei bambini.

In questo senso, la moltiplicazione delle iniziative alle quali assistiamo sul nostro continente – possiamo citare l'app del CERT-EU, ben pensata e facile all'uso – risponde alla richiesta dei cittadini di essere informati meglio e più tempestivamente su vecchie e nuove minacce e su come difendersi contro di esse.

Un'altra iniziativa che considero molto rilevante è quella che riguarda la *"Coordinated Vulnerability Disclosure"* che si inserisce nel contesto più ampio dello scambio di informazioni, diventato una priorità in molti Stati europei. Questa iniziativa viene a sottolineare la doverosa necessità di un partenariato efficace tra pubblico e privato che, speriamo, di vedere adottato quanto prima. ■

Marco Obiso

1 Libro disponibilegratuitamente su www.itu.int/pub/S-GEN-WFS.01
2 Libro disponibilegratuitamente su www.itu.int/pub/S-GEN-WFS.02

L'Organizzazione Mondiale del Commercio (WTO) e il mondo digitale

Intervista VIP con l'Ambasciatore em. Pierre-Louis Girard

Pierre-Louis Girard

autore: Laurent Chrzanovski

Laurent Chrzanovski: *L'Organizzazione Mondiale del Commercio (WTO) è un'istituzione della quale tutti parlano mentre pochi sanno di che cosa si occupa precisamente. Lei ha presieduto diversi gruppi di lavoro, tra i quali quello che ha portato all'adesione della Cina alla WTO. Può spiegarci il ruolo della WTO, anche in quello che la distingue dal suo predecessore, il GATT?*

Pierre-Louis Girard: La WTO svolge tre ruoli fondamentali. Il primo è offrire un quadro di regole stabili agli attori del commercio internazionale di beni e di servizi. Il secondo ruolo promuove, attraverso negoziazioni commerciali, la liberalizzazione degli scambi di beni e di servizi o lo sviluppo di nuove regole che si applicheranno a questi scambi – queste negoziazioni si svolgono sotto forma di cicli, come l'Uruguay Round e adesso il Doha Round, oppure sotto forma di sessioni dedicate ad un tema o a un settore specifico. Il terzo ruolo della WTO, infine, è di mettere a disposizione dei suoi membri un sistema di risoluzione dei contenziosi, al quale essi possono indirizzarsi quando sospettano che uno dei loro partner abbia violato le regole del sistema e causato un danno ai loro interessi.

In molti aspetti, la WTO costituisce lo sviluppo e il raggiungimento parziale di molti obiettivi che si erano fissati, nel 1947, i negoziatori dell'Accordo Generale sulle Tariffe doganali e il Commercio (GATT). E' proprio così che uno degli scopi all'epoca, quello di coprire pure il settore dei servizi, è stato parzialmente realizzato nel quadro dell'Uruguay Round e delle negoziazioni specifiche ai servizi finanziari, che si sono svolte immediatamente dopo. Possiamo aggiungere anche l'accordo sulla protezione della proprietà intellettuale applicata ai beni e ai servizi, che ha definito le regole del commercio internazionale.

Laurent Chrzanovski: *Quali sono le principali direzioni di lavoro della WTO, o quantomeno le principali categorie di prodotti e commerci dei quali si occupa?*

Pierre-Louis Girard: I principali ambiti di lavoro non sono fondamentalmente cambiati, perché tutto quello che riguarda le condizioni degli scambi costituisce un «work in progress» come dicono gli anglosassoni. Gli sforzi di liberalizzazione del commercio dei prodotti agricoli e dei prodotti manufatti rimangono una componente centrale dell'attività della WTO. Ciò nonostante, quando si tratta di acquisti governativi oppure di aspetti ambientali del commercio dei beni e dei servizi, i requisiti imposti da regolamenti o normative sin dalla loro adozione hanno acquisito un'importanza sempre crescente nel quadro generale delle attività della WTO. Infine, da alcuni anni la WTO e i suoi membri tentano di elaborare – in particolare a beneficio dei paesi in via di sviluppo – procedure e programmi di sostegno per facilitare il commercio, specialmente per snellire le procedure doganali e rendere più semplice i trasporti dei beni.

Laurent Chrzanovski: *Il summit de Cancún ha sancito non solo l'inizio di una forma di ostilità aperta, nella quale la WTO figura come capro espiatorio principale, da parte di molti movimenti altermondialisti, ma anche l'inizio di critiche aspre da parte di non pochi governi. Perché?*

Pierre-Louis Girard: Il GATT così come la WTO sono stati sempre oggetto di contestazioni. Queste manifestazioni si sono anche, a volte, rivelate

BIO

L'Ambasciatore Pierre-Louis Girard è stato Rappresentante permanente della Svizzera presso il GATT (1984-1988), poi Direttore delle negoziazioni di adesione della Svizzera al GATT e alla WTO (1991-2000) e infine Rappresentante permanente della Svizzera presso la WTO (2000-2007). Dal 1988 al 2001, è stato Presidente del Gruppo di Lavoro sull'adesione della Cina alla WTO.

particolarmente violente come durante l'Uruguay Round, dove potremmo citare le azioni dei contadini europei - ed in particolare quelli svizzeri -, giapponesi e coreani. Peraltro, sin dalla fine degli anni novanta, tutte le negoziazioni sono state, a livelli molto diversi, accompagnate da azioni e manifestazioni. A quell'epoca risale l'espressione dello malcontento di diverse ONG di paesi sviluppati come di paesi in via di sviluppo, venute ad appoggiare le posizioni governative di questi ultimi paesi o perlomeno quello che le ONG hanno creduto essere nell'interesse di questi paesi.

Uno dei punti culminanti dell'azione degli «altermondialisti» è stato di sicuro raggiunto nel 1999, durante la conferenza ministeriale di Seattle, quando abbiamo assistito a un'alleanza tra ONG in favore dei paesi in via di sviluppo, movimenti a difesa dell'ecologie, delle tartarughe, delle foche e ben altro ed i rappresentanti delle centrali sindacali americane AFL-CIO che protestavano contro il dumping salariale da parte dei paesi in via di sviluppo. Questa alleanza eteroclita di movimenti è riuscita a bloccare qualsiasi attività nella città di Seattle per ben due giorni interi. Ciò nonostante, la vera causa dell'assenza di risultato della conferenza di Seattle risiede nel fatto che i paesi membri della WTO, e in particolar modo i paesi industriali, non avevano tra di loro un minimo accordo sulla base del quale poter lanciare una negoziazione.

Pe quanto riguarda il Summit di Cancún, abbiamo osservato lo stesso fenomeno di divergenze tra i principali membri industrializzati, in primis tra l'Unione Europea e gli Stati Uniti d'America sul dossier dell'agricoltura. Questa assenza di consenso ha offerto a parecchi membri in via di sviluppo un'ulteriore opportunità per presentare richieste ancor più importanti rispetto alle promesse che gli erano state fatte due anni prima a Doha. Ricordiamo che sono stati proprio gli stessi paesi dell'Unione Europea e gli Stati Uniti d'America ad aver dichiarato ufficialmente che il Doha Round sarà un «Development Round».

Laurent Chrzanovski: *Oggi, molti stati tra i più potenti tendono a privilegiare incontri o gruppi di lavoro basati su una regione, un'alleanza bi- o plurilaterale o un prodotto specifico. Come si spiega che, ciò nonostante, la WTO non solo rimanga al centro del dibattito, ma che continui ad attrarre persino nuovi membri importanti come la Russia, che ha aspramente negoziato la sua adesione, ottenuta solo nel 2012 (ovvero 9 anni dopo Cancún).*

Pierre-Louis Girard: Semplicemente perché il quadro giuridico rappresentato dagli accordi della WTO costituisce ancora oggi la base multilaterale più sviluppata, stabile ed efficace sulla quale possono far leva i paesi per sviluppare i propri scambi e proteggersi contro azioni predatrici lanciate dai partner commerciali. Peraltro, diventando membri della WTO, paesi come la Cina, la Russia e le Repubbliche dell'Ex-URSS, hanno dato una nuova dimensione al loro statuto di soggetto indipendente in termini di diritto internazionale, e di attori attivi nello sviluppo del framework giuridico internazionale.

Laurent Chrzanovski: *Oggi, tranne le materie prime, quasi tutti i «prodotti finiti» diventano sempre più ibridi e la percentuale di prodotti dotati di funzione di ricezione/trasmissione di informazioni è in crescita esponenziale. Questo dato non mette in pericolo le negoziazioni svolte in passato con successo sui «servizi» e i «prodotti» così com'erano considerati prima dell'Internet of Things?*

Pierre-Louis Girard: Questo fenomeno non è nuovo. La maggior parte delle esportazioni di beni erano già abbinate, nel passato, con elementi del campo dei servizi. Basti pensare al montaggio di una turbina, al servizio post-vendita di macchinari tessili, ecc. Il fatto che i servizi potessero già apparire allora come un'esportazione parallela a quella del bene in sé non cambia nulla al fatto che erano considerati, come un tutto unitario. Esattamente come oggi, quando acquistate un'automobile, comprate probabilmente anche la possibilità di ricorrere ad almeno due servizi integrati nel vostro acquisto: un ricevitore/trasmettitore GPS e uno Bluetooth.

Laurent Chrzanovski: *Pochi Stati, ma spesso tra i maggiori (si possono citare gli USA oppure la Cina) chiamano la WTO per fare eliminare ostacoli che pesano su questo genere di prodotti, quando altri paesi li rifiutano invocando l'eccezione di sicurezza nazionale – rimasta com'era stata definita già nell'articolo XXIb del GATT (datato 30 ottobre 1948!) e poi riprodotto nel 1994 (TRIPS art. 73) e in corso di riadozione, quasi senza nessuna novità, nel GATS (art. 14bis). Pensa che la WTO sarà capace di emettere verdetti su «prodotti» che includono servizi multipli in aggiunta al bene fisico intrinseco?*

Pierre-Louis Girard: L'articolo sulla sicurezza nazionale è un articolo fondamentale, che è facile da comprendere ma anche facile da abusare basti pensare alle misure prese ai suoi tempi dall'amministrazione Reagan contro il Nicaragua. Invocare questo articolo implica generalmente considerazioni varie, e spesso non è facile apprezzarne la validità. Non vedo in conseguenza né i membri della WTO, né l'Organo di risoluzione dei litigi, essere disposti a far prova di temerarietà su questo aspetto.

Laurent Chrzanovski: *Come si spiega il mancato adattamento della WTO all' «era digitale» nella quale viviamo oggi? Pensa che sia ragionevole rimanere sui concetti di «mercanzie», «servizi», «beni agricoli e industriali», «prodotti» nonché «diritti di proprietà intellettuale attinenti al commercio» senza considerare prodotti o servizi a forte valore aggiunto che sono ormai automatizzati, digitali, transnazionali?*

Pierre-Louis Girard: Le basi giuridiche che esistono oggi sono chiare e solide. Gli eventuali sviluppi inerenti prodotti o servizi «a forte valore aggiunto/automatizzati/digitali/transnazionali» bisognerebbe che tutti gli Stati membri si accordassero sulla natura esatta di questi prodotti e soprattutto che le disposizioni giuridiche attuali, ovvero quelle internazionali (tra le quali spiccano quelle della WTO) e quelle nazionali (leggi sulla protezione dei dati, leggi sul rispetto della privacy) si rivelino palesemente insufficienti.

Laurent Chrzanovski: *Un ricordo particolare della Sua attività alla WTO?*

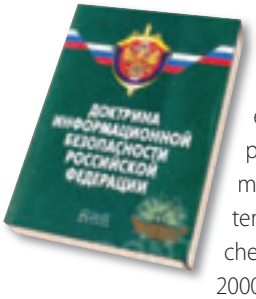
Pierre-Louis Girard: Mi viene immediatamente in mente una mia visita, alla fine degli anni novanta, alla Ministra del Commercio Estero della Cina. Appena entrato nel suo ufficio, lei mi interpellò: "Allora, Ambasciatore Girard, che ne pensa della Cina di oggi?". Una domanda alla quale mi venne naturale esclamare: "E' capitalismo selvaggio!". E lei non riuscì a trattenere una lunga risata, riconoscendo il lunghissimo cammino in termini di riforme eseguite sin dal 1988, anno della creazione del Gruppo di lavoro per l'entrata della Cina al GATT. ■

La nuova dottrina di sicurezza delle informazioni della Federazione Russa di dicembre 2016

autore: Yannick Harrel

Gentili lettori,

Molti tra di voi hanno saputo, probabilmente in modo frammentario e purtroppo ritrasmesso con non pochi errori da numerosi media occidentali, che la Federazione Russa si è dotata di una nuova dottrina sulla sicurezza delle informazioni (Доктрина информационной безопасности Российской Федерации) pubblicata ufficialmente il 5 dicembre 2016.



Considerate le informazioni pubblicate dai vari media europei e non solo sono doverose due precisazioni. In primis, questa è non la prima dottrina pubblicata dalle massime autorità della Federazione Russa su queste tematiche, basta consultare il volume *"La cyberstratégie russe"*[1] che analizza l'ukaze (decreto presidenziale) del 9 settembre 2000 dalla prima all'ultima parola. La seconda precisazione di ordine deontologico, è che per "bon ton" quando si cita un testo si dovrebbe indicare la fonte esatta soprattutto quando la citazione è redatta in una lingua terza. Purtroppo, la duplicazione su larga scala dell'informazione (chiamata anche più volgarmente "copia-incolla") non considera la fonte come un elemento necessario da replicare.

La nuova dottrina del 2016 colpisce immediatamente per la sua brevità, nulla a che vedere quindi con la pesantissima compilazione di articoli del primo opus e della loro ripartizione in quattro sezioni, la cui lettura è complicata da molte ridondanze e da cambi di prospettive.

Sin dall'inizio della nuova politica, le autorità russe propongono una definizione di quello che denominano "spazio informazionale", con il riferimento esplicito ma non limitativo alla rete Internet (senza tuttavia rinchiudervisi). Ci troviamo davanti a una differenza radicale col testo iniziale, che non menzionava in alcun modo Internet rimanendo fedele a una stretta neutralità dal punto di vista tecnologico, perché con la scelta di non dare una definizione completa, i redattori di allora avevano optato per un'enumerazione dei settori e dei punti tecnici mirati.

Nel documento, la formulazione è sensibilmente diversa e, la "rete delle reti" viene menzionata in diversi punti.

La definizione scelta dalla Russia è la seguente: *"La sfera informazionale deve essere compresa come un insieme di oggetti, di sistemi, di siti basati sulla rete Internet, di reti di telecomunicazioni, di tecnologie, di entità la cui funzione è di costituire e di trattare l'informazione, gestire e sviluppare le tecnologie afferenti la sicurezza*

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 specialità. 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.

УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

dell'informazione ed anche i meccanismi di regolamentazione delle relazioni pubbliche".

Il seguito del testo è alla fine una riconduzione dei principi stabiliti nella dottrina del 2000; con un richiamo rilevante alla difesa degli interessi nazionali, prevalentemente nel campo della sfera informazionale. Ci permettiamo una precisazione tutto tranne che insignificante: sin dall'inizio dell'articolo 2 vengono evocati i tre livelli di questa sicurezza informazionale. Proprio dove la visione americana si basa su tre strati (software, materiale, informazionale), quella del suo alter-ego russo sceglie di fondarsi su di un altro trittico costituito dall'individuo, dalla società e dallo Stato. Questo concetto era già incluso nel testo di sedici anni fa ma non in modo così evidente. Questa particolarità è tra l'altro ricordata nel punto 20 (articolo 4).

Nel campo della sicurezza delle informazioni, viene proposta una definizione relativamente dettagliata ma che ha beneficiato delle riflessioni espresse nei testi di questi ultimi anni: «La sicurezza delle informazioni è l'implementazione dei mezzi giuridici, organizzativi, operativi, investigativi analitici, di *intelligence*, di *counterintelligence*, tecnologici e scientifici destinati a predire, rivelare, dissuadere, prevenire e respingere le minacce o a cancellarne le conseguenze".

È importante sottolineare anche che questa dottrina, oltre ad aggiornare quella del 2000 fa seguito alla Strategia di Sicurezza Nazionale della Federazione Russa del 31 dicembre 2015 (Стратегия национальной безопасности Российской Федерации).

Il testo chiarisce poi l'insieme che viene a costituire gli interessi della Federazione Russa nella sfera informazionale. Non manca nessuno degli elementi elencati nel 2000, ma viene rimarcata la necessità di utilizzare le tecnologie dell'informazione non solo per migliorare la democrazia e le relazioni tra la società civile e lo Stato ma anche per preservare l'essenza stessa della Russia, cioè l'eredità culturale, spirituale e morale del suo spazio multietnico.

Questo punto, ribadito nel testo, è sintomatico della visione culturale e sociale caratteristica dei testi russi, aspetto spesso eluso nei documenti occidentali analoghi.

L'obiettivo dello sviluppo dell'industria delle tecnologie dell'informazione e dell'elettronica russa ci fa ricordare un documento passato inosservato al momento della sua pubblicazione benché essenziale, ovvero la Strategia di sviluppo dell'industria delle tecnologie dell'informazione nella Federazione Russa per il periodo 2014 - 2020. In quest'ultimo documento, sono citati tutti i metodi da impiegare per riuscire nella protezione e nello sviluppo dell'industria, in particolare studiando il successo delle società americane e mobilizzando il settore militare-industriale.

Il testo del 2016 oggetto del nostro studio riafferma questo obiettivo, considerato come strategico. Lo stesso aspetto viene completato ulteriormente, nell'articolo 17, dal richiamo sulla sovranità tecnologica che deve essere percorribile tramite un insieme di compagnie nazionali di dimensione significativa nei settori dell'IT e dell'elettronica. Dal testo del 2014, l'articolo 18 del decreto del 2016 riprende il paragrafo dove viene deplorata la troppo limitata ricerca nei campi di questo sviluppo, penalizzando l'emergenza di un quadro globale di sicurezza delle informazioni.

Viene, inoltre ricordato un altro passo tratto dal testo del 2000 ovvero il bisogno di produrre un'informazione più precisa sui soggetti che riguardano la Russia e le sue azioni, e questo sia per il pubblico russo che per quello internazionale. Questo ci ricorda ovviamente la creazione della struttura Rossia Segodnia, operata dalla fusione della «Voce della Russia» e di RIA Novosti nel 2013.

L'obiettivo di assicurare la sovranità della Russia è evocato ripetutamente nel testo, in termini tanto laconici quanto imperativi. Questo obiettivo, viene ribadito, deve essere effettuato tramite una coordinazione a livello internazionale. Questa precisione non ci stupisce, poiché la Russia aveva già deposto un testo in questo senso presso l'ufficio del Segretariato delle Nazioni Unite e che garantisce il suo supporto all'Unione Internazionale delle Telecomunicazioni in iniziative similari. È doveroso precisare, in rapporto a questa problematica, che la legge federale N 242 FZ del 21 luglio 2014 richiede che i dati riguardanti i cittadini russi siano trattati in server che siano fisicamente presenti sul territorio nazionale. Se Google e Apple si sono piegati a questa esigenza, rispettivamente nell'aprile e nel settembre 2015, la rete professionale LinkedIn è stata sconnessa dal web russo su richiesta diretta delle autorità russe. Rimane a carico delle altre società che contravvengono alla legge di procedere a una locazione dei server in Russia o di delocalizzare una parte dei propri server nella Federazione Russia.

Leggiamo poi la dualità dello "spazio informazionale" e delle tecnologie connesse: da una parte, permettono una crescita dell'economia e un miglioramento dei rapporti tra l'amministrazione e gli amministrati, dall'altra introducono minacce specifiche che possono destabilizzare il paese.

Il punto 13 è specificamente mirato – ed è una novità perché il documento del 2000 non era così esplicito su questo punto – alla minaccia terroristica, individuale o organizzata, che può pregiudicare il sistema informazionale. Questa può paralizzare in modo critico le infrastrutture oppure diffondere una propaganda che attenta agli interessi della Federazione.

È presente nella dottrina anche una parte focalizzata sulla cyber criminalità, in particolare nella sua componente finanziaria. Quest'ultimo aspetto era già abbordato nel 2000, con una lungimiranza notevole se teniamo conto dello stadio di evoluzione delle tecniche e delle reti di allora. Nella nuova dottrina, non poteva certo mancare questo tema, tenendo conto dei numerosi cyber attacchi criminali che avevano appena colpito gli enti bancari russi proprio a novembre e dicembre 2016 (citeremo come esempio il furto di due miliardi di rubli alla Banca Centrale).

Il cyber nel settore militare viene accennato a più riprese, ma in modo molto succinto e senza apporto reale se teniamo conto degli altri testi ufficiali dedicati a questo settore e molto più eloquenti. L'articolo 21 dettaglia un po' meglio il ruolo delle forze armate nella sicurezza informazionale, in quattro componenti: dissuasione e prevenzione di qualsivoglia

conflitto che può nascere come conseguenza dell'uso delle tecnologie dell'informazione; miglioramento della preparazione e dei mezzi connessi alla guerra informazionale all'interno del settore militare; preparazione alla protezione degli interessi della Russia nello spazio informazionale; neutralizzazione delle operazioni psicologiche informazionali mirate a compromettere l'eredità patriottica e storica della nazione russa. Quest'ultimo elemento sottolinea l'interesse dimostrato dalle autorità russe su questo aspetto della guerra, eredità di fatto di una lunga tradizione sovietica in questo campo.

L'articolo 23 si presenta come una litania delle azioni della sicurezza dello Stato che devono essere implementate tramite lo spazio informazionale. Fondamentalmente, questo elenco è un riassunto di tutti i punti dettagliati in precedenza, ad esempio la sovranità del paese, la protezione delle infrastrutture informazionali, l'impiego di contromisure per evitare danni ai valori propri della Russia, la preferenza per i prodotti locali di tecnologia dell'informazione che rispondano all'obbligo di un livello preciso di sicurezza informazionale, ecc. (etc.)

Un punto trattato in modo laconico ma che merita la nostra attenzione è quello che si riferisce alla vigilanza contro gli atti di un potere straniero, commessi da individui o da servizi speciali (da intendersi come servizi di intelligence) o da organizzazioni suscettibili di impiegare le tecnologie dell'informazione per minacciare la sicurezza dello Stato. Questo vuol dire prendere chiaramente atto che il cyber-spazio, o spazio informazionale, è un settore strategico perché può giungere a mettere in pericolo – tramite i suoi autori, le sue tecnologie o dal loro uso – la stabilità politica, economica, finanziaria e militare di uno Stato.

Poi viene dettagliata in modo più capillare l'interconnessione tra la sicurezza informazionale e il settore economico. Vi ritroviamo le preoccupazioni espresse nella dottrina del 2000, con il bisogno di avere a disposizione un'industria IT ed elettronica locale capace di limitare l'importazione di prodotti di origine terza. Questo vale tanto per i beni quanto per i servizi. Potremmo riassumere l'articolo come segue: protezione, innovazione, competitività e sicurezza di una fitta rete industriale nazionale nel campo delle tecnologie dell'informazione. Il termine preoccupazione non è esagerato se si tiene conto dell'insistenza di questa problematica, presente in diversi testi ufficiali sin dal 2000. Ci ritroviamo in una configurazione elaborata dal famoso teorico – e praticante – del protezionismo, Friedrich List, poiché le previsioni sono identiche: proteggere le ditte in un settore industriale nascente, accompagnarle e favorirle finché siano competitive, per poi lasciarle affrontare il mercato mondiale quando sono giunte a maturità.

Questa strategia, sul piano economico, è identica a quella applicata nel campo dell'educazione, della formazione e della ricerca scientifica. Vi ritroviamo lo stesso ragionamento: creare fondamenta solide per poter poi raggiungere un livello di competitività. Questa similitudine non è fortuita: denota una strategia globale che rifiuta di scindere gli sforzi in funzione dei settori ma piuttosto in funzione degli stadi di progressione di ognuno di essi.

Infine, vi è una volontà evidente, identica a quella precisata già nel 2000, di promuovere una visione comune e internazionale del concetto della sicurezza informazionale. Su questo tema, è sottolineato che lo spazio informazionale è uno spazio conflittuale che può essere usato per destabilizzare degli Stati per motivi di ambizioni politico-militari.

È proprio la sovranità della Federazione Russa ad essere al centro della ricerca e della conclusione di partenariati e di un quadro internazionale nel campo informazionale. Un dettaglio rimane però relativamente impreciso, il suggerimento di un segmento della rete Internet (che è esplicitamente nominato ancora una volta) [1] sotto la gestione nazionale. Trattasi di un nuovo progetto di una rete nazionale resa sicura da un sistema operativo sovrano? Oppure trattasi di recintare, o piuttosto di filtrare, la parte russa della rete Internet? Questo punto meriterebbe ulteriori dettagli da parte dalle autorità perché le poche righe analizzate sono troppo stringate per trarne una qualsivoglia prospettiva tangibile.

Gli articoli 30 e i seguenti sono principalmente richiami al codice giuridico, con un punto di spicco per la menzione che il Presidente della Federazione Russa rimane il solo competente a definire l'orientamento in materia di politica di sicurezza informazionale (assecondato dal Consiglio di Sicurezza della Federazione oppure dalla Commissione militare-industriale). Segue la lista degli attori di primo piano, che sono implicati nella sicurezza informazionale, che senza sorpresa integra tutte le componenti dell'esecutivo e degli enti e compagnie sotto la loro tutela (anche indiretta come la Banca do Russia).

È, dunque, ricordata la volontà di preservare i diritti dei cittadini pur mantenendo gli obiettivi di sicurezza informazionale, così come di migliorare l'interconnessione dei mezzi di sicurezza informazionale tra le diverse componenti delle strutture di forza militari e civili, a tutti i livelli territoriali.

Per seguire la progressione degli effetti voluti da questa dottrina, il Segretario del Consiglio di Sicurezza della Federazione ha l'onere di redigere un rapporto annuo.

Il testo, quindi, non presenta nulla di rivoluzionario. È nello stesso tempo una riaffermazione della dottrina del 2000 e un condensato di documenti connessi pubblicati dopo di essa, anche se arricchito da alcuni punti tratti dalle esperienze degli ultimi anni.

È così che vediamo rinforzato l'interesse per la sicurezza informazionale dei campi economici e finanziari nonché il riferimento a Internet (è questa, tra l'altro, l'unica concessione di un testo tecnologicamente molto neutro).

Nella forma, notiamo uno sforzo sostanziale per rendere la nuova dottrina più leggibile della precedente, mentre nel contenuto, si percepiscono nettamente gli orientamenti futuri, improntati di pragmatismo.

Non dubitiamo che documenti ufficiali settoriali seguiranno a breve, come già avvenuto dopo la pubblicazione della dottrina di settembre 2000.

[1] *д) развитие национальной системы управления российским сегментом сети «Интернет»*

Dottrina di sicurezza informazionale di dicembre 2016 (in russo) : https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

Strategia di sicurezza nazionale di dicembre 2015 (in russo) : http://www.consultant.ru/document/cons_doc_LAW_191669/61a97f7ab0f2f3757fe034d11011c763bc2e593f/ ■

1 Editions Nuvis, Collection Cyberespace et Cyerdéfense, dir. N. Arpagian, Paris 2013

Buongiorno Charlotte! Un esempio di ingegneria sociale su LinkedIn.

autore: Battista Cagnoni

Security Expert

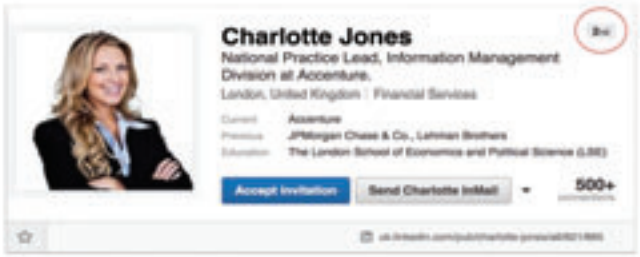
"Charlotte" è solo uno dei tanti casi di ingegneria sociale che ho trattato recentemente in una mia breve indagine.

Nel nostro mondo virtuale, tutto parte ormai dall'immagine che, se scelta bene, porta con sé una fortissima componente emotiva. L'esempio che andremo ad analizzare è reale. Trattasi di Charlotte, una bella donna bionda, sorridente, che ci ha chiesto di poter entrare nella mia cerchia di contatti su LinkedIn. Era un invito di secondo livello, il che vuol dire che qualcuno tra i miei contatti ha già accettato Charlotte. Ciò significa, se fossimo tutti attenti, vorrebbe significare – in linea di massima – che il mio contatto conosce Charlotte.

BIO

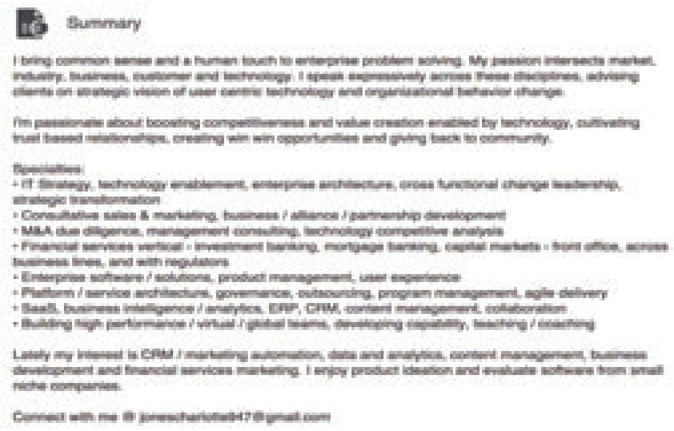
Battista Cagnoni (CISSP GCFA GCIH) è un esperto di sicurezza con una lunga esperienza in diversi settori verticali dell'industria, dove ha assunto incarichi come Security Engineer, Security Analyst, SOC Lead. E' appassionato della diffusione della cultura di Cyber Security, in particolare sui temi della presa di coscienza in questo campo e della comprensione delle modalità per affrontare i problemi di sicurezza. Battista è GIAC Certified Forensic Analyst e GIAC Certified Incident Handler.

Charlotte is in my network



Ricevo quindi una mail di Charlotte via LinkedIn, che vuole connettersi con me. Vado quindi a guardare il suo profilo che si rivela impressionante. La giovane professionista ha molte competenze e una ricca esperienza professionale. Non c'è quindi in apparenza nulla di sospetto nel suo curriculum che dovrebbe perciò incitarmi ad accettarla nella mia cerchia di contatti.

Come "vittima" potenziale che ha però conoscenze in cyber security nel campo delle reti sociali, osservo sin dall'inizio che il profilo di Charlotte è quasi troppo ricco, troppo bello per essere reale. Un dettaglio in particolare attrae la mia attenzione: non vi è



Summary

I bring common sense and a human touch to enterprise problem solving. My passion intersects market, industry, business, customer and technology. I speak expressively across these disciplines, advising clients on strategic vision of user centric technology and organizational behavior change.

I'm passionate about boosting competitiveness and value creation enabled by technology, cultivating trust based relationships, creating win win opportunities and giving back to community.

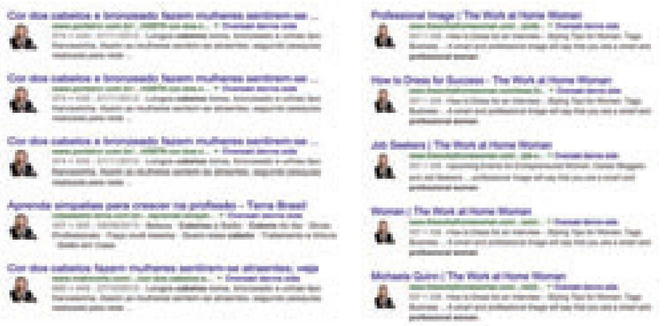
Specialties:
- IT Strategy, technology enablement, enterprise architecture, cross functional change leadership, strategic transformation
- Consultative sales & marketing, business / alliance / partnership development
- M&A due diligence, management consulting, technology competitive analysis
- Financial services vertical - investment banking, mortgage banking, capital markets - front office, across business lines, and with regulators
- Enterprise software / solutions, product management, user experience
- Platform / service architecture, governance, outsourcing, program management, agile delivery
- SaaS, business intelligence / analytics, ERP, CRM, content management, collaboration
- Building high performance / virtual / global teams, developing capability, teaching / coaching

Lately my interest is CRM / marketing automation, data and analytics, content management, business development and financial services marketing. I enjoy product ideation and evaluate software from small niche companies.

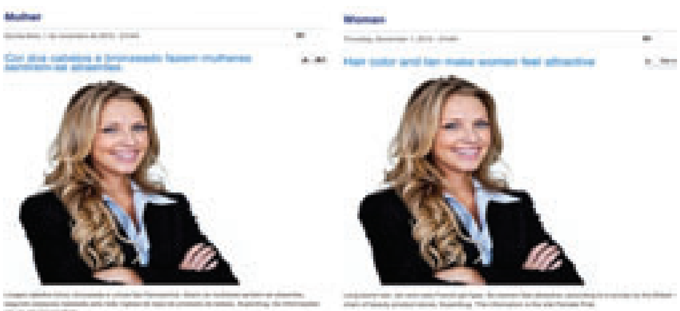
Connect with me @ jonescharlotte947@gmail.com

nessuna raccomandazione da terzi, né scritta, né semplicemente approvata nella lista delle competenze professionali individuali scelte dalla signora.

Mi chiedo di conseguenza se questo profilo corrisponde a una persona reale o se è stato appositamente creato per essere usato in operazioni di ingegneria sociale. In pratica, nel secondo caso l'obiettivo è riuscire a guadagnare la fiducia delle persone che accettano l'invito portandole, pian piano, a non mettere in dubbio le mail future che "Charlotte" invierà loro direttamente e non via LinkedIn inducendoli a cliccare– se tutto va bene per i furfanti – proprio sui link raccomandati dalla "giovane professionista" nelle sue mail.

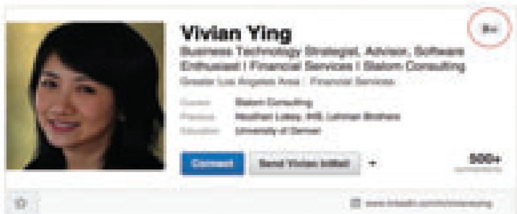


Nel mio ruolo di analista, facilmente riesco a verificare se il profilo è di una persona reale. Inserisco la foto del profilo di Charlotte nel motore di ricerca di immagini di Google. E lì ho una prima sorpresa: il ritratto della giovane donna appare su numerosi siti internet, alcuni brasiliani, altri inglesi. Tutti questi siti, attivi e onesti, hanno in comune di essere nello stesso e unico campo di attività: quello del coaching, delle formazioni e dei servizi destinati a donne che desiderano avere successo professionalmente.



L'immagine è dunque stata scelta con grandissima cura, per il suo carattere meramente emotivo destinato a mirare in particolare a uomini d'affari; è una bella donna bionda, giovane, attraente e in più molto intelligente grazie agli elementi sapientemente scelti per costruire il suo curriculum: è proprio una professionista dal successo incontestabile.

Sempre usando solo il semplicissimo Google, introduco nel motore di ricerca parti intere del curriculum inserendole tra virgolette. Dopo solo tre banali ricerche, vedo che "Charlotte" ha fatto copia-incolla di molte frasi esistenti. Da Wikipedia, ritroviamo la medesima descrizione esatta – ma più lunga – della azienda dove dice di lavorare, mentre proprio da LinkedIn viene fuori il profilo di una certa Vivian Ying, che ha un percorso lavorativo identico, con frasi e competenze professionali in tutto e per tutto uguali.



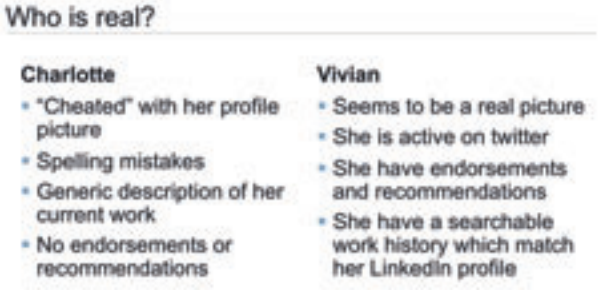
A questo punto è importante determinare chi, tra Charlotte e Vivian, è una persona reale. Guardo attentamente il profilo di Vivian. Innanzitutto, vedo che Vivian è già nella mia lista di contatti e cioè mi fornisce una prima prova che "chi" che ha creato "Charlotte" ha anche fatto ricerche sui miei contatti per meglio studiare gli interessi comuni che mi legano alle persone che ho accettato.

Il curriculum di Charlotte è proprio identico a quello di Vivian! Solo l'ultima riga, quella che comporta l'indirizzo mail, è stata cambiata.

Per capire meglio i dettagli della "trappola-Charlotte", paragoniamo ora i due profili. Abbiamo già dimostrato che "Charlotte" ha un profilo

costituito da una foto rubata, da un percorso professionale fatto di copia-incolla e da un curriculum integralmente plagiato. Però, se osserviamo più attentamente, scoveremo pure un po' di errori di ortografia, constateremo che le descrizioni del suo lavoro attuale sono molto – troppo – generiche, una leggerezza raddoppiata dal fatto che l'inesistente personaggio non è professionalmente raccomandato da nessuno.

Da parte sua, Vivian ha una foto reale, è attiva anche su Twitter, ha decine di raccomandazioni e soprattutto, dimostra di avere un iter professionale in cui ogni singolo elemento viene confermato da una semplice ricerca sui siti ufficiali della società dove lavora e delle aziende dove ha lavorato in passato.



Poiché abbiamo stabilito con massima certezza che Charlotte non è una persona reale, rifiutiamo evidentemente la sua richiesta di entrare nella nostra cerchia di contatti.

Ma perché esistono così tante "Charlotte" su LinkedIn? Vi sono diverse ragioni che sono complementari tra loro. Tramite questa rete professionale, chi si nasconde dietro alle varie "Charlotte" lo fa per scoprire le competenze delle loro vittime e rivenderle a dei reclutatori o più su, a ditte specializzate nell' *"head-hunting"* al servizio delle grandi organizzazioni. Al peggio, e molto più frequentemente, queste tecniche sono utilizzate da criminali per raccogliere le informazioni dei contatti della vittima per poi mandare mail di spam con contenuti sempre più pericolosi senza attirare troppi sospetti. Infine, questo metodo non va sottovalutato come un'operazione di intelligence e di *profiling* dei bersagli: la fase di *information gathering* è spesso la prima necessaria per lanciare cyber-attacchi di successo sia contro una vittima e suoi contatti, sia più frequentemente, contro la società nella quale la vittima e molti dei suoi contatti lavorano. ■

In conclusione

In conclusione, dobbiamo tutti aumentare il nostro livello di vigilanza quando usiamo le reti sociali. Idealmente, quando riceviamo un invito da parte di uno sconosciuto, dovremmo sempre verificare che si tratti di una persona reale usando il metodo che abbiamo presentato, denominato nel gergo usato dagli specialisti in sicurezza *"sanity checking"*. Non bisogna dimenticare che si può pure chiedere alla persona che vi invita quali sono i motivi per i quali desidera conoscervi; per quanto banale, è il miglior metodo possibile perché gli *"scammers"*, di solito non rispondono mai. Come ultima raccomandazione direi che, come misura cautelativa, non si dovrebbe mai accettare inviti da persone che non si conoscono e che, soprattutto, hanno profili ben troppo "generici".

Internet, terrorismo e opportunità

autore: Alessandro Trivilini,
responsabile del Laboratorio
di informatica forense della SUPSI

Il numero di utenti che contraddistingue Facebook è senza dubbio una peculiarità che lo rende unico e attrattivo sotto diversi punti di vista: una realtà per i giovani, una scoperta per gli adulti, una miniera d'oro per le aziende e uno strumento di intelligence per gli Stati.

A memoria d'uomo non è mai esistito un ambiente strategico di queste dimensioni in cui le persone, a prescindere dalla loro natura, colore e provenienza, pubblicano volontariamente e gratuitamente informazioni personali sulle proprie abitudini e sulla propria quotidianità. Un ecosistema complesso usato anche dai terroristi per l'avvicinamento e il reclutamento di nuovi lupi solitari, attraverso dialoghi atti ad avvicinare e persuadere giovani utenti a intraprendere un percorso di radicalizzazione.

Da un punto di vista sociale è senza dubbio un fenomeno allarmante da non trascurare, ma da un punto di vista tecnico informatico, e anche di business, potrebbe essere una grande opportunità da cogliere con coraggio e decisione. Fare di necessità virtù significa in questo caso aggregare competenze interdisciplinari, per esempio informatiche, psicologiche, didattiche, giuridiche e linguistiche, per progettare e sviluppare nuovi automi intelligenti (cyber bot) per l'analisi linguistica e semantica dei dialoghi che intercorrono fra gli utenti nei social network. Un business in forte crescita in cui anche la comunità europea ha deciso di investire cifre a sei zeri. Le caratteristiche del linguaggio naturale utilizzato dagli utenti all'interno delle fonti aperte come Facebook, sono una risorsa ricca di informazioni che non può più essere trascurata. Nasce quindi la necessità di sviluppare nuovi agenti smart debitamente addestrati capaci di riconoscere gli atti comunicativi degli utenti malintenzionati, il loro stile comunicativo e soprattutto il rapporto fra motivazione, emozioni e comportamenti interpersonali. Una sfida nella sfida, in cui le giovani generazioni di nativi digitali, attraverso la loro forma mentis informatica, la loro dimestichezza e la loro resilienza professionale, potrebbero contribuire ad affrontare e, forse, risolvere. Nessuno meglio di loro è in grado di codificare e decodificare la forma del linguaggio utilizzato oggi in rete, sempre più sintetico,

BIO

Il Dr. Alessandro Trivilini è responsabile del Laboratorio di informatica forense della SUPSI, nato in collaborazione con la Polizia e la Magistratura del Cantone Ticino. In SUPSI è inoltre docente di ingegneria del software, informatica forense e information security. Autore di libri e pubblicazioni scientifiche, ha lavorato nella Silicon Valley (California) in qualità di ingegnere del software nel campo della sicurezza aeroportuale. Ha un dottorato di ricerca conferito con lode dal Politecnico di Milano nel campo dell'intelligenza artificiale, con applicazione nel campo forense. Partecipa come chairman e public speaker a conferenze e congressi nazionali e internazionali su aspetti di cyber security e digital forensics. Dal 2016 membro del comitato scientifico internazionale dell'IMA World Maintenance Forum per temi di cyber security.

destrutturato e metaforico. Di fatto, ampiamente sfruttato per il reclutamento di nuovi adepti da avvicinare alla radicalizzazione. È opportuno quindi fare lo sforzo di provare, anche se in punta di piedi, a entrare nel loro terreno comune, spesso mediato da ore interminabili alla playstation, formulando le opportune domande e interpretando le rispettive risposte.

Le più grandi aziende informatiche al mondo, come Google, Facebook, Yahoo, e altre ancora, hanno fatto il primo grande passo investendo pesantemente nell'alfabetizzazione informatica delle nuove generazioni, e in particolare in progetti didattici utili a insegnar loro i paradigmi di programmazione logica che consentono di acquisire una buona capacità di astrazione. Ora spetta a noi, docenti e professionisti, dar loro i contesti operativi concreti e stimolanti in cui possano dare spazio alla creatività, sperimentando in forma guidata soluzioni eclettiche e originali che potrebbero davvero cambiare il corso degli eventi, di natura sociale, economica ma anche e soprattutto di sicurezza personale.

La triste cronaca delle ultime settimane porta alla luce la crescente necessità di avvalersi di nuovi modelli sostenibili, da utilizzare per affrontare adeguatamente i rischi emergenti di un mondo che cambia ad alta velocità. Le stesse forze dell'ordine, locali o globali che siano, arrancano nel fronteggiare attacchi alla sicurezza con l'imbarazzo di chi, fino a poco tempo fa, era convinto che la semplicità non fosse per niente il livello più alto della complessità.

Il rischio in questo momento è persistere a porsi le stesse domande, fondate su esperienze di un mondo ormai lontano, meravigliandosi di volta in volta della monotonia delle risposte. Purtroppo nessuno, autorità comprese, è in grado di scorgere all'orizzonte una soluzione che possa affievolire la confusione e la paura in corso. Per un genitore che ha perso un figlio durante uno degli ultimi attentati terroristici in Francia, la domanda sorge spontanea: come è possibile che alla soglia della quarta rivoluzione industriale, caratterizzata dalla tanto acclamata intelligenza artificiale, non vi siano strumenti (automi) informatici (possibilmente resilienti e intelligenti) da impiegare per il monitoraggio continuo e approfondito della rete Internet?

Forse, il monitoraggio in corso dei social network è sì necessario, ma non più sufficiente, almeno per come è concepito oggi. L'analisi dei tanto acclamati «big data», contraddistinti dalle famigerate quattro «V» (Volume, Velocità, Varietà e Veracità) richiede l'aggiunta di due nuovi componenti: il contesto di provenienza dei dati e la loro cultura. Sì, proprio quest'ultima potrebbe arricchire ulteriormente l'analisi tecnico-scientifica, con l'intento di estrapolare informazioni utili a determinare per tempo la spinta sociale che ha portato un particolare utente a formulare un determinato atto comunicativo. A questo proposito, un approccio interessante potrebbe

Come è possibile che alla soglia della quarta rivoluzione industriale, caratterizzata dalla tanto acclamata intelligenza artificiale, non vi siano strumenti informatici da impiegare per il monitoraggio continuo e approfondito della rete Internet?

unire gli algoritmi di «artifical intelligence», le fasi di «machine learning» ed i processi di organizzazione delle informazioni proposti dalla «big data analytics». Una convergenza strategica, ma anche ambiziosa, perché i risultati oggi, purtroppo, parlano chiaro: la radicalizzazione e la propaganda non possono essere automaticamente identificati nella loro forma completa.

Ed è proprio qui che si annidano le grandi opportunità di sviluppo, fortemente interdisciplinari, per chi di mestiere ha il compito e il dovere di pensare a soluzioni innovative ed efficaci. Per il drammatico strascico di morti degli ultimi mesi, non possiamo più permetterci il lusso di attendere il riavvio del sistema affinché il problema si risolva «magicamente» da solo. Dal mio punto di vista, ognuno di noi nel suo contesto sociale e professionale, è detentore di un piccolo ma importante pezzo di soluzione, che per dare buoni frutti dovrà per forza essere condiviso e nel suo insieme sostenuto. Di fatto, dobbiamo imparare dai nostri avversari, la loro efficacia pone le sue radici, per quanto drammatiche, pericolose e deplorevoli, in un unico grande e globale terreno comune, condiviso e difeso. ■

A chi appartiene veramente un'automobile autonoma?

Un esempio per capire l'ecosistema della sicurezza in un mondo di IoT.

autore: Mika Lauhde

Per tutti quelli che stanno aspettando un «boom» dei fenomeni che metteranno a confronto la cyber security con l'Internet of Things (IoT), siamo spiacenti di deludervi: il treno è partito da un bel po'.

L' l'Internet of Things è già fortemente presente nei nostri ambienti quotidiani e il vero problema è quello di monitorare chi ne assicurerà la sicurezza. Perciò la «challenge» fondamentale ormai è ottenere il controllo della nuova generazione di ecosistemi di sorveglianza e di business.

La cyber security, malgrado la sua importanza, non può essere paragonata alla scelta vitale del «decidere» cosa vogliamo difendere o cosa abbiamo paura di perdere; è proprio in funzione delle risposte che ognuno di noi darà a questa affermazione che bisognerà adattare le nostre capacità.

Siamo tutti sicuri che la cyber security migliorerà con il passare degli anni, ma al contempo, siamo altrettanto sicuri che anche gli attacchi contro i sistemi aumenteranno. Per chi come noi si occupa di cyber security, l'incremento degli attacchi garantirà sicuramente l'occupazione, ma questa non è certo una notizia positiva per il singolo cittadino.

In questo contesto, come si può essere sufficientemente lungimiranti e non aspettare in modo passivo le prossime brecce nella nostra sicurezza? La prima necessità per ognuno di noi è capire i nuovi ecosistemi e i ruoli che giocano i diversi attori chiave al loro interno!

L'esempio che abbiamo scelto per illustrare l'ampia problematica della sicurezza IoT è tratto dall'industria dell'automobile e dallo scenario delle vetture senza conducente. Come sapete, queste ultime circolano già autonomamente negli Stati Uniti e sono già stati svolti i primi test in Europa.

Questo tipo di vettura necessita una quantità impressionante di informazioni generate dai sensori del mondo fisico che circonda la vettura e dai diversi sistemi di back-end del veicolo. Con il termine «back-end» non intendiamo i vari sistemi che forniscono servizi di intrattenimento, che naturalmente sono oggi la parte più interessante per i passeggeri delle macchine autonome, bensì l'informazione vitale che serve a controllare il movimento e a garantire una buona guida della vettura.

Ed è proprio da questo punto che nasce il bisogno di proteggere i sistemi dei veicoli. Ma da che cosa?

Iniziamo a esaminare, di seguito, gli elementi principali di questo ecosistema:

a. *macchine programmate per guidare in modo autonomo e l'azienda produttrice responsabile della programmazione della navigazione, del controllo, e di altre funzionalità del veicolo;*

b. *condizioni stradali critiche impossibili da prevedere anche dal più intelligente dei software;*

c. *l'essere umano a bordo della macchina ha un valore e i valori attribuiti ad ogni singolo individuo possono essere diversi;*

families of those killed in the Malaysian Air disasters last year, said British parents who lose an adult child can expect compensation of around £20,000 ($30,000), while American parents could expect £1.5 million ($2.222 million).

d. *Scelte da fare in caso di un incidente tra due vetture autonome su condizioni stradali critiche, che potrebbe richiedere di sacrificare delle vite per minimizzare il totale dei danni. Quali saranno i fattori decisivi che peseranno su questa decisione?*

A questo punto bisogna individuare tutti gli «stakeholder» della vettura IoT e, per capire i loro obiettivi di sicurezza, dovremo prima capire quali sono le reali motivazioni di ognuno.

Il "conducente" ovvero il proprietario del veicolo: oltre al desiderio di controllare pienamente i sistemi di intrattenimento si preoccuperà soprattutto della propria sopravvivenza; quindi, il suo obiettivo sarà quello di interferire con i sistemi affinché possa sia controllare il veicolo in modo completamente autonomo, ma anche, quando serve, mandare informazioni ad altri veicoli per evitare collisioni con la propria macchina.

La compagnia di assicurazioni: i premi assicurativi per la perdita di vite umane o per disabilità dovute a incidenti non sono uguali, pertanto le compagnie dovrebbero avere un forte interesse alla programmazione sicura del veicolo e dei sistemi anti-collisione per far sì che ogni incidente risulti il meno costoso possibile per loro. Dopo tutto, il loro ruolo è anche quello di assicurare dividendi cospicui ai propri azionisti.

Interessi governativi: ogni governo dovrebbe proteggere i suoi cittadini, ma spesso la sicurezza promessa dai governi può limitare, anche solo temporaneamente, alcune libertà. Se un governo non agisse in questo modo, potrebbe rimanere al potere? Ci sono molte ragioni per credere che i governi vogliano influire sul comportamento dei veicoli autonomi.

Polizia e indagini: nella maggior parte degli Stati, un incidente stradale con decesso è automaticamente seguito da un'indagine da parte delle Forze dell'Ordine per identificare il responsabile dell'incidente, ma anche proporre rapporti sul caso, in modo da migliorare la sicurezza ed evitare incidenti simili in futuro. Quindi, per la polizia, l'accesso a tutti i dati presenti nel sistema del veicolo, cosi come nei sistemi back-end, è assolutamente vitale. Ma come potrà ottenerne l'accesso?

Hackers: in questo campo le motivazioni dell'attacco ai sistemi del veicolo possono essere diverse. Per alcuni, sarebbe solo un modo per "diventare famosi" o per avere i propri "15 minuti di gloria", per altri si tratterebbe invece di provocare veri e propri danni. In tutto ciò gli hacker dovranno comunque penetrare nel sistema e fargli fare quello che vogliono (l'esempio dell'hackeraggio di una Jeep Cherokee del 2015, ripetuto nel 2016).

Il produttore di automobili: in questo caso non è per forza stabilito in un solo paese, ma le decisioni del management sono generalmente legate alle regolamentazioni e alle leggi in vigore nel paese in cui ha sede sociale l'azienda.

In questo campo, i produttori stanno già affrontando la "challenge" legata al richiamo del "service" dei veicoli per vari problemi. Ora, questi richiami sono ormai quasi sempre dovuti al cattivo funzionamento dei sistemi tecnologici ogni giorno più complicati e con costi sempre più alti. Si è visto che pericoli esterni indirizzati ai sistemi dei veicoli fanno danni sempre più estesi; in questo senso, tutti gli altri stakeholder hanno un conflitto di interessi con i produttori di veicoli.

La sfortunata realtà per i produttori di automobili è che sono loro ad avere la connessione con i veicoli e quindi si assumono un grande rischio di responsabilità legale. Il sistema posto nel veicolo è solo un "client", mentre il server è situato da qualche parte nel "cloud" del produttore. Ma in che Stato e sotto quale giurisdizione si trova l'hardware che gestisce il cloud?

In questo scenario noi europei siamo molto "sicuri". Dopo tutto, abbiamo perso già da anni la componente fondamentale chiamata modem, che è la pietra angolare di ogni IoT wireless e non viene più prodotta da nessuna azienda europea. Recentemente, l'Europa si è concentrata sull'implementazione dell'"eCall", ma nessuno Stato membro ha osato chiedere da dove tutte queste automobili europee ricevono gli updates dei software per i loro modem e se esistono dei "side-channels" che comunicano e con chi. Forse tra qualche anno, magari con l'aiuto del prossimo "Snowden", scopriremo questi "side-channels".

Quando finalmente saremo certi che l'"eCall" funzionerà davvero, avremo già risolto probabilmente tutte le problematiche attuali esistenti tra gli stakeholders e senza nessuna implicazione da parte dall'Europa.

In conclusione, non dite più che l' l'Internet of Things sta arrivando, poichè tutte le decisioni vitali sono già state prese altrove e sono già in implementazione. ■

BIO

Nel suo ruolo di Vice-President, Government Relations and Business Development, SSH Communications Security, Mika è responsabile delle relazioni con i governi e del Business Development della SSH. Prima di raggiungere la SSH Communications Security, Mika ha diretto la Business Security & Continuity nella corporazione Nokia, dove ha assunto le responsabilità delle relazioni con i governi nel settore della sicurezza IT ed anche in quelli della gestione di crisi, della criminal compliancy, della prevenzione delle frodi e delle soluzioni crypto per i terminal.
Mika ha un'esperienza estesa in tematiche di sicurezza anche in seno a Istituzioni governative, sia in Europa che negli USA. Ad oggi, è membro del Permanent Stakeholder Group dell'ENISA (European Network and Information Security Agency), del management della European Cyber Security Research Center, nonché del gruppo di lavoro sulla cyber-security del Governo finlandese. È anche membro della Leuven University European Crypto Task Force; del gruppo di lavoro dell'Europol; è stato membro fondatore del TDL (Trust in Digital Life), del security advisory board Member del Governo dell'UE government (RISEPTIS); dell'ICT security advisory board del Governo finlandese e del critical infrastructure protection group (CPNI) del Governo del Regno Unito.

Università e impresa devono allearsi per generare ricchezza e sviluppo

Luciano Violante

autore: Massimiliano Cannata

Il Rapporto Italiadecide 2017[1] si è focalizzato su un trinomio complesso, che riveste una rilevanza strategica per lo sviluppo: Ricerca, Università e crescita. Si tratta di fattori interdipendenti che stanno trovando un punto oggettivo di convergenza nella "società della conoscenza". Il sapere, nell'ambito di questo variegato orizzonte, è il "primo motore" di progresso e di produttività, in assenza del quale risulta di fatto impossibile progettare il futuro. Solo riaffermando la centralità dell'Università come Istituzione e della ricerca, quale attività qualificante, potremo sperare di ridare slancio al nostro *sistema - Paese*, fiaccato da una crisi grave e interminabile. Partendo da questa consapevolezza abbiamo chiesto a Luciano Violante, Presidente di Italiadecide, di ripercorrere i tratti salienti dello studio di quest'anno e di riassumere le proposte di intervento che potranno ridare slancio innovativo alle politiche pubbliche di un mondo della ricerca che per incidere sul PIL deve impegnarsi sempre più a individuare degli efficaci scambi di comunicazione e di *know-how* con il fitto tessuto delle nostre PMI, che rimane il "cuore pulsante" dell'industria e dunque la fonte essenziale da cui proviene occupazione e ricchezza.

Massimiliano Cannata: *Presidente, Università, ricerca, crescita il Rapporto 2017 di Italiadecide ha deciso di orientare la sua indagine su un orizzonte incrociato di problematiche. Quali sono state le ragioni di questa scelta e quale messaggio di fondo l'Associazione intende lanciare alle Istituzioni e all'opinione pubblica?*

Luciano Violante: Una delle parole d'ordine di *Italiadecide* è "sinergia". Non c'è oggi sinergia tra ricerca e impresa e bisogna favorirla. Spesso i centri di ricerca, universitari e non, ignorano quello che serve alle imprese e le imprese non conoscono i prodotti della ricerca scientifica che possono esser utili per la loro produzione. Fare sinergia è dunque il primo messaggio.

Massimiliano Cannata: *Globalizzazione e digitalizzazione sono le componenti che stanno mutando il profilo del capitalismo. Siamo di fronte a un «passaggio d'epoca», per usare una definizione del filosofo Salvatore Natoli, che non ha precedenti. Questo profondo salto di paradigma di fatto sta modificando il ruolo dell'Università e la funzione stessa della ricerca. Quali sono le conseguenze?*

Luciano Violante: L'intelligenza artificiale e l'interdipendenza frutto della globalizzazione delle merci e della finanza sono i grandi fattori che stanno determinando, non da soli, ma in modo prevalente, il cambiamento d'epoca. Oggi il paese più competitivo, quello che favorisce meglio la vita dei propri cittadini, è quello che punta sulla ricerca di nuovi materiali, sulla più razionale utilizzazione dell'esistente, su nuove applicazioni dell'intelligenza artificiale. Questo vale soprattutto per l'Italia che, come sappiamo, è povera di materie prime, ma ricchissima di intelligenze creative come dimostrano le migliaia e migliaia di giovani che vengono chiamati da università e centri di ricerca stranieri e da grandi imprese multinazionali in misura assai superiore alla media dei colleghi europei. Naturalmente tutto va fatto in sintonia con il sistema produttivo non per farsi condizionare, ma per moltiplicare l'utilità della ricerca e potenziare lo sviluppo produttivo della nazione.

L' VIII Rapporto Italiadecide

L'importanza di trasmettere alle imprese e alla pubblica amministrazione i risultati della ricerca universitaria, mettendo quest'ultima a servizio dell'innovazione, è l'argomento centrale del Rapporto 2017 (cfr. intervista a Luciano Violante) realizzato in collaborazione con la Conferenza dei Rettori delle Università italiane. Lo studio parte dalla consapevolezza che una delle sfide oggi più impegnative deve portare al rafforzamento dell'attività di ricerca quale soggetto propulsore di sviluppo e di benessere sociale. Per troppo tempo abbiamo considerato le istituzioni universitarie come isolate "repubbliche degli studiosi", quali monadi chiuse e impermeabili alle sollecitazioni che provengono dal corpo collettivo, ora bisogna cambiare passo. Il tema, sviscerato da studiosi ed esperti del settore in coerenza con il rigore di un metodo ormai consolidato, riveste un'importanza cruciale per gli impatti sulla spesa pubblica che implica oltre che per la spinta all'innovation, che da un tale capovolgimento di paradigma e di concezione potrà trarre il sistema – Italia, che ha più che mai bisogno di recuperare terreno sul piano della competitività.

Un modello di *Governance* aperto alle imprese

Massimiliano Cannata: *Il mondo dell'impresa deve vivere oggi di innovazione e di conoscenza. Malgrado questo è difficile creare un ponte di comunicazione tra questi due universi tradizionalmente distanti. Quali sono le proposte di Italiadecide per abbattere questo grave gap che rischia di compromettere il percorso della crescita?*

Luciano Violante: Ne cito alcune: riformare le lauree professionali; innovare sui requisiti della docenza, definire un modello di governance aperto a imprese, professioni e pubblica amministrazione; riordinare e concentrare il sistema dei finanziamenti, oggi troppo polverizzato; definire lo stato giuridico dei ricercatori e dei tecnologi che superi l'attuale incompatibilità tra la docenza, la ricerca e l'attività d'impresa; individuare un sistema di governo della ricerca più unitario, nel quale siano identificate sedi di indirizzo strategico delle attività di ricerca e di coordinamento per lo sviluppo di grandi infrastrutture di ricerca.

Massimiliano Cannata: *Tra le proposte enucleate nel Rapporto si parla di "politiche industriali più integrate alla ricerca" Che cosa vuol dire in concreto? L'Università potrà dare un effettivo contributo all'esecutivo nella definizione di politiche industriali efficaci e realmente innovative?*

Luciano Violante: Certamente si. Nelle Università italiane, che nella media sono superiori per la qualità dell'insegnamento a quelle di molti altri importanti paesi, si pensa, si elabora, si studiano i problemi concreti, si scelgono soluzioni, si é in perenne contatto con tutto il mondo scientifico, dal Giappone agli Stati Uniti. Esse perciò detengono saperi essenziali per il Governo. Se poi il Governo decidesse di non interloquire, ma va detto che ora lo sta facendo bene e con continuità, i guai sarebbero gravi per tutto il Paese.

Verso una nuova antropologia

Massimiliano Cannata: *Il piano Industria 4.0 è un asset strategico su cui l'Esecutivo sta puntando molto. Che cosa occorre perché tutto il sistema delle PMI, che rappresentano la spina dorsale del nostro capitalismo, possa incamminarsi sui nuovi linguaggi del digitale?*

Luciano Violante: Lei tocca uno dei problemi più gravi. Nelle piccole imprese, accanto a fenomeni di straordinaria innovazione, c'è un largo bacino di indifferenza o di timore per l'innovazione. Occorre insistere, mostrando soprattutto quello che di positivo piccole imprese hanno fatto, per stimolare tutte le altre.

Massimiliano Cannata: *Ruggero Gramatica nella Lectio Magistralis che si è tenuta alla Camera in occasione della presentazione del vostro Rapporto ha toccato un punto critico che caratterizza la società dei Big Data: il complesso rapporto che deve intercorrere tra informazione e conoscenza, dietro cui si profila il territorio spesso accidentato dei nuovi saperi e della formazione. La nostra scuola e l'Università sono attrezzate per affrontare i livelli di complessità crescenti che la digital society impone?*

Luciano Violante: La piattaforma *Yewno*, creata da Ruggero Gramatica, mette in connessione non parole ma concetti; se per esempio io scrivo la parola jaguar, la piattaforma è in grado di comprendere, sulla base del concetto di cui fa parte la parola, se intendo riferirmi all'animale o alla casa automobilistica. Gramatica, inoltre, ci ha letto una poesia alla "Montale", scritta da un algoritmo al quale è stato chiesto di scrivere una poesia sull'amore come l'avrebbe scritta il grande poeta usando cioè la sua metrica, i suoi concetti, le sue parole. Una macchina che pensa e costruisce concetti. Come fa ciascuno di noi quando studia e scrive. Si impone, dunque, una grande riflessione sui rapporti tra il pensante umano e il pensante non umano. Credo stia nascendo una nuova antropologia, cui tutti devono partecipare, a partire, naturalmente dalle Università

BIO

Luciano Violante è docente di Diritto pubblico presso l'Università "La Sapienza" di Roma e l'Ateneo della Valle d'Aosta. Giurista e Magistrato, negli "anni di piombo" ha ricoperto il delicato incarico di giudice istruttore a Torino dove si è subito distinto per l'impegno sistematico e l'azione di contrasto del fenomeno del terrorismo. Parlamentare di lunga militanza nelle file del Pci, del Pds e dei Ds, è stato presidente della Commissione parlamentare antimafia (1992-1994) e della Camera dei deputati (1996-2001) ed ha fatto parte della commissione di "10" saggi, nominati dal Presidente emerito della Repubblica Giorgio Napolitano, con la finalità di definire le riforme istituzionali e economico-sociali necessarie per lo sviluppo del Paese. Attualmente è al vertice di "Italiadecide" l'associazione bipartisan che può vantare tra i soci fondatori personalità del calibro di Carlo Azeglio Ciampi, Giuliano Amato, Gianni Letta, Pier Carlo Padoan, Giulio Tremonti. Lo scopo di questa realtà associativa è quello di contribuire al miglioramento della qualità delle politiche pubbliche e di valorizzare i diversi livelli di governance territoriale attraverso un'applicazione puntuale e rigorosa della logica della sussidiarietà. Alcune delle sue pubblicazioni per Einaudi: Non è la piovra, Un Mondo asimmetrico, Magistrati, Politica e Menzogna, Il dovere di avere doveri. Ha inoltre curato i volumi degli Annali della Storia d'Italia su: La criminalità, Legge, diritto, giustizia, Il Parlamento.

Massimiliano Cannata: *Nel corso della presentazione Lei ha anticipato una iniziativa legata alla realizzazione di una "show room". Si tratta di una originale vetrina aperta all'innovazione. Quali attori coinvolgerà?*

Luciano Violante: Ci siano già incontrati con il vicepresidente di Confindustria che cura le risorse umane, Giovanni Brugnoli, insieme al presidente della conferenza di Rettori, Gaetano Manfredi, al presidente del CNR, Massimo Inguscio e al vice presidente Riccardo Pietrabissa, per discutere della realizzazione di questo progetto. Confindustria tiene ogni anno una importante conferenza sulla ricerca. In quella sede potrebbero essere invitati ad esporre i loro risultati università e centri di ricerca che abbiano in corso o abbiano effettuato ricerche particolarmente significative per le imprese. Dall'altra parte le imprese potrebbero sollecitare la ricerca ad impegnarsi su temi che riguardano più da vicino le produzioni in corso per renderle più competitive e più soddisfacenti per i cittadini. Il percorso dell'innovazione che porta al domani, è dunque già tracciato. ■

1 www.italiadecide.it

La strada verso la Resilienza: mezzo secolo di pensiero del mondo accademico e industriale sintetizzato nello studio di BSI e Cranfield School of Management

autore: Luigi Brusamolino

I responsabili delle aziende si trovano ad affrontare una serie di cambiamenti politici, finanziari, sociali e tecnologici come non era mai successo prima d'ora: nell'ultimo quinquennio vi è stata un'accelerazione improvvisa, e i mutamenti avvenuti sono equiparabili a quanto successo nei 20 anni precedenti.

Le nuove tecnologie, come i sistemi integrati con intelligenza artificiale, l'Internet of Thing e l'"economia circolare', presentano nuove opportunità ma anche potenziali minacce. Molte industrie sono diventate globalizzate, con conseguente dispersione internazionale dei loro prodotti e servizi, una disaggregazione delle loro supply chain e una conseguente difficoltà nel garantire standard di qualità adeguati.

Queste nuove situazioni costringono le aziende a riesaminare, ripensare, ridisegnare le proprie attività per restare sul mercato e questo genera notevole preoccupazione da parte di chi ha compiti decisionali: da uno studio condotto da British Standards Institution (BSI), in collaborazione con Economist Intelligence Unit, è emerso che solo un terzo degli amministratori delegati sono sicuri della sopravvivenza a lungo termine, delle proprie imprese e che nove su dieci vedono la Resilienza Organizzativa come un priorità per il proprio business perché aiuterà a sviluppare le proprie attività e proteggerne la continuità.

Nel 2014, BSI ha prodotto il primo standard mondiale sulla Resilienza Organizzativa, BS 65000, che viene definita come *"the ability of an organization to anticipate, prepare for, respond and adapt to incremental change and sudden disruptions in order to survive and prosper."*

"Cosa può fare la leadership aziendale per assicurare la Resilienza Organizzativa per la propria attività?"

Identificare delle "common practices", o addirittura delle "best practices", quando si parla di Resilienza Organizzativa è una sfida impegnativa poiché

BIO

Luigi Brusamolino è Managing Director per il Sud Europa di British Standards Institution e vanta oltre 25 anni di esperienza manageriale a livello internazionale. Durante la sua carriera professionale ha effettuato numerose e prestigiose esperienze nel campo dei servizi e dell'Information Security ed è certificato CISM e CRISC. È stato Vice Presidente di Symantec per i servizi di consulenza, managed services, formazione e supporto tecnico a livello EMEA, dopo aver ricoperto il ruolo di Senior Manager della divisione Security & Technology nella sede milanese di PricewaterhouseCoopers e ancora prima quello di Regional Manager & Partner presso Securteam (Gruppo Atos Origin).

esistono diverse fonti e documentazioni spesso contrastanti. Per questo, BSI e Cranfield School of Management, hanno realizzato uno studio che sintetizzasse il pensiero manageriale di quasi mezzo secolo, dal 1970 ad oggi. L'analisi è partita da 600 documenti accademici si è concentrata su 181 di essi utilizzando, a supporto, altri saggi e relazioni dedicate alla materia.

L'evoluzione del pensiero e le 5 fasi della Resilienza Organizzativa

Lo studio descrive come l'evoluzione della Resilienza Organizzativa sia guidata da due strategie opposte: una difensiva/reattiva dove l'obiettivo è impedire l'avvenimento di eventi dannosi e conservare il business esistente, una progressiva nella quale la finalità è favorire l'accadimento di eventi positivi e anticipare i cambiamenti per favorire la crescita.

Allo stesso modo sono stati indentificati due diversi approcci basati uno sulla coerenza e uno sulla flessibilità. La combinazione di questi elementi ha portato alla definizione di diversi fasi di Resilienza Organizzativa.

Storicamente, c'è stata una preoccupazione verso le azioni di difesa quindi una strategia difensiva che ha guidato le prime due fasi:

1 **Controllo preventivo.** La Resilienza Organizzativa è raggiunta attraverso la gestione dei rischi, l'attivazione di barriere fisiche, la ridondanza (capacità di riserva), i sistemi di back-up e procedure standardizzate che proteggono l'organizzazione dalle minacce consentendo il 'ripristino della situazione stabile precedente' in seguito alle interruzioni. In questa fase si parla di strategia difensiva basata sulla coerenza.

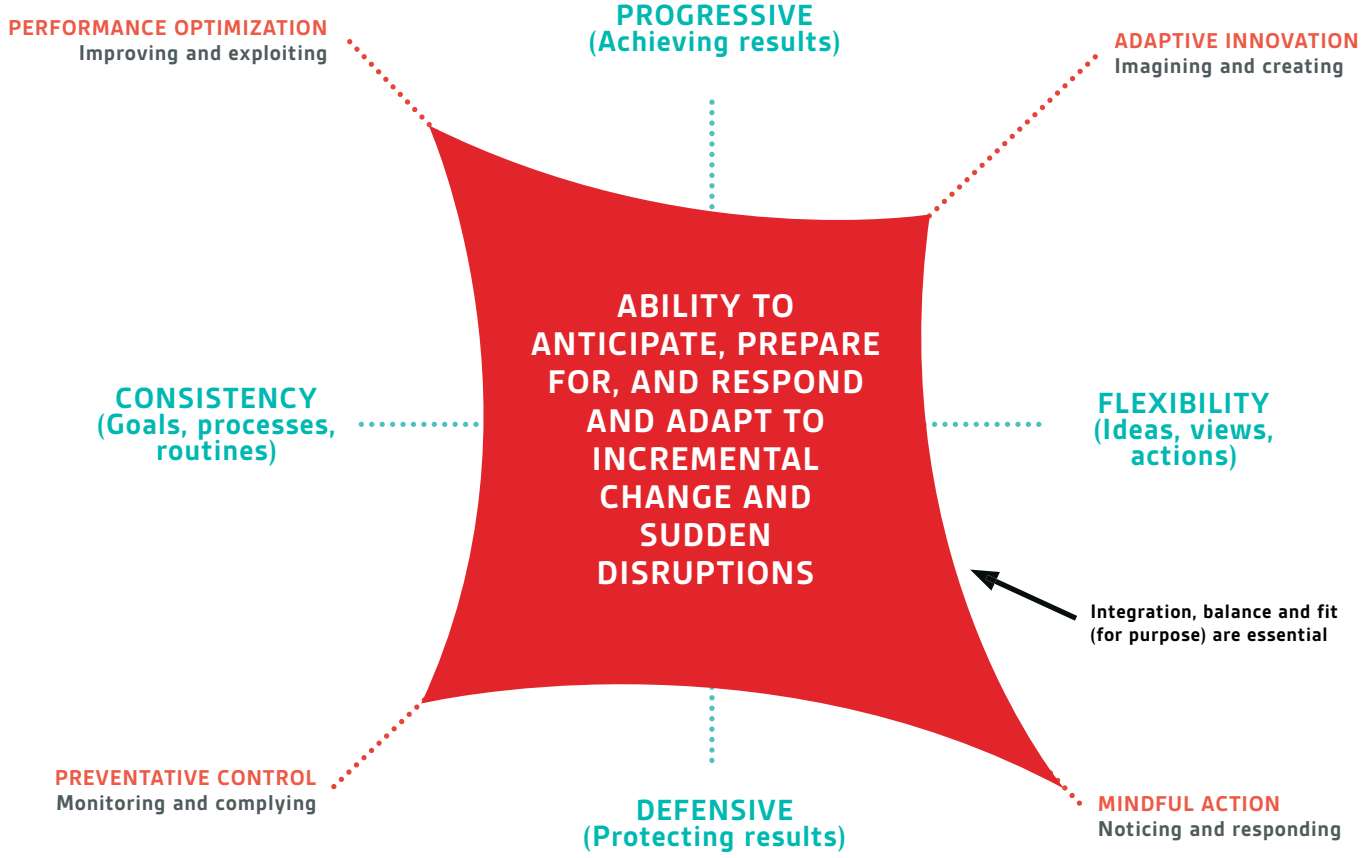
2 **Azione consapevole.** La Resilienza Organizzativa è generata da persone che utilizzano la propria esperienza, competenza e il lavoro di squadra per anticipare e adattarsi alle minacce rispondendo efficacemente a situazioni impreviste o difficili. Anche qui si ha una strategia difensiva ma basata sulla flessibilità.

Passando ad una strategia progressiva si è intesa la Resilienza Organizzativa come la capacità di effettuare un "salto in avanti" e questa ha portato ad altre due fasi successive:

3 **Ottimizzazione delle prestazioni.** La Resilienza Organizzativa è costituita dall'ottimizzazione dei processi, dal continuo miglioramento, perfezionamento e ampliamento delle competenze esistenti, con l'obiettivo di sfruttare le attuali tecnologie per dare servizi più efficiente e efficaci. I fattori sono una strategia progressiva basata sulla coerenza.

4 **Innovazione adattabile.** La Resilienza Organizzativa è raggiunta creando, inventando ed esplorando nuovi mercati, nuove tecnologie e nuove soluzioni. Il punto di rottura col passato, in ottica evolutiva, nasce proprio all'interno dell'azienda. Strategia progressiva basata sulla flessibilità.

La combinazione delle due strategie e dei due diversi approcci può essere riassunta nel modello rappresentato dall'Organizational Resilience Tension Quadrant.



Il posizionamento all'interno del Quadrante varia a seconda della natura dell'organizzazione, dell'ambiente e delle circostanze che questa deve affrontare. Un business potenzialmente ad alto rischio, come può essere quello legato all'energia nucleare, è molto probabile che abbia un orientamento verso la coerenza difensiva ma, un importante cambiamento come un ritiro di sovvenzioni statali porterebbe con tutta probabilità ad uno spostamento verso una maggiore flessibilità e una strategia progressiva. Al contrario, un'attività fortemente imprenditoriale, che normalmente dovrebbe essere orientata verso una flessibilità progressiva, potrebbe indirizzarsi verso una maggiore coerenza difensiva a causa di un imprevisto, come il richiamo di un prodotto.

Ne consegue che non esiste una forma «giusta» o «sbagliata» per posizionarsi all'interno del Tension Quadrant ma la scelta va fatta considerando svariati fattori.

Lo studio Cranfield identifica le diverse fasi distinte come diversi gradi di maturazione della Resilienza Organizzativa. Come illustrato nel grafico seguente, lo stato iniziale è dato dal controllo preventivo l'evoluzione avviene attraverso diversi step fino ad arrivare all'ultimo, definito come il pensiero paradossale.

Paradoxical thinking

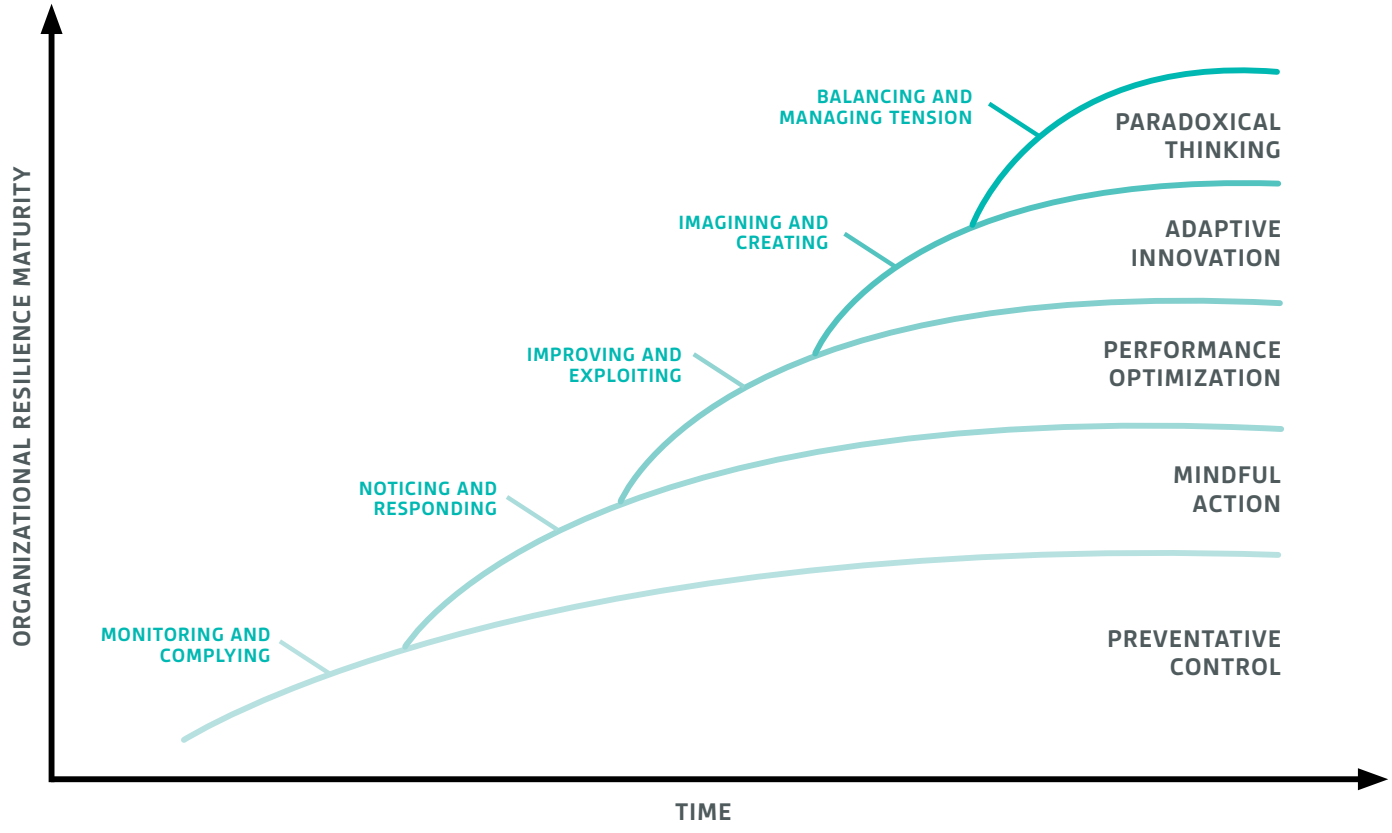
La Resilienza Organizzativa richiede un equilibrio adeguato tra obiettivi e le esigenze di controllo preventivo, azione consapevole, ottimizzazione delle prestazioni e innovazione adattativa anche se in contrasto fra loro. Il Paradoxical thinking consente questo "equilibrio", aiutando i leader a passare da una scelta "o / o" a poter decidere di utilizzare "entrambi": entrambe le strategie (difensiva e progressiva) ed entrambi gli approcci (coerente e flessibile).

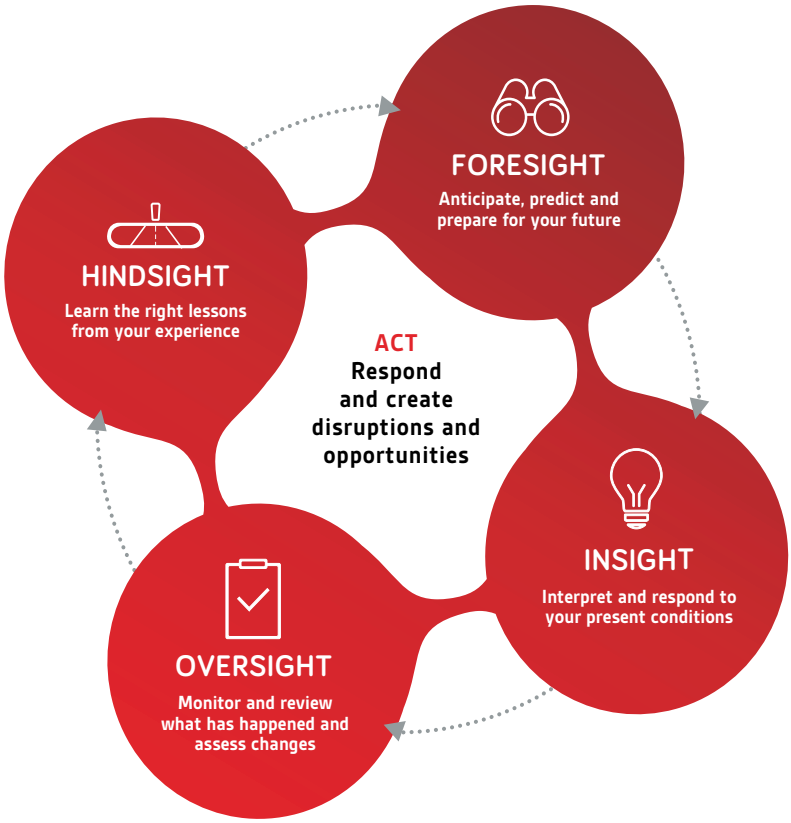
Guardare al futuro con la metodologia 4Sight

Per rispondere alla domanda *"Cosa può fare la leadership aziendale per assicurare la Resilienza Organizzativa per la propria attività?"* lo studio Cranfield e BSI suggerisce di adottare la nuova metodologia, "4Sight", per introdurre e sostenere la Resilienza Organizzativa. 4Sight descrive un processo ripetibile composto da quattro processi di base:

- **Foresight** - Prevedere e preparare il futuro della propria organizzazione: richiede una sorveglianza costante per individuare potenziali minacce e possibili opportunità.
- **Insight** - Interpretare e dare risposte basate sulle situazioni attuali: comporta una raccolta sistematica di informazioni e prove da fonti diverse per creare una comprensione condivisa dello stato delle operazioni in corso e dell'ambiente a cui ci si trova.
- **Oversight** - Monitorare e rivedere ciò che è accaduto e valutare le modifiche da attuare: include la realizzazione di un processo robusto per identificare, gestire e monitorare i rischi critici.
- **Hindsight** - Imparare le lezioni giuste sulla base dell'esperienza: richiede una cultura "non colpevolizzante" e una volontà di imparare dal successo e dal fallimento.

Il modello 4Sight è particolarmente utile per affrontare problemi complessi come lo sviluppo di una nuova tecnologia, la pianificazione di





un nuovo sistema di infrastrutture, l'attuazione di un importante programma di cambiamenti o la gestione di una crisi. Tali sfide sono difficili da risolvere a causa della conoscenza incompleta o contraddittoria, del numero di stakeholder e delle opinioni coinvolte, del rischio finanziario e della natura interconnessa di questi problemi con altri problemi.

Lo studio rileva che la soluzione di problemi complessi richiede spesso impieghi contemporanei di diversi concetti e 4Sight integra la metodologia ben definita di «Plan-Do-Check-Act» (PDCA): mentre PDCA fornisce la coerenza, 4Sight offre la flessibilità per affrontare le grandi e complesse questioni odierne.

I modelli PDCA e 4Sight utilizzati congiuntamente offrono un quadro strutturato per i responsabili aziendali per contrastare atteggiamenti di eccessivo autocompiacimento, promuovere la vigilanza e abbracciare una cultura di continuo miglioramento. In tal modo, possono mitigare l'impatto derivante dalle interruzioni, incentivare l'innovazione e cogliere le opportunità, aggiungendo un valore reale alle parti interessate.

Una miscela delle due metodologie, prodotte dal **Paradoxical thinking**, è fondamentale per ottenere una vera Resistenza Organizzativa. ■

Il nuovo Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica

autore : Massimo Cappelli

La Presidenza del Consiglio dei Ministri ha pubblicato, lo scorso marzo, il nuovo "Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica". Il Piano è stato rivisto congiuntamente dalle *"Amministrazioni che compongono l'architettura nazionale cyber"*. Non è chiaro se al tavolo siano state invitate anche le Infrastrutture Critiche che avrebbero potuto comunque fornire raccomandazioni e suggerimenti in base alla loro esperienza. Leggendo il Piano, si nota che non vi sono stravolgimenti rispetto quello pubblicato nel 2013, la linea di condotta e il framework rimangono identici. Il Piano contiene tutti gli elementi potenzialmente utili per costruire un sistema di sicurezza cibernetica nazionale solido e innovativo in linea con i Paesi più evoluti, anche se sarebbe stato opportuno chiarire maggiormente alcuni aspetti. Infatti, soprattutto per i lettori esterni al sistema alcuni elementi potrebbero risultare di difficile interpretazione o attribuzione.

La prima considerazione riguarda la necessità di una maggiore chiarezza sui servizi che il sistema nazionale di sicurezza dovrebbe erogare. Nelle linee di azione si intravedono una decina di servizi, come ad esempio, risk management; cyber threat intelligence; incident response, test & quality assurance, formazione e così via.

Esempio accorpamento linee di azione in servizi (Piano 2013)

La definizione dei servizi è essenziale per poterne attribuire le responsabilità e definire i canali di comunicazione con il settore privato. Attualmente, il settore privato si trova a dialogare per le stesse tematiche con più attori e questo comporta anche un dispendio di energie che potrebbero essere indirizzate a potenziamento di altre attività.

Prendendo l'esempio di eventi recenti, *Wanna Cry e Petya* (o *Not Petya*), alcune aziende hanno impiegato tempo e risorse per comparare gli Indicatori di Compromissione ricevuti da più attori pubblici. Ovviamente è meglio ricevere da più fonti la stessa informazione che non riceverne, ma un'ottimizzazione di scambio informazioni lato pubblico con un unico canale di erogazione all'esterno potrebbe evitare ridondanze informative e quindi di analisi.

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.

Un esempio di approccio, sopra descritto, è la piattaforma OF2CEN per lo scambio di dati strutturati fra le banche e la Polizia Postale. La Polizia Postale funge da hub o centro stella. Le banche inviano i dati della transazione fraudolenta al hub centrale che le raccoglie, ne anonimizza quota parte e trasferisce quella parte di informazione utile alle altre banche per contrastare il replicarsi della frode.

La piattaforma potrebbe essere unica e modulare con viste in base alle autorizzazioni e alle esigenze, con anonimato della fonte (conosciuta solo dal hub centrale). Questo si sposerebbe con il principio *"Need to share"*, permettendo la condivisione di informazioni soprattutto di natura tattica, in maniera immediata. Nel caso, poi, un attore riscontri un'evidenza nel suo sistema, identica a quella segnalata nella piattaforma, allora potrebbe entrare in gioco il principio *"Need to know"* e l'attore potrebbe fare richiesta all'amministratore del sistema per maggiori dettagli e per essere messo in contatto con il segnalante. In questo modo si può mantenere un certo grado di anonimato, di efficienza e di efficacia del sistema di condivisione.

Ritornando al piano, una chiara visione dei servizi erogati dal sistema nazionale sarebbe stato utile per indirizzare gli investimenti in maniera precisa, attribuire la responsabilità, definire il ruolo degli altri attori e il piano di sviluppo. Alcune linee di azione sembrano ridondanti o sovrapposte. Una definizione dei perimetri di azione e dei servizi a monte avrebbe diminuito aree interpretative grigie.

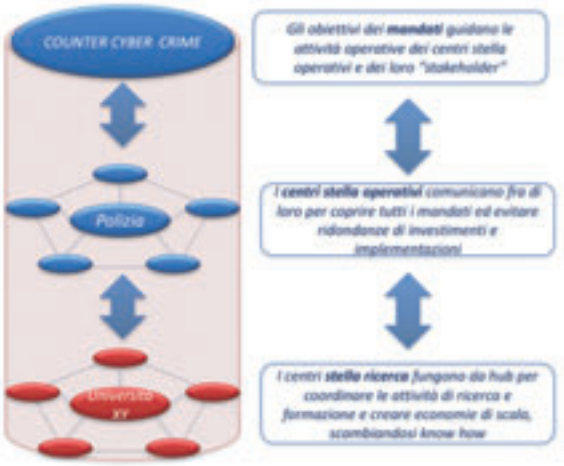
Stessa cosa vale anche per lo stato di avanzamento dei lavori. Sarebbe stato interessante averne visione per comprendere lo stato delle cose, anche a grandi linee. Una maggiore definizione dei compiti fra i diversi attori, con anche una rinuncia all'erogazione di determinati servizi per verticalizzare le competenze su altri, potrebbe portare ad economie di scala sia in termini di risorse umane che economiche.

L'importante è capire il progetto del Sistema Paese in modo da poter sfruttare al meglio i pochi finanziamenti disponibili. Non siamo super potenze e non abbiamo disponibilità di budget paragonabili a Stati Uniti, Russia o Cina. Pertanto, una definizione dell'architettura non solo in termini di "caselle" ma anche di servizi e flussi informativi potrebbe aiutare a risparmiare. In ambito risorse umane vale lo stesso concetto chiave, ridistribuire le risorse in base alle esigenze e alle competenze, purché si faccia sistema.

Il rischio altrimenti è di investire tutti negli stessi servizi, duplicando i costi, il numero di risorse ingaggiato, la formazione erogata e così via. L'Italia non può permetterselo.

E' fondamentale che per agire da sistema, si ragioni come un sistema in cui ognuno ha un ruolo funzionale all'interno del sistema stesso. Una macchina, un corpo umano sono sistemi in cui ogni componente ha un ruolo preciso.

Attribuendo a un ente il ruolo e i servizi che deve erogare, gli si permette di focalizzare la sua attenzione, i suoi investimenti e il suo tempo a migliorare i servizi stessi. Inoltre, diverrebbe anche il referente per attività di ricerca e sviluppo in grado di migliorare e rafforzare le attività. Le Università e i centri di ricerca avrebbero dei referenti specifici su determinate tematiche a cui rivolgersi per partecipare assieme a bandi europei, ad esempio. Lo stesso mondo accademico potrebbe strutturarsi in modo da avere dei coordinatori tematici per le attività di ricerca e sviluppo in ambito cyber (es. sicurezza sistemi industriali di controllo, sicurezza sistemi finanziari…).



Ad esempio, prendendo i 5 mandati tematici previsti nel *"National Cyber Security Framework Manual"* del NATO Cooperation Cyber Defence Centre of Excellence *(Internet Governance & Cyber Diplomacy; Crisis Management & Critical Infrastructure Protection; Counter Cyber Crime;…)*, si potrebbe identificare l'ente responsabile del mandato e i servizi che deve coordinare ed erogare. Per coordinare ed erogare si intende, definire il processo, gli attori coinvolti, le informazioni necessarie, l'output da disseminare e i livelli autorizzativi per visionare l'output.

Discorso a parte richiederebbe il reparto Difesa dove le implicazioni sono di maggior rilievo. Sistemi di puntamento, sistemi di navigazione, sistemi di controllo, sistemi integrati interforze e altro ancora si basano su reti informatiche.

Come venne riportato in un report della Northrop Grumman, consegnato alla U.S. – China Economic and Security Review Commission, un router Internet tipicamente può avere componenti prodotti in 16 aree geografiche diverse. Il controllo della supply chain è fondamentale per evitare eventuali manomissioni di uno o parte dei componenti. Si dovrebbero instaurare controlli sulla catena del valore, come è stato fatto in passato dagli Stati Uniti per il controllo delle importazioni con il C-TPAT (Customs-Trade Partnership Against Terrorism), dopo le vicende dell'11 settembre 2001.

Lo spazio cibernetico si presta a fenomeni di guerra ibrida, molto più di altri. Lo hanno dimostrato le campagne di Anonymous che si basano sul movimento di aggregazione delle persone verso tematiche specifiche, unendo persone di culture, razze e religioni diverse. Il concetto geopolitico è stato espresso da Bertrand Badie nel *"La fin des territories"* mentre sul fenomeno specifico di aggregazione di Anonymous ne ha parlato Gabriella Colemann in "I mille volti di Anonymous".

Lo dimostrano le tecnologie software e hardware, prodotte all'estero e che vengono dispiegate in settori chiave, anche della Difesa. In qualche settore si sta cercando di evitare troppe dipendenze da fornitori esteri ma è una battaglia ardua da portare avanti e di lungo periodo. Aziende private straniere sono presenti globalmente. Solo per darvi alcuni numeri:

- 400 milioni di device in tutto il mondo montano la stessa versione di sistema operativo;
- 100 milioni di smartphone di un unico marchio venduti in tutto il mondo;
- 1,65 miliardi di persone usano lo stesso social network.

Sono numeri impressionanti che rendono l'idea di come la tecnologia sia pervasiva e diffusa. Inoltre, effetti distorsivi sulla vita politica, mediante uso di fake news o dei social, sono stati evidenziati durante le ultime elezioni politiche di alcuni Paesi con campagne di disinformazione o "distrazione popolare".

Le teorie geopolitiche del passato avevano un concetto chiave, una sorta di filo rosso che le accomunava. Chi dominava un determinato settore o area, avrebbe dominato il mondo. T. Mahan parlava di egemonia dei mari; H. Mackinder del centro della terra o *Heartland*; N. Spykman del *Rimland*; P. de Servesky dell'*Air Power*. Queste teorie condizionarono strategie e politiche di rafforzamento militare. E' un argomento che riprendo spesso.

Chissà che questo filo rosso non sia valido anche per il cyber spazio. Fatto sta che da questo punto di vista, l'Italia sarebbe disarmata. In caso di conflitto mondiale, alcune aziende tecnologiche straniere si troverebbero fra l'incudine e il martello. Dove l'incudine è il governo che probabilmente richiederebbe lo sfruttamento delle tecnologie civili a scopo militare e il martello, rappresentato dalla reputazione nei confronti dei clienti in caso di schieramento durante il conflitto. Le *National Mobilization Law* servono a questo: autorizzare la nazione all'utilizzo di settori o aziende private a scopi bellici. E' successo in passato in Giappone, USA, UK, lo ha ribadito pure la Cina con la *Nationa Defense Mobilization Law* del 2010. Nulla osta che in futuro si possano ripetere queste dinamiche anche nel settore cibernetico.

Non era mia intenzione divagare, ma è necessario considerare tutti gli aspetti per comprendere dove e come possiamo agire per proteggere i nostri servizi, le nostre reti e i nostri dati. Analizzare gli scenari di impatto e le derive anche più catastrofiche sono la base per poi comprendere quali sono le forze che dovrebbero essere idealmente messe in campo per poi definire quali possono effettivamente essere realizzate in base alle risorse disponibili.

Ed è il divario fra dovere e potere che deve essere colmato attraverso sistemi nazionali integrati intelligenti in grado di sfruttare al meglio tutte le risorse disponibili per raggiungere un livello di resilienza accettabile.

Questo significa conoscere le proprie reti, conoscere gli effetti dell'interruzione di servizio, gli impatti sulla popolazione e contromisure da prendere per mantenere resiliente il Paese.

Non mi stancherò mai di esortare gli addetti al settore a leggersi un libro interessante al riguardo, *"Blackout"* di Marc Elsberg, in cui si prospetta un attacco alla rete smart grid europea e si illustrano le potenziali conseguenze di un attacco persistente. E' un romanzo ma gli scenari sono plausibili.

Concludendo, il Piano Nazionale presenta tutti gli ingranaggi essenziali per costruire uno splendido "motore", ma il manuale di istruzione e la raffigurazione finale del motore potrebbero essere più chiari. ■

Privacy e intelligenza artificiale

L'uso dell'intelligenza artificiale e la conseguente possibilità di analizzare in modo analitico grandi quantità di dati costituisce un pericolo per la privacy degli individui o può contribuire a proteggerla?

autore: Giancarlo Butti

BIO

Giancarlo Butti (LA BS7799, LA ISO/IEC27001, CRISC, ISM, DPO, CBCI, AMCBI) ha acquisito un master di II livello in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Si occupa di ICT, organizzazione e normativa dai primi anni 80 ricoprendo diversi ruoli: security manager, project manager ed auditor presso gruppi bancari; consulente in ambito sicurezza e privacy presso aziende dei più diversi settori e dimensioni. Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, white paper, manuali tecnici, corsi, seminari, convegni. Svolge regolarmente corsi in ambito privacy, audit ICT e conformità presso ABI Formazione, CETIF, ITER, INFORMA BANCA, CONVENIA, CLUSIT, IKN… Ha all'attivo oltre 700 articoli e collaborazioni con oltre 20 testate tradizionali ed una decina on line. Ha pubblicato 21 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 7 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT… È socio e proboviro di AIEA, socio del CLUSIT e del BCI. Partecipa ai gruppi di lavoro di ABI LAB sulla Business Continuity e Rischio Informatico, di ISACA-AIEA su Privacy EU e 263, di Oracle Community for Security su frodi, GDPR, eidas, sicurezza dei pagamenti…, di UNINFO sui profili professionali privacy, di ASSOGESTIONI sul GDPR. È membro della faculty di ABI Formazione, del Comitato degli esperti per l'innovazione di OMAT360 e fra i coordinatori di www.europrivacy.info .

Ho recentemente assistito ad un interessantissimo convegno sulle applicazioni dell'intelligenza artificiale.

Una delle applicazioni più promettenti fra quelle presentate era sicuramente quella legata alla profilazione della clientela con un sistema CRM, che abbinava i dati già in possesso dall'azienda con altri recuperati dal WEB, dall'attività sui social dei clienti e altro ancora.

Mentre assistevo alla presentazione avevo dei buoni motivi per rallegrarmi.

Il primo è che nel corso del convegno era stato presentato come "IA first" fosse il nuovo mantra delle grandi aziende tecnologiche, rendendo di fatto obsoleto il "mobile first" attualmente imperante.

Un'ottima notizia per me che, nelle pause fra gli interventi, stavo leggendo le bozze finali del mio ultimo libro[1], dedicato guarda caso alle applicazioni pratiche dell'IA. "IA first" aumenta le aspettative di vendita del mio libro e questo significa che io e Lorenzo[2], mio coautore, abbiamo individuato il momento esatto per uscire con un'opera che in realtà avevamo ipotizzato già da diversi anni.

Il secondo motivo per rallegrarmi era che non ero fortunatamente fra i clienti dell'azienda che presentava il suo CRM. Il mio occuparmi di sicurezza e soprattutto di privacy, nonché il mio essere un auditor, hanno di fatto prevalso sul mio interesse per l'IA e nel corso della presentazione ero terrorizzato dal fatto che qualcuno potesse elaborare un profilo delle mie abitudini, nel modo che il relatore stava presentando.

Mi chiedevo: ma i loro clienti lo sapranno? Saranno stati adeguatamente informati? Avranno dato il loro consenso? Sono realmente consapevoli di come questa azienda tratta i loro dati? Sono realmente consapevoli che i dati che loro diffondono sul web saranno aggregati da questa o da altre aziende per costruire un loro profilo sempre più preciso?

E come farà l'azienda a conciliare questa sua brillante creazione con quanto richiesto dal nuovo Regolamento europeo sulla privacy (GDPR)?

Preoccupazioni in tal senso sono state del resto recentemente espresse dal Presidente dall'Autorità Garante per la protezione dei dati personali, che in suo intervento[3] ha dichiarato fra gli altri:

La capacità di estrarre dai dati informazioni che abbiano un significato e siano funzionali, richiede infatti lo sviluppo di sofisticate tecnologie e di competenze interdisciplinari che operino a stretto contatto.

In questo quadro i progressi nella potenza di calcolo svolgono un ruolo centrale per l'analisi dei Big Data e per l'acquisizione della conoscenza.

E in un futuro non troppo lontano l'intelligenza artificiale, grazie ad algoritmi capaci di apprendere e migliorare autonomamente le proprie abilità, offrirà soluzioni efficaci per soddisfare le più disparate esigenze.

…

La capacità di elaborare, anche in tempo reale, tramite algoritmi sempre più potenti un'ingente mole di dati consente di estrarre conoscenza e, in misura esponenziale, di effettuare valutazioni predittive sui comportamenti degli individui nonché, più in generale, di assumere decisioni per l'intera collettività.

…

Dobbiamo chiederci quante delle nostre decisioni siano in realtà fortemente condizionate dai risultati che un qualche algoritmo ha selezionato per noi e ci ha messo davanti agli occhi.

…

Il legislatore, pur con le difficoltà di stare al passo con una tecnologia in rapidissima evoluzione, sta tentando di intervenire e in tale direzione si muovono le prescrizioni previste dal GDPR.

Prima di tutto è necessario informare adeguatamente l'interessato, come richiesto dagli articoli 12, 13 e 14. In particolare l'articolo 13, relativo alla informativa da rilasciare all'interessato quando i dati sono raccolti presso il medesimo, recita al comma 2 f:

2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

…

f) ***l'esistenza di un processo decisionale automatizzato****, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.*

Che viene proposto in forma assolutamente analoga al comma 2 g dell'articolo 14, relativo alla informativa da rilasciare all'interessato qualora i dati personali non siano stati ottenuti presso lo stesso:

g) *l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.*

A prima vista una richiesta apparentemente semplice, ma in realtà particolarmente complessa in quanto spesso le logiche di elaborazione dei dati non sono note a priori e questo è particolarmente vero nel caso in cui si utilizzino tecnologie, quali le reti neurali[4], che imparano da sole. Inoltre spesso non sono nemmeno noti gli obiettivi per i quali in futuro si effettueranno delle elaborazioni dei dati raccolti e questo, in base alle prescrizioni del GDPR, non può ovviamente accadere.

Non è possibile raccogliere dati personali a scatola chiusa, pensando poi di poterli elaborare a proprio piacimento in funzione, ad esempio, delle esigenze produttive o di marketing di un'azienda.

Ulteriore e ancor maggiormente vincolante è l'articolo 22 ***Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione*** del GDPR, che recita al comma 1:

1 *L'interessato ha il diritto* ***di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato,*** *compresa la profilazione,* ***che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona****.*

Che dire quindi dei sistemi automatizzati di valutazione ad esempio del merito creditizio di un cliente antecedentemente alla concessione di un prestito?

In realtà il comma 2 sembra proporre una via di uscita, almeno nei casi previsti:

2 *Il paragrafo 1 non si applica nel caso in cui la decisione:*

a) *sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;*

b) *sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;*

c) *si basi sul consenso esplicito dell'interessato.*

Ma tale via di uscita è in realtà in parte sbarrata dal comma 3:

3 *Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato,* ***almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento,*** *di esprimere la propria opinione e di contestare la decisione.*

Questo pone dei vincoli in particolare all'uso di un processo totalmente automatizzato. In altri termini un trattamento automatizzato dei dati potrà dare ad un operatore umano gli strumenti per effettuare la valutazione finale o comunque operatore umano e trattamento automatizzato dovranno cooperare nel formulare una valutazione.

È importante considerare che quanto sopra vale anche se l'interessato ha espresso il suo consenso esplicito.

Inoltre il processo di valutazione, salvo casi particolari, non potrà avvalersi dei dati che oggi rientrano per lo più nella definizione di dati sensibili:

4 *Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.*

Un percorso quindi tutto in salita per le applicazioni CRM intelligenti o per altri analoghi ambiti applicativi anche perché il mancato rispetto delle prescrizioni del GDPR espone le aziende a sanzioni milionarie.

Per evitare tuttavia di considerare l'applicazione dell'IA come nemica della privacy passo a citare alcune applicazione nelle quali è esattamente vero il contrario.

Come primo esempio lo sviluppo un sistema esperto proprio per verificare la conformità ai requisiti del GDPR del proprio CRM o più in generale della propria organizzazione. La complessità del GDPR e delle sue richieste può trovare proprio nell'IA un valido strumento di supporto.

Il secondo caso è un modello di analisi dei rischi, che ho descritto sommariamente nell'articolo **Misurare la physical cyber security**[5] nella rivista La Comunicazione N.R.&N. edita dall'ISCOM e più dettagliatamente nel già citato libro scritto con il prof. Lorenzo Schiavina.

Si tratta di un semplice sistema esperto realizzato con logica fuzzy[6] che può essere ulteriormente sviluppato e sofisticato nella sua articolazione.

Il terzo esempio riguarda i sistemi di prevenzione delle frodi, che grazie alla analisi dei comportamenti nell'uso della carta di credito da parte di un cliente, sono in grado di individuare situazioni anomale e intervenire con blocchi e allertamenti di vario tipo. Recentemente la mancanza dell'uso di uno strumento di questo tipo è stata considerata una negligenza nell'adozione di adeguate misure di sicurezza da parte di una banca, che è stata condannata al risarcimento del danno subito da un cliente.

Un quarto esempio riguarda una situazione in parte analoga a quella descritta.

Il provvedimento dell'Autorità Garante per la protezione dei dati personali *Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie* obbliga da alcuni anni le banche a effettuare una tracciatura degli accessi ai dati della clientela da parte dei propri operatori ed alla predisposizione di opportuni ALERT:

4.3.1. *Implementazione di alert.*

Deve essere prefigurata da parte delle banche l'attivazione di specifici alert che individuino comportamenti anomali o a rischio relativi alle operazioni di inquiry eseguite dagli incaricati del trattamento.

Anche a tal fine, negli strumenti di business intelligence utilizzati dalle banche per monitorare gli accessi alle banche dati contenenti dati bancari devono confluire i log relativi a tutti gli applicativi utilizzati per gli accessi da parte degli incaricati del trattamento.

La definizione degli eventi o meglio dell'insieme di eventi che possono scatenare un alert è tutt'altro che semplice ed anche in questo caso l'uso dell'IA può agevolare notevolmente il rispetto della prescrizione normativa permettendo agli esperti di individuare la combinazione di fattori che possono portare ad una reale violazione.

Questo obbligo con il GDPR viene in realtà esteso (anche se non in forma esplicita) a tutti i titolari di trattamento che, in una logica di protezione dei dati fin dalla progettazione, devono mettere in atto misure per prevenire una violazione di dati personali.

Vige infatti con il GDPR l'obbligo di notificare una violazione di dati personali, un obbligo che sotto forme diverse (notifica di incidenti di sicurezza) oggi interessa un crescente numero di normative (PSD2, eIDAS, NIS, Circolare 285 di Banca d'Italia…). È quindi nel pieno interesse delle aziende prevenire violazioni di dati o incidenti di sicurezza, onde evitare di doversi esporre ad una notifica pubblica che avrebbe importanti ripercussioni anche in termini di immagine.

In conclusione l'uso della IA può essere una significativa minaccia per la privacy o una formidabile alleata per la sua tutela, dipende dall'uso che ne faranno le aziende. ■

---

1 L. Schiavina, G. Butti, Intelligenza artificiale e soft computing. Applicazioni pratiche per aziende e professionisti (2017) FrancoAngeli

2 Il prof. Lorenzo Schiavina si occupa da oltre 30 anni di programmazione ad oggetti e IA ed ha realizzato numerosi sistemi esperti in uso presso aziende, ospedali, squadre di calcio…

3 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6013519

4 RETI NEURALI
La rete neurale simula, pur in forma molto semplificata, il funzionamento di neuroni e sinapsi.
Il cervello umano impara a gestire una quantità rilevantissima di informazioni, ad esempio muoversi senza cadere, grazie a ripetuti tentativi. Tuttavia nessuno di noi è in grado di formalizzare quali regole il proprio cervello ha ideato per riuscire a camminare, tanto è vero che riuscire a tradurre questa acquisita capacità in formule utilizzabili ad esempio da un robot, è particolarmente difficile. La nostra mente si comporta al riguardo come una black box e le reti neurali fanno altrettanto, salvo casi particolari, come quelli descritti nel mio libro precedentemente citato, dove le regole di comportamento della rete neurale sono osservabili ed integrabili manualmente.

5 http://www.isticom.it/documenti/rivista/rivista2016/6_85-118_misurare_la_sicurezzaiscom.pdf

6 LOGICA FUZZY: La logica fuzzy è una estensione della logica tradizionale (che è un caso particolare della logica fuzzy) nella quale non è valido il principio del terzo escluso (chi è giovane non è vecchio, chi è alto non è basso, chi è bianco non è nero….)
La logica fuzzy è nata per trattare tutte le sfumature di grigio che ci sono tra il bianco ed il nero e che rappresentano l'incertezza, cosa del tutto differente dalla probabilità.In determinate condizioni un sistema fuzzy è una rete neurale a 2 strati che rende osservabili le sue regole di comportamento.

PSD2 cambiano le regole del gioco

autore: Nicola Sotira

Diverse le compliance e le normative che nel 2018 avranno impatti sulle aziende e richiederanno ripensamenti sulle infrastrutture IT oltre ad un ridisegno di processi e organizzazione.

NIS e GDPR hanno riempito gli spazi di pagine e convegni sottolineando scadenze, sanzioni e concetti da applicare in azienda per la buona implementazione nel rispetto delle scadenze. Il 2018 sarà anche l'anno in cui PSD2 (Revised Payment Service Directive) cambierà le regole del gioco per le banche, questa direttiva UE rompe il monopolio che oggi le banche detengono sui servizi di pagamento, aprendo alla concorrenza di aziende interessate e di fatto lasciando ai clienti la possibilità di decidere quando e se consentire l'accesso al proprio conto a terze secondo un modello di banca aperta. Il cliente, in questo nuovo scenario, potrà decidere in completa autonomia quale piattaforma utilizzare per gestire i propri fondi ed erogare pagamenti. Di sicuro, i criteri che guideranno la scelta, saranno innovazione e *customer experience*. In questo contesto normativo il mercato nel settore finanziario è piuttosto in fermento mosso da una schiera di startup fortemente focalizzate sull'innovazione tecnologica che offrono servizi in numerosi ambiti, tra i quali il *crowdfunding*, i prestiti peer-to-peer oltre a servizi basati sulle crypto valute. Ovviamente a questa offerta proveniente dal mondo start up si vanno ad aggiungere i servizi provenienti dalle grandi multinazionali quali Amazon, Apple, Google e Facebook per esempio.

I nuovi player entrano in campo grazie a questa direttiva che obbligherà a facilitare l'accesso ai conti dei clienti alle applicazioni di terza parte, ovviamente previo il consenso dei correntisti, e quando parliamo di applicazioni stiamo parlando in modo significativo di App. Significa che le banche dovranno permettere un accesso sicuro ai conti dei loro clienti implementando delle API (Application Programming Interface). Sempre più evidente ormai che l'approccio che gli utenti hanno con le banche passa dall'utilizzo degli smartphone dove velocità, semplicità e user experience sono sfidanti.

Due nuovi soggetti nel mercato PISP e AISP

Da questa direttiva si evince che nuovi soggetti entreranno nel mercato dei servizi di pagamento, tra i quali PISP e AISP. Gli acronimi stanno per: *Payment Initiatiation Service Provider* (PISP) e *Account Information Services Provider* (AISP). Questi nuovi soggetti, se saranno autorizzati dal cliente, potranno avere accesso e operare sul conto corrente. Questo permetterà, attraverso interfacce di accesso (API) che le Banche dovranno rendere disponibili, lo sviluppo di nuovi servizi; servizi che saranno maggiormente integrati e armonizzati con gli altri attori del nuovo ecosistema. Nell'attuale scenario se un utente on-line decide di acquistare un servizio da Apple completerà la sua transazione utilizzando una carta di credito. Apple (*merchant* nella terminologia PSD) si servirà di un *acquirer* (istituzione finanziaria che gestisce pagamenti da determinate marche di carte di credito e di debito). L'*aquirer* contatterà, infine, il circuito della carta di credito del cliente addebitando sul suo conto corrente (FIG. 1)

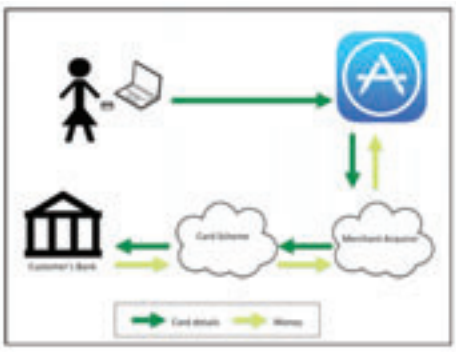


Figura 1

BIO

Nicola Sotira è Direttore Generale della Fondazione Global Cyber Security Center GCSEC e Responsabile di Tutela 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.

Figura 2

Facciamo un salto in avanti e rivediamo lo scenario sopra descritto alla luce della PSD2. Il nostro cliente sta nuovamente facendo acquisti da Apple, ma, invece di inserire i propri dati di carta di credito, gli viene chiesto se si accetta l'addebito sul conto. Laddove il premesso venga concesso sarà data a Apple l'autorizzazione ad eseguire il pagamento, per nostro conto, tramite il conto corrente (FIG. 2).

La direttiva, quindi, consente a una azienda di gestire la fase di avvio del pagamento, *Payment Initiatiation Service Provider* (PISP) che in questo esempio è Apple. Pertanto il PISP è un prestatore di servizi di pagamento che si pone come intermediario tra il cliente e il suo conto fornendo l'impulso al pagamento. Tecnicamente il PISP si inserisce nel processo di pagamento nelle transazioni online e non può in alcun modo accedere ai fondi depositati sul conto. Il cliente in questo scenario dà, pertanto, vita a una transazione on line connessa direttamente al proprio conto corrente addebitandolo lui stesso tramite le prestazioni offerte dal PISP.

Nella PSD2 è poi previsto un'altra tipologia di servizi rappresentata dagli AISP, con questi servizi il cliente può aggregare informazioni derivanti da più conti rendendole disponibili attraverso un'unica interfaccia. Gli AISP potranno quindi collegarsi ai conti e recuperare le informazioni necessarie per offrire ai clienti, ad esempio, una visione d'insieme della loro situazione finanziaria, una puntuale analisi delle loro abitudini di spesa il tutto in modo facile e interattivo. Questi servizi saranno utili anche per fornire servizi come il monitoraggio degli investimenti o per supportare la pianificazione finanziaria. Giuridicamente gli AISP possono agire solamente dietro a uno specifico consenso del cliente, autenticarsi con il PSP comunicando con tutti i soggetti coinvolti nella transazione, accedere solamente ai conti autorizzati e coinvolti nella transazione, non possono in alcun modo fare accessi per finalità diverse da quelle previste dal servizio. Nodale è chiaramente il tema della sicurezza e l'esigenza di armonizzare per tutte le Banche criteri di *Strong Customer Authentication*.

PSD2 Strong Customer Authentication (SCA)

Nel contesto della PSD2 tutti I fornitori di servizi di pagamento (PISP) sono tenuti ad adottare strumenti di autenticazione forte (SCA) ogni volta che si avvia una transazione di pagamento elettronica.

I costi di progettazione e implementazione dell'infrastruttura, nonché della verifica dell'efficacia delle misure SCA ricadono sugli *Account Servicing Payment Service Providers* (ASPSP), ovvero le banche. Mentre per quanto concerne PISP e AISP dovranno garantire che l'SCA sia correttamente applicata, ovvero faranno affidamento sulla procedura di autenticazione fornita dagli ASPSP.

Nella procedura SCA, una combinazione valida degli elementi di autenticazione genererà un codice di autenticazione sul PSP del pagatore, specifico per l'importo e il beneficiario convenuto dal pagatore all'avvio della transazione. Questa procedura viene definita *"dynamic linking"*. Questo meccanismo di sicurezza applicato alle operazioni serve a proteggere da attacchi *man in the browser e man in the middle*.

Sono esenti dai meccanismi di SCA i terminali per il pagamento di parcheggi o pedaggi, questo per non creare inutili disagi o code, inoltre cadono nella stessa regola i pagamenti da remoto sino a 30 Euro. Da notare che la norma introduce una deroga sulla SCA sulla basa del livello di rischio del pagamento sino a 500 euro. L'esenzione pertanto può essere applicata qualora il fornitore di servizi presenti un tasso di frode complessivo inferiore al tasso di frode complessivo indicato nella norma. Questo introduce delle semplificazioni che non possono che giovare al business e alla competizione se saranno introdotti strumenti tecnologici innovativi che garantiscano nelle transazioni on-line tassi di frode compatibili con quanto richiesto nelle diverse applicazioni.

Altra considerazione è la decisione dell'EBA di utilizzare certificati eIDAS per l'autenticazione di ASPSP, AISP e PISP. Decisione sicuramente audace perché ancora non è chiaro se saranno presenti anche autorità di certificazione eIDAS in tempo per la data di attuazione dell'ottobre 2018.

Distributed Ledger e Blockchain

La *Distributed Ledger Transaction* (DLT) propone un nuovo paradigma che potrebbe rivoluzionare fortemente il sistema economico sulla base dei concetti di transazione e fiducia. In generale i processi bancari e finanziari richiedono processi approvativi nei quali è necessario ottenere elevati livelli di garanzia; in tale contesto DLT e Blockchain possono esser un campo di sperimentazione alternativo alle logiche tradizionali.

Le tecnologie Blockchain possono gestire i processi autorizzativi tramite infrastrutture nelle quali alle chiavi pubbliche vengono associati asset con relativa chiave privata che valida la transazione. Un processo che è simile a quello della firma digitale ma senza l'obbligo di avere una Certification Authority (CA) accreditata.

Basandosi su questi concetti è chiaro come questa tecnologia elimini di fatto i *single point of failure* e aumenti la sicurezza; tematiche che oggi minacciano i sistemi di pagamento. In questo si rendono anche le transazioni trasparenti e controllabili senza che vi sia una autorità centrale. Scenario sul quale anche la Banca Mondiale si è espressa dicendo che l'eliminazione di questi costi potrebbe portare a notevoli risparmi.

Conclusioni

Uno dei punti qualificanti di questa direttiva è quello di avere consentito l'ingresso di nuovi soggetti all'interno della catena del valore dei pagamenti elettronici, cosa che determinerà una maggiore pressione competitiva all'interno del mercato e sicuramente un reale vantaggio per il consumatore e per le banche che sapranno cogliere gli aspetti innovativi allargando il loro portafogli di servizi e rivedendo i modelli tradizionali. ■

PSD2, una nuova sfida? Piccola guida su come un ente bancario dovrebbe scegliere una soluzione che gli permetta di mantenere il suo posto sul mercato.

autore: Mihai Scemtovici,
direttore generale SolvIT Networks

La Payment Service Directive (PSD2) è una nuova regolamentazione europea che dovrà essere rispettata nel settore finanziario-bancario sin dall'inizio del 2018. Questa direttiva porterà a maggiori cambiamenti per gli enti che operano in questo settore.

BIO

Al seno della compagnia SolvIT Networks, dove lavora da più di 12 anni, Mihai Scemtovici ha sviluppato e diretto progetti di management delle infrastrutture e di management della sicurezza in Romania, in diversi paesi dei Balcani e del Medio Oriente, in Turchia e nei paesi scandinavi. I progetti da lui implementati sono stati svolti in priorità per il settore bancario, le Telco ed anche per conto di enti Governativi. Durante gli ultimi anni, Mihai Scemtovici si è specializzato in proietti specifici al management della sicurezza e della cybersecurity. In questa qualità, è esperto e membro permanente dell'ANSSI (Associazione Nazionale per la Sicurezza dei Sistemi Informatici - l'equivalente rumeno del CLUSIT).

Payment Services Directive (PSD2)

I principali cambiamenti previsti si riferiscono alla necessità di fornire interfacce ai cosiddetti fornitori terzi, di rafforzare i sistemi di autenticazione dei clienti bancari e di fornire il l'autentificazione tramite due o più elementi *(multi factor authentication)*, e questo per la maggior parte delle opzioni di pagamento. In questo modo, i fornitori di servizi di autenticazione saranno anche in grado di fornire servizi utili a dare informazioni sui pagamenti e sui conti dei clienti. Inoltre saranno anche in grado di rivendere servizi bancari sotto forma di offerte "pacchetti" che propongono nuovi benefici per i portafogli dei clienti. Immaginate ad esempio l'attrattività dei servizi bancari aggiuntivi che potrebbe proporvi, nel suo pacchetto di offerte, il vostro operatore di telecomunicazione oppure la vostra catena preferita di supermercati?

Per quanto unanime l'opinione degli esperti di settore sulle conseguenze di questa direttiva, sulle banche, è bene precisare anche i vantaggi che apporterà. Ad esempio, una banca che ha che ha già aperto interfacce di accesso ad un fornitore ha automaticamente accesso ad una base di clienti molto più ricca di quella che è riuscita a riunire in un approccio diretto con

i suoi canali classici. Questo dato viene rafforzato se consideriamo la rete di penetrazione delle aziende telco in seno alla popolazione (oltre il 100 %) a confronto di quella delle banche (massimo 60%); anche le catene di supermercati hanno una rete di penetrazione, in aree non-urbane, superiore a quella delle banche.

Perciò, le banche devono adoperarsi ad offrire interfacce, da un lato affidabili e, dall'altro, quanto più sicure possibili, vista la sensibilità altissima delle informazioni che saranno l'oggetto delle transazioni. Le banche annunciano già che vi sarà una grande competizione. In questo senso, gli enti che opteranno per interfacce facili all'uso, con funzionalità estensive potrebbero fare una scelta vincente per essere più attrattive e quindi in miglior posizione per negoziare termini preferenziali nei contratti commerciali con i fornitori di servizi.

Cosa dovrebbe quindi fare una banca? Dovrebbe innanzitutto sviluppare interfacce verso le sue applicazioni interne ed esporle alle parti terze. Queste interfacce (API) dovranno quindi essere sviluppate e poi testate costantemente in termini di sicurezza, poiché l'industria bancaria è, per essenza, un mondo dinamico. Pure le risorse umane impegnate saranno decisive, sia nel momento dello sviluppo delle interfacce e sia durante le connessioni con i sistemi del fornitore di servizi. Dovranno inoltre garantire una presenza continua, e permanente per assicurare la perfetta gestione delle stesse.

Esistono già applicazioni che risolvono in modo esaustivo questi bisogni? Si, esistono: fanno parte delle soluzioni della categoria API Management. Però ogni ente finanziario deve saper scegliere nella gamma di prodotti disponibili quello che fa per lui: per questa ragione ho scelto di presentare qui un compendio che aiuti le banche nella valutazione delle possibili soluzioni

In primo luogo, bisogna chiedersi quali sono i passi decisivi che deve compiere la banca e le funzionalità chiave che vuole mettere a disposizione dei fornitori. In questo modo, i dirigenti potranno assicurarsi che la soluzione di API Management scelta non solo risponderà veramente ai bisogni attuali e futuri, ma soprattutto garantirà alla loro banca una posizione di favore sul mercato, *in primis* di fronte alle scelte della concorrenza.

Un primo passo può essere la scelta di una soluzione già leader del mercato nel suo campo, o perlomeno in quella dei nuovi challengers così come riportato negli studi indipendenti di nicchia (ad esempio i rapporti Gartner).

Poiché le API che bisognerà sviluppare saranno al servizio di un'applicazione di una banca, cioè uno degli obiettivi privilegiati dagli attacchi cibernetici, il primo aspetto da verificare è che offra funzionalità robuste nel campo della sicurezza informatica. In questo senso, le domande da porre nel dialogo con i rivenditori sono soprattutto le seguenti: l'API richiesto avrà una protezione *"by design"* contro le minacce? Sarà coerente con le metodologie della community dell'*Open Web Application Security Project* (OWASP)? Permetterà un'integrazione facile con le applicazioni di tipo *Single Sign-On* oppure *Identity Management* garantendo una sicurezza completa di tutte le applicazioni terze, mobili e cloud?

In un secondo tempo, bisogna imperativamente considerare che si parla di un'applicazione che dovrà essere capace di supportare centinaia di migliaia o addirittura milioni di transazioni, ad unità di tempo, e quindi si pone il problema, per le banche, di verificare la scalabilità del prodotto. L'API richiesto sarà in grado di mantenere una performance di alto livello nei giorni di picco, come ad esempio durante il periodo natalizio? Potrà effettuare misure di *prioritization*, di *routing* intelligenti e dinamici delle richieste provenienti dalle applicazioni che vi saranno collegate?

Un terzo elemento di grande importanza, visto che l'applicazione dovrà anche competere con altri fornitori, è quello della flessibilità dell'applicazione e della sua facilità d'uso, non solo per la banca stessa, ma soprattutto per i partner esterni all'ente. Bisogna immaginare ad esempio un fornitore di servizi che intende collegare le sue operazioni a due banche diverse. La prima banca gli offre un'API facile da usare, flessibile, con interfacce di amministrazioni ergonomiche ed accoglienti, mentre l'API della seconda banca riscontra tanti problemi. I clienti potrebbero avere errori d'utilizzazione, e di conseguenza il fornitore dovrebbe rivolgersi alla banca per risolvere i vari casi. In queste condizioni, il fornitore raccomanderà ai suoi clienti i servizi della prima banca, anche nel caso in cui questi siano un po' più costosi paragonati a quelli del secondo ente bancario. Non vi pare uno scenario già conosciuto oggi?

Gli ultimi aspetti da valutare, anche se non sono per nulla di ultima importanza, sono quelli legati alla facilità di realizzare delle API dedicate alle applicazioni mobili, tenendo conto che i nostri supporti IT mobili sono numericamente già ben superiori a quelli fissi. In un altro registro, la banca deve avere la possibilità di controllare con esattezza i tipi di accesso usati e di contabilizzarli in vista della fatturazione. Personalmente, considererei anche la possibilità di offrire un accesso diretto dal *cloud* verso l'applicazione della mia banca. Anche qui, bisogna tener conto che la migrazione verso il *cloud* ha già raggiunto una massa critica che rende inarrestabile questo trend. E quindi, perché no, a me piacerebbe poter creare un'API con funzionalità di *"drag and drop"*. Perché a questo punto, come utente, mi è indifferente il fatto di dovermi collegare con un'applicazione che non ha più di base un supporto, ma una base di dati o un'altra fonte di dati.

In conclusione, se fossi un amministratore di banca, vorrei che la mia soluzione di API Management fosse molto scalabile, coprisse tutto il ciclo di vita di un API e mi offrisse la possibilità di creare un nuovo API in pochi minuti. Soprattutto, esigerei che mi fornisca un supporto mobile di qualità con funzionalità avanzate di amministrazione per la mia banca e per i partner che si collegheranno alle risorse della mia banca. Così, nello stesso tempo, potrei assicurare anche ai clienti della mia banca non solo il controllo totale sui diritti che gli sono conferiti dai fornitori di servizi TPP, ma anche di avere la possibilità, in qualsiasi momento, di attivare/disattivare opzioni oppure di accedere alle nuove funzionalità proposte dalle applicazioni. ■

PSD2 e gli impatti sui processi antifrode

autore: Teo Santaguida
Responsabile Centro Competenza Anti-frode IKS

BIO

Dopo gli studi in informatica e le prime esperienze nel settore ICT in particolare come Software Configuration Manager, nel 2000 inizia il suo percorso professionale nell'ambito dell'ICT Security come analista di sicurezza presso uno dei primi SOC italiani. Con il passare degli anni assume il ruolo di Manager in progetti di consulenza, system integration ed erogazione di servizi gestiti principalmente nel contesto ICT Security e per il settore finance, maturando esperienze consolidate in particolar modo negli ambiti log management, SIEM, SOC e Fraud Management. Nel 2012 approda in IKS, in linea con l'obiettivo aziendale di consolidare il proprio posizionamento nel mercato antifrode italiano e diventa riferimento aziendale per l'ingegnerizzazione dell'offerta antifrode e Product Manager della soluzione SMASH, soluzione di transaction monitoring sviluppata dal gruppo IKS. In virtù della crescita aziendale nel settore, nel 2014 ottiene il ruolo di Responsabile del Centro Competenza Antifrode, divisione di IKS specializza in servizi contro le frodi finanziare su canali di online banking.

Entro il 13 gennaio 2018 gli Stati Membri dovranno recepire all'interno dei propri ordinamenti nazionali la direttiva 2015/2366/UE, nota come PSD2.

La **PSD2** rappresenta solo l'ultimo di una serie di interventi del legislatore europeo in ambito di servizi di pagamento con l'obiettivo di proseguire nello sviluppo di un mercato unico integrato, uniformando le regole tra Prestatori Servizi di Pagamento **(PSP)**.

Il contesto di riferimento

La PSD2 interviene in un momento storico caratterizzato da un forte cambiamento delle abitudini degli utenti relativamente le modalità di pagamento, le quali risultano sempre più orientate verso strumenti di **digital payment**.

La maggiore propensione degli utenti all'utilizzo di **dispositivi mobili**, il cambiamento nelle abitudini dei consumatori che prediligono sempre di più pagamenti caratterizzati da una **user experience** semplificata e personalizzata e le strategie di **marketing** per aumentare l'adozione dei dispositivi mobili e raccogliere informazioni legate al comportamento dei clienti sono i driver principali che hanno motivato la nascita e lo sviluppo di nuovi operatori di servizi di pagamento, che negli ultimi anni si sono affacciati sul mercato affiancando gli operatori tradizionali (banche e circuiti di carte di credito).

Altro fattore ponderante da considerare nella descrizione del contesto di riferimento è il fenomeno fraudolento, che vede trend di crescita non trascurabili nel settore dei pagamenti elettronici ed in particolar modo nel settore dei pagamenti **CNP (Card-Not-Present)**.

Il fenomeno è sotto osservazione da parte del legislatore Europeo, ed è uno dei razionali più significativi che hanno portato all'emissione di diverse raccomandazioni e normative negli ultimi anni, relativamente la necessità di innalzamento dei sistemi di sicurezza dei pagamenti elettronici.

La normativa PSD2

Il campo di azione della PSD2 è molto ampio, così come i relativi impatti sui processi degli istituti di pagamento tradizionali e non. L'applicazione della PSD2 impatta su tutte le principali direzioni degli istituti di pagamento: dall'ufficio Finance alla Compliance, dalle infrastrutture IT agli aspetti legali, la PSD2 pone sfide enormi, in un contesto di business

che prefigura un cambio di paradigma del rapporto tra istituti finanziari tradizionali e utenti finali.

La PSD2 introduce il concetto di Third Party Payment Service Providers **(TPP)**, parificando gli istituti di pagamento tradizionali e i nuovi operatori **(FINTECH)** sotto un'unica generica definizione di **PSP** (Payment Service Provider), e impone agli **ASPSP** (gli enti di radicamento del conto, tipicamente quindi i PSP tradizionali quali banche e circuiti di carte di credito) di permettere l'accesso alle terze parti per reperire informazioni sul conto, verificare la disponibilità di fondi per un trasferimento di denaro e inizializzare un pagamento.

Attraverso l'articolo 97, la PSD2 impone un aumento del livello di sicurezza basato sul principio di autenticazione forte dell'utente in fase di accesso al conto e/o transaction signing in fase di disposizione di un pagamento elettronico e rimanda all'**EBA** (European Banking Authority) la descrizione delle specifiche tecniche e di sicurezza inerenti il processo di autenticazione forte.

Nel Draft finale di EBA vengono enunciati principi e descritti requisiti che, oltre ad avere un ovvio impatto sui servizi di pagamento offerti agli utenti finali (e ai TPP), pongono diversi spunti di riflessione sugli impatti che la PSD2 ha sui processi antifrode in essere.

E' facile desumere il massiccio livello di impatti della PSD2 su tutte le principali direzioni degli istituti di pagamento: dall'ufficio Finance alla Compliance, dalle infrastrutture IT agli aspetti legali, la PSD2 pone sfide enormi, in un contesto di business che prefigura un cambio di paradigma del rapporto tra istituti finanziari tradizionali e utenti finali.

Gli impatti sul processo antifrode

A prescindere dai requisiti imposti dalla normativa, è opportuno considerare l'estensione dei processi antifrode al monitoraggio del canale dedicato alle Third Party per altri importanti aspetti quali per esempio: la responsabilità del rimborso all'utente in caso di disconoscimento, di responsabilità dell'ASPSP; poter avere visibilità dello storico utente anche se questo opera tramite servizi offerte da terze parti; mantenere e monitorare un trend degli eventi fraudolenti provenienti dalle terze parti in funzione di una congrua gestione del rischio operativo

In linea con le evoluzioni del mercato, le abitudini degli utenti e la necessità di semplificare la user-experience utente, è plausibile ipotizzare che molti PSP concentreranno le proprie scelte tecnologiche di soluzioni di strong authentication basate su software token per dispositivi mobili. Questa scelta permetterebbe di far convergere su unico dispositivo l'accesso ai propri servizi (per esempio mobile banking) e le procedure di autenticazione forte e transaction signing. Non a caso l'**RTS** EBA (**Regulatory Technical Standards** on strong customer authentication and secure communication under PSD2) insiste, tramite diversi articoli, sulla messa in opera di sistemi di monitoraggio del livello di rischio dei dispositivi mobili e sistemi anti-compromissione atti a prevenire la compromissione di elementi della Strong Authentication gestiti nel contesto di un dispositivo mobile. D'altro canto, il canale mobile e la sua sicurezza erano state escluse come ambito di applicazione dalla precedente normativa EBA relativa alla sicurezza dei pagamenti Internet, rimandando la gestione della problematica nell'ambito dell'emissione della PSD2, così come è puntualmente accaduto.

La direttiva PSD2 pone sfide enormi, in un contesto di business che prefigura un cambio di paradigma del rapporto tra istituti finanziari tradizionali e utenti finali.

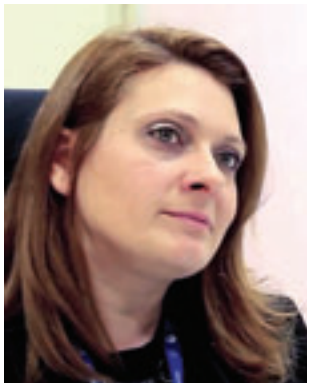
Oggi è opportuno considerare il canale mobile come elemento focale nell'ambito del business dei pagamenti elettronici: è ormai consolidato che sia i servizi offerti dai PSP tradizionali, che quelli forniti da TPP (Fintech), stiano centralizzando il proprio funzionamento attraverso il canale mobile. E' chiaro quindi che il contesto di sicurezza in cui gira la propria applicazione di business, o il meccanismo di **SCA** (Strong Customer Authentication) fornito all'utente, assume un valore fondamentale nell'ambito della valutazione del rischio della transazione.

L'RTS EBA norma diverse condizioni, molto articolate, per le quali è possibile non effettuare la procedura di SCA in determinate condizioni quali per esempio tipologie di canali (per esempio pagamenti su terminali non presidiati), soglie di importo, tipologie di dati acceduti e tempo occorso dall'ultima autenticazione forte effettuata e, infine, in base alla valutazione del rischio della transazione.

Il **transaction monitoring** può essere utilizzato per determinare se la transazione rientra o meno nelle condizioni di eccezione, accentrando tutte le logiche in un unico punto del processo di autorizzazione e fungendo da fonte dati certificata per ogni eventuale attività di reporting e auditing sulle modalità di gestione delle eccezioni applicate. ■

Fonti:
http://www.osservatori.net/it_it/pubblicazioni/il-mobile-payment-commerce-alla-conquista-del-mondo
https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money
http://www.xtn-lab.com/smart_authentication/

PSD2 e sicurezza



La PSD2 ha portato in campo un prorompente mutamento, che si traduce non solo in nuove aree di business, ma anche in maggiori complessità tecnologiche connesse a vari temi quali ad esempio la *strong customer authentication* nonché le modalità attraverso le quali sarà richiesto ai PSP di implementare meccanismi in grado di prevenire, rilevare e bloccare in tempo reale time le operazioni fraudolente prima della loro autorizzazione.

autore: Veronica Borgogna
Consorzio BANCOMAT®

In sostanza, non sarà più sufficiente fare prevenzione frodi nelle migliori modalità identificate al proprio interno, in quanto viene richiesto di elaborare ed applicare vere e proprie strategie di *Fraud Management*, basate su analisi degli incidenti, patterns sospetti e abitudini comportamentali.

BIO

Veronica Borgogna è la Responsabile del Nucleo Processi e Controlli del Consorzio BANCOMAT®. All'area Processi e Controlli fanno capo le Funzioni di Audit, Risk Management e Fraud Management. Sotto la sua responsabilità ci sono le attività di monitoraggio e controllo dell'erogazione dei servizi legati all'utilizzo dei marchi BANCOMAT® e PagoBANCOMAT®, di rischiosità dei processi e prodotti dell'intero Sistema e dell'andamento dei fenomeni fraudolenti. Attraverso il Centro Antifrode coordina le attività di analisi, prevenzione e contrasto e partecipa a tavoli di lavoro nazionali e internazionali sul tema della lotta alle frodi come GIPAF, Osservatorio Sicurezza e Frodi informatiche, Security Working Group EPCA, EC3 Europol ed è Board Member E.A.S.T. (European ATM Security Team). Svolge inoltre attività di Auditing presso Licenziatari, Aderenti, fornitori e stakeholder del Sistema.

Tali mutamenti costringeranno peraltro gli operatori specializzati a rivedere le proprie logiche organizzative, in ottica evolutiva, e approcciando a nuove strategie di adattamento nel bilanciamento tra sicurezza e business.

Si parte dalla logica per cui il contrasto ai fenomeni fraudolenti è un'attività che richiede tempestività e aggiornamento continuo, analisi puntuali dei trend del momento, adeguamento dei sistemi antifrode e dei device di sicurezza, azioni sinergiche, strategiche, studiate e organizzate sia per contrastare che per prevenire.

Questa esigenza porta inevitabilmente all'innalzamento del livello tecnologico nel rafforzamento dei sistemi antifrode, ma non solo; la sicurezza non è infatti solo un fatto tecnologico, in quanto interessa asset aziendali diversi: organizzativi, umani e di business.

Occorre pertanto porsi nella prospettiva di costruire un modello di sicurezza integrato. Va peraltro detto che, nonostante le novità siano rilevanti, le stesse attengono ad un tema – quello del Fraud – assolutamente noto agli operatori del mercato che da anni – anche grazie agli input degli Schemi di pagamento - hanno appreso concetti e tecniche di resilienza.

A vari livelli e con diverse priorità di intervento Schemi di Pagamento, PSP, Provider tecnologici hanno effettuato profonde ricognizioni dei propri sistemi di Governance raggiungendo la consapevolezza e in molti casi la maturità per ristrutturarsi e adeguarsi.

Anche anticipando alcuni concetti oggi sviluppati dalla PSD2, il Consorzio BANCOMAT ha da tempo intrapreso un approccio alla prevenzione, costruendo una metodologia di analisi e monitoraggi Risk Based.

L'applicazione del metodo si dipana nella costruzione del "risk shield", risultato di una gestione del rischio che mira a dettare istruzioni organizzative, individuare soluzioni – anche tecnologiche – per la rilevazione automatica degli eventi e a dare altresì un framework di riferimento per la gestione procedurale di tutti gli interventi da attuare.

Tali interventi preventivi vengono raccolti nell' attività di risk profiling che consente di concentrare gli sforzi e le attenzioni sulle aree maggiormente esposte al rischio senza disperdere risorse ed energie

in controlli affannosi escludendo tutto ciò che ha scarsa probabilità di accadimento e scarso impatto.

Non è possibile controllare tutto; la tattica migliore è concentrarsi sul contenere i danni che si verificano dove le nostre difese sono eluse implementando i "giusti" monitoraggi (specifici e mirati).

Bisogna pertanto automatizzare il rilevamento dei fenomeni noti creando bibliografie di eventi (event collection) e delle risoluzioni di successo al fine di applicare strategie efficaci e "provate" nel minor tempo possibile (filtering):

- identificare i fenomeni sconosciuti scartando gli eventi noti e permettendo, per esclusione, un tempestivo rilevamento dei fenomeni sconosciuti che abbiano eluso i controlli preventivi (classification).
- incanalare le informazioni nella giusta direzione avendo piena conoscenza delle organizzazioni, competenze e processi, così da farle confluire verso i nodi "strategici" della catena di erogazione dei servizi (advice)
- prioritizzare gli interventi concentrando gli sforzi laddove siano accertate vulnerabilità a maggiore impatto, evitando la dispersione delle risorse e alleggerendo al contempo le attività di monitoraggio (detection).

A tale scopo il Consorzio ha di recente anche implementato un framework di sicurezza formato che muove dal nuovo approccio al Rischio integrato e che si compone di:

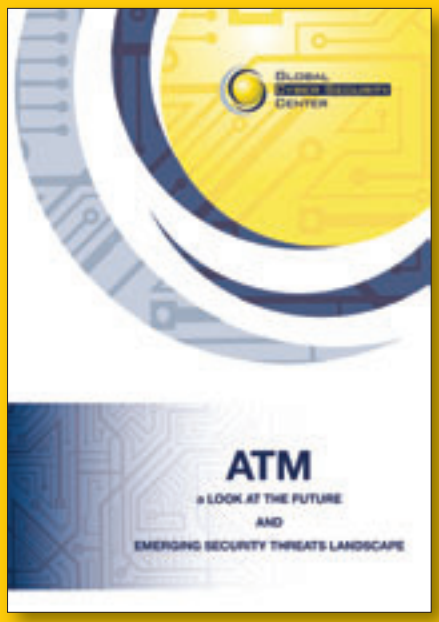
- requisiti per il rafforzamento dei presidi di sicurezza antifrode,
- best practice per l'espletamento dei processi,
- elementi specifici di controllo e verifica – a livello organizzativo, tecnologico e di processo.

La ridondanza di sistemi di alert può essere controproducente, perché impegna troppi processi e risorse creando ingessature e lungaggini.

Non esiste una ricetta valida per qualsiasi soggetto, in qualsiasi momento, contro qualsiasi rischio.

Per preservare l'autonomia nell'offerta dei servizi di mercato, sposare progresso tecnologico ed esperienza del consumatore il Consorzio suggerire a tutti gli operatori come raggiungere lo

stesso livello di sicurezza, pur nella complessità della catena di erogazione, attraverso un irrobustimento del proprio sistema di Governance. ■



GLOBAL CYBER SECURITY CENTER

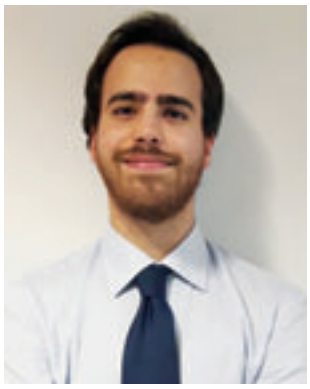
ATM - A look at the future and emerging security threats landscape

La pubblicazione, disponibile previa registrazione sul sito www.gcsec.org, offre una panoramica della stato attuale della sicurezza degli ATM, delle minacce classiche ed emergenti a cui sono soggetti e delle misure di sicurezza implementabili . Lo studio prende in considerazione anche l'evoluzione futura dei sistemi e dei servizi degli ATM e delle implicazioni di sicurezza che ne conseguono.

ADVANCED PERSISTENT THREATS - Case study

La pubblicazione offre una panoramica dei modelli di attacco APT e dei relativi indicatori di minaccia. Le varie tecniche, tattiche e procedure di attacco così come le raccomandazioni di sicurezza sono rappresentate in ogni singola fase della cyber kill chain. È possibile richiedere una copia della pubblicazione scrivendo a info@gcsec.org.

Cyber Authentication: regolamentazione per un'autenticazione veloce e sicura



autore: Michele Gallante

"Non è vero che abbiamo poco tempo: la verità è che ne perdiamo molto" - De Brevitate Vitae,
Lucio Anneo Seneca.

Il tempo sembra non bastare mai, e se da un lato l'evoluzione tecnologica ha velocizzato l'accesso ad alcuni servizi, dall'altro ha dovuto fare i conti con le problematiche e i pericoli di sicurezza. Per questo si è passati da semplici autenticazione con "nome utente" e "password", fino a procedure lunghe e complesse con l'inserimento di "codici pin" associati all'utente tramite una *"grid card"*, l'utilizzo di token (OPT = *one-time password*) e altri strumenti volti a prevenire la frode informatica, i quali, inevitabilmente, hanno rallentato la procedura e la semplice disponibilità del servizio.

Ovviamente la fluidità dell'esperienza vissuta con questi metodi di riconoscimento (MFA = *Multi Factor Authentication*) e, la necessità di dover ricordare molte password, ostacola il propagarsi di questi strumenti elettronici. Ad esempio, in Italia, l'e-Commerce sta pian piano crescendo, ma rimane preferito l'acquisto in contanti, dove l'affidabilità della transazione che si sta per compiere viene percepita come sicura ed immediata.

Per queste ragioni le multinazionali leader del mercato online stanno cercando di semplificare il più possibile l'utilizzo di metodi di pagamento elettronici, in modo tale da incentivare il loro utilizzo e aumentare i profitti. Basti pensare come "Amazon" abbia introdotto la modalità di vendita con un solo *"click"* (avendo preventivamente associato le credenziali della carta di credito), o il nuovo *"Dash Botton"* che permette, per mezzo di un piccolo pulsante fisico, di inoltrare l'ordine del prodotto senza neanche accendere il computer. Nel prossimo futuro soprattutto le banche vedranno il loro business sempre più indirizzato verso i metodi di pagamento digitali, e per questo stanno implementando soluzioni di *"Cybersecurity Fraud Prevention"* garantendo l'affidabilità del sistema attraverso autenticazioni protette.

Per ovviare alle diverse problematiche, sia che si utilizzi per acquisti online, che per accesso fisico o logico ad un'infrastruttura, si sta cercando di passare a sistemi di riconoscimento biometrici, poiché per loro natura sono direttamente, univocamente e tendenzialmente stabili nel tempo, collegati all'individuo attraverso una profonda relazione tra corpo, comportamento e identità della persona. La biometria (dal greco *"bios"* = vita e *"metros"* = misura) è definita come la disciplina che studia le grandezze biofisiche allo scopo di identificare i meccanismi di funzionamento, di misurare il valore e di indurre un comportamento desiderato in specifici sistemi tecnologici. Convenzionalmente questi sistemi di autenticazione sono ricavati da "proprietà biologiche, aspetti comportamentali, caratteristiche fisiologiche, tratti biologici o azioni ripetibili laddove tali caratteristiche o azioni sono tanto proprie di un certo individuo quanto misurabili, anche se i metodi usati nella pratica per misurarli tecnicamente comportano un

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.

certo grado di probabilità". (ISO/IEC 2382-37 *"Information Technology - Vocabulary - Part 37: Biometrics"*).

Per la loro particolare specificità è necessario garantire adeguate cautele in caso di trattamento; infatti, in ragione della tecnica prescelta, del contesto di utilizzazione, del numero e della tipologia di potenziali interessati, delle modalità e delle finalità del trattamento, può comportare rischi specifici per i diritti e le libertà fondamentali. Questi sistemi di riconoscimento rispecchiano in modo assoluto i requisiti di esclusività (capacità distintiva per ogni persona), permanenza (in quanto rimane inalterato nel tempo o si modifica lentamente) e universalità (presenza in ogni individuo), ma sfortunatamente sono ancora troppo deboli e vulnerabili.

Ad esempio, in caso di furto o perdita di tradizionali credenziali di login si può semplicemente impostarne di nuove, differentemente, il dato biometrico è impossibile da cambiare (tralasciando il naturale mutamento nel tempo), risultando unico nel suo genere. Quindi sarà determinante un'adeguata crittografia che tenga al sicuro queste informazioni. I rischi incombenti sui dati biometrici, impongono, in coerenza con le previsioni del Regolamento Europeo eIDAS in tema di identificazioni, autenticazione e firma digitale, l'obbligo di comunicare al Garante il verificarsi di violazioni di dati o incidenti informatici entro 24 ore dalla conoscenza del fatto (secondo lo schema delle Linee Guida Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014, Allegato B, tramite posta elettronica all'indirizzo databreach.biometria@pec.gpdp.it).

Tra i le varie categorie di dati biometrici (Tabella 1), il sistema di riconoscimento basato sull'impronta digitale rappresenta quasi il 90% delle tecnologie applicate che stanno guadagnando lentamente spazio. Si veda ad esempio, l'impiego in device mobili dove vengono utilizzati oltre che per l'autorizzazione ad accedere a servizi d'informazione, anche per usufruire ad accessi fisici delle infrastrutture (come banche e biblioteche o aree aziendali riservate). Ad ogni modo, Il Garante, impone che questo tipo di riconoscimento sia utilizzato solo per "usi facilitativi", sempre con il consenso dell'interessato ed inoltre con l'obbligo di garantire modalità alternative di accesso per chi non volesse usufruire di tali strumenti biometrici.

Dal punto di vista giuridico l'utilizzo di dati biometrici impone il rispetto di alcuni principi generali dell'ordinamento (liceità, necessità, finalità e proporzionalità) in virtù del fatto che si trattano dati personali c.d. semi-sensibili, capaci di rendere una

persona identificata o identificabile. Antecedentemente alla fase di *"enrollement"* (acquisizione del campione biometrico, memorizzazione ed estrazione fino alla generazione del dato di riferimento archiviato), il titolare del trattamento dovrà obbligatoriamente fornire l'informativa riguardo le finalità perseguite (ad esempio, l'utilizzo dell'impronta digitale per accedere ad un'area riservata, non potrà essere usato per controllare l'orario di accesso dei dipendenti), la modalità di trattamento, le cautele adottate (misure di sicurezza applicate), e, infine, i tempi di conservazione dei dati stessi. Ai sensi dell'art. 17 del Codice della Privacy, è necessario richiedere al Garante una verifica preliminare, salvo l'esonero consentito se adottate determinate condizioni.

Sono attese importanti novità, a seguito delle direttive europee GDPR *(General Data Protection Regulation)* e PSD2 *(Paymnents Service Directive 2)* che diverranno definitivamente vincolanti a partire dal 2018. La regolamentazione comunitaria in materia di privacy, oltre a definire quali siano i dati importanti da proteggere (ad esempio il dato biometrico viene inserito nella categoria di dati sensibili), richiede anche un'analisi dei rischi per evitare usi discriminatori di questo strumento che potrebbe trasformarsi da risorsa in sicurezza in uno strumento di controllo generalizzato sulla salute, l'etnia o la razza. Infatti, ad esempio, si richiede di privilegiare l'uso di sistemi biometrici che richiedano la cooperazione consapevole dell'interessato, e, ove possibile, con minore quantità di informazioni, in modo da ridurre un'ipotetica ricostruzione del campione in fase di trattamento. Importantissima anche la direttiva sui pagamenti elettronici, la quale richiede delle autenticazioni "forti" per garantire la sicurezza delle transazioni. Del 23 Febbraio 2017 il Final Report *(Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication under Article 98 of Directive 2015/2366)* che specifica le norme tecniche in materia di autenticazione e comunicazione. Dalla normativa in esame si evince l'obbligo per gli Stati membri di provvedere a che un prestatore di servizi di pagamento applichi l'autenticazione forte del cliente quando: accede al suo conto di pagamento online, dispone di un'operazione di pagamento elettronico, oppure, quando effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. L'introduzione di nuovi servizi di pagamento (PISP e AISP) dovrà così essere accompagnata dall'applicazione di sistemi in grado di garantire la sicurezza senza possibilità di errore.

Sfortunatamente, un tema delicato che affligge i sistemi biometrici è rappresentato proprio dalla possibilità dell'errore. Infatti, la tecnologia in questione è colpita da una predisposizione all'errore durante la fase di riconoscimento, dove il sistema crea un punteggio denominato *"score"*, in base a quanto il *template* risulti simile a quello di riferimento acquisito nella fase di *ernrollment*. Lo *"score"* viene confrontato con un valore di soglia predefinito, denominato *"matching score"*, il quale potrà variare a seconda di come vengono tarate le apparecchiature. Su quest'argomento il Gruppo di Lavoro dei Garanti Europei, nel Parere n. 3/2012 sugli sviluppi delle tecnologie biometriche ha affermato che *"con un corretto aggiustamento del sistema e un'esatta regolazione delle impostazioni è possibile ridurre al minimo gli errori"*. Alla luce delle considerazioni, quindi, la soglia di errore dovrà tenere conto della finalità del trattamento, in modo tale che un elevato FRR (False Acceptance Rate) sarà messo in relazione alla sicurezza rispetto al caso di specie.

Per quanto riguarda la conservazione del dato, le normative non specificano particolari metodi di custodia. Ad esempio potrà trovarsi nella disponibilità del titolare del trattamento, conservato in una banca dati centralizzata (in forma di *Hardware Security Module*), nelle postazioni di lavoro informatiche, o altrimenti sugli stessi dispositivi di acquisizione biometrica sicuri (es. token, smart card) affidati alla diretta ed esclusiva disponibilità degli interessati, dotati di adeguate capacità crittografiche e certificati per le funzionalità richieste in conformità alla norma tecnica: ISO/IEC 15408 o FIPS 140-2. I dati biometrici grezzi *(raw data)* generati nel corso del procedimento di acquisizione biometrica *(biometric capture)* dovranno inoltre essere cancellati dall'area di memoria temporanee in modo da garantire la sicurezza e riservatezza assoluta.

Il riconoscimento dell'utente, quindi, può essere basato su verifica biometrica (processo in cui il soggetto dichiara la sua identità e il sistema effettua un confronto fra il modello biometrico rilevato e quello memorizzato e corrispondente all'identità dichiarata) anche detto "confronto uno-a-uno" oppure su identificazione biometrica (processo in cui il sistema confronta il modello rilevato con tutti i modelli disponibili per individuare l'identità del soggetto), "confronto uno-a-molti", operazione certamente più complessa. In entrambi i casi, come descritto dalle Raccomandazioni ENISA, i dati andranno protetti con strumenti crittografici o in database che supportino la cifratura a livello di record o di colonna.

Nel prossimo futuro già si intravedono progetti all'avanguardia, come il programma PIDaas *(Private Identity as a Service)*, che prevede il coinvolgimento di dipendenti del CSI i quali, per poter visualizzare la busta paga e altri documenti, potranno usare il servizio di riconoscimento biometrico. Anche l'annuncio di Augustin de Romanet, numero uno di Aéroports de Paris, che riferendosi all'autenticazione biometrica ha detto *"in prospettiva è probabilmente una soluzione verso cui potremmo orientarci"* e per questo si è recato all'aeroporto di Ben Gurion di Tel Aviv per studiare i metodi messi in campo dalla security locale.

Come abbiamo visto una disciplina appropriata non è ancora in atto, ma sicuramente le nuove regolamentazioni che entreranno in vigore il prossimo anno getteranno le basi per una chiara, trasparente e uniforme interpretazione della materia. È vero sì che la velocità di autenticazione sarà essenziale per spostare il mercato in questa direzione, ma la sicurezza dei dati, intesa come integrità, disponibilità e riservatezza, è un diritto fondamentale che deve essere protetto ad ogni costo. ■

Tabella 1: Riepilogo determinato in base alle Linee-Guida in materia di Riconoscimento Biometrico e Firma Grafometrica del Garante Privacy, Allegato A, 2014.

DATO BIOMETRICO	Modalità di rilevamento	Caratteristiche	Commento
Impronte digitali	Acquisizione tramite dispositivi di rilevamento ottico, che riproducono la disposizione delle creste di Galton e delle valli cutanee presenti sui polpastrelli delle dita	Necessaria una partecipazione attiva dell'interessato anche se può essere tracciata senza la sua volontà; le proprietà rimangono stabili nel tempo	Alto grado di unicità differendo addirittura tra gemelli omozigoti
Firma autografa	Acquisizione tramite tablet grafometrici in grado di rilevare oltre il tratto grafico, anche una serie di parametri dinamici associati all'atto della firma (velocità di tracciamento, pressione, inclinazione, salti in volo…)	Necessita di una partecipazione attiva dell'interessato, non risulta stabile nel tempo e per questo è difficile la sua tracciabilità	Tassi elevati di falsi negativi che rendono poco efficiente l'utilizzo fuori contesti particolari in cui sia possibile l'intervento umano.
Emissione vocale	Autenticazione dell'individuo effettuato tramite interlocuzione telefonica tradizionale, o via Internet, oppure su scala locale interagendo con un dispositivo connesso o integrato in un personal computer o altro dispositivo informatico. Il riconoscimento viene dedotto dal tratto vocale, alla sua lunghezza, alle risonanze, alla morfologia della bocca e delle cavità nasali	Necessita di una partecipazione attiva dell'interessato, ma risulta facile una sua tracciabilità senza la volontà dello stesso. La sua stabilità nel tempo è soggetta ad un mutevole cambiamento naturale	L'analisi dei segnali vocali può essere effettuata anche tramite procedure di "sfida" con le quali l'interessato viene invitato a ripetere delle frasi, nomi o numeri, in modo tale da aumentarne la sicurezza,
Struttura venosa delle dita della mano	Acquisizione tramite sensori che rilevano la forma e la disposizione delle vene delle dita, del dorso o del palmo della mano, utilizzando una sorgente luminosa a lunghezza d'onda prossima all'infrarosso	Necessita di una partecipazione attiva dell'interessato, risulta difficile una sua tracciabilità a scopo di replica, ma non è certa una sua stabilità permanente nel tempo	L'accuratezza elevata della corrispondenza con il modello di riferimento va a discapito dell'ingombro necessario per lo strumento.
Struttura vascolare della retina	Acquisizione tramite l'utilizzo di un fascio di luce a infrarosso a bassa intensità che illumini la parte posteriore dell'occhio	Necessita di una partecipazione attiva dell'interessato, difficile la sua tracciabilità senza la volontà del soggetto, ed inoltre è caratterizzata da una stabilità elevata nel tempo	Viene utilizzato per sistemi di sicurezza particolarmente elevati. Inoltre, non è possibile utilizzare tessuti di persone decadute, poiché il sensore rileva la circolazione sanguigna
Forma dell'iride	Tecnica di lettura dell'iride che consente il rilevamento della forma della pupilla e della parte anteriore dell'occhio mediante immagini ad alta risoluzione	I sensori più comuni prevedono una partecipazione nell'atto di rilevamento, ma non è obbligatoria. La sua tracciabilità non è facile e la stabilità nel tempo è garantita	Elevata accuratezza e velocità di comparazione. Il tasso falsi positivi è basso anche se ne segnalano elevati di falsi negativi
Topografia della mano	Rilevazione delle proprietà geometriche dell'arto (bidimensionali o tridimensionali), acquisite mediante un apposito dispositivo di ripresa che coglie determinate caratteristiche quali la forma, la larghezza e lunghezza delle dita, la posizione e la forma delle nocche o del palmo della mano	Necessita di una partecipazione attiva dell'interessato, ma può essere tracciata senza la volontà dell'interessato. Precaria la sua stabilità nel tempo	Non sono descrittive al punto da risultare uniche e adatte all'identificazione biometrica, ma nel contempo sono sufficientemente adatte per essere impiegate efficacemente ai fini della verifica biometrica
Caratteristiche del volto	L'analisi delle sembianze facciali è un procedimento complesso (algoritmo) che utilizza immagini video in luce visibile o "termiche" a infrarosso	La partecipazione attiva non è richiesta, è possibile una tracciabilità e il dato rimane stabile nel tempo	Confronti biometrici complicati (capigliatura, occhiali, posizione assunta, illuminazione)

Numero e complessità degli attacchi informatici in crescita, nuove minacce ogni giorno: come difendersi?

autore : Elena Mena Agresti

Il numero e la complessità degli attacchi informatici, delle vulnerabilità e delle nuove minacce, sta via via aumentando e le organizzazioni devono essere al passo con i tempi e saper rispondere con altrettanta velocità in uno scenario in continua evoluzione.

Il compito già impegnativo delle imprese di proteggersi contro le minacce cyber è aggravato dal fenomeno globale della skill shortage, ovvero mancanza di competenze nel settore della cyber security.

Il fenomeno, infatti, non è locale ma globale come emerge anche da uno studio condotto da Mcafee[1]. Tale studio ha coinvolto otto paesi (Australia, Francia, Germania, Israele, Giappone, Messico, Inghilterra e Stati Uniti) che seppur caratterizzati da diverse dimensioni, sistemi educativi, livelli di reddito e strutture politiche, ha evidenziato come la domanda di professionisti di sicurezza informatica sia di gran lunga superiore all'offerta di personale qualificato.

La mancanza di forza lavoro nel settore della cyber security viene definita proprio in questo studio come "una vulnerabilità critica di aziende e Paesi". L'82% dei rispondenti riportano una carenza di competenze di cyber security nelle proprie organizzazioni, il 71% dichiara che tale mancanza

produce un danno diretto e misurabile per l'azienda. Le tre competenze maggiormente richieste sono la capacità di identificare intrusioni, sviluppo sicuro di software, e attack mitigation.

Tale fenomeno è concreto e avvalorato da dati e stime impressionati. Da un'analisi effettuata da ISACA nel 2016 emerge che 2 milioni di posti di lavoro nel settore della sicurezza informatica resteranno vacanti nel 2019 a causa di mancanza di skill e competenze adeguate. Già nel 2015, solo negli Stati Uniti circa 209.000 posti di lavoro di sicurezza informatica sono rimasti vuoti.

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.

Cosa è possibile fare in questo scenario? Le organizzazioni, così come i governi, possono iniziare a intraprendere una serie di iniziative per ridurre al minimo questo gap esistente di competenze che con il tempo tenderà ad aumentare con il sempre maggiore sviluppo di nuove tecnologie e nuove minacce cyber.

- AUTOMATIZZARE il più possibile le attività e i processi più semplici ed elementari della cyber security anche tramite l'applicazione di tecniche di machine learning che attraverso processi di autoapprendimento possano pian piano riuscire a svolgere attività sempre più complesse. Ciò consentirebbe ai team di cyber security, quasi sempre sotto staffati, di dedicarsi alle attività di analisi che realmente richiedono skill e competenze elevate, dopo uno screening effettuato direttamente dalle macchine;
- INSTAURARE COLLABORAZIONI con le Università nell'organizzazione di corsi post laurea o master universitari, per far svolgere tirocini formativi o progetti di dottorato industriale presso le proprie organizzazioni. Tali collaborazioni consentirebbero alle organizzazioni di identificare nuovi talenti e di poter creare startup e sviluppare prodotti e servizi tecnologici innovativi grazie ai rapporti instaurati con i ricercatori, dottoranti e in generale gli startupper;
- INVESTIRE NEL PERSONALE, creando dei programmi di crescita economica e professionale realmente meritocratici, stimolanti e trasparenti per i dipendenti che gli incoraggino all'impegno e allo sviluppo continuo di skill e competenze;
- DEFINIRE PROGRAMMI FORMATIVI aziendali mirati rispetto alle reali necessità e ai gap di competenze presenti in azienda. Soprattutto nel settore della cyber security caratterizzato da uno sviluppo velocissimo delle nuove tecnologie, tecniche di attacco e di difesa, risulta necessario mantenere il proprio personale sempre aggiornato. A volte però i team della security sono oggetto di formazione "generalista" e non tecnica mirata in grado di rafforzare realmente le competenze e acquisirne di nuove. Il catalogo corsi aziendali di cyber security soprattutto per gli aspetti più tecnici dovrebbe essere aggiornato periodicamente e risponde alle necessità formative aziendali;
- ORGANIZZARE CAMPAGNE DI SENSIBILIZZAZIONE per tutto il personale e non solo per gli addetti ai lavori. La cyber security così come il digitale non sono rappresentati solo dagli strumenti tecnologici ma anche dal modo in cui l'individuo si rapporta con le tecnologie come erogatore e fruitore di servizi. La trasformazione digitale così come la cyber security deve interessare e coinvolgere tutte le persone dell'azienda perché tutte partecipano, ognuna a proprio titolo, al percorso di cambiamento dell'azienda;
- CREARE MOMENTI DI INCONTRO tra i vari team aziendali che collaborano tra loro nel settore della cyber security (es. CERT, SOC, R&D, legale, anti frode, …) e con team similari di altre organizzazioni (es. CERT e SOC di altre aziende) per uno scambio fattivo di conoscenze e competenze;
- SELEZIONARE I PROFILI TECNICI non solo attraverso colloqui tradizionali, sicuramente indispensabili per un primo screening tecnico e per valutare i soft skill delle risorse, ma avvalendosi anche di piattaforme di cyber range in grado di testare le reali competenze tecniche operative acquisite dal candidato (es. capacità di identificazione e analisi delle minacce cyber, tecniche di difesa e protezione degli asset aziendali);
- DEFINIRE PROGRAMMI DI "MOBILITY MANAGEMENT" che consentano al personale di poter ricoprire più ruoli all'interno dei team della cyber security al fine di creare una figura professionale completa. Soprattutto nel campo della cyber security, oltre alle competenze tecniche e tecnologiche, è richiesta la conoscenza dei processi, servizi e del business dell'azienda per poter proteggere al meglio il patrimonio informativo aziendale;
- DEFINIRE UN PIANO EDUCATIVO NAZIONALE che includa nei programmi scolastici delle scuole di ogni ordine e grado, e in particolar modo nel mondo universitario, le competenze digitali e di cyber security richieste sia per la digitalizzazione che per lo sviluppo del Paese

La fondazione GCSEC ha instaurato numerose collaborazioni con le principali università italiane (es. Università degli studi di Roma La Sapienza, Campus Biomedico di Roma, Link Campus University, Università di Perugia, Università di Trento, Università della Calabria, Università Mediterranea di Reggio Calabria). Tali collaborazioni rientrano in una serie di iniziative volte a rafforzare la cultura della cyber security in Italia.

Recentemente, insieme a Poste Italiane, ha instaurato una collaborazione con l'Università della Calabria per l'istituzione di due Master Universitari di II livello sulla Cyber Security dedicati rispettivamente alla Sicurezza delle Informazioni, focalizzato sugli aspetti di governance dell'information security, e di Ethical Hacking, operativo orientato ad acquisire competenze sulle principali tecniche di attacco cyber.

In particolare, il Master in Ethical Hacking è il primo nel suo genere in Italia e mira a formare esperti in grado di identificare, prevenire e contrastare le principali tipologie di attacco cyber che possono essere perpetrate a danno di organizzazioni pubbliche e private. Gli studenti impareranno a utilizzare in modo responsabile le tecniche di attacco e analizzare gli aspetti di sicurezza dal punto di vista dell'hacker al fine di elevare il livello di protezione e sicurezza delle organizzazioni. Potranno sperimentare, in ambienti virtuali appositamente predisposti, tecniche di attacco alle infrastrutture, ai sistemi di autenticazione, dispostivi mobile, all'hardware.

Sono previste, per ciascun Master, 1575 ore di cui 368 di formazione in aula/laboratorio, 500 ore di training on the job e 700 di studio individuale. Gli studenti saranno selezionati tramite bando pubblico nei mesi di settembre/ottobre 2017. In particolare il master in Ethical Hacking sarà selezionato tramite una competizione "caputure the flag". Per maggiori informazioni sui master potete scriverci a info@gcsec.org . ■

1 https://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf

Intervista con Marianna Cicchiello, Distretto Cyber Security Cosenza, referente della mostra permanente *"Eroi e vittime dei social media".*

Marianna Cicchiello

autore: Laurent Chrzanovski

Laurent Chrzanovski: *Sig.ra Cicchiello, quali sono i messaggi principali di questa iniziativa?*

Marianna Cicchiello: Considerando che il contenuto principale della mostra illustra come nel corso dei millenni i social media siano sempre esistiti e sempre abbiano avuto il potere di esaltare o mettere in ombra la reputazione delle persone sulle quali si concentravano, in particolare parlando delle moderne tecnologie si pone l'attenzione sull'utilizzo consapevole di queste ultime in modo da non rischiare di venirne "travolti" diventandone una vittima. Un'iniziativa, oggi, rivolta ai giovani e giovanissimi, che aumenta il loro livello di consapevolezza e conoscenza e che gli permetta di trarre a pieno i vantaggi offerti dalla rete senza correre rischi.

Laurent Chrzanovski: *Avviare una campagna di sensibilizzazione sui pericoli della rete una mostra storico-culturale, come ha reagito il pubblico?*

Marianna Cicchiello: Le scolaresche che hanno visitato la mostra hanno avuto reazioni entusiastiche che hanno contagiato anche chi lavora sull'iniziativa. Moltissime le domande tecniche sui social media e la gestione della privacy, nonché un'alta attenzione alle tematiche di cyber bullismo. La mostra è un momento importante per fare prevenzione sui rischi e pericoli della rete con linguaggi semplici ma espliciti adatti a tutte le fasce di età. La presenza della Polizia Postale, che collabora con noi su questa iniziativa ha facilitato la condivisione di esperienze personali creando un dibattito costruttivo. Da maggio, apertura al pubblico della mostra, è partito un mese di lavoro intenso che ha visto 130 studenti e cinque scuole ospiti del Distretto Cyber Security di Cosenza. Dopo la pausa scolastica ricominceremo: sono già molte le richieste delle scuole che hanno chiesto di visitare la mostra.

BIO

Laureata in DAMS Multimediale presso l'Università della Calabria, Marianna Cicchiello lavora in Poste Italiane dal 2002 dove si è occupata di servizi amministrativi nell'area Posta, Comunicazione e Logistica che presidia l'area di business concernente i servizi postali, logistici e di comunicazione commerciale. Nel 2014 entra a fare parte del team del Distretto di Cybersecurity di Cosenza dove, con altri ricercatori, lavora al progetto di ricerca e sviluppo che attiene la protezione dell'utente finale. Oggi si occupa di alcune iniziative che riguardano i temi di sensibilizzazione e in particolare cura la mostra permanente "Eroi e vittime dei social media" in collaborazione con la Polizia Postale.

Laurent Chrzanovski: *Come si articola la collaborazione con la Polizia Postale?*

Marianna Cicchiello: La Polizia Postale collabora da sempre con Poste Italiane e ha aderito sin da subito a questa iniziativa. Il loro personale partecipa alle sessioni con gli studenti contribuendo a creare quel sodalizio proficuo necessario a instaurare una discussione con i ragazzi, sempre pronti a fare domande e osservazioni, alle quali i funzionari della Polizia rispondono con esempi pratici chiarendo i rischi possibili sulla rete, insegnando loro come difendersi e soprattutto prevenire.

Laurent Chrzanovski: *Blue Whale un caso anche italiano? Ne avete parlato con i ragazzi? C'è consapevolezza del fenomeno e quali sono i messaggi che portate all'attenzione delle scuole?*

Marianna Cicchiello: L'origine di questo gioco, se così lo possiamo chiamare, nasce on-line. Il fenomeno avrebbe origine in Russia e si è successivamente diffuso in America Latina per poi arrivare anche in Europa. Il "gioco" si articola in una serie di prove sempre più perverse a base di autolesionismo, così spinto che come conseguenza porta al suicidio i ragazzi.

In Italia viene dato risalto al fenomeno dai media attraverso il servizio del programma televisivo "Le Iene". Google Trends evidenzia come proprio dopo la messa in onda del servizio siano aumentate le ricerche in rete sul fenomeno. Il nostro contributo è stato quello di tenere, durante le visite, un dialogo sempre vivo su questo caso e sulla sicurezza della rete, cercando un confronto costruttivo con i ragazzi e provando a intercettare la loro opinione.

Laurent Chrzanovski: *Gli specialisti del CERT sono stati coinvolti in questa iniziativa?*

Marianna Cicchiello: I colleghi del CERT hanno collaborato attivamente al progetto; in special modo, sono stati coinvolti nell'ambito dell'esplicazione e dell'approfondimento delle tematiche toccate attraverso dei brevi video realizzati da Poste Italiane che hanno fatto da contorno alla mostra, rappresentando la possibilità di stimolare la curiosità degli studenti su argomenti precisi e consentendo così di spaziare e poter toccare gli aspetti più tecnici della cyber security.

Laurent Chrzanovski: *Sono previste altre iniziative a corollario della mostra?*

Marianna Cicchiello: Durante la mostra sono proiettati dei video su "Phishing" e "Mobile Security"; in questi video sono illustrate queste tematiche con parole semplici, dando istruzioni e accorgimenti necessari alla protezione dei propri dati in rete. Inoltre, la mostra fa parte di un più ampio programma di sensibilizzazione promosso da Poste Italiane nell'ambito del quale sono previste numerose altre iniziative anche dirette al personale interno. Tra queste spicca l'App CyberSecQuiz; con quest'applicazione è possibile mettere alla prova la propria conoscenza sulla sicurezza e scoprire quali sono i propri punti deboli, sui quali lavorare per accrescere la consapevolezza. Quest'applicazione verrà anche utilizzata all'interno dell'azienda per verificare la conoscenza di questi temi presso il personale di Poste Italiane e avviando in seguito campagne di formazione puntuali sull'argomento.

Lavori in corso, invece, su un'iniziativa in collaborazione con il Museo del Fumetto di Cosenza. Andremo nelle scuole a spiegare i temi di sicurezza sulla rete e chiederemo agli studenti di realizzare delle strisce sulla cyber security. Un modo di comunicare questi temi con uno strumento le cui origini risalgono al 1895 quando, sul New York Journal, appare per la prima volta un racconto comico in vignette dal titolo Yellow Kid.

Laurent Chrzanovski: *La trasformazione digitale di cui si parla richiede un ecosistema sicuro. Quale contributo da questa iniziativa?*

Marianna Cicchiello: I temi della sicurezza e della resilienza dei dati hanno un rilievo sempre maggiore nel quadro dello sviluppo dei servizi e delle infrastrutture digitali. La trasformazione digitale è una delle principali priorità di business per le aziende: la nuova sfida di chi opera nella sicurezza è di mettere le aziende nelle condizioni che permettano di sfruttare appieno i vantaggi di queste nuove tecnologie piuttosto che di bloccarle. La sicurezza informatica deve pertanto essere parte integrante della trasformazione digitale. La Pubblica Amministrazione e le aziende devono investire maggiormente in sicurezza, acquisendo le conoscenze necessarie a garantire un ecosistema digitale sicuro. La campagna di sensibilizzazione in corso pone l'accento sulla sicurezza, trattando questa come un abilitatore al digitale che avanza, contribuendo ad aumentare la conoscenza di questi strumenti ed un comportamento responsabile. ■

Security, vita privata, fiducia e... il cloud

autore: Eduard Bisceanu

I servizi associati al concetto del cloud esistono già dalla nascita di Internet; sono i nuovi modelli di business basati sul cloud che, invece, evolvono costantemente, venendo a trasformare nello stesso tempo i modelli classici di "IT Governance". Questa tendenza è più che un'evidenza se osserviamo le statistiche sulla crescita del mercato del cloud, abbinate all'evoluzione tanto rapida quanto complessa dei prodotti e dei servizi lanciati sul mercato dai grandi attori di questo settore.

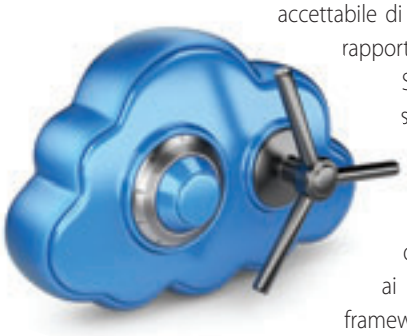
A fronte di un numero ridotto di mercati "maturi" in cui le evoluzioni di questo settore sembrano prevedibili e irreversibili, non sono poche le regioni, gli Stati oppure i settori di affari che si avvicinano ancora con timore alle soluzioni basate su infrastrutture pubbliche di cloud.

Il nostro obiettivo è quello di di passare brevemente in rassegna le principali problematiche legate al cloud che verranno fatte, poichè riteniamo che gli attori principali non possano più ignorare le evoluzioni del cloud computing e i costi implicitamente collegati.

- La stragrande maggioranza dei fornitori di prodotti e servizi dedicati al cloud basano la loro promozione sull'impatto significativo delle loro soluzioni a livello dei costi e sulla professionalità dei propri impiegati. Di norma, se prendiamo la prospettiva dei costi, è molto più efficace usare un'infrastruttura IT flessibile (hardware e software) basata sui bisogni reali di consumo di un'organizzazione, facilmente adattabile e immediatamente scalabile in base alla crescita di questi bisogni.

È altrettanto evidente che una compagnia leader di mercato, che vanta come profilo esclusivo di attività l'elaborazione di soluzioni IT utilizzate a livello globale, detiene tecnologie migliori di quelle della stragrande maggioranza delle aziende che non hanno l'IT come attività principale.

Ciò nonostante, bisogna tenere conto che vi sono settori di business che, per motivi estremamente pragmatici, non possono trasferire completamente i loro affari sul cloud, perché persino le soluzioni ibride non offrono ancora un livello accettabile di scalabilità e, non sono competititve nel rapporto qualità-prezzo.



Se riassumiamo quanto scritto sinora, siamo convinti che ogni venditore di cloud (qualsivoglia sia la sua configurazione), dovrebbe promuovere i suoi servizi utilizzando risorse che conoscono nel dettaglio non solo i settori economici ai quali intende rivolgersi, ma anche il framework finanziario e legislativo nel quale vivono i suoi potenziali clienti.

- Da molti anni leggiamo articoli, o ascoltiamo conferenze specifiche di settore più o meno aperte al grande pubblico, che sottolineano come i bisogni e le conseguenti esigenze di sicurezza siano considerate come un fattore vincolante per l'evoluzione del mercato del cloud. Crediamo che questo tipo di affermazioni non presenti di fatto la realtà.

Anzi, è proprio l'industria del cloud, e specialmente il suo ambito marketing e di integratori di soluzioni, che non si è ancora pienamente adattata alle esigenze di sicurezza o ad alcune condizioni specifiche che riguardano la protezione della vita privata online.

Se osserviamo la diversità e l'evoluzione permanente del mercato attuale del cloud, siamo convinti che non è la sicurezza e/o la protezione della privacy che bloccano il l'adozione del cloud in un'organizzazione, ma proprio la mancanza di comprensione da parte del mercato e della tecnologia. A questi bisogna aggiungere la mancanza di competenze per portare avanti un tale progetto; un mercato spesso immaturo e

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.

disattento ai bisogni locali, che non è quindi capace di generare un grado sufficiente di personalizzazione delle soluzioni proposte; ed infine un conservatorismo di molte mentalità dirigenziali. Tutti questi sono ostacoli che dovrebbero essere superati si da parte degli attori maggiori del mercato che da quella dei beneficiari, che si tratti indifferentemente di enti pubblici o di strutture private.

- Lato fornitori sarebbe opportuno concentrare gli sforzi per poter offrire quello che ricercano tutte le organizzazioni dal punto di vista della security e safety: la FIDUCIA, piuttosto che la risoluzione specifica di singole istanze di sicurezza o di protezione della privacy. Solitamente, in un'azienda non IT, quando il comitato dirigente fa la valutazione della fattibilità di un progetto, è alla ricerca, nel contratto, di argomenti solidi in particolare sui costi ma anche sulle garanzie necessarie per avere fiducia nella ditta e nel prodotto. Ci troviamo davanti ad un obiettivo molto più ampio di quello prettamente legato alla sicurezza delle operazioni che verranno esternalizzate sull'infrastruttura di un terzo.

Un contributo significativo alla valutazione dell'affidabilità di prodotti e servizi di un fornitore potrebbero essere *almeno* le risposte chiare alle seguenti domande:

- dove, esattamente, saranno archiviati i dati della mia organizzazione?

La presentazione di un'infrastruttura associata a servizi e prodotti di tipo cloud che verrebbe distribuita geograficamente a livello globale è certo una strategia di marketing mirata ad offrire un'immagine delle dimensioni impressionanti di una gestione di questo tipo, ma è insufficiente ad assicurare un grado adeguato di fiducia. Nella maggioranza delle presentazioni promosse dall'industria del cloud, viene affermato che l'epoca dei data-centers sta per finire, e questo proprio mentre tutti gli affari basati sul cloud non possono esistere senza un'infrastruttura robusta proprio di data center. La scalabilità di questa infrastruttura, la localizzazione dei data centers e le loro condizioni di sicurezza fisica sono dei fattori essenziali per contribuire alla fiducia di un cliente potenziale. Spesso il fattore geografico è parte degli obblighi legali, senza il rispetto dei quali una parte dei clienti potenziali dovrebbero, pur migrando sul cloud, continuare ad assumersi i costi ed i rischi legati alla gestione dei loro propri data center.

- Come sono misurabili la disponibilità e la ridondanza dei canali di comunicazione utilizzate dal cliente per accedere a questa infrastruttura e/o ai servizi di cloud? I piani di business continuity sono obbligatori in non pochi settori economici, e devono contenere risposte e soluzioni chiare su questo aspetto, che raramente viene considerato nel quadro delle strategie di marketing dell'industria del cloud.

- Quali sono le garanzie sulla sicurezza delle infrastrutture e delle applicazioni nel cloud? Troppo spesso, tali garanzie sono generiche: sono presentati dati statistici che dimostrano il livello scarso di incidenti di sicurezza, la professionalità degli specialisti in sicurezza del fornitore di cloud – senza tener conto che anche il cliente ha dei professionisti molto qualificati! L'esternalizzazione delle infrastrutture e di una parte dei servizi sul cloud trasferisce la responsabilità della loro amministrazione ad un terzo, e quindi il potenziale cliente ha bisogno di più dettagli e prove tangibili sulla sua professionalità, sicurezza e scalabilità del cloud. Vi è pure la possibilità che le autorità nazionali di regolamentazione o di controllo in questo campo di attività sollecitino in modo esplicito i dati riguardanti l'architettura di sicurezza delle infrastrutture esternalizzate per verificarne la conformità con le norme in vigore – ad oggi, sono rarissime le descrizioni di prodotti e supporti di tipo cloud nelle quali ritroviamo questo tipo di informazioni.

- Perché credete, ancora in merito all'uso del cloud, che i paesi più piccoli o quelli meno sviluppati economicamente non abbiano bisogno degli stessi approcci di quelli usati nei paesi dell'Europa Occidentale o negli Stati Uniti? Internet permette ormai l'accesso degli stessi fornitori per diverse zone del mondo, e le differenze vi saltano agli occhi. Per esempio, si possono osservare senza grandi sforzi le differenze di approccio del mercato associati alle analisi degli investimenti diretti nell'infrastruttura IT sul territorio degli Stati in questione. Certamente, le ditte specializzate nel cloud tengono conto delle opportunità e delle dimensioni di un mercato, ma è altrettanto possibile che molti clienti potenziali dei paesi dell'Est europeo abbiano esattamente lo stesso livello di pretese che quelli dell'Europa occidentale. Ignorare totalmente questa realtà in una strategia di affari è uno sbaglio che porta un danno significativo nell'acquisizione della fiducia del cliente.

- (Per i fornitori di sicurezza nel campo del cloud computing o delle infrastrutture di tipo cloud) A che tipologie esatte di dati si potrà avere accesso tramite l'infrastruttura locale del cliente e che dati saranno immessi in questa infrastruttura? Anche se i vantaggi dell'uso di un'infrastruttura complessa di tipo cloud, per l'analisi di dati risultanti da diversi tipi di incidenti e di attacchi cibernetici sono molteplici, sarebbe preoccupante se ci si dovesse addirittura proteggere dai propri partner. In poche parole, se non ci si conosce e non è stata ancora costituita una vera relazione di affari basata sulla fiducia, sarà difficile proporre una soluzione «automatizzata» basata sul cloud e che abbia un accesso esteso proprio all'infrastruttura che noi siamo pagati per difendere

- Qual è la comprensione comune e corretta del concetto di cloud ibrido? Anche se questo tema meriterebbe un ampio approccio concettuale e tecnico come preludio, esso è una soluzione potenziale per molti campi ancora inaccessibili per il mercato del cloud. Ora, dalle discussioni che abbiamo avuto con diversi fornitori, abbiamo potuto costatare che esistono ancora delle differenze significative sulla comprensione e i modelli di promozione e di implementazione di questo tipo di cloud. Anche se troppo spesso la sincerità viene sanzionata, direi a nome mio e di molti altri colleghi che il nostro sforzo per poter capire l'offerta di un potenziale fornitore dovrebbe essere minimo. ■

Evoluzione degli APT. Gli ultimi trend negli attacchi avanzati.

autore: Giampaolo Dedola
(Security Researcher - GReAT - Kaspersky Lab)

I dati relativi alle analisi da noi effettuate nei primi mesi del 2017 hanno confermato i trend relativi alle nuove evoluzioni delle minacce APT (Advanced Persistent Threat), ovvero quel tipo di attacchi avanzati, storicamente legati ad azioni sponsorizzate da governi, ma che sempre più spesso vengono utilizzate anche da cyber criminali che attaccano spinti da interessi economici.

In particolare durante il 2015 ed il 2016 sono state identificate diverse azioni ai danni d'istituti finanziari, vere e proprie rapine portate a segno attraverso attacchi APT aventi come obiettivo il furto di denaro tramite la compromissione della intranet aziendale e la modifica del normale comportamento dei sistemi informatici per la gestione delle transazioni quali, ad esempio, i server dedicati alla gestione del circuito SWIFT.

Attualmente stiamo monitorando più di 100 gruppi criminali specializzati in attacchi avanzati ed i dati in nostro possesso mostrano che le loro attività sono in costante aumento, gli attacchi sono sempre più specializzati e che gli aggressori continuano a migliorare costantemente i loro strumenti e le loro TTP (tattiche, tecniche e procedure). Per un criminale, uno degli obiettivi più importanti è il non farsi trovare, rimanere nascosto e talvolta complicare le analisi portando gli investigatori su false piste. Le ultime evoluzioni confermano l'importanza di questi obiettivi e mostrano come i cyber criminali tentino di raggiungerli attraverso l'utilizzo di sistemi anti analisi forense e l'utilizzo di tecniche di depistaggio.

Risulta sempre più frequente l'utilizzo di malware residenti in memoria, ovvero minacce informatiche che non utilizzano file presenti sul "file system", ma riescono a svolgere le loro attività lavorando nella sola RAM, aggirando molti sistemi di controllo. Inoltre la realizzazione di questi strumenti non necessità lunghe e costose attività di sviluppo in quanto, al giorno d'oggi, gli attaccanti possono sfruttare diversi framework pubblici, progettati per attività di "penetration testing" ed utilizzati solitamente per migliorare la sicurezza delle aziende. Alcuni di questi strumenti sono, ad esempio, Metasploit, Nishang, Powercat, Powersploit, etc. Alcuni di questi sono open-source, pubblici, altri sono software proprietari, ma hanno in comune la capacità di fornire, in pochi minuti, script in grado di mantenere il controllo di un sistema infetto, acquisire informazioni ed effettuare movimenti laterali.

Nonostante questa nuova tendenza presenti alcuni limiti, quali una maggior difficoltà nel mantenere la persistenza senza l'ausilio di una connessione remota, l'utilizzo degli strumenti sopracitati porta anche diversi vantaggi.

L'analisi forense tradizionale, basata sull'analisi del "file system", risulta molto più complessa data l'assenza di artefatti; l'evasione dagli strumenti di sicurezza quali gli anti-virus è più semplice e gli approcci di identificazione basati sull'utilizzo di IOC (indicatori di compromissione) tradizionali quali gli hash dei file, o basati su "application whitelisting", risultano molto meno efficaci. Inoltre gli attaccanti, spesso, utilizzano minacce "monouso" che vengono personalizzate in base alla

(Continua a pagina 48)

BIO

Giampaolo Dedola è un ricercatore del Global Research and Analysis Team (GReAT) della Kaspersky Lab. Prima di unirsi al GReAT ha lavorato nel SOC di Telecom Italia in qualità di principale analista malware e analista forense. Ha lavorato all'interno del team di Incident Response specializzandosi nella gestione di incidenti critici. Durante gli anni ha sviluppato competenze sulla gestione degli attacchi DDoS ed ha partecipato a esercitazioni di sicurezza quali "Cyber Italy" e "Cyber Europe". Precedentemente ha lavorato come analista di sicurezza nel gruppo Finmeccanica ed ha contribuito all'"Italian chapter" dell'organizzazione Honeynet Project in qualità di analista malware e sviluppatore.

Sicurezza IT, in Italia la paura è il cyberspionaggio

Ricerca Trend Micro sullo stato della cybersecurity. Nel 2016 il 79% delle aziende ha subito almeno un attacco, ma i ransomware fanno meno paura.

autore: Carla Targa

Senior Marketing and Communication Manager Trend Micro Italia

I responsabili IT temono di essere vittima di azioni di cyberspionaggio. Questo è quello che rivela l'ultima ricerca Trend Micro, leader globale nelle soluzioni di sicurezza informatica, che ha intervistato oltre 2.400 responsabili decisionali IT in Europa e Stati Uniti per fare luce sullo stato attuale della cybersecurity.

Le minacce che colpiscono le aziende italiane sono numerose e di diversa natura, il 79% degli intervistati ha affermato infatti di aver subito un attacco di notevoli dimensioni nel 2016, il 25% di aver subito più di 11 attacchi, mentre il 9% è stato attaccato più di 25 volte. Si tratta di percentuali di infezioni informatiche tra le più alte in Europa. La minaccia prevalente nel 2016 è stata il ransomware, con l'84% dei responsabili IT che ha dichiarato di essere stato infettato almeno una volta e il 31% di essere stato colpito cinque o più volte. Al secondo posto il phishing (22%) e a seguire altre tipologie di malware (20%), lo spionaggio informatico (20%), i "dipendenti canaglia" (20%) e la compromissione di account/identità (20%).

E per i prossimi 12 mesi? La minaccia più temuta dai responsabili IT è appunto il cyber spionaggio, per il 36% degli intervistati (percentuale più alta nel mondo). A seguire gli attacchi mirati (22%), quelli Business Email Compromise (11%) e i ransomware (7%) che sembrano intimorire meno rispetto l'anno passato.

I responsabili IT italiani fanno del loro meglio per proteggersi dalla crescente varietà e dal volume delle minacce, ma riconoscono che ci sono delle sfide da affrontare per avere successo nella lotta al cybercrime, come una mancanza di comprensione reale delle minacce (28%), le infrastrutture obsolete (28%) e la mancanza di innovazione da parte dei fornitori (27%). Anche le organizzazioni hanno poi i loro punti deboli. Quelli maggiormente citati dal campione sono le impostazioni di sicurezza obsolete (16%) e la sicurezza dei dispositivi non adeguata (15%), nel momento in cui il 91% dei responsabili IT italiani è convinta che smartphone, tablet, laptop e i dispositivi indossabili aumenteranno il livello delle minacce in futuro. Le soluzioni principali per far fronte alle minacce mobile sono la formazione dei dipendenti (32%), la containerizzazione dei software per separare attività personali e lavorative (30%) e misure di sicurezza obbligatorie (26%).

Al contrattacco con misure di sicurezza avanzate

L'87% degli intervistati comprende le sfide che la propria impresa deve affrontare per quanto riguarda il cyberspazio e tutto ciò che ruota attorno. In questo, gli Italiani sono secondi solo ai francesi in ambito europeo. I responsabili IT italiani sono attratti da strumenti di sicurezza avanzata come il

Metodologia e campione della ricerca

La ricerca è stata commissionata da Trend Micro e condotta dalla società Opinium nel mese di febbraio 2017.Sono stati intervistati 2.402 responsabili decisionali IT (ITDM) in Austria, Francia, Germania, Italia, Norvegia, Paesi Bassi, Regno Unito, Stati Uniti, Svezia e Svizzera. In Italia il campione è di 103 *decision makers* rappresentanti di organizzazioni operative su tutto il territorio e in vari settori, in ambito pubblico e privato.

BIO

Nata nel 1971 a Latina, Carla Targa si è laureata in Lettere presso l'Università degli Studi di Siena e ha un Master in "Relazioni Pubbliche Europee", conseguito presso l'Ateneo Impresa di Roma.
Con una carriera di oltre quindici anni in aziende prestigiose del settore Information & Communication Technology, Carla Targa vanta un'esperienza significativa nel mondo del digitale e delle tecnologie e una propensione forte all'innovazione, non solo tecnologica, che da sempre ha posto al centro della propria attività. Nel 2012 le è stato assegnato il secondo posto al premio "Donna Comunicazione Azienda". In Trend Micro dal giugno 2008, Carla ha la responsabilità dell'area Marketing & Communication definendo, coordinando e gestendo i programmi a supporto delle strategie di business e di vendita dell'azienda per tutti i segmenti di mercato di riferimento (consumer, small & medium business, large account) e delle politiche per i partner del canale distributivo. Prima di essere chiamata in Trend Micro, è stata, dal 2003 al 2008, Marketing & Communication Manager di Apple Computer Italia e nei tre anni precedenti Marketing & Communication Manager per la Southern Region di D-LINK. Vive a Milano, ha pubblicato saggi e articoli su temi di comunicazione e branding, nel tempo libero ama praticare numerosi sport come sci, windsurf, diving.

machine learning e l'analisi del comportamento. L'85% ritiene che questi tool siano efficaci per bloccare le minacce informatiche e più di tre quarti (77%) dichiara di utilizzarli già, mentre l'88% inizierà a farlo nei prossimi 12-18 mesi.

Il solo utilizzo della sicurezza avanzata nella lotta contro le minacce moderne non è sufficiente. La stragrande maggioranza degli intervistati (89%) preferisce impiegare più livelli di protezione, anche se questo approccio ha costi maggiori. Quasi un terzo (31%), ad esempio, ritiene che il *machine learning* è più efficace se integrato in una soluzione di questo tipo. Più della metà (63%) dichiara poi che un'unica soluzione integrata offerta da un solo fornitore ha più valore rispetto a un approccio che impiega i prodotti migliori del settore di diversi fornitori.

I dati globali

La maggioranza del campione (20%) indica che anche a livello mondiale è il cyberspionaggio la minaccia più temuta. A seguire gli attacchi mirati (17%) e il phishing (16%). Per quanto riguarda il cyberspionaggio è l'Italia il Paese dove è più temuto (36%), poi Francia (24%), Germania (20%) e Paesi Bassi (17%).

Le sfide maggiori da affrontare sono la crescente imprevedibilità dei cyber criminali (36%), l'assenza di comprensione delle minacce (29%) la fatica a tenere il passo con il panorama in rapida evoluzione e la crescente complessità dell'attività cybercriminale (26%).

Il 64% delle aziende su scala globale ha subito un attacco di grandi dimensioni negli ultimi 12 mesi e il ransomware è stato la tipologia di minaccia più comune, con il 69% degli intervistati che ha affermato di essere stato attaccato almeno una volta nel periodo esaminato. Anche a livello internazionale è interessante notare come solamente il 10% delle aziende ritenga che il ransomware costituirà una minaccia nel 2017. ■

Evoluzione degli APT. Gli ultimi trend negli attacchi avanzati.

(In seguito a pagina 46)

vittima e che quindi non forniscono dati utilizzabili per identificare altri attacchi.

Inoltre l'uso di strumenti pubblici rende molto più difficile l'identificazione dell'attaccante. L'attribuzione degli attacchi è uno dei compiti più complessi in quanto i criminali hanno tutti gli interessi a nascondere la propria identità e spendono molte energie per raggiungere questo obiettivo. Spesso gli autori di queste azioni sono spinti da motivazioni politiche, gli attacchi avanzati hanno un ruolo sempre più importante nelle relazioni internazionali e quindi gli attaccanti hanno ancora maggior interesse a fuorviare gli analisti. Il depistaggio viene attuato fornendo false informazioni per confondere le acque, vengono inseriti, all'interno dei codici malevoli, degli indizi sbagliati, dei "False Flag" che portano ad attribuire gli attacchi a soggetti terzi ed allontanare i sospetti dai reali autori.

L'evoluzione delle minacce porta gli addetti ai lavori della security davanti a nuove sfide sempre più complesse che per essere affrontate necessitano di tecnologie di difesa sempre più avanzate, di personale esperto e di collaborazione. Per affrontare questo tipo di minacce sarà sempre più importante il ruolo delle attività di "Incident Response" e della loro pianificazione. L'estrema volatilità delle informazioni presenti sulla memoria RAM necessità di tempi di intervento ancora più rapidi e di personale formato per gestire non solo analisi "tradizionali", ma anche analisi su memoria volatile.

Risulta fondamentale anche l'utilizzo di nuovi sistemi di sicurezza in grado di analizzare i dati presenti sulla RAM e di effettuare azioni di "pattern matching" con strumenti quali, ad esempio, Yara. Di particolare importanza anche l'utilizzo di soluzioni in grado di identificare anomalie non ancora note, comportamenti sospetti attraverso l'analisi comportamentale dei file e dei processi.

Infine, *last but not least,* lo scambio di informazioni e l'utilizzo di dati di intelligence è uno degli aspetti chiave per affrontare gli attacchi avanzati. I criminali cercheranno di migliorare sempre più le loro TTP, lasceranno sempre meno artefatti, evidenze e pertanto la condivisione dei dati e delle conoscenze con governi, forze dell'ordine e organizzazioni private e l'utilizzo di dati di intelligence avrà un ruolo fondamentale nella difesa dei sistemi informatici. ■

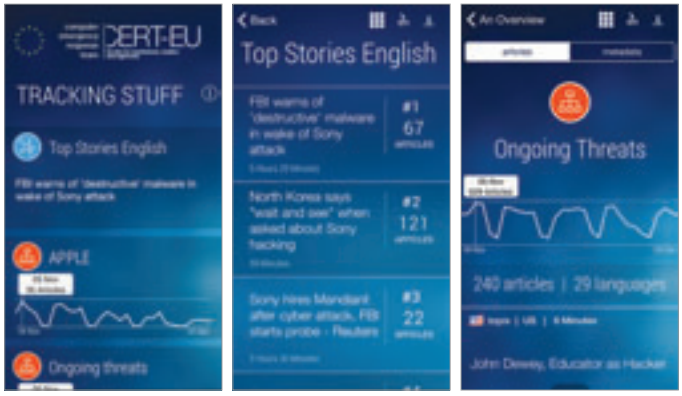
Proteggere i bambini on-line è una sfida globale che richiede un approccio globale. Mentre molti sforzi per migliorare la protezione online dei bambini sono già in corso, la loro portata finora è stata più di carattere nazionale che globale. L'ITU (Unione Internazionale delle Telecomunicazioni) ha avviato 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

Bibliografia - Cybersecurity Trends

App del CERT-EU



Il CERT-EU dell'Unione Europea ha dato prova di una straordinaria proattività, proponendo agli analisti ma anche a tutti i cittadini un'App disponibile per gli smartphone (Android e iPhone). Questa piattaforma è ergonomica, molto ben pensata e disponibile in ben 10 lingue. Di fatto, consta di un monitoraggio di migliaia di media online tramite tecnologie di ultima generazione che permettono di estrarre e classificare le notizie in categorie molto ben gerarchizzate, che spaziano dalle «top 20 news» del momento a sezioni dedicate a tematiche (con sotto-tematiche) più specifiche come ad esempio «Ongoing Threats»; «Strategic Threats»; «Cybercrime», Economic»; «Products Vulnerabilities»; «Malwares», ecc.

Questa App, permetterà ad ogni utilizzatore di proteggere rapidamente i suoi affari, la sua vita professionale e privata, le sue tools ed i suoi software tramite una semplice consultazione giornaliera delle ultime notizie che lo riguardano prioritizzate a seconda delle sue scelte.

https://cert.europa.eu/

Eric Diehl, *Ten Laws for Security*, Springer, Cham 2016

Eric Diehl, specialista francese trai i più noti crittografi al mondo, ci offre un vero capolavoro di interdisciplinarità e di buon senso. Per chi è già solito al suo stile, fluido e diretto, che ritroviamo in ogni "news" pubblicata sul suo blog (https://eric-diehl.com), è un vero piacere poter leggere un volume intero scritto di suo pugno. Destinato a diventare un'opera di riferimento tanto per i ricercatori, quanto per le istituzioni specializzate, il testo è strutturato attorno a dieci "leggi" introdotte e illustrate da esempi reali, per poi mettere a disposizione del lettore le diverse possibilità che gli sono offerte per risolvere le problematiche legate ad ognuna di esse, che riproduciamo qui per una migliore comprensione:

Law 1: Attackers Will Always Find Their Way
Law 2: Know the Assets to Protect
Law 3: No Security Through Obscurity
Law 4: Trust No One
Law 5: Si Vis Pacem, Para Bellum
Law 6: Security Is no Stronger Than Its Weakest Link
Law 7: You are the Weakest Link
Law 8: If You Watch the Internet, the Internet Is Watching You
Law 9: Quis Custodiet Ipsos Custodes?
Law 10: Security Is Not a Product, Security Is a Process

In questo libro, dove ogni "legge" meriterebbe una recensione individuale, abbiamo scelto di evidenziare tre elementi fondamentali. Il primo è che un sistema si giudica a partire dal suo anello più debole, cioè il fattore umano, e non da quello più performante – come potrebbe essere un firewall di ultima generazione. Il secondo, all'epoca delle nuove leggi sulla privacy, è che per quanto qualificati e professionisti siano i "guardiani del sistema" *(Custodes),* devono anch'essi essere sottomessi a una verifica e a un controllo costante da una parte terza, sia per evitare possibili abusi, sia per osservare un'eventuale perdita di performance dello specialista anno dopo anno. Diehl ha scelto per la fine l'argomento più importante, che potrebbe sembrare una banalità ma che purtroppo è tristemente presente e che ha conseguenze catastrofiche nella realtà proprio perché non viene compreso: la sicurezza non è, e non sarà mai, un "prodotto" ma un insieme di tecnologie e di uomini educati alla sicurezza in continua evoluzione per non essere sorpassati rapidamente dalle nuove soluzioni elaborate dai criminali che migliorano le loro tecniche di attacco giorno dopo giorno.

A.A.V.V., *Cybersecurity Futures 2020* (Center for Long-Term Cybersecurity, School of Information, University of California), Berkeley 2016.

Questo volume è come un thriller di fantascienza. I coordinatori dell'Università di Berkeley con team pluridisciplinari propongono 5 scenari di cyber security plausibili per i prossimi 3 anni. Testi e immagini sono pensati affinché il libro sembri pubblicato nel 2020 ma con lo sguardo indietro nel tempo. Impressiona subito l'altissima probabilità che molte delle ipotesi formulate in ogni scenario potrebbero realizzarsi se non adottiamo sin da oggi un atteggiamento più prudente e se non poniamo le basi di una vera educazione nel campo della sicurezza digitale.

Il primo scenario *"The new normal"* ci presenta una società che ha accettato sin dall'inizio il furto o la pubblicazione di tutte le informazioni personali. Gli attacchi diventano quindi sempre più mirati, gli hacker collaborano tra di loro a livello mondiale, mentre i legislatori e gli enti nazionali di sicurezza non riescono né a fare evolvere il corpus legale né a collaborare sistematicamente e proattivamente a livello internazionale. In queste condizioni, alcuni cittadini scelgono di vivere sconnessi, mentre altri scelgono di contrattaccare con gli stessi strumenti

usati dagli hacker. Il mondo digitale è ormai un vero "Wild West", dove chi vuole riparare a un torto subito deve procurarsi le risorse per farsi giustizia da solo.

Il secondo scenario, *"Omega"*, ci propone una società che è ridotta a una certa forma di schiavitù, sottomessa ad algoritmi e a tecnologie capaci di anticipare e manipolare il comportamento di ogni uomo connesso proprio quando inizia a intraprendere una certa azione o a prendere una certa decisione, sia nella sua vita privata sia in quella professionale. In questo caso gli specialisti in sicurezza sono surclassati dalle nuove minacce nelle quali le vulnerabilità dei sistemi e la prevedibilità delle azioni permettono agli hacker di prendere in mano i destini di centinaia di migliaia di cittadini, con danni economici e umani colossali.

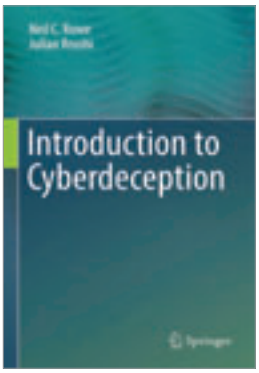
Il terzo scenario, *"Bubble 2.0"* prevede una nuova crisi dei titoli in borsa dei giganti del web dovuta alla caduta libera dei ricavi pubblicitari nel campo digitale. I criminali e le aziende superstiti sono in piena competizione per accaparrarsi i dati raccolti dalle compagnie che sono fallite. La "guerra dei dati", a questo punto, si svolge nelle peggiori circostanze possibili: stress e panico dei mercati, diritti di autore ambigui, settori economici opachi e "data trolls" che pullulano ovunque. In questo scenario, se i criminali e gli impiegati delle aziende, che lavorano con questa gigantesca mole di dati, iniziassero ad analizzarli e sfruttarli, il collasso dell'industria IT lascerebbe disoccupati centinaia di ricercatori.

Il quarto scenario *"Intentional Internet of Things"* suggerisce invece una rivoluzione sociale, dove gruppi di cittadini prendono il potere per far fronte ai problemi educativi, ecologici, sanitari, professionali e personali. Molti problemi che si credevano impossibili da affrontare – come i cambiamenti climatici o il miglioramento del sistema di sanità – sono quasi risolti. Invece, sono giunte agli estremi le tensioni tra i paesi ricchi, che sanno utilizzare questo "nuovo Internet", e quelli poveri, che non hanno accesso alle tecnologie di ultima generazione. Gli hacker trovano innumerevoli modalità per manipolare e mettere in pericolo i sistemi IoT, spesso senza che le loro azioni vengano scoperte. Siccome l'IoT è ormai dovunque, la "sicurezza cibernetica" è ridotta ormai ad una semplice "sicurezza della vita quotidiana".

L'ultimo scenario, chiamato *"Sensorium o l'Internet delle emozioni"* anticipa l'esistenza di strumenti portatili *(wearables)* che possano prendere il controllo degli stadi emotivi dell'utilizzatore tramite il monitoraggio a ogni istante del livello ormonale, del ritmo cardiaco, delle espressioni facciali, del tono della voce. Internet è diventato un sistema di lettura delle emozioni, raggiungendo gli aspetti più intimi della psicologia umana. I singoli individui possono essere seguiti e manipolati in funzione del loro umore e sia i criminali quanto gli Stati che riescono a penetrare nelle basi di dati emotivi ne approfittano in modo massiccio per esercitare ricatti su misura. La sicurezza cibernetica è completamente ripensata e ha come scopo la difesa dell'intera società mantenendo sicure le basi dei dati emotivi. Si tratta di proteggere l'immagine pubblica dei cittadini e l'intimità (o *privacy*) essendo diventata ormai emotiva.

https://cltc.berkeley.edu/scenarios/

Neil. C. Rowe, Julian Rrushi, *Introduction to Cyberdeception*, Springer, Cham 2016



Questo manuale è un pezzo raro, perché riesce, tramite uno stile molto chiaro e gradevole da leggere, a proporre un approccio a 360° della „deception", dal suo concetto fisiologico al suo utilizzo civile o militare, difensivo o offensivo. Le tematiche si susseguono con un chiaro filo conduttore, dai ritardi volontari ai falsi, dalle mimetizzazioni difensive alle false informazioni e, naturalmente, all'uso della „deception" come arma di difesa contro azioni di ingegneria sociale. Usando un'etica idonea, descritta in un intero capitolo dedicato, si possono costruire software di „deception" fino al livello di SCADA, cioè strumenti nuovi e molto meno costosi in paragone con gli schemi normali di difesa ai quali dovrebbero essere abbinati, implicando tecnologie di avanguardia. Non possiamo che applaudire la retrospettiva storica, troppo spesso esente dai libri di IT, che dimostra non solo l'antichità dei fenomeni della delusione, dell'intossicazione, delle bugie, ma anche il loro uso, sempre attuale ed efficace, contro i criminali. Gli autori propongono una serie di tecniche per misurare il successo della „deception" e per vedere quantitativamente come può essere migliorata. Presi dall'entusiasmo di una lettura così accattivante, ci metteremmo quasi a sognare che in un futuro prossimo, accanto al CIO, al CSO ed al CISO vi si troverà pure un Chief Deception Officer –anche se è certo che alcuni CIO eccellono già nell'uso della „deception", ma sono ancora pochi.

Steve Grobman, Allison Cerra, *The Second Economy. The Race for Trust, Treasure and Time in the Cybersecurity War,* Apress, New York 2016

"According to the Center for Strategic and International Studies, a Washington think tank, the estimated global costs of cybercrime and economic espionage are nearly $450 billion, placing cybercrime in similar company with drug trafficking in terms of economic harm.

Put another way, if cybercrime were a country, its GDP (gross domestic product) would rank in the top 30 of nations, exceeding the economies of Singapore, Hong Kong, and Austria, to name just a few." Con questa constatazione, il cui intento è di darci fin da subito una scossa, gli autori aprono una riflessione impressionante sulla drammatica situazione odierna; in ogni capitolo vengono narrate le radici storiche di tutte le forme di criminalità e di spionaggio per spiegarci meglio come siamo arrivati, pian piano, ad oggi.

Il libro è stato pensato per il grande pubblico, specialmente per i dirigenti, affinché questi possano capire la complessità

dell'ecosistema che hanno oggigiorno sotto la loro direzione e responsabilità. L'intenzione degli autori è anche di semplificare il modo di affrontare i tre elementi chiave di qualsiasi struttura: la fiducia, le finanze e soprattutto il fattore tempo, che è il peggior nemico di ogni vittima di reato informatico. Infatti, più un attacco di successo è breve e semplice, più diviene quasi impossibile da contrastare. Anche se un'azienda è ben difesa con tecnologie adeguate e personale idoneo e qualificato, può comunque essere soggetta ad attacchi in cui sono sfruttate le debolezze umane (ingegneria sociale, phishing, relazioni dubbie).

Il cinismo degli autori quasi ci obbliga a quell'onestà, che dovrebbero avere enti e aziende quando parlano di queste problematiche. Sottolineeremo in seguito alcune delle frasi-shock che evidenziano come il pragmatismo e la difesa proattiva di un'azienda non hanno nulla a che vedere né con le leggi, né con la morale.

Il primo assioma è riassunto in modo perfetto da una citazione del celebre giurista indiano B.R. Ambedkar: *"History shows that where ethics and economics come in conflict, victory is always with economics".* In due parole, o un'azienda è vincente perché è all'avanguardia in termini di tecniche di difesa, cioè ha integrato nella sua équipe sia *black hats* che *white hats* senza dimenticare il crisis *management response team* e quindi chiudendo gli occhi su alcuni aspetti etici, oppure a vincere saranno gli attaccanti, che non conoscono né pietà né morale. Con ironia, gli autori sottolineano che, da sempre, nel settore privato, il "chiudere un occhio" su alcuni aspetti etici conta molto nella ricetta del successo sul mercato globale e quindi voler essere "etici" quando si parla di difesa di fronte ad un attacco criminale è ben più un discorso propagandistico che un fattore reale.

Il secondo assioma, un'evidenza per chi non è molto "politically correct" ma che corrisponde perfettamente alla realtà, è che al di fuori di alcuni casi, attribuire la colpa di un attacco contro un'azienda privata a uno Stato non rileva soltanto dell'assurdo, ma rivela anche una tecnica di comunicazione che non può che far perdere tempo e portare "l'intox" così avanti che molti, tecnici inclusi, inizieranno a credere che è questa la verità. Le morfologie degli attacchi e i modus operandi osservati durante gli ultimi anni dimostrano bene quanto l'attribuzione certa di un attacco ad un'azienda privata è diventata pressoché impossibile, anche nel caso dove è possibile risalire e identificare in modo generico un gruppo di "black hats" noto per avere legami con uno Stato, ma che a sua volta agisce anche e spesso per conto proprio (o in "pay per service"), in primis per meri interessi economici.

Una citazione tra molte, che ci fa ben capire in che mondo viviamo, è tratta da una riflessione del poeta e filosofo inglese Gilbert K. Chesterton, che viene qui a parlare direttamente alle nostre élites dei settori pubblici e privati: *"It isn't that they can't see the solution. It is that they can't see the problem."* Molti aspetti ci ricordano che viviamo in una realtà sfuggita a ogni controllo per colpa della frenesia dell'innovazione, portando giorno dopo giorno i manager ad una più ampia incomprensione del sistema. Un parallelo scelto dagli autori è stupefacente. L'insieme dei compiti svolti dalla NASA per riuscire a portare Neil Armstrong e la sua équipe sulla luna si riassume a un programma che conta 145.000 linee di codici. Oggi, il semplice sistema operativo di uno smartphone di tipo Android (senza aggiunta di software, app, ecc.), riposa su più di 12 milioni di linee di codici.

Javier Parra-Arnau, Félix Gómez Mármol, David Rebollo-Monedero, Jordi Forné, *Shall I post this now? Optimized, delay-based privacy protection in social networks,* in Knowledge and Information Systems (Posted November 2016, in print), 33 pp.

Questo articolo, evidentemente matematico, si rivela però essenziale anche per i non addetti ai lavori. Infatti, se lasciamo da parte gli algoritmi che permettono a un utilizzatore esperto di creare i suoi propri metodi per disseminare contenuti sulle reti sociali durante l'intero arco di una giornata, un'attenta lettura delle prime e delle ultime pagine del testo ci dimostra l'interesse fondamentale di questo ragionamento e ciò indifferentemente dal metodo che useremo per metterlo in pratica. In particolare, impariamo leggendo qual è ormai l'impatto di un tale "ritardo volontario e scalato" dell'immissione dei nostri contenuti online nella nostra vita quotidiana.

© Parra-Arnau, Gómez Mármol, Rebollo-Monedero, Forné, Fig. 1

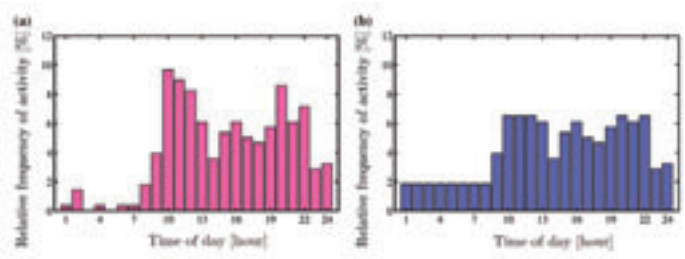
Gli autori hanno scelto di iniziare la loro ricerca elencando tutti i rischi che corriamo (per la sicurezza, la privacy ma anche per altri campi) usando le reti sociali in modo immediato e istintivo. Per fare ciò, illustrano il loro proposito con un caso di studio di grande impatto mediatico, basato su fatti reali.

Vi si racconta la storia di Isabella, una cittadina americana, giovane studentessa che ha appena terminato un master in giurisprudenza con risultati straordinari e che è stata chiamata da numerosi studi di avvocati per primo colloquio di lavoro. Ed è proprio qui l'inizio di una storia che per fortuna non si è conclusa in modo tragico. Il cognome della giovane è di origine araba, fattore questo che, nelle grandi città degli USA, non costituisce a *priori* un problema. Per di più, consapevole che potrebbe essere discriminata o attaccata per le sue origini o per la sua religione, Isabella si è sempre astenuta dal postare in rete sui suoi profili professionali messaggi di carattere politico o che svelino la sua vita personale, mentre svela molto di più le avventure del suo cagnolino che le sue in quelli privati. Ma c'è un problema. Durante gli ultimi anni, Isabella, musulmana moderata, ha utilizzato principalmente il momento del pranzo per postare informazioni online, ma solo durante un periodo specifico dell'anno, quello delle settimane del Ramadan. Ed è così che questo aspetto seppur banale, analizzato dalle tecnologie delle risorse umane degli studi legali che volevano ingaggiarla, ha fatto sì che quasi tutti i colloqui lavorativi degenerassero in domande scomode

sulla sua etnicità, con lo scopo evidente di saperne di più sulle sue convinzioni religiose. Per fortuna, la storia della brillante studentessa Isabella si conclude con l'assunzione in un grande studio.

Molti cittadini postano online sulle reti sociali, gli autori propongono di trovare un compromesso che, senza far perdere il piacere di usare questi canali, permetta sia di postare contenuti online "in diretta", sia di scegliere quelli da pubblicare in un secondo momento, con lo scopo di raggiungere una certa omogeneità giornaliera nelle statistiche della cronologia dei "post" usate dagli analisti dei big data.

Questo semplice sfasamento orario permette, secondo gli autori, non solo di aumentare la propria sicurezza personale, ma soprattutto di ridurre drasticamente la capacità delle aziende specializzate nell'estrazione dei dati con criteri cronologici. Ancora di più, se questa tecnica venisse adottata da un numero cospicuo di cittadini, renderebbe questo tipo di analisi completamente inutile.



© Profilo normale di un utilizzatore dei social media secondo le ore del giorno (in rosa) e stesso profilo dopo l'applicazione del metodo proposto (in blu). Parra-Arnau, Gómez Mármol, Rebollo-Monedero, Forné, Fig. 2.

Casey Inez Canfield, Baruch Fischhoff, Alex Davis, *Quantifying Phishing Susceptibility for Detection and Behavior Decisions*, in Human Factors: The Journal of the Human Factors and Ergonomics Society 58: 8 (December 2016), pp. 1158-1172

Questo articolo riassume una ricerca svolta nel 2015 su ben 162 persone volontarie, ma scelte in funzione del loro profilo socio-professionale per costituire un campione rappresentativo della componente umana di una compagnia di dimensioni medie. L'analisi è stata finanziata e approvata dall'Institutional Review Board della Carnegie Mellon University e la sua metodologia ha seguito passo dopo passo il codice etico dell'American Psychological Association, Code 196 of Ethics.

In questo caso non si tratta, come in altri studi nello sesso campo, di un esperimento svolto durante campagne di awareness del personale, che in genere consistono nel lanciare una campagna di phishing prima del corso e una seconda subito dopo, per misurare la comprensione del fenomeno e delle regole da seguire.

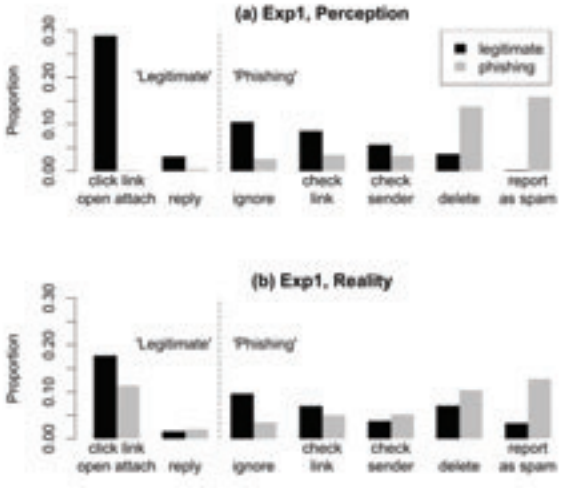
Si è trattato invece di una simulazione di una situazione reale, ottenendo un indicatore il più preciso possibile su quanto è ancora incompresa, nella pratica quotidiana, la teoria divulgata tramite campagne di awareness, proprio perché tutti i volontari del campione sono stati educati sul fenomeno, in adempimento delle norme aziendali in vigore negli USA per combattere i fenomeni di criminalità informatica, in primis quello del phishing.

I risultati sono più che preoccupanti. Prima di ricevere le mail da analizzare, tutti i partecipanti hanno ricevuto messaggi del tipo *"State in guardia, più della metà delle mail che riceverete saranno di tipo phising".*

Per di più, non sono stati trasmessi mail complicate, bensì mail con tutti i segnali che indicano che ci si trova davanti ad un tentativo di phishing, ovvero: (1) Saluto impersonale, (2) URL o indirizzi IP dubbi e mandati con nomi creati intenzionalmente per non ispirare fiducia 3) contenuti anomali in tutto quello che riguarda sia il destinatario che il "falso" mittente (4) domande di azione urgente, e infine (5) errori grammaticali ed ortografici.

Nel dettaglio, la percezione del phishing come elemento quasi "costitutivo" dell'inbox quotidiano è abbastanza buona: il campione dimostra di sapere che si trova di fronte a mail di phishing e che ha la possibilità di analizzarli o di distruggerli direttamente. Questo risulta dal primo esperimento, nel quale i partecipanti dovevano rispondere alle domande seguenti: (1) "è questa una mail di phishing?" (Si/No); (2) "Cosa farebbe se ricevesse questa mail?" (domanda con risposte a scelta multiple).

Al contempo però, quando i volontari si sono trovati realmente davanti a una mail dubbia, la fiducia in sé stessi sembrava essersi offuscata completamente nella maggioranza dei partecipanti e gli errori sono andati moltiplicandosi.



© Canfield, Fischhoff, Davis, Figura 3.

Le conclusioni, come si può osservare nel grafico soprastante, sono devastanti e siamo convinti che se si facesse un test identico su cittadini europei, dove la presa di coscienza sul rischio cyber è spesso inesistente, i risultati sarebbero ancora più catastrofici. Grazie a questo raro tipo di ricerca, che speriamo si ripeta spesso, avremo finalmente delle evidenze per convincere sia gli Enti statali che le aziende private, che è arrivato il momento di reagire per limitare i danni, soprattutto dopo gli ultimi due anni dove, in tutta Europa, vere e proprie ondate mensili di ransomware hanno raggiunto le vittime proprio tramite mail di phishing. ■

Le recensioni sono state eseguite da Laurent Chrzanovski e non esprimono necessariamente il punto di vista della rivista e dei suoi editori

Un pò di cyber-cultura in un mondo di cyber-intox

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

Le *"breaking news"* della stampa generalista degli ultimi mesi non hanno nulla di rassicurante: *"cyber-guerra", "attachi globali", "sistemi compromessi", "elezioni rubate 4.0"*… A priori, il primo effetto di questi titoli potrebbe essere proprio quello, nefasto, di smobilitare cittadini e imprenditori, dando loro l'impressione che l'individuo o l'azienda media non sia più una vittima potenziale, in un quadro dipinto dai media come una nuova e apocalittica *"Guerra stellare"*…

Proprio in contrasto a questi fenomeni possiamo citare due importanti pubblicazioni, disponibili da questa primavera.

L'indispensabile *Associated Press Stylebook,* nell'edizione 2017 ha cambiato la definizione della parola *"cyberattack"*, che verrà ormai usata solo per indicare eventi che portano ad una distruzione massiccia e di grandi dimensioni – sottolineeremo che il termine *"cyberwar"*, così caro a troppi giornalisti, governanti e militari, non è mai stato accettato nella terminologia accettata dallo *stylebook*. Tale cambiamento, che potrebbe sembrare banale, avrà conseguenze importantissime in uno stato come gli USA dove la giurisprudenza è, per definizione, evolutiva. Il sospetto di aver condotto un attacco è certamente l'accusa *"cyber"* più grave possibile; in questo senso, anche la giustizia americana e, per estensione, quella di quasi tutti i paesi che utilizzano la terminologia anglosassone nel campo digitale, dovranno adattarsi e stabilire con precisione, nei testi normativi, i vari gradi dei reati commessi.

All'attenzione dei governanti, dei militari e dei giuristi invece, è stato redatto il magistrale *"Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations"*, edito dalla Cambridge University Press, opera dei migliori esperti occidentali del settore, sostenuti dal *NATO Cooperative Cyber Defence Centre of Excellence*. I *"policy makers"* hanno così a disposizione una guida modernissima quanto capillare per distinguere i diversi gradi di un'azione illegale nel mondo virtuale, dalla breccia all'intrusione, dal phishing al malware, dallo spionaggio al sabotaggio per arrivare alle azioni, tanto rare quanto gravissime, dell'incidente grave ed *in finis* del cyber-attacco. Il volume viene a raddoppiare e ad affiancare le definizioni precise, a uso del settore privato, create e costantemente attualizzate, dal NIST[1] (National Institute of Standards and Technology).

L'impatto globale di *"WannaCry"* sembra essere stato la goccia che ha fatto traboccare il vaso, anche per l'audace presa di posizione del Presidente e Responsabile degli Affari Legali della Microsoft. Brad Smith ha finalmente detto chiaro e tondo quello che nessun governo aveva avuto il coraggio di esprimere prima. O scegliamo, a livello mondiale e in tutti i settori, di adottare delle regole comuni e di creare una cultura della cybersecurity, oppure continueremo ad andare a gonfie vele verso la nostra fine.

Molti, tra i quali ufficiali dell'FBI e rappresentati di grandi aziende di cyber security, ribadivano già da tempo che vi sono al mondo due tipi di aziende: quelle che sono state attaccate e quelle che verranno attaccate. Non hanno espresso ciò per incutere paura, ma per incentivare le aziende a investire e a collaborare tra di loro, proprio come proposto dal *Manifesto di Coordinated Vulnerability Disclosure* promosso dal GCSEC. C'è anche un sottointeso molto importante in questo "statement": non è vergognoso essere stati vittime di un attacco, dal momento che si è fatto di tutto, umanamente e tecnologicamente, per contrastarlo, per ridurre al minimo i danni e per gestire al meglio sia la crisi che il dopo-crisi. Ma per fare ciò, bisogna prima avere una vera cultura della sicurezza.

Volens nolens, quasi tutto si gioca ormai in – gran – parte nel mondo digitale. L'info, l'intox, i crimini come le azioni più nobili. E soprattutto, è proprio oggi che decidiamo il futuro che lasceremo in eredità alle nuove generazioni: al di sopra di un ecosistema collettivo ancora privo di una cultura di sicurezza necessaria, il Cloud, l'IoT e, pian piano, l'intelligenza artificiale stanno invadendo case, uffici, strade e governi. è diventato quindi, più urgentemente che mai, auto-educarsi per capire il nostro ecosistema e saperlo rendere sicuro; solo così potremo affrontare le sue mutazioni, viverci e lavorarci in un'atmosfera di prudente serenità e di fiducia. ■

1 https://www.nist.gov/cyberframework

CyberSecQuiz

CyberSecQuiz è la piattaforma di Poste Italiane che testa il livello di conoscenza sulla sicurezza informatica e consente di aumentare e "alimentare" regolarmente la consapevolezza della sicurezza delle informazioni su internet attraverso dei test.

La piattaforma è stata ideata come uno strumento ludico che presenta all'utente un test quiz a risposta multipla, di difficoltà variabile, riguardante operazioni comunemente effettuate online, raggruppate nelle seguenti categorie: Internet, Posta Elettronica, Sistemi di Pagamento Online, Social Network e Smartphone.

CyberSecQuiz può essere utilizzato da qualunque dispositivo (mobile o fisso) ed è dedicato a studenti, lavoratori, aziende, associazioni e Istituzioni. Il quiz è composto da domande a risposta multipla selezionate in ordine casuale. Ogni domanda presenta 4 risposte di cui due sbagliate, una corretta ed una perfetta.

Un algoritmo intelligente assegna le domande in funzione delle risposte dell'utente, in base a tre livelli di difficoltà basso, intermedio e alto. Il grado di difficoltà delle domande varia in base alle risposte; aumenta se l'utente risponde perfettamente, rimane uguale se risponde correttamente, diminuisce in caso di errore.

Alla fine del quiz, l'utente viene inserito in un ranking generale in cui può comprendere il proprio livello di conoscenza sia comparandolo agli altri, sia comparandolo al quiz effettuato precedentemente.

L'utente può accedere a CyberSecQuiz in maniera del tutto anonima, oppure tramite login (Email e Password), o, in alternativa, compilando il form di registrazione per ottenere delle credenziali di accesso.

Cimentati con CyberSecQuiz di Poste Italiane per valutare quanto navighi sicuro perché la sicurezza online inizia dalla consapevolezza dei rischi ! ■

Quanto ne sai di Sicurezza Informatica?
Fai un test su www.distrettocybersecurity.it/cybersecquiz/

Realizzata per essere esposta nel 2013 all'ITU (l'Unione Internazionale delle Telecomunicazioni), premiata dall'ITU e quindi tradotta ed esposta consecutivamente in 28 città di Romania, Polonia e Svizzera, la mostra è stata tradotta in italiano per le Poste Italiane, col patrocinio della Polizia Nazionale. E stata presentata in anteprima nel 2016 presso la "MakerFaire - European Edition" di Roma (dove ha superato i 130.000 visitatori). In 30 pannelli, l'esposizione illustra l'evoluzione delle tecniche di comunicazione e di manipolazione delle informazioni dai tempi più antichi ai social media usati oggi da tutti. Consente senza essere moralizzatrice di educare giovani ed adulti ad una fruizione consapevole e protetta di Internet.
La mostra è integralmente visitabile sul sito del Distretto di Cyber Security delle Poste Italiane, dove l'esposizione reale è allestita in modo permanente :
https://www.distrettocybersecurity.it/mostra-2/

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

UNIVERSITÀ DELLA CALABRIA

DIPARTIMENTO DI INGEGNERIA INFORMATICA, MODELLISTICA, ELETTRONICA E SISTEMISTICA

MASTER II LIVELLO

Ethical Hacking

Finalità: Il Master mira a formare esperti in grado di identificare, prevenire e contrastare le principali tipologie di attacco cyber che possono essere perpetrate a danno di organizzazioni pubbliche e private. Gli allievi impareranno a utilizzare in modo responsabile le tecniche di attacco e analizzare gli aspetti di sicurezza dal punto di vista dell'hacker al fine di elevare il livello di protezione e sicurezza delle organizzazioni. Potranno sperimentare, in ambienti virtuali appositamente predisposti, tecniche di attacco alle infrastrutture, ai sistemi di autenticazione, ai dispostivi mobile, all'hardware.

Requisiti: Laurea magistrale o specialistica nella classe Ingegneria Informatica o nella classe Scienze e Tecnologie Informatiche o nella classe Sicurezza Informatica, Ingegneria Elettronica, Ingegneria delle Telecomunicazioni, Ingegneria dell'Automazione, Ingegneria Gestionale, Ingegneria della Sicurezza, Scienze Statistiche Informatiche.

Obiettivi formativi: Il Master intende creare figure professionali in grado di:

- Padroneggiare le tecniche di attacco e gli strumenti utilizzati dagli hacker e i principali strumenti di cyber threat intelligence;
- Testare la rete e i sistemi con i metodi e le tecniche utilizzate dagli hacker, per verificare la presenza di vulnerabilità di sicurezza ;
- Identificare le migliori misure di sicurezza da mettere in atto per prevenire, intercettare e contrastare prontamente attacchi cyber.

Posteitaliane

NTT DATA FireEye

proofpoint. KASPERSKY

TS-WAY accenture High performance. Delivered.

ADS GROUP ALFA GROUP

QUOTA DI PARTECIPAZIONE
La quota di partecipazione al Master è di € 2000

DURATA
12 mesi

CREDITI
63 CFU

SCADENZA AMMISSIONI
Pubblicazione bando Settembre 2017

INIZIO LEZIONI
Novembre 2017

DIDATTICA
Venerdì pomeriggio (14-20) e Sabato mattina (8-14)

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