Cybersecurity Trends

Edizione italiana, N. 4 / 2017

- Nuovi modelli dinamici di protezione e simulazione

INTERVISTE VIP:

- Roberto CINGOLANI
- Stefano VENTURI

GLOBAL CYBER SECURITY CENTER

ISSN 2559 - 1797 / ISSN-L 2559 - 1797

Speciale Intelligenza Artificiale

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

Editoriale - Cybersecurity Trends

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,

Su questo numero troverete un nostro contributo sul tema dell'intelligenza artificiale. Non potevamo esimerci visto che anche lo scrittore Dan Brown nel suo ultimo libro mette l'intelligenza artificiale contro la religione. Origin, il titolo dell'ultima fatica di Dan Brown, propone una nuova pericolosa avventura che ha come protagonista il Prof. Robert Langdon ed un suo eccentrico ex allievo Edmond Kirsch; diventato milionario grazie a brevetti e invenzioni legate alle tecnologie più avanzate come le neuroscienze, la robotica, le nanotecnologie e l'intelligenza artificiale. Nel libro troviamo anche un altro protagonista, Winston un assistente che guida il Prof. Langdon attraverso il Guggenheim Museum. Ma Winston non è umano, è un assistente digitale che coniuga una tecnologia nel settore dell'intelligenza artificiale (IA) che si chiama Neural Language Processing (NLP). Tecnologie, quelle di IA, che promettono di rivoluzionare tutti i settori industriali garantendo efficienza e redditività alla nuova industria 4.0. I numeri stimano una crescita vertiginosa degli investimenti in questo settore e le grandi della rete stanno correndo ad acquisire startup e persone con competenze sull'intelligenza artificiale. In molte applicazioni di marketing i sistemi IA sono già utilizzati nella gestione della relazione con gli utenti, chatbot sempre più evoluti e basati su algoritmi di IA sono in grado di riconoscere il linguaggio naturale, capire le abitudini e i comportamenti dei clienti. Nell'area di Fraud Management sono ormai molte le piattaforme che utilizzano questa tecnologia per correlare dati in tempo reale e anticipare attività fraudolente. Potremmo continuare a elencare aree e soluzioni che ormai da tempo utilizzano IA e che cambieranno la nostra esperienza d'uso e le aziende così come le conosciamo. L'approccio dell'utente sarà simile alla chiacchierata del Prof. Langdon con Winston e l'industria 4.0 si allontanerà dalla staticità delle catene di produzione andando verso modelli più flessibili. Hardware e software più intelligenti, auto configuranti che possono prevedere problemi e lanciare azioni in modo da ridurre al minimo il rischio di arresto della produzione. Come potrete leggere nei nostri articoli, però la rincorsa tecnologica deve andare di pari passo con lo sviluppo di un ecosistema digitale sicuro. I vantaggi derivanti da innovazione e Industria 4.0 possono essere facilmente vanificati senza una strategia efficace in tema di CyberSecurity. Proprio mentre scrivo questo editoriale apprendiamo che Uber ha subito una violazione di dati che coinvolgerebbe 57 milioni utenti e sembrerebbe che abbia ha pagato 100.000$ per fare cancellare i dati trafugati nascondendo la violazione. Sempre in queste ore apprendiamo che Google traccia gli spostamenti degli utenti Android anche quando la funzionalità di localizzazione è spenta. La buona notizia? Da fine novembre il colosso di Mountain View dichiara di cessare questa pratica. Sicuramente ancora molto da fare su questo tema. ■

Buona lettura…

Indice

International Telecommunications Union,
ONU Ginevra

Raccomandazioni per proteggersi dai ransomware

autore: Cătălin Pătraşcu

CERT.RO

Da pochi anni, privati cittadini come aziende e strutture di ogni tipo si confrontano con una minaccia informatica conosciuta sotto il nome di "ransomware", che non è altro che un malware che ha come scopo di impedire alle vittime l'accesso ai loro files o addirittura all'intero sistemo informatico contaminato, finché esse non pagano una somma di denaro come riscatto ("ransom").

Così, il ransomware è diventato una delle forme più snervanti di malware, soprattutto perché può produrre danni o quanto meno dispiaceri presso quasi ogni tipo di utilizzatore. La maggioranza di noi possiede, archiviate sui nostri dispositivi – dai PC agli smartphone – almeno qualche fotografia alla quale tiene molto e per le quali siamo disposti a fare sforzi, anche finanziari, per poterle recuperare. Ed è esattamente su questa nostra 'debolezza' che si basano i criminali che si occupano della creazione e della distribuzione dei ransomware, un affare, secondo le statistiche internazionali, tra i più redditizi a livello di guadagni.

Di seguito, proponiamo una serie di misure e raccomandazioni per prevenire le infezioni da ransomware, ma anche per diminuire i danni nel caso di un'eventuale contaminazione. Queste misure sono riprese dalla guida elaborata da un collettivo di autori dei quali facciamo parte e che il Centro Nazionale di Risposta agli Incidenti di Sicurezza Cibernetica (CERT-RO) ha messo a disposizione per il pubblico rumeno (1).

BIO

Cătălin Pătraşcu è a capo del servizio di Sicurezza informatica e Monizorizzazione al CERT-RO. In questa funzione, a coordinato numerose attività di risposta ad incidenti cibernezici, ma anche proietti tecnici nonché esercizi cibernetici.

Misure di prevenzione

1 Essere cauti

Questa raccomandazione è basilare per aumentare la sicurezza dei sistemi informatici che utilizzate o amministrate. È ormai ben noto che l'utilizzatore rappresenta l'anello più debole dell'ecosistema della sicurezza informatica e perciò la maggioranza degli attacchi mirano a colpire la componente umana (social engineering, phishing, spear phishing, spam etc.). Vi raccomandiamo quindi di non accedere a dei link o a dei file allegati ricevuti tramite delle mail sospette prima di averne verificato sia il mittente che la sua legittimità. Un ragionamento simile deve essere posto sui siti web che visitate e sulle risorse online che utilizzate per scaricare o attualizzare le vostre applicazioni.

2 Eseguite copie di sicurezza dei vostri dati (backup)

Il metodo più efficace per combattere le minacce di tipo ransomware è la realizzazione periodica di backup per tutti i dati archiviati o processati dai vostri sistemi informatici. Così facendo, anche se l'accesso diretto ai dati vi viene bloccato da un ransomware, potrete rapidamente ripristinarli ed i danni provocati saranno minimi.

IMPORTANTE! Per il backup, usate un sistema di storage esterno che non sia connesso in permanenza al sistema e alla rete, perché esiste il rischio di essere colpiti da ransomware avanzati che criptano anche i file dell'intero ecosistema connesso, anche quello di archivio esterno.

3 Attivate le opzioni del tipo "System Restore"

Nel caso dei sistemi Windows, vi raccomandiamo di attivare le opzioni "System Restore" per tutte le componenti di archivio. Nel caso di un'infezione o di una compromissione di alcuni file (persino quelli del sistema) i dati

possono essere prontamente ripristinati riportando il sistema al suo stadio precedente.

ATTENZIONE! Non basatevi esclusivamente su questa possibilità, perché alcune varianti recenti di ransomware eliminano pure i dati dal "System Restore".

4 Implementate dei meccanismi del tipo "Application Whitelisting"

L' "Application Whitelisting" presuppone la messa in opera di un meccanismo che assicura il fatto che l'insieme del sistema informatico usi soltanto software autorizzati e conosciuti. Il concetto in sé non è nuovo, rappresentando in pratica un'estensione dell'approccio detto "default deny" (non permettere in modo implicito) che viene utilizzato da tempo dalle soluzioni di sicurezza del tipo firewall. Oggi, l'"Application Whitelisting" viene considerata come una delle strategie più importanti per combattere le minacce malware ed esiste una grande diversità di soluzioni tecniche che ci aiutano ad implementarla, anche se siamo semplici utilizzatori casalinghi, in particolare nel quadro dei sistemi Windows, dove la messa in opera può essere fatta tramite tools già incluse nel sistema operativo, quali **SRP (Software Restriction Policies), AppLocker** (che è raccomandata a cominciare dal sistema Windows 7 ed ha lo stesso scopo e uso che la SRP del Policy Group).

5 Disattivate dagli elenchi l'esecuzione di programmi come %AppData% oppure %Temp%

Una soluzione alternativa ai meccanismi di tipo "Application Whitelisting" (che però non è altrettanto efficace, ma aumenta comunque il livello di sicurezza) è di bloccare l'esecuzione di programmi da elenchi come **%AppData% e %Temp%**, grazie a delle misure di sicurezza esistenti (**GPO** – Group Policy Object) oppure utilizzando una soluzione del tipo **IPS** (Intrusion Prevention Software).

6 Rendete sempre visibili le estensioni dei file

Molti tipi di ransomware sono consegnati sotto la forma di file con un'estensione nota (.doc, .docx, .xls, .xlsx, .txt etc.) alla quale viene aggiunta l'estensione ".exe", caratteristica dei file **eseguibili** – si ottengono così delle estensioni di tipo ".docx.exe", ".txt.exe" ecc. La visibilità delle estensioni facilita grandemente l'individuazione di file sospetti o pericolosi. Rimane comunque raccomandato di non aprire mai dei file **eseguibili** ricevuti tramite mail.

7 Attualizzate in permanenza i sistemi operativi e le applicazioni

L'attualizzazione delle applicazioni e dei programmi utilizzati è una misura obbligatoria per assicurare un livello di sicurezza adeguato al proprio sistema informatico. Nella maggioranza dei casi, un software non attualizzato è l'equivalente di una porta aperta (backdoor) per i cyber-criminali. In generale, i produttori di software pubblicano in modo regolare attualizzazioni (update) per i sistemi operativi e le applicazioni, l'utilizzatore avendo la possibilità di scegliere il download e l'installazione automatica delle attualizzazioni. Vi raccomandiamo quindi di attivare l'opzione di attualizzazione automatica laddove è possibile e di sapere quali sono le modalità più efficaci per attualizzare tutti gli altri programmi (verificare periodicamente le ultime versioni proposte sul sito del produttore).

ATTENZIONE! Spesso, i programmi di tipo malware si spacciano come degli update dei software: verificate con attenzione su quale sito vi è proposto il download e l'attualizzazione del software.

8 Utilizzate soluzioni di sicurezza efficaci ed attualizzate

Una misura assolutamente necessaria per premunirsi dai malware è l'uso di una o più soluzioni di sicurezza – sofwtare – efficienti, attualizzate e che siano dotate delle facilità seguenti: antivirus, antimalware, antispyware, antispam, firewall ecc. Recentemente, non pochi prodotti antimalware propongono anche una protezione dedicata anti-ransomware.

9 Utilizzate software per monitorare i vostri file

L'uso di software per monitorare i file (accesso, modifica, eliminazione ecc.) aiuterà ad osservare rapidamente comportamenti sospetti del sistema informatico o della rete.

10 Siate sempre attenti se accedete alle pubblicità del web (ads)

Alcune delle più recenti versioni di ransomware sono state iniettate tramite pubblicità malevoli (malvertising) che figuravano su siti web molto popolari (notizie, negozi online etc.). Vi raccomandiamo di evitare quanto possibile di accedere a queste pubblicità e meglio, utilizzare software del tipo "add block" che vengono a bloccare la visibilità della pubblicità o l'apparizione di una pagina in modo automatico.

Misure di eradicazione e di limitazione degli effetti

1 Sconnessione dei mezzi di archivio esterni

Sconnettete urgentemente tutti i mezzi esterni connessi al PC (chiavetta USB, memory card, hard drive esterno etc.), sconnettete il cavo della rete / disattivate tutte le connessioni alla rete (WiFi, 3G, 4G ecc.). Potrete così prevenire l'infezione di file archiviati sui mezzi esterni così come quelli accessibili online (network share, cloud storage ecc).

2 [Opzionale]. Realizzate una cattura di memoria (RAM)

Se si desidera un'investigazione ulteriore dell'incidente ed eventualmente rimuovere dalla memoria le chiavi di criptaggio utilizzate dal ransomware, realizzate al più presto una cattura di memoria (RAM), prima di spegnere il PC, utilizzando una soluzione specializzata.

ATTENZIONE! Esiste il rischio che sino alla fine del processo di realizzazione della cattura di memoria

vengano infettati (e criptati) ancora più file – in alcuni casi il malware può raggiungere la totalità del contenuto. La decisione di spegnere subito il PC o di effettuare prima una cattura di memoria deve essere presa in funzione delle priorità: è più importante salvare i dati o avere la possibilità di effettuare indagini ulteriori. Per esempio, se avete un backup di tutti i dati archiviati sul PC o i file che contiene non sono importanti, si può prendere la decisione di realizzare la cattura della memoria.

3 Spegnete il PC (Shutdown)

Se sospettate che un PC è stato contaminato da un ransomware e decidete di non fare una cattura di memoria, vi raccomandiamo di spegnere immediatamente il PC per limitare al massimo il numero di file criptati dal malware.

4 [Opzionale] Realizzate una copia (immagine) dell'HDD

Nel caso in cui si desidera un'ulteriore investigazione dell'incidente e l'eventuale recupero di una parte dei file con strumenti del tipo "Data Recovery", realizzate una copia tip "bit per bit" (immagine) dell'hard-disk infettato dal malware, utilizzando un software speciale.

5 Realizzate un back-up "offline" dei file

Accendete il PC (boot) usando un sistema operativo che si carica da uno storage esterno (CD, DVD, chiave USB ecc.), come permettono la maggioranza dei PC moderni, in particolar modo se usano il sistema linux. Copiate su un altro supporto di archivio tutti i file dei quali avete bisogno, includendo quelli compromessi (criptati).

6 Restaurate i file compromessi

Il metodo più rapido di ricuperare i file contaminati da ransomware è di restaurarli da una copia di sicurezza (backup). Se non avete una tale copia, vi raccomandiamo di cercare di recuperare i file tramite "System Restore" oppure usando software specializzati per il recupero di dati (del tipo "Data Recovery").

ATTENZIONE! Vi raccomandiamo di cercare di recuperare i dati con software del tipo "Data Recovery" conformemente alle immagini (copie) dell'HDD (realizzate secondo il punto 4), altrimenti si corre il rischio di compromettere le possibilità di successo di una procedura più complessa, che presuppone il recupero dei dati direttamente dagli storage. Esistono soluzioni per cercare di recuperare i dati direttamente dai mezzi di storage, ma richiedono un livello elevato di expertise e delle dotazioni tecniche specifiche.

7 Disinfettate i sistemi informatici contaminati

Il metodo più sicuro col quale potete assicurarvi che il sistema informatico non contiene più nessun malware (o parti di malware) è di re-installare completamente il sistema operativo, tramite la formattazione di tutti gli HDD/ed *in primis* delle loro componenti. Nel caso in cui questo non fosse possibile (per esempio se si vogliono recuperare i dati direttamente dall'HDD contaminato), vi raccomandiamo di utilizzare una o più soluzioni di sicurezza del tipo antivirus/antimalware/antispyware per scansionare il sistema e poi disinfettarlo.

ATTENZIONE! Nel caso in cui desiderate cercare di recuperare i dati dagli HDD contaminati, come detto al punto 6, vi raccomandiamo di non provare a disinfettarli bensì di usare altri HDD per re-installare il sistema operativo.

In ultima istanza, se i vostri file sono stati compromessi e nessun tentativo di recuperarli ha avuto successo, dovete rimanere molto prudenti sulla possibilità di riscattarli pagando la somma richiesta nel messaggio del ransomware. Quest'accettazione non solo incoraggia i criminali che si occupano di questo business, ma soprattutto non vi da nessuna garanzia reale che recupererete i dati dopo aver pagato, anzi, molte statistiche dimostrano la crescita del numero di criminali che incassano somme di denaro senza poi mandare nessuna chiave di decriptaggio. ■

Bibliografia

[1]. https://www.us-cert.gov/ncas/alerts/TA14-295A

[2]. http://www.symantec.com/connect/blogs/ransomware-how-stay-safe

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

Infrastrutture Critiche Finanziarie. Nuovi modelli dinamici di protezione e simulazione.

Autore : Francesco Corona

1.0 Infrastruttura Critica Finanziaria (FCI)

Il termine «Infrastruttura Critica Finanziaria (FCI)» si riferisce ad un gruppo di assets istituzionali e di corporate del mercato finanziario interconnessi su reti di comunicazione *wireless e/o wireline* che sono di vitale importanza per i sistemi europei di pagamento e di negoziazione dei titoli. Ricordiamo che la recente normativa europea di riferimento è del luglio 2016 ed

afferisce alla Direttiva comunitaria 1148 per la sicurezza delle reti e dell'informazione, nota anche come Direttiva NIS (Network and Information Security), che stabilisce i requisiti minimi per la sicurezza informatica per gli operatori di servizi essenziali e servizi digitali incluse le banche. I quattro servizi e processi che sono considerati critici dalla comunità di esperti europei per il settore finanziario sono:

- **Pagamenti da punto vendita (POS)**
- **Pagamenti a distanza**
- **Trasferimenti interbancari di alti valori monetari**
- **Operazioni su titoli**

L'ultima normativa europea di prossima introduzione relativa alle transazioni economiche (PSD2), prevista per gennaio 2018, imporrà inoltre scenari economici evolutivi non più basati sull'attuale modello di fiducia tra clienti e banche ma su logiche del consenso nelle quali vedremo nuovi soggetti intermediari delle transazioni. I soggetti facenti parte di una catena di valore economico (transazione) saranno proprietari di un blocco di informazioni con le proprie chiavi di accesso. Pertanto una transazione economica andata a buon fine, sarà composta da differenti blocchi di proprietà del soggetto bancario che disporrà dei consensi e quindi delle chiavi di accesso di tutti i singoli soggetti.

Questi modelli detti block-chain hanno già dimostrato una loro intrinseca robustezza con pagamenti basati su moneta elettronica bitcoin ma appena introdotti nel sistema euro aumenteranno di certo le preoccupazioni dei security manager nella definizione ed implementazione di apposite infrastrutture di gestione e contromisure idonee che a questo punto necessiteranno sempre più di sistemi dinamici di analisi semantica delle minacce ed allertamento preventivo, oltre a sistemi di simulazione in grado di studiare fenomeni di propagazione degli effetti di attacchi sulle infrastrutture correlate. Di seguito analizzeremo i quattro processi giudicati critici del settore finanziario e le nuove strategie di Threat Intelligence dinamica e modelli di simulazione applicati al settore delle Infrastrutture Critiche Finanziarie.

1.1 Pagamenti da punto vendita

I pagamenti in contanti ed elettronici da punti vendita (POS) includono quelli che utilizzano banconote e monete e quelli che utilizzano carte

BIO

Francesco Corona è docente e direttore del master di Hacking ed Ingegneria della Sicurezza presso Link Campus University Rome, già docente a contratto presso la Facoltà di ingegneria gestionale di Roma2 Tor Vergata Dipartimento di Ingegneria dell'Impresa. Ha svolto intensa attività di ricerca in ambito MIUR ed attività professionale d'impresa nel settore della sicurezza per conto di primari player nazionali ed internazionali. Nel 2013 consegue il prestigioso Premio Nazionale per l'innovazione e il premio ICT Confindustria. f.corona@unilink.it

di debito e di credito. Sono inclusi anche i prelievi in contanti da ATM. I consumatori si basano su pagamenti agevolati in luoghi come negozi, luoghi di intrattenimento e stazioni di servizio. Se i pagamenti POS dovessero bloccarsi in tutto o in parte, potrebbe verificarsi un enorme disagio sociale dovuto al ritardo o all'arresto dei pagamenti. I pagamenti con carta di debito sono il principale mezzo di pagamento nei negozi e i disservizi possono avere un impatto importante sia sui consumatori che sui rivenditori. I cosiddetti Webstores, che sono "rivenditori virtuali", ricevono la maggior parte dei loro pagamenti tramite operazioni bancarie online, con i consumatori che utilizzano la loro carta di credito o diversi sistemi di commercio elettronico e saranno a breve coinvolti nella nuove dinamiche che la normativa europea PSD2 trascinerà con se.

1.2 Pagamenti a distanza

I pagamenti remoti gestiti dal settore finanziario comprendono i pagamenti dei creditori (trasferimenti di crediti tramite operazioni bancarie online e trasferimenti di pagamento), strumenti di riscossione (addebiti diretti) e pagamenti ricorrenti, quali stipendi, prestazioni sociali e pensioni. Se il sistema di gestione dei pagamenti con copertura di massa dovesse collassare, in uno scenario più che concreto si potrebbero provocare rivolte sociali di portata globale. Un esempio per tutti può essere l'eventuale mancato pagamento prolungato nel tempo di stipendi e pensioni e quindi l'indisponibilità prolungata dei servizi connessi.

1.3 Trasferimenti interbancari di alti valori monetari

I trasferimenti interbancari di alti valori monetari sono pagamenti tra banche e altre istituzioni del capitale e del mercato monetario, compresi i trasferimenti di tesoreria delle grandi società e la liquidazione di operazioni di cambio e di compravendita di oro. Le transazioni sono tipicamente poche, ma coinvolgono grandi quantità monetarie, banche centrali e corretta gestione delle valute. Mentre una ripartizione dei trasferimenti interbancari o delle operazioni su titoli di valore elevato è meno probabile che provochi squilibri sociali, le perdite finanziarie dovute ad attacchi cyber, crack finanziari, speculazioni internazionali, possono essere sostanziali nei rapporti di stabilità sociale a causa delle grandi perdite che ne deriverebbero. Alla fine, le perdite potranno anche essere intangibili, ma si manifesteranno come perdita di fiducia nel settore finanziario o in una parte di esso. Ciò potrebbe anche avere conseguenze economiche a medio e lungo termine come avvenne nella crisi dei subprime statunitensi [B008].

1.4 Operazioni su titoli

Le operazioni in titoli comprendono la negoziazione, la compensazione e la liquidazione regolamentata di titoli e derivati. La prolungata ripartizione delle operazioni in titoli può causare notevoli perdite finanziarie ed economiche per gli investitori. Se invece una piattaforma di trading diventa improvvisamente non disponibile, il mancato trading potrebbe ingenerare effetti collaterali globali su intere nazioni.

1.5 Impatto dei disservizi bancari e rischi associati

Sulla base delle considerazioni precedentemente esposte, la tabella seguente fornisce una sintesi dell'impatto indotto nel collasso di servizi finanziari e nei processi critici associati nel caso di brevi disservizi o disservizi prolungati:

Impatto della indisponibilità di servizi critici nel settore finanziario		
Asset	Brevi interruzioni	Disservizio prolungato
POS	· Perdite finanziarie ed economiche · Effetti a cascata limitati · Lieve interruzione	· Problematiche sociali · Perdite finanziarie ed economiche sostanziali · Effetti a cascata limitati · Perdita di fiducia nel settore finanziario
Pagamenti Remoti	· Lieve interruzione · Perdite finanziarie ed economiche · Effetti a cascata limitati	· Problematiche sociali · Perdite finanziarie ed economiche sostanziali · Perdita la fiducia nel settore finanziario
Trasferimenti interbancari di alti valori monetari	· Significative perdite finanziarie ed economiche · Rischi sistemici	· Perdite finanziarie ed economiche sostanziali · Rischi sistemici · Perdita di fiducia nel settore finanziario
Securities trading	· Perdite finanziarie ed economiche · Rischi sistemici	· Perdite finanziarie ed economiche sostanziali · Rischio sistemico · Perdita di fiducia nel settore finanziario

Tabella 1: Impatto della caduta di servizi e processi critici nel settore finanziario

A questo punto è fondamentale identificare i rischi generali e sistemici per le infrastrutture critiche del settore finanziario e fornire una guida nella classificazione di queste cause e le necessarie contromisure. Nella tabella successive una sintesi di questi importanti aspetti da non sottovalutare:

Soggetti danneggiati	Cause di disservizio	Contromisure prese o da prendere
• **Enti governativi** • **Persone fisiche** • **Sistemi IT** • **Comunicazioni** • **Edifici** • **Azionisti** • **Fornitori**	• **Catastrofi naturali** (ad esempio incendi, terremoti, inondazioni) • **Malfunzionamento tecnico** (ad esempio interruzioni hardware o software, interruzione di corrente) • **Attacchi Cyber** • **Errori organizzativi** (ad esempio errore umano, malattia) • **Minacce intenzionali** (attacchi terroristici)	• **Misure preventive** • **Misure investigative** • **Misure correttive** • **Misure di risposta**

Tabella 2: Minacce nel settore finanziario

Come possiamo osservare, le cause di disservizio coinvolgono differenti soggetti e possono essere dirette o indirette. Un esempio di quest'ultime è l'inaccessibilità di un edificio a causa di un incendio nelle vicinanze, il che significa che la causa non è all'interno dell'edificio stesso. Altre cause possono presentarsi in diverse categorie di rischio, come un corto circuito (guasto tecnico) o una esplosione da atto terroristico (minaccia terroristica intenzionale). Le classificazioni servono quindi solo come guida, piuttosto che come struttura rigida. Considerando le forti interdipendenze del settore finanziario con strutture finanziarie interne e strutture esterne anche gli effetti secondari devono essere presi in considerazione in modo serio. In altre parole, gli effetti causati da una catastrofe con la scarsissima disponibilità di infrastrutture critiche (per esempio nel settore delle comunicazioni) avrà effetti a cascata che potranno produrre interruzioni nel settore finanziario creando nuovi scenari che ha senso prevedere in fase di allertamento preventivo della minaccia stessa.

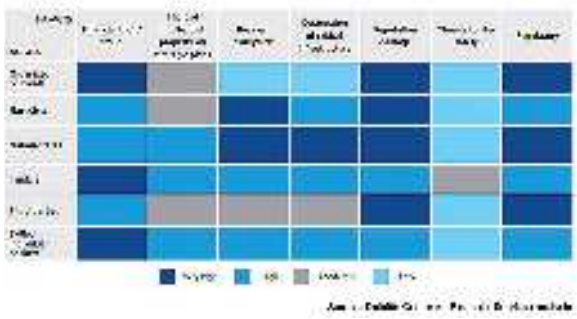


Fig. 1 – Cross Reference Attori – Impatti su attacchi Cyber - Fonte Deloitte

In questa cross reference di Deloitte Center per i Servizi Finanziari un attacco distruttivo alle infrastrutture critiche finanziarie avrebbe un coinvolgimento **Very high** sugli stessi stati nazionali che ospitano le infrastrutture attaccate.

2.0 Infrastrutture Critiche Finanziarie e Cybersecurity

Dal punto di vista "Cyber" queste criticità intrinseche alle Infrastrutture Critiche Finanziarie impongono due azioni distinte in linea con le recenti disposizioni europee e con le direttive ENISA:

- **Utilizzo di sistemi dinamici di allertamento preventivo ed analisi semantica della minaccia** onde meglio rispondere ad attacchi cyber improvvisi e repentini. In buona sostanza si considera sempre tecnologia SIEM (Security Information and Event Management) come base di supporto alla tracciabilità delle minacce ma a questo punto integrabile via API con sensoristica periferica presente su network elements di nuova generazione basati su tecnologia proprietarie come ad esempio STIX (Structure Threat Information eXpression) e Taxii (Trusted Automated Exchange of Intelligence Information) e tuttavia nuove tecnologie OpenThreat che saranno sempre più presenti sul mercato della sicurezza.
- **Utilizzo di sistemi di simulazione e modelli di propagazione degli effetti** e ripercussioni su infrastrutture critiche finanziarie.

2.1 Sistemi dinamici di allertamento preventivo ed analisi semantica della minaccia

Un sistema di allarme rapido distribuito gerarchicamente va pensato come parte sensoristica integrata con le piattaforme di Security Information and Event Management (SIEM) e le infrastrutture di Cyber Security Operations Center (CSOC). Il sistema acquisisce informazioni dai sensori sulle reti degli utenti finali, anonimizza i dati (privacy by design) e trasmette le informazioni a un "nodo di elaborazione" dove, utilizzando algoritmi come moduli probabilistici, grafici di minacce semantiche ed analisi di sicurezza predittiva determina la probabilità di attacchi in corso. In questo modo un gruppo di informazioni è derivato da questi sistemi Distributed Hierarchical Early Warning e condiviso con altre organizzazioni e strutture CERT.

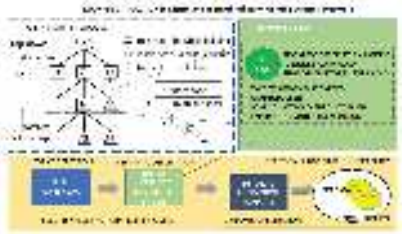
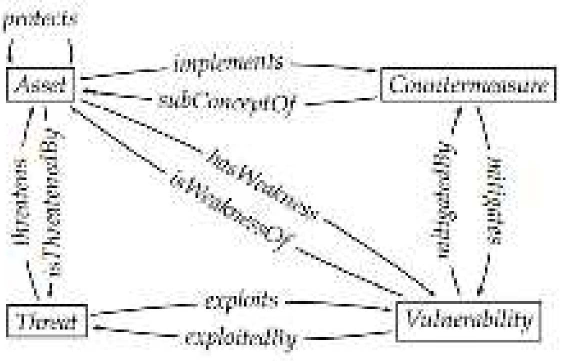


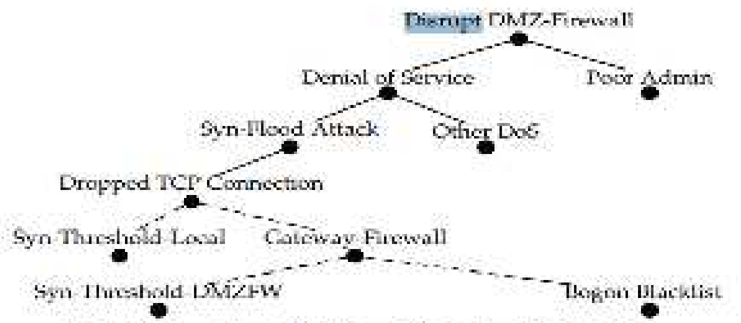
Fig.2 – Schema di reazione dinamica ad un attacco cyber utilizzando sistemi di distribuzione gerarchica di allertamento preventivo



Abstract Semantic Threat Graph Model.

Le minacce vengono quindi rilevate sui nodi gerarchici occupati dai network elements della architettura di rete come ad esempio un DMZ Firewall o un Gateway Firewall che implementano specifiche di direttive come la NIST-800-41 pertanto forniscono le contromisure da adottare in tempo reale. Nell'esempio un albero gerarchico di un attacco Syn-FloodDoS. Fig. 3 [B007].

Il metodo di protezione dinamica proposto consente di disporre delle giuste contromisure necessarie, assicurando che il problema si risolva in modo efficace e riduca in modo significativo i costi. Ad esempio, nella Fig.2 la protezione dei dati può essere effettuata con sistemi dinamici di crittografia dei dati e di mascheramento dopo che il sistema Distributed Hieralchical Early Warning ha commutato il descrittore semantico al nodo che gli appartiene. Tutto il layer di informazioni semantiche condivise può a sua volta essere gestito con meccanismi di crittografia e di gestione della sicurezza dei dati.



(b) Partial Threat Tree: DMZ Firewall Syn-Flood DoS Attack.

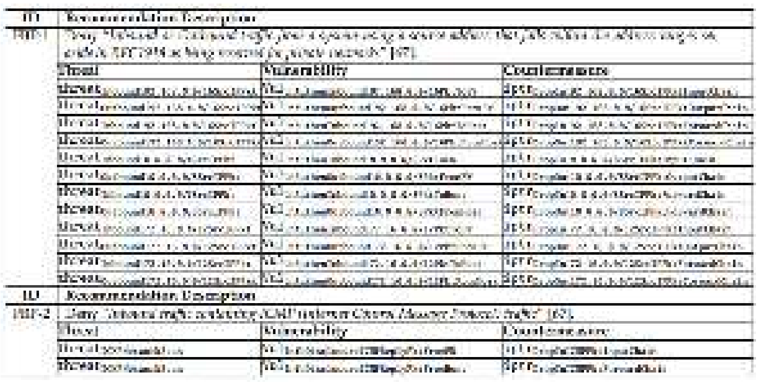


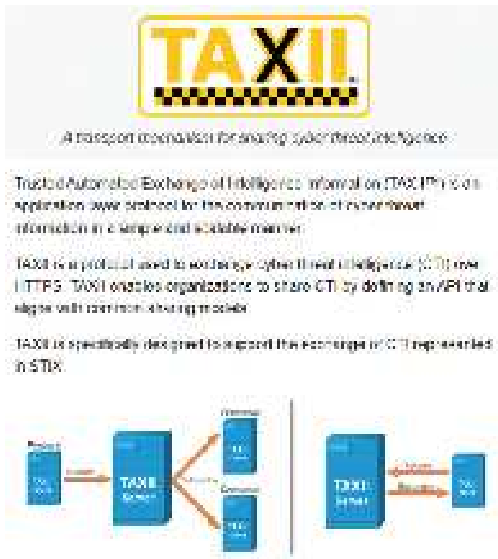
Table I: Semantic Threat Graphs Extracted for NIST-800-41: Guidelines on Firewalls and Firewall Policy

Fig. 4 – Esempio di tabella di descrittori semantici NIST-800-41 per Firewall policy.

Concludendo, i benefici di questa tecnologia innovativa possono così riepilogarsi:

- Allarmi rapidi distribuiti gerarchicamente sulla rete e centralizzabili su SIEM
- Protezione dello spazio dei dati condivisi come middleware per condividere le informazioni sugli attacchi informatici. Questo utilizzerà i concetti di privacy by design in cui i dati sono resi anonimi prima della condivisione.
- Migliore rilevamento e condivisione di attacchi noti e nuovi e/o sconosciuti
- Esplorazione e determinazione dei tipi e/o modelli di attacco
- Apprendimento automatico dai dati (etichettati) di nuovi modelli di attacco.
- Report di vulnerabilità e minacce in un formato gestibile e facilmente utilizzabile per gli utenti finali

Note aggiuntive schede STIX e TAXII:



2.2 Sistemi di simulazione e modelli di propagazione degli effetti

L'esigenza progettuale di aumentare la resilienza dei sistemi Cyber-Fisici nel settore delle Infrastrutture Critiche Finanziarie ha un impatto immediato su quali sono i modi per analizzare il rischio associato ai vari eventi critici. Infatti, l'equazione classica per la caratterizzazione del rischio R = P x V x C collega il rischio "R" a tre fattori, che sono, in particolare: Probabilità "P" di occorrenza di un evento (quanto è probabile che una determinata minaccia per concretizzare / manifestare); Vulnerabilità del sistema "V" all'evento specifico (che rappresenta una misura di sistema robusta contro la minaccia specifica); le Conseguenze (impatti) "C" prodotte dal verificarsi dell'evento (cioè quali sono le conseguenze negative in termini di vite umane, danni economici, immagine, ecc.). Un altro aspetto chiave è la mitigazione dei rischi informatici negli attacchi alle infrastrutture cyber fisiche primarie. Il modello di propagazione all'infrastruttura eterogeneo noto come **modello Leontieff** [B001] [B005] potrebbe essere adattato alle nostre esigenze di ricerca in base ai profili richiesti per Infrastrutture Critiche Finanziarie. Nel modello, i degradi subiti da ciascun settore / infrastruttura sono descritti dal grado di inattività xi (cioè una variabile il cui valore è compreso nell'intervallo [0,1] dove xi = 0 indica la piena funzionalità, mentre xi = 1 indica la completa distruzione delle capacità operative). Il calcolo di quale sia l'effetto di ordine diretto e di ordine superiore, indotto sul sistema da un evento esterno, viene effettuato mediante l'equazione di matrice:

$$\mathbf{x}(n+1) = \mathbf{A}\,\mathbf{x}(n) + \mathbf{c}$$

Dove A è una matrice mxm di coefficienti di Leontieff (con m uguale al numero di infrastrutture esaminate), e i cui elementi rappresentano la frazione di inoperabilità che l'infrastruttura j-esima viene trasmessa all'infrastruttura i-esima.

2.2.1 Modello Leontief applicato ad Infrastrutture Critiche Finanziarie

Prima di tutto, definiamo il concetto di Asset per i nostri scopi di progettazione e ricerca come una funzione infrastrutturale attiva o un cluster di funzioni attivo, inserito in un dominio Cyber interdipendente su reti di comunicazione wireless e wireline (def.1).

L'interdipendenza degli Asset è la risultante di attività funzionali sinergiche distribuite tra gli assets, che è misurata in modo univoco con un valore compreso [0,1] con 0 massima funzionalità e 1 massima non funzionalità (Def.2). Quindi un patrimonio aziendale è un insieme di risorse logiche e fisiche interconnesse che sono funzionali ai fini della Corporate (Def. 3)

Fig.1 - Intra-Inter dependency layers of a Corporate[Fonte B004]

Per stimare, ad esempio, l'impatto complessivo che un attacco informatico può avere su una Infrastruttura Critica Finanziaria, dobbiamo prima di tutto misurare le interdipendenze tra Asset1 (ATM), Asset2 (BANK OFFICE), Asset3 (DATA NETWORK) e Asset4 (DATA BASE) intesi come sottosistemi distribuiti anche geograficamente all'interno dell'azienda stessa, è necessario innanzitutto identificare il grado di dipendenza esistente tra i diversi Asset (vedi esempio in Tabella 1-Matrix dei coefficienti di Leontief) in funzione del tipo di infrastrutture e del contesto nazionale ed europeo ed è questo il grosso lavoro di chi è preposto a definire questa tipologia di modelli. Quindi considerando la matrice A (mxm detta dei coefficienti di Leontief), la colonna i-esima descriverà l'impatto che la distruzione dell'i-esimo Asset implica sugli altri Assets). Ad esempio, se si desidera valutare gli effetti di un evento cyber che rende non operativo l'80% degli ATM (ATM), si applica il seguente modello[B004]:

$$\bar{x} = (I - A)^{-1} c = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0.2 & 0 & 0 \\ 0.4 & 0 & 0 & 0.1 \\ 0.6 & 0.8 & 0 & 0.2 \\ 1 & 0.2 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0.8 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0.88 \\ 0.48 \\ 1 \\ 0.96 \end{bmatrix}$$

Con $\bar{x}$ = risultato vettoriale che misura il valore di degradazione su ciascuna delle quattro risorse Asset, I = matrice Identità, A = matrice dei coefficienti di Leontief e c = vettore Test che misura l'80% di inattività. Con questi dati di test possiamo simulare la propagazione del degrado globale che viene introdotto su tutti i 4 asset coinvolti, quindi un 80% di indisponibilità di Asset1 si traduce in un aumento dell'89% nel degrado sempre di Asset1 (ATM), 46% su Asset2 (BANK OFFICE) , Degradazione del 100% su Asset3 (DATA NETWORK) e degradazione del 98% su Asset4 (DATA BASE)

2.2.2 Calcoli su foglio elettronico

I = IDENTITY MATRIX

1,00	0,00	0,00	0,00
0,00	1,00	0,00	0,00
0,00	0,00	1,00	0,00
0,00	0,00	0,00	1,00

Tab.1 - A = COEFFICIENTS OF LEONTIEF MATRIX

	AST1	AST2	AST3	AST4
AST1	0,00	0,20	0,00	0,00
AST2	0,40	0,00	0,00	0,10
AST3	0,60	0,80	0,00	0,20
AST4	1,00	0,20	0,00	0,00

		I-A	MATRIX	
	AST1	AST2	AST3	AST4
AST1	1,00	-0,20	0,00	0,00
AST2	-0,40	1,00	0,00	-0,10
AST3	-0,60	-0,80	1,00	-0,20
AST4	-1,00	-0,20	0,00	1,00

	INV (I-A)					
	AST1	AST2	AST3	AST4	Test	DECAY
AST1	1,11	0,23	0,00	0,02	0,80	0,89
AST2	0,57	1,14	0,00	0,11	0,00	0,46
AST3	1,37	1,14	1,00	0,31	0,00	1,00
AST4	1,23	0,45	0,00	1,05	0,00	0,98

2.2.3 Requisiti fondamentali del modello

I requisiti fondamentali di tale modello per le Infrastrutture Critiche Finanziarie sono cosi riepilogabili:

1. Definizione della metodologia per determinare la corretta matrice dei coefficienti di Leontief per il settore delle Infrastrutture Critiche Finanziarie [B004][B005][B006]
2. La corretta definizione di un asset
3. Il Raggruppamento degli Assets (cluster)

3.0 Considerazioni finali

Il ruolo centrale delle Infrastrutture Critiche Finanziarie sarà sempre più enfatizzato dalle crescenti esigenze di un mercato globalizzato, nomadico, dinamico e virtuale in special modo nelle quattro categorie di processi critici evidenziate in questo studio come i pagamenti POS, i pagamenti nomadici, i trasferimenti di elevati valori monetari e le operazioni di trading. La domanda che ci si pone è se gli Istituti Finanziari proprietari delle infrastrutture saranno disposte a cedere loro spazi di attività ai nuovi intermediari; probabilmente sì sotto **precisi vincoli di controllo e sicurezza** sia delle transazioni economiche viste in ottica di consenso tra le parti coinvolte sia dai sistemi Cyber-Fisici di supporto ad esse. Tali vincoli visti in questo nuovo scenario necessiteranno di innovative metodologie dinamiche di gestione delle minacce ed allertamento preventivo nonché di sistemi di simulazione in grado di studiare per tempo il verificarsi di fenomeni che potrebbero avere forti impatti sociali[B008].

Bibliografia Utile

[B001]https://www.math.ksu.edu/~gerald/leontief.pdf

[B002] A FRAMEWORK FOR MODELING INTERDEPENDENCIES IN JAPAN'S CRITICAL INFRASTRUCTURE http://ai2-s2-pdfs.s3.amazonaws.com/f952/c5412200f98834e2f7dbb8169ef81585de0a.pdf

[B003] An Input-Output Framework for Assessing Disaster Impacts on Nashville Metropolitan Region https://www.iioa.org/conferences/20th/papers/files/691_20120501071_JoostSantos-IIOABratislava.pdf

[B004] R. Setola "La Protezione delle Infrastrutture Critiche Informatizzate", Automazione e Strumentazione, luglio 2003

[B005] Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research http://cip.management.dal.ca/publications/Critical%20Infrastructure%20Interdependency%20Modeling.pdf

[B006] Managing Critical Infrastructure Interdependence through Economic Input-Output Methods https://www.cmu.edu/gdi/docs/managing-critical.pdf

[B007] Management of Security Policy Configuration using a Semantic Threat Graph Approach https://pdfs.semanticscholar.org/8192/b903fc3d1a8da3fe67646f8733bca84a8f04.pdf

[B008] Francesco Corona, Flussi finanziari verso una nuova politica della BCE

http://docplayer.it/1300295-Flussi-finanziari-verso-una-nuova-politica-della-bce-a-cura-di-francesco-corona.html ■

La campagna di sensibilizzazione di Poste Italiane incontra le scuole per l'iniziativa "Navigare con prudenza"

Autore : Marianna Cicchiello

Poste Italiane prosegue nella sua opera di sensibilizzazione in merito ai temi della sicurezza informatica, che costituisce un impegno fondamentale per l'azienda, cosciente della necessità di diffondere la cultura della navigazione consapevole e sicura sul web. In quest'ottica si inserisce la partecipazione dell'azienda al Festival del Fumetto *Le Strade del Paesaggio* con cui Poste Italiane ha organizzato una serie di eventi

ed iniziative rivolte alle giovani generazioni per raccontare la cyber security attraverso i fumetti: una scelta in linea con la campagna di sensibilizzazione promossa da Poste Italiane che mira a diffondere l'uso consapevole degli strumenti digitali soprattutto presso i giovani, e con l'attività del Distretto Cyber Security Poste Italiane, centro operativo dedicato all'analisi delle minacce cyber, alla protezione dei dati personali e alla formazione e sensibilizzazione sui temi della cyber security a livello locale e nazionale.

La presenza dell'azienda con un proprio spazio espositivo all'XI edizione del Festival *Le Strade del Paesaggio* presso il Museo del Fumetto di Cosenza tenutosi dal 22 al 24 settembre, è stata l'occasione per puntare sulla sensibilizzazione e informazione: all'interno dello spazio il personale del Computer Emergency Response Team di Poste Italiane ha fornito le conoscenze necessarie e gli opportuni consigli sulla sicurezza informatica ai visitatori; questi ultimi hanno potuto cimentarsi nel CyberSecQuiz, il quiz online per testare le proprie competenze in materia ed effettuare approfondimenti e hanno potuto prendere visione delle

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. Svolge attività in ambito cyber security dal 2014, dapprima contribuendo al progetto di ricerca e sviluppo che attiene la protezione dell'utente finale, oggi occupandosi di alcune iniziative che riguardano i temi di sensibilizzazione in particolare la mostra "Eroi e vittime dei social media".

video pillole "Phishing", "Mobile Security" e "Utilizzo corretto della posta elettronica" realizzate dall'azienda e finalizzate a educare su alcuni aspetti potenzialmente pericolosi durante la navigazione in rete.

A questo ha fatto seguito la correlata iniziativa dell'azienda "Navigare con Prudenza", una serie di workshop sulla cyber security organizzati nel mese di ottobre nei licei artistici delle principali città calabresi organizzati dal Festival del Fumetto *Le strade del Paesaggio* in collaborazione con Poste Italiane, legati al concorso a premi per la realizzazione di una strip a fumetti in grado di trasmettere un messaggio sui temi del cyberbullismo, dei social network e della mobile security.

Gli incontri si sono tenuti nelle sedi dei cinque licei artistici delle province di Cosenza, Catanzaro, Crotone, Lamezia Terme e Reggio Calabria dal 10 al 14 ottobre alla presenza del personale del Computer Emergency Response Team, del rappresentante del Festival del Fumetto e della disegnatrice Lorenza Di Sepio, testimonial dell'iniziativa, oltre che di docenti e dirigenti scolastici degli istituti e hanno visto la partecipazione di 218 studenti e la presentazione di 180 strisce partecipanti.

Nella parte di workshop dedicata alla sensibilizzazione sono stati illustrati i contenuti della campagna di sensibilizzazione promossa dall'azienda, sono state mostrate le video pillole e sono state esplicate le tematiche oggetto del concorso, così da istruire e informare gli studenti sui pericoli di una navigazione non consapevole, facendo loro dunque acquisire le conoscenze necessarie per rappresentare la loro visione attraverso il fumetto che avrebbero realizzato nelle ore successive del workshop, durante la fase del laboratorio creativo coordinato dalla disegnatrice Lorenza Di Sepio. Al termine del concorso, tutti i contributi in tema sono stati valutati da un'apposita giuria composta da due membri del direttivo del Festival del Fumetto *Le Strade del Paesaggio* e da un membro di Poste Italiane. La premiazione avverrà il prossimo 19 dicembre presso il Distretto Cyber Security.

Questi incontri hanno rappresentato l'occasione per ulteriormente diffondere la cultura di un uso consapevole degli strumenti digitali attraverso la sensibilizzazione dei giovani sui rischi che si corrono in rete. La scelta di Poste Italiane in merito al concorso mira chiaramente ad arrivare alle giovani generazioni attraverso l'utilizzo di uno strumento narrativo ad esse molto caro, come il fumetto, facendo così seguito alla serie di attività che l'azienda sta portando avanti da tempo. ■

Sfide e minacce nell'ambito della cyber-security viste da un risk manager

Intervista a Jean-Luc Habermacher

Jean-Luc Habermacher

autore: Laurent Chrzanovski

Laurent Chrzanovski: Descriva il suo percorso

Jean-Luc Habermacher: Dirigente in grandi gruppi industriali internazionali da circa trent'anni, ho operato in diversi livelli di funzioni e specialmente come Risk Manager e Responsabile di Sicurezza Centrale.

Formato all'Istituto degli Hautes Etudes de la Défense Nationale (IHEDN), ho assunto anche la responsabilità dello sviluppo delle azioni dell'Intelligenza Economica presso le imprese e offro anche il mio sostegno per la prevenzione dei rischi e dei cyber-rischi attraverso una missione come Luogotenente-Colonello (R) nella Gendarmeria.

Preoccupato della necessità di creare una cultura della gestione dei rischi nell'impresa, sono anche insegnante in molte componenti universitarie e membro dell'Associazione nazionale per il Management dei Rischi et delle Assicurazioni dell'impresa.

Partecipo anche attivamente ai lavori di parecchi comitati nazionali sui diversi soggetti legati alla sicurezza.

Una decina di anni fa ho creato il 1° cluster francese delle industrie dell'Energia battezzata "Vallée dell'Energie" di cui sono il Presidente. Operiamo qui per promuovere e sviluppare le industrie della filiera energetica in Francia.

Ho avuto la opportunità di sostenere un mandato parlamentare ciò che mi ha permesso e mi permette ancora, di poter lavorare strettamente su certi soggetti legislativi legati alla sicurezza.

Laurent Chrzanovski: Come è arrivato ad interessarsi alla cyber-sicurezza?

Jean-Luc Habermacher: Da parecchi anni, a causa delle mie diverse attività presso delle imprese e degli attori economici e con la mia cultura di Risk Manager, mi sono interessato a cercare di capire come questi ultimi analizzavano i loro rischi e le loro esposizioni e ciò nel quadro di una visione globale.

Mi sono reso conto molto presto che la digitalizzazione delle tecnologie all'interno stesso delle imprese non era afferrata con la percezione dei "rischi cyber" nelle loro reali dimensioni.

Durante le discussioni con i Responsabili delle Imprese e senza essere sistematicamente "paranoico", allorquando affrontavo la loro propria

BIO

Fondatore e Presidente della Energy Valey - primo cluster europeo di aziende produttrici di energia, Jean-Luc è senior risk manager, con esperienza professionale in ditte molto importanti quali CEGELEC, ALSTOM, CONVERTEAM e GENERAL ELECTRIC. Vice-Presidente regionale dell'Associazione degli Auditori dell'Istituto di Alti Studi di Difesa Nazionale (IHEDN), Jean-Luc è anche nella direzione dell'Università di Bourgogne-Franche-Comté e Locotenente-Colonnello di Gendarmeria (RC). Jean-Luc è anche Project Manager nell'implementazione di soluzioni di Business Intelligence presso numerose aziende private.

percezione riguardo alla loro propria esposizione dei diversi rischi, la componente digitale non era analizzata se non in modo tecnologico senza percepirne le componenti delle strategie globali economiche.

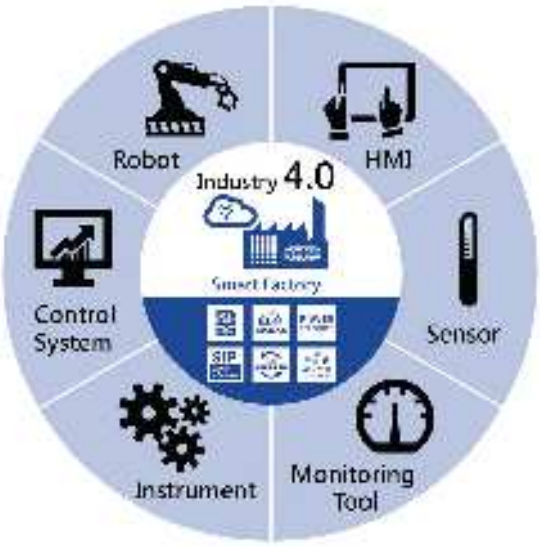
A mio parere, questo era un reale diniego della presa in conto dei rischi economici legati alla digitalizzazione industriale.

La mia formazione in Intelligenza Economica mi ha fatto prendere coscienza della necessità di sensibilizzare e di interpellare gli ambienti economici su questa lacuna importante nell'approccio dell'analisi dei rischi delle imprese.

Laurent Chrzanovski: Quali aspetti del mondo cyber La preoccupano oggi?

Jean-Luc Habermacher: La dipendenza tecnologica delle imprese verso gli strumenti ed i sistemi informatici è tale che un'analisi sbagliata della sua esposizione può essere fatale.

Durante numerosi anni, i responsabili d' impresa si focalizzavano sulle perdite dei dati sviluppando delle strategie di backup, moltiplicando così l'interconnessione degli strumenti e dei sistemi.



L'industria 4.0 non è stata sufficientemente analizzata nella prospettiva delle vulnerabilità delle apparecchiature e dei sistemi connessi. Gli ultimi esempi di cyber-attacchi hanno fatto prendere coscienza delle brecce importanti negli strumenti di produzione o di supervisione. È adesso che una parte molto grande delle architetture globali dei sistemi connessi in seno alle imprese devono essere ripensati e ripresi.

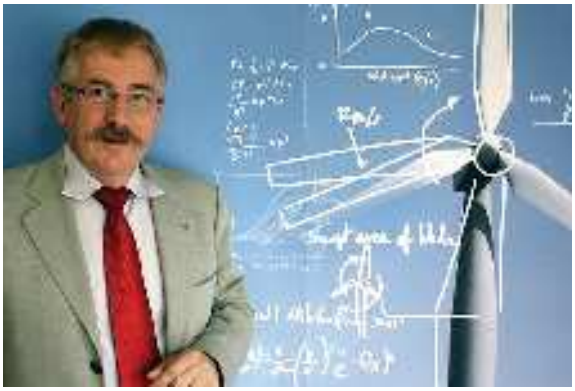
Le poste in gioco di geo-strategia economica non sono purtroppo percepite dai responsabili delle piccole e medie imprese ed è evidente che "interessi superiori" stanno dietro numerosi attacchi cyber che toccano le reti economiche e le imprese.

I cyber-attacchi sono il riflesso della versione moderna della guerra economica che è portata avanti dalle grandi potenze sia statali che private. L'interconnessione degli strumenti e dei sistemi trascina una interdipendenza che apre delle vulnerabilità molto importanti. Le posizioni dominanti di certi attori tecnologici creano a termine degli schemi di dipendenza strutturali estremamente critici.

Siamo entrati nella «3° guerra mondiale" e le poste sono economiche e soprattutto geopolitiche. Sarebbe irresponsabile non volerle capire da questo angolo.

Laurent Chrzanovski: Come giudica lo stato della presa di coscienza nelle imprese dove Lei è stato attivo/è attivo?

Jean-Luc Habermacher: I grandi gruppi industriali hanno realizzato da parecchi anni che i loro sistemi di informazione potrebbero essere bersagli per attacchi di destabilizzazione e delle procedure di messa in sicurezza sono state approntate. Le piattaforme e la connettività



dei mezzi di produzione erano in gran parte sfuggiti all'analisi dei rischi e gli ultimi avvenimenti vengono ad attivare una presa di coscienza di questi nuovi punti di vulnerabilità.

Bisogna anche migliorare la collaborazione con i prestatori incaricati coi servizi di manutenzione e di gestione degli equipaggiamenti, perché essi sono dei possibili ricettori di attacchi, che non sempre sono dotati di una sicurezza efficace.

Le politiche della sicurezza delle grandi imprese si sono seriamente rinforzate in questi ultimi tre anni ed i comportamenti a rischio dei loro collaboratori sono perseguiti. I PC ed i materiali connessi sono contenuti in formati molto regolamentati e sistematicamente controllati.

A mio parere, i datacenter esternalizzati utilizzati da numerose imprese rimangono dei reali punti di debolezza e non sarei sorpreso di apprendere da qui a poco tempo che scopriremo perdite maggiori di informazioni o gravi attacchi che avranno sfruttato questo vettore.

Laurent Chrzanovski: E in seno al cluster della Vallée de l'Energie?

Jean-Luc Habermacher: Il cluster della Vallée de l'Energie raggruppa gli industriali e gli attori della filiera energia in Francia e in quanto Presidente, porto avanti delle azioni per sensibilizzare e ben informare i miei membri specialmente sui rischi ai quali potrebbero essere confrontati nelle loro attività.

Le tecnologie digitali fanno ormai parte dell'insieme della catena di fabbricazione dei componenti e sono diventate un elemento di base per i progettisti di software di controllo/ comando che monitorizzano le unità di produzione e di distribuzione dell'energia.

Le conseguenze sono dunque differenti in ciascuno di questi due contesti. La reale apprensione delle vulnerabilità dell'impresa connessa è molto recente fra i responsabili delle Piccole e Medie Imprese, è quindi necessario mettere a disposizione delle formazioni in questo campo ed eventualmente aiutare le imprese a realizzare degli audit globali.

Un altro settore molto delicato è quello del pilotaggio dei sistemi di produzione, di gestione e di distribuzione dell'energia. Su questo punto è evidente che ci sono dei rischi maggiori poiché le piattaforme ed i soft che pilotano e gestiscono le attrezzature non sono purtroppo abbastanza sicuri al giorno d›oggi.

È quindi essenziale lavorare in coordinazione con le imprese che fabbricano e sviluppano i sistemi di gestione per integrare correttamente le protezioni necessarie e mettere in atto dei procedimenti di intervento controllabili, ma questo nuovo modo di capire l›ecosistema necessita un cambiamento della cultura attuale dei diversi attori.

Mi sembra importante diffondere dei messaggi in questo senso e di ritrasmetterli attraverso differenti riviste specializzate con il sostegno di strutture quali le Camere di Commercio e dell'Industria, i Comitati Industriali, i Sindacati professionali …

Dobbiamo anche lavorare a mettere in atto delle formazioni specifiche sull'analisi e la gestione dei cyber-rischi in seno alle Università e alle Scuole di Ingegneri poiché le nostre imprese hanno bisogno di supporto su questi argomenti. Noi lavoriamo in stretta relazione con i servizi dello Stato (Polizia e Gendarmeria) per diffondere ai nostri membri le allerte ed eventualmente accompagnarli nelle loro pratiche amministrative in caso di attacco.

Laurent Chrzanovski: Quali campi della sicurezza del mondo digitale Le appaiono particolarmente sottovalutati in rapporto ai comportamenti fisici?

Jean-Luc Habermacher: Come ho esposto in precedenza la connettività dei sistemi, sia interna che esterna all'impresa, è diventata una necessità sociale con la quale dobbiamo convivere. Le barriere tecnologiche saranno difficili da mettere in opera tanto più che, per natura, i comportamenti umani cercheranno di sviarle. La moltiplicazione dei dati raccolti nell'ambiente che circonda gli individui e gli sfruttamenti incrociati che potranno esserne fatti sono percepiti come enormi poste in gioco economiche future.

Per questo, numerosi attori desiderano iscriversi in questa catena di collette dirette o indirette dei dati. Per fare ciò vediamo il dispiegarsi di una molteplicità di applicazioni che in modo subdolo raccolgono e in seguito trasferiscono dei dati sia individuali che collettivi, questi ultimi sfuggono evidentemente al controllo di ciascuno di noi, ma potrebbero esserci posti in opposizione a termine.

La volontà di associare le tecnologie digitali a numerose attività quotidiane deve farsi con una reale presa di coscienza delle dipendenze tecniche che generano ma anche delle conseguenze nella società che ne derivano.

Laurent Chrzanovski: Chi dovrebbe assumere la cultura della difesa digitale nelle imprese e sotto quale forma, a Suo parere?

Jean-Luc Habermacher: Al giorno d'oggi, in molte strutture, la strategia della difesa digitale è portata avanti dai Responsabili dei Sistemi d'Informazione, ciò che fanno con approccio e una cultura molto "tecnica".

Come ho già detto, le poste in gioco sono sempre più economiche e l'impresa deve essere in misura di analizzare la sua vulnerabilità attraverso delle sfaccettature. La tecnologia, o più esattamente gli strumenti tecnologici digitali diventano i vettori o le armi di attacco che saranno utilizzate contro l'impresa. Da qui diventa essenziale avere una visione con una vera analisi a 360°.

Jean-Luc Habermacher and the French Delegation at the Cybersecurity-Romania congress

Per questo, bisogna sviluppare una cultura del rischio differente, incominciando con l'identificare bene le ragioni per cercare in seguito di anticipare i meccanismi che potrebbero essere dispiegati contro l'impresa, ma anche di comprendere bene l'insieme delle conseguenze con le quali l'impresa sarà confrontata in differenti scenari.

In questo contesto, non sono sicuro che il profilo "Tecnico Sistema di Informazione" sia il più pertinente per portare a termine questa riflessione e sviluppare la cultura del rischio nell'impresa.

I Dirigenti di imprese (DG, Amministratori …) devono essere informati ed interessarsi alle vulnerabilità strategiche alle quali le loro imprese potrebbero essere esposte e prendere coscienza che le risposte alle parate non sono solo tecnologiche. Le componenti umane, culturali, di società, vuoi anche geo-politiche, devono essere prese in conto.

The EU Commission «Berlaymont» building © EU Parliament Magazine

L'installazione dei mezzi di copertura dei rischi deve necessariamente integrare questa dimensione, bisogna certo prevedere di coprire i danni materiali, ma è anche altrettanto essenziale prevedere la copertura o l'assunzione dei danni immateriali.

Il profilo del gerente del rischio dovrà dunque integrare tutte queste componenti.

Laurent Chrzanovski: Perché, secondo Lei, l'Europa ha per troppo tempo ignorato la nostra transizione al digitale e le sfide di sicurezza nuove per rapporto alle grandi potenze?

Jean-Luc Habermacher: Non so se realmente l'Europa abbia ignorato le sfide di sicurezza legate ai mutamenti digitali, ma quello che è certo è che lo spiegamento delle nuove tecnologie non è sempre stato percepito nel quadro di una analisi globale. L'interesse immediato per certi strumenti o certe applicazioni ha in qualche modo occultato le conseguenze indirette che esse potevano generare a termine.

D'altra parte, non abbiamo forse sufficientemente anticipato le conseguenze delle dipendenze tecnologiche che i grandi attori non contornabili dei software di gestione, delle reti ed i gestori delle reti di informazione digitale avrebbero messo in opera. Le convergenze economiche, attraverso i differenti attori, non sono forse state sufficientemente comprese per permettere di preparare delle parate alle dipendenze tecnologiche che esse avrebbero generato. I quadri legislativi internazionali non sono anch'essi stati adattati per permettere di evitare situazioni critiche.

Per di più gli interessi economici degli Stati prevalgono sugli interessi collettivi europei. L'Europa è una grande casa in cui ciascun locatario vorrebbe utilizzare e gestire secondo i propri interessi l'apertura delle porte e delle finestre, la rete elettrica o del riscaldamento, bloccando l'interesse comunitario alla porta di ogni appartamento. Dare e imporre regole comunitarie significa anche imporre a sé stessi delle costrizioni al proprio sviluppo.

Essendo il consenso la regola di governo, gli atti e le decisioni prese saranno sempre 'al minimo'.

Certi progetti come GALILEO vanno nel senso della installazione di certe indipendenze tecnologiche, ma come abbiamo potuto vedere la loro messa in opera è molto complicata e soprattutto molto lunga.

L'evoluzione delle tecnologie e delle strutture digitali necessitano di tempi di reazione molto corti che purtroppo sono in gran parte incompatibili con le pesantezze della direzione amministrativa delle istituzioni europee.

Laurent Chrzanovski: E' ancora possibile in un continente in pace dal 1945 instaurare di nuovo uno spirito di vigilanza senza farsi trattare da big-brother o da guerrafondaio?

Jean-Luc Habermacher: Gli atti di terrorismo che toccano molti paesi europei da parecchi anni hanno riattivato un certo spirito di vigilanza e tendono anche a riattivare una coscienza civica.

Purtroppo i cyber-attacchi non hanno la stessa visibilità degli attacchi e attentati di strada, anche se in un certo modo le loro conseguenze possono essere simili in quanto ad impatto economico e di società. I supporti tecnologici sui quali si appoggiano gli autori dei cyber-attacchi sono sia individuali che collettivi; i comportamenti umani sono anch'essi dei vettori di trasmissione delle loro armi di attacco.

Cercare di regolamentare certe pratiche ci porterà ad impattare i comportamenti individuali e ad abbordare sia le nozioni di libertà che di ingerenza. La corsa alle tecnologie digitali e la molteplicità delle applicazioni di servizi ai quali aderisce spontaneamente una gran parte della popolazione rende anche molto difficile un'azione di regolazione. La presa di coscienza "politica" non è ancora sufficientemente matura per costituire un perno di influenza per generare delle reali misure di vigilanza collettiva e civica.

Bisognerebbe anche tentare di rinforzare il quadro legislativo per permettere delle azioni di investigazione molto più larghe e poter sanzionare più severamente, ma per questo, bisognerà far accettare ai nostri concittadini che la loro sicurezza passa forse attraverso qualche restrizione delle loro "libertà individuali".

Laurent Chrzanovski: Perché si è così poco sensibili alle buone pratiche dei nostri vicini in seno all'UE quando queste ultime hanno fatto le loro prove e invece si riscopre l'acqua calda in ogni paese?

Jean-Luc Habermacher: Mi sembra che è nello spirito di molti fra di noi e specialmente dei nostri governanti, di voler sistematicamente personalizzare i procedimenti e le azioni.

Quando si tratta di ricondurre una "buona pratica", c'è sempre pretesto a riconsiderarla al fine di cercare di personalizzarla per forse, adattarla meglio al nostro contesto e lo spirito nazionalista rimane molto presente nei nostri politici. I sindacati o le federazioni professionali nei campi della perizia sono praticamente inesistenti e non possono quindi tenere il loro ruolo di leva di influenza per federare azioni a livello europeo.

È questo un vero piano d'azione da mettere in atto.

Bisognerebbe quindi creare delle istanze professionali rappresentative dei nostri campi di competenza che potrebbero così lavorare in modo trasversale per promuovere i lavori realizzati e capitalizzarli. ■

Sfide e problemi nella realizzazione di un SOC visti con gli occhi del Management

Nel corso dell'ultimo anno, il paesaggio della sicurezza cibernetica ha conosciuto mutazioni significative, portate dall'onda della crescita dell'impatto degli attacchi realizzati su scala mondiale e l'uso di strumenti specializzati creati *ad hoc* e che ne hanno assicurato il successo, strumenti sviluppati da agenzie governative d'élite, rivelati e messi a disposizione di tutti tramite canali di distribuzione del tipo Wikileaks.

Autore : Eduard Bisceanu

Anche se questa repentina evoluzione meriterebbe da sola un'analisi molto più attenta e senza interpretazioni partigiane, lo scopo del nostro articolo è quello di identificare alcune delle sfide con le quali si confrontano le strutture di sicurezza attive nelle società private di affari, ma anche nelle istituzioni pubbliche che hanno una gran parte della loro attività esposta on line. Alla fine, metteremo in luce un certo numero di tendenze che dovrebbero essere osservate di continuo per proteggere con successo sia i dati che le infrastrutture che sono loro associate.

Abbiamo letto con grande interesse una panoplia di articoli e pubblicazioni che attraggono l'attenzione del pubblico di specialità su di una serie di innovazioni tecnologiche (*blockchain, machine learning, big data analytics, artificial intelligence* etc.), che cambieranno radicalmente le modalità di progettazione e di implementazione dei sistemi informatici, in tutti i settori di attività. Se parliamo però di trasformazione digitale nell'ambito delle grandi strutture o di settori economici strettamente regolamentati (ad esempio quello delle banche e della finanza), così come i costi significativi che impone qualsiasi programma strategico e disruttivo di informatizzazione, è doveroso rendersi conto che l'implementazione delle nuove tecnologie non si potrà realizzare con la rapidità con la quale le innovazioni sono implementate, ad esempio, nei prodotti e servizi commerciali.

Sotto questa luce, gli specialisti di sicurezza si trovano ormai posti davanti a scelte difficili, dovendo proteggere infrastrutture realizzate secondo dei concetti che hanno dato loro una viabilità tecnologica che non permette più di mantenerne un grado elevato di sicurezza oppure, all'opposto, infrastrutture nuove che implicano dei cambiamenti organizzativi maggiori nonché costi molto importanti. Dovendo osservare un mercato della sicurezza in costante evoluzione, ma disponendo di risorse limitate, non potranno di certo adattarsi permanentemente alle tendenze messe in evidenza dalla realtà della cyber-security.

In funzione del grado di maturità organizzativa, di profittabilità e della disponibilità di fare nuovi investimenti, siamo convinti che ci troviamo in

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 frode attraverso l'uso di 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. Dopo essere stato CSO presso la UniCredit Bank Romania, Eduard occupa oggi la funzione di National Technology Officer alla Microsoft Romania.

un momento cruciale, durante il quale il management di ogni istituzione o azienda interessato al proprio livello di sicurezza dovrà adattare la sua linea di investimenti alle nuove tendenze e chiedere ai dipartimenti interni specializzati (CIO, CISO) di lavorare assieme per identificare le strategie più idonee così come le modalità pragmatiche per fronteggiare con successo le nuove categorie di minacce cibernetiche che si manifestano a livello globale.

Questa opportunità consentirà un ampio sviluppo ma, secondo noi, raramente si ritrovano in una singola persona sia le competenze che le conoscenze necessarie all'identificazione di soluzioni viabili, indifferentemente dai vari profili professionali e dei gradi di specializzazione. Perciò abbiamo ritenuto opportuno soffermarci su di un singolo processo, complesso, che può e deve essere ottimizzato nell'ambito di qualsivoglia struttura che utilizza un'infrastruttura complessa: il monitoraggio, al servizio della prevenzione, della rilevazione e della risposta agli incidenti di sicurezza informatica. Per essere più precisi, parliamo qui del quadro organizzativo, procedurale e tecnologico necessario all'implementazione di un tale processo tramite una struttura di tipo SOC– Security Operation Center.

Dalla nostra esperienza e dagli scambi con diversi membri della comunità di esperti nel campo della sicurezza IT, constatiamo che esistono molte visioni e valori diversi su quello che dovrebbe significare un SOC. Se accenniamo all'efficienza e ad una concezione funzionale di una tale struttura, abbiamo identificato pure aspetti negativi già nell'approccio del soggetto, generate specialmente da valutazioni esclusivamente tecniche che sono centrate su di una soluzione tecnologica specifica messa sul mercato da un *player* che ha identificato in questo nuovo bisogno aziendale un'opportunità di affare.

Per diventare una costruzione funzionale e di successo, la realizzazione di un SOC deve partire da una chiara definizione dei bisogni per i quali una tale struttura è necessaria. Ad esempio, se parliamo di una banca che propone servizi online 24/7, come quasi tutte le istituzioni finanziarie al giorno d'oggi, l'attività di monitoraggio svolta normalmente dall'équipe di sicurezza esclusivamente nel corso del programma lavorativo non è più sufficiente, anche se l'ente dispone delle più avanzate tecnologie di sicurezza.

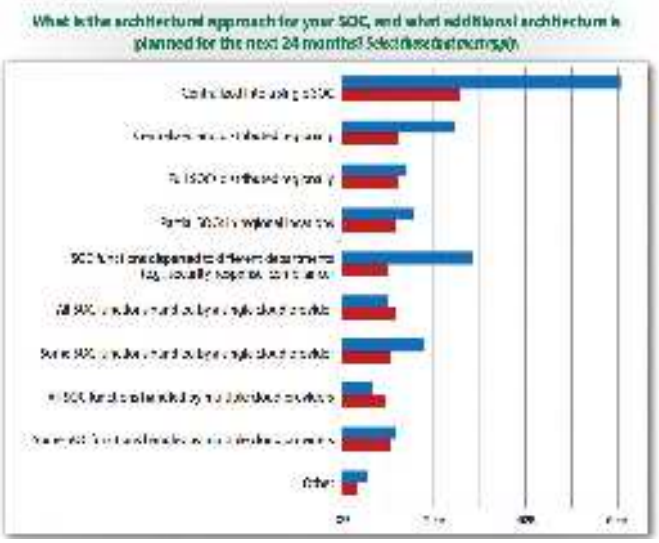
Il monitoraggio degli incidenti di sicurezza diviene quindi un processo di business, che deve essere trattato costantemente, iniziando nello sfruttare appieno i meccanismi tecnologici già esistenti nell'organizzazione. Spesso, manager con esperienza, tra i quali molti con un solido background tecnologico, ci chiedono da dove iniziare le procedure di sviluppo e di messa in opera di un SOC, in un periodo dove siamo già soffocati dal volume delle informazioni specializzate aggiornate a cottimo sullo spazio pubblico.

Quasi sempre, le soluzioni sono a portata di mano e non presuppongono altro che decisioni chiare, misure organizzative semplici e costi accettabili, almeno in una prima fase, e cioè:

- Bisogna identificare il personale-chiave disponibile, valutare le competenze necessarie e le risorse di tempo che devono essere allocate per assicurare la funzionalità permanente del SOC. Questo implica un'ottimizzazione delle attività correnti ed una quantificazione precisa del personale necessario. E poi, si deve procedere alla valutazione dell'opportunità di avere tutte le funzionalità del SOC all'interno dell'azienda oppure di esternalizzarne alcune.

- Bisogna poi fare un inventario preciso delle tecnologie di sicurezza esistenti per identificarne le capacità di monitoraggio che codeste dispongono già, o meno. In modo generale, ad oggi, tutte le infrastrutture che sono in uso online e sostengono la funzionalità di un business dispongono già al minimo di alcune piattaforme tecnologiche di base che permettono di essere adoperate in condizioni minime di sicurezza (*network firewall, application firewall, antivirus/antimalware, IPS/IDS, end-point security, DLP, SIEM* ecc.). Se non è già stato ideato come tale, il primo passo verso la realizzazione di un SOC è di identificare uno spazio comune, adeguato, in seno al quale verranno centralizzate ed integrate (lì dove la tecnologia lo consente) tutte le capacità di monitoraggio già identificate.

- Molto importante è la fase di creazione di procedure semplici di lavoro e di selezione del personale necessario a svolgere le operazioni richieste. Le procedure debbono essere semplici e devono necessariamente coprire, in adeguazione con le capacità tecnologiche esistenti, non solo tutti i tipi di attività correnti, ma anche le situazioni



© Christopher Crowley, Future SOC: SANS 2017 Security Operations Center Survey, SANS May 2017

di crisi potenziali. Bisogna soprattutto ricordarsi che la funzione, prevalentemente preventiva, di un SOC, ovvero la gestione degli incidenti di sicurezza cibernetica individuati è un processo che esige una documentazione adeguata e tempestiva. Al di là del quadro procedurale, le competenze e le risorse a disposizione dell'équipe che opererà il SOC, la capacità di identificare indicatori di attacco o di compromissione e di generare allerte specifiche, così come i meccanismi di escalation decisionale in caso di un incidente, sono altrettanti aspetti che possono generare differenze con un impatto maggiore sul grado di operatività e di efficienza di una tale struttura. Non bisogna neppure ignorare, in funzione dei bisogni propri ad ogni business, le capacità specifiche ai processi di *business continuity* e di *disaster recovery*.

▸ Infine, è doverosa una buona valutazione dei rischi di sicurezza e dell'evoluzione / delle tipologie delle nuove minacce cibernetiche, mettendo a confronto la particolare esposizione dell'azienda ad atti criminali, permettendo così di identificare le lacune tecnologiche e funzionali da colmare per rendere operativo il SOC.

Questa prima tappa, che può avere gradi diversi di complessità, permette all'azienda di realizzare, con costi minimi, la piattaforma di base necessaria all'ulteriore messa in opera del SOC, in conformità coi bisogni attuali, le possibilità tecnologiche proposte sul mercato e le proprie disponibilità sulle somme da investire.

In questa ottica, il mercato della sicurezza ha iniziato ad adattarsi e a livello globale vi sono dei players importanti che hanno adattato le loro prestazioni per poter assicurare servizi di tipo SOC. La forte crescita del mercato del cloud indica che una delle possibili tendenze del futuro sarà basata sull'esternalizzazione, almeno parziale di alcune funzionalità critiche specifiche ad un SOC. I vantaggi dell'esternalizzazione provengono dalla qualità delle risorse specializzate disponibili all'interno del fornitore, della possibilità di un'esternalizzazione controllata di certi rischi, che vengono coperti contrattualmente, dall'ottimizzazione dei costi – si comperano servizi e non tecnologie – col loro corollario di alti costi di gestione, ed i rischi di essere sorpassate dall'evoluzione tecnologica sia nel loro campo, sia in quello delle minacce, ecc. Tra gli svantaggi di una tale scelta meritano di essere menzionate le limitazioni legali generate dall'impatto del quadro delle regolamentazioni vigenti su certi settori, le difficoltà di rendere trasparente il rapporto tra l'investimento ed i servizi acquisiti e soprattutto, l'identificazione dei meccanismi di fiducia tra il fornitore di servizi ed il cliente. Quest'ultimo punto

è sicuramente il più grande challenge nonché ostacolo all'evoluzione del mercato del cloud in certe parti del mondo (L'Europa centrale ed orientale ne è un esempio lampante).

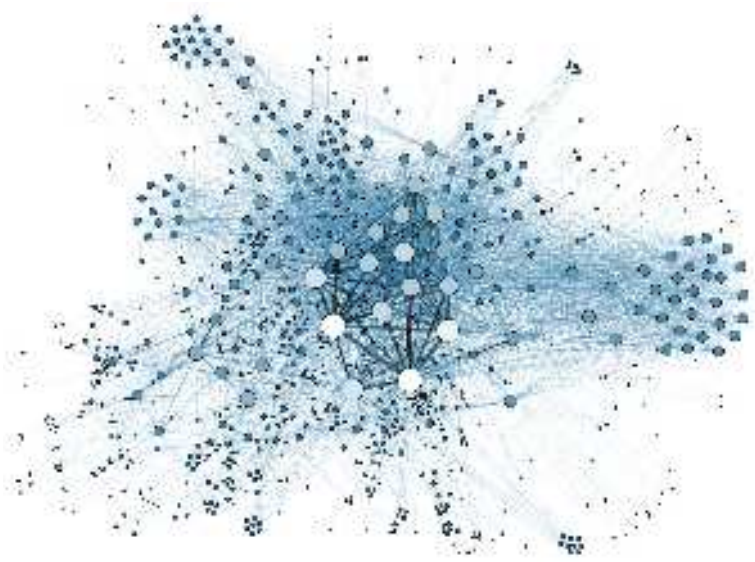
Il monitoraggio dell'infrastruttura con lo scopo di identificare quanto più rapidamente dei possibili attacchi cibernetici, così come lo svolgimento regolare di monitoraggio delle vulnerabilità esistenti nelle proprie infrastrutture IT, sono altri due processi che possono difendere con successo l'esistenza online di un'azienda.

Ciò nonostante, se osserviamo le nuove sfide poste dalla tipologia evolutiva degli ultimi attacchi cibernetici svolti su scala globale ed in particolare le caratteristiche dei vettori di distribuzione di programmi di tipo malware doppiate dalla capacità distruttiva o persistente di queste ultime al livello delle infrastrutture infettate, si nota come delle semplici misure organizzative o l'uso come tale delle capacità offerte dalle tecnologie di sicurezza classiche e consacrate, non sono più sufficienti per assicurare un'efficace funzione preventiva e neanche delle capacità tecniche per rispondere in modo adeguato a tali attacchi.

Per di più, sebbene il mercato della sicurezza digitale stia generando oggi dei nuovi prodotti e servizi, basati su innovazioni tecnologiche spettacolari, la loro mancanza di maturità e di efficacia dimostrata o dimostrabile, doppiate dai loro costi di acquisizione vengono a creare non pochi problemi nella corretta identificazione della soluzione idonea e ciò indifferentemente dal tipo di ente o di società che desidera irrobustire la sua difesa.

In questa prospettiva, dopo aver percorso con successo tutte le tappe iniziali dell'iter descritto sopra, per rendere realmente operativo un SOC nel quadro attuale della sicurezza cibernetica, bisogna considerare con attenzione le sfide e le necessità funzionali seguenti:

- La crescita del grado di automatizzazione nel quadro del SOC tramite la corretta integrazione ed il consecutivo smistamento dei dati raccolti, in modo da generare allarmi realmente utili. L'integrazione del più gran numero di *data sources* e la capacità del loro filtraggio per poter identificare indicatori rilevanti sono ormai gli obiettivi dichiarati della



stragrande maggioranza delle ditte di sicurezza che forniscono soluzioni del tipo *big data analytics* destinate alle componenti della sicurezza cibernetica. È doveroso fare una parentesi personale, intendo dire che non facciamo qui riferimento alle soluzioni consacrate di tipo SIEM che, pur rilevanti nell'architettura di una struttura di tipo SOC, hanno sempre più un'efficacia limitata, in particolare per quanto riguarda la componente di prevenzione. Tra le soluzioni che abbiamo personalmente valutato in questo campo, molte non ci hanno convinto per le loro funzionalità, mentre alcune mi hanno scoraggiato quando ne ho saputo i costi.

- L'integrazione nelle tecnologie esistenti di *data sources* affidabili specifiche a indicatori di attacco o di compromissione è vitale. Anche qui, troviamo sul mercato un grande numero di *players*, sia tra i produttori di soluzioni di sicurezza che integrano nei loro propri prodotti o servizi delle funzionalità di *Cyber Threat Intelligence*, sia tra i fornitori specializzati che raccolgono dati da molteplici datasources rilevanti e le forniscono in formati diversi adattati al cliente. Però anche qui, il mercato non è di gran lunga maturo, e le differenze tra i prodotti e servizi sono talvolta molto grandi. Esse sono dovute soprattutto alle loro capacità di integrarsi con altre tecnologie (l'integrazione di una piattaforma di tipo CTI con una piattaforma analitica può rivelarsi vitale per generare allerte credibili di sicurezza), ma anche alla rapidità ed all'affidabilità degli indicatori forniti. Possiamo osservare, al giorno d'oggi, che numerose strutture comperano servizi di CTI che offrono loro indicatori di rilievo ma che non dispongono di capacità manuali od automatiche di uso o ricerca in funzione di quelli necessari alla propria attività, venendo a rendere tali soluzioni praticamente inutili per l'azienda.

- L'integrazione, nel quadro dell'architettura di sicurezza esistente, di soluzioni tecnologiche che utilizzano algoritmi di *machine learning*. Anche qui, sebbene esistano già sul mercato degli attori importanti che raccomandano la sostituzione totale delle soluzioni consacrate di sicurezza con tecnologie basate sul *machine learning*, rimaniamo personalmente molto cauti e non raccomandiamo al momento un tale approccio. Ditte di peso come la Microsoft, ad esempio, hanno già integrato nei loro servizi 'convenzionali' di sicurezza anche servizi che si basano su questo nuovo approccio. Microsoft e CrowdStrike propongono così soluzioni atte ad analizzare quantità enormi di dati raccolti nel cloud, mentre ditte come Dark Trace o VECTRA si basano sull'identificazione di anomalie tramite l'apprendimento del comportamento "normale" dell'infrastruttura monitorata. Le nuove tecnologie basate sul machine learning vengono ad offrire soluzioni uniche con un grande valore aggiunto per l'architettura di sicurezza di qualsivoglia azienda, facendo anche crescere in modo sostanziale il livello di funzionalità di un SOC. La nostra raccomandazione per le aziende, in questo campo, è di richiedere test estesi nella propria infrastruttura prima di acquisire tali tecnologie ed esigere che gli scenari dei test siano quanto più vicini alla realtà dell'azienda, perché i costi di acquisto e poi i costi aggiuntivi di tali soluzioni non sono da poco e devono essere messi a confronto svolgendo un'analisi comparativa tra prodotti e servizi che hanno, in verità, funzionalità molto simili tra di loro.

Senza avere la pretesa di aver coperto esaustivamente il soggetto e nemmeno abbordato tutti i suoi dettagli, crediamo che questo nostro testo, basato meramente sulla nostra propria esperienza, possa aiutare in una prospettiva manageriale un *decision-maker* nella sua comprensione del fenomeno e delle sfide con le quali si confronta ormai ogni azienda che desidera organizzare, realizzare e rendere operativo un suo Security Operation Center. ■

La rivoluzione dei robot ridefinisce saperi e competenze

INTERVISTA VIP con Roberto Cingolani

Roberto Cingolani

Autore : Massimiliano Cannata

Roberto Cingolani è un fisico che rientra nel novero dei "campioni" dell'innovazione italiana, con circa 48 brevetti al suo attivo. Autore e co-autore di circa 750 pubblicazioni su riviste internazionali e ha inoltre lanciato 3 aziende spin-off. La sua attività scientifica riguarda, in particolare, i settori della scienza dei materiali, delle nanotecnologie e della nanomedicina. Dal 2001 è membro di diversi Consigli della Commissione Europea nel campo delle nanotecnologie e dei nuovi materiali e membro del Consiglio della Presidenza del Comitato Nazionale per la Biosicurezza, le Biotecnologie e le Scienze della Vita. Per la sua attività di ricerca scientifica è stato insignito dei titoli di Alfiere del Lavoro (1981) e di Commendatore della Repubblica (2006) dal Presidente della Repubblica, nonché del premio Guido Dorso (2006) dal Senato della Repubblica e nel 2010 del premio Grande Ippocrate promosso da Unamsi e Novartis. Dal dicembre 2005 è direttore scientifico dell'Istituto Italiano di Tecnologia di Genova, eccellenza internazionale nel campo della ricerca applicata alle macchine intelligenti, basti pensare che la piattaforma umanoide più diffusa al mondo *"iCub"*, creata e testata nel capoluogo ligure, viene utilizzata in trentasei laboratori nel mondo come strumento di ricerca e sviluppo nella robotica. L'Istituto italiano è stato per altro tra i primi ad applicare l'ausilio di sofisticati strumenti meccanici nel delicato campo della riabilitazione. *Cybersecurity Trends* si trova insomma, nel contesto giusto per cercare di analizzare gli scenari di innovazione che si stanno aprendo, non solo sul versante della sicurezza e della protezione dei dati, ma anche più in generale per valutare i contraccolpi sociali e culturali di una "rivoluzione" destinata a cambiare la nostra vita.

L'intervista

Professore l'avvento dei robot ha determinato un profondo salto di paradigma e un cambio di passo probabilmente superiore a quello imposto da Internet e dal processo di digitalizzazione. Qual è il suo giudizio da esperto e ricercatore in merito?

Bisogna fare chiarezza su una differenza molto importante. Intelligenza artificiale, umanoidi, automazione, fanno parte di mondi diversi che presentano potenzialità, caratteristiche e pericoli diversi, L'automazione è essenzialmente un campo presidiato da robot che hanno una intelligenza algoritmica, con delle potenzialità utilizzabili per migliorare la produzione, affinare la qualità della manifattura e la sostenibilità, in una generale ottimizzazione dei processi. Per dirla in sintesi queste macchine dovrebbero finalmente permettere il sospirato innalzamento del PIL, riducendo nel contempo emissioni, impatto ambientale e consentendo un risparmio dell'energia.

Se prendiamo in esame l'intelligenza artificiale, quali riflessioni vanno fatte?

In questo caso siamo di fronte a un immenso computer, che può anche custodire la sua memoria in un luogo remotissimo, che è capace di fare miliardi di operazioni al secondo. Queste potenzialità esaltate da modelli di calcolo molto evoluti consentono a queste macchine di fare previsioni, analizzare e trovare correlazioni molto sofisticate. Basta pensare ai sistemi predittivi nel campo del fisco, della salute, del clima, per non parlare della efficienza di motori di ricerca come GOOGLE che ormai tutti siamo abituati ad usare. Il vantaggio che ci offrono queste macchine è evidente: la mente umana non sarebbe in grado di trattare una mole infinita di dati e informazioni e di ricavarne interpretazioni utili e plausibili, per imparare e soprattutto prevedere i fenomeni. Abbiamo dunque: da un lato un "tutto corpo" costituito dai robot, dall'altro "tutto mente".

Una dicotomia difficile da comporre, qual è il punto di connessione tra questi due versanti?

Provo a fare un esempio a tutti familiare: il telefonino. Ormai non possiamo più separarci da questo oggetto che di fatto è un'estensione del nostro io. Con il cellulare abbiamo migliorato le nostre *performance* mentali. Proviamo ora ad andare oltre e a mettere al nostro cellulare le braccia, creando uno strumento

che mette insieme le potenzialità intangibili dell'intelligenza artificiale e quelle pratiche della potenza meccanica.

Il connubio tra automazione e IT non è una minaccia per la specie

Il cambio di paradigma di cui tanto si discute comincia da qui?

Si innesca dall'incrocio tra l'universo dell'automazione, cui in fondo siamo abituati da decenni, le ruspe ci hanno sollevato dai lavori più pesanti da tempo e l'IT. E' questo il connubio che stiamo vivendo come una minaccia della specie, un connubio che conduce alla concreta progettazione e realizzazione di strumenti che non amplificano solamente le capacità mentali, come succede con il telefonino, ma che sono in grado di fare movimenti molto precisi che impattano in misura profonda sulle nostre esistenze.

Come vanno definite queste nuove "presenze" artificiali che stanno per popolare il nostro quotidiano?

Volendo essere realisti occorre dire che siamo ancora lontani dalla realizzazione di strumenti simili all'essere umano. Però se consideriamo la sembianza umanoide di oggetti che collegati al cloud e alle reti wireless, cominciano a praticare comportamenti intelligenti e, magari grazie a un'antenna, sono in grado di guidare una macchina, girare in casa, prendere bottiglie che desiderano al nostro posto e magari frugare nel frigorifero allora è evidente che lo scenario muta e la nostra fantasia corre molto in avanti.

A fronte di ritmi evolutivi che come sta descrivendo Lei si presentano molto rapidi e per certi versi sconvolgenti, cosa dobbiamo aspettarci?

Il futuro si prospetta come un ECOSISTEMA in cui avremo macchine intelligenti che comunicheranno sempre di più con l'essere umano. L'interrogativo di fondo riguarderà la nostra capacità culturale oltre che psicologica di interagire con una macchina, cosa che sappiamo fare perfettamente con il telefonino. La differenza sta nel fatto che questa macchina ci parla, ci prende le cose, si muove e può anche sostituirsi a noi, facendo cose per conto nostro. Le questioni di cui parliamo stanno ormai assumendo una valenza antropologica. La coesistenza umani – umanoidi, uomo - macchina spinta fino a livelli in cui la macchina pensa e prende decisioni apre scenari sicuramente impegnativi. Attenzione però: ricordiamoci che queste macchine non prenderanno il nostro posto, la biologia è ancora molto superiore, l'uomo possiede creatività, ormoni, sentimenti, passioni che non sono facilmente replicabili in laboratorio.

BIO

Roberto Cingolani è Direttore Scientifico dell'Istituto Italiano di Tecnologia (IIT) di Genova dal dicembre 2005. Programma e supervisiona la realizzazione del Piano Scientifico coordinando l'attività dei Dipartimenti del laboratorio centrale di Genova e dei Centri della rete multidisciplinare promossa sul territorio nazionale insieme a università e istituti di ricerca d'eccellenza. Tra i "campioni" dell'innovazione italiana, conta circa 48 brevetti al suo attivo, è autore e co-autore di circa 750 pubblicazioni su riviste internazionali e ha inoltre lanciato 3 aziende spin-off. La sua attività scientifica riguarda, in particolare, i settori della scienza dei materiali, delle nanotecnologie e della nanomedicina. Nel 2000 ha assunto il ruolo di professore ordinario di Fisica Generale presso il Dipartimento di Ingegneria dell'Innovazione dell'Università del Salento. Nel 2001 ha fondato e diretto fino al 2004 il Nanotechnology National Laboratory (NNL) dell'Istituto Nazionale di Fisica della Materia del CNR. È stato Visiting Professor alla Virginia Commonwealth University (VCU) e alla University of Tokyo, nonché staff member al Max Planck Institut (Stoccarda). Dal 2001 è membro di diversi Consigli della Commissione Europea nel campo delle nanotecnologie e dei nuovi materiali e membro del Consiglio della Presidenza del Comitato Nazionale per la Biosicurezza, le Biotecnologie e le Scienze della Vita. Per la sua attività di ricerca scientifica è stato insignito dei titoli di Alfiere del Lavoro (1981) e di Commendatore della Repubblica (2006) dal Presidente della Repubblica, nonché del premio Guido Dorso (2006) dal Senato della Repubblica e nel 2010 del premio Grande Ippocrate promosso da Unamsi e Novartis. È laureato in Fisica ed ha conseguito il dottorato in Fisica presso l'Università degli Studi di Bari. Ha inoltre ottenuto il diploma di perfezionamento in Fisica alla Scuola Normale Superiore di Pisa.

Verso la rivoluzione dei saperi tradizionali

A che punto è la ricerca in questo delicato settore? Le macchine intelligenti che cosa saranno abilitate a fare e in quali ambiti dobbiamo prevederne la maggiore diffusione?

In linea di principio abbiamo già le macchine molto intelligenti e dei robot che già si muovono come noi. L'essere umano esprime però un nesso mente corpo che è frutto di tre miliardi di anni di evoluzione, cosa difficile se non impossibile da imitare per quella che resta per

delle macchine al nostro servizio, che potranno sostituire l'uomo negli incarichi gravosi, quelli più rutinari, pesanti, assistendoci in tutte quelle cose in cui è richiesta una grande capacità di calcolo. Come dicevo prima la ruspa faceva già il lavoro dei cantieri, oggi si è aggiunto il robot che svolge delle mansioni in ufficio, il problema sarà quando avremo una "ruspa intelligente" che si muove, spingendosi a livelli ancora poco prevedibili. Nessuna macchina potrà mai avere una capacità computazionale paragonabile a quella del cervello umano, perché avremmo bisogno di una stanza molto grande per replicare tutti i circuiti neuronali che presiedono alle nostre facoltà superiori con uno spreco enorme di energia. L'innovazione con cui dovremo fare i conti ci proporrà un telefonino che avrà gambe e braccia, che svolgerà delle faccende fisiche e non solo mentali, rimanendo collegato a una struttura di rete potente e veloce, sono queste le due connotazioni distintive della rivoluzione digitale in atto.

I ricercatori del'IIT di Genova in quali settori stanno focalizzando il loro lavoro di studio e di sperimentazione?

"ICub" la nostra piattaforma umanoide è la più diffusa al mondo, sono trentasei i laboratori sparsi nel globo che la utilizzano come strumento di ricerca e sviluppo nel campo della robotica. Abbiamo macchine che coprono il variegato universo della zoologia, dal robot centauro, al quadrupede, al bambino, applichiamo inoltre la robotica all'assistenza per la riabilitazione. Nel mondo le strutture veramente competitive saranno sette otto, quello che veramente formidabile è l'accelerazione della ricerca in questo campo. Intelligenza artificiale, automazione, Information Technology sono ambi ti che si intrecciano. Tutto quello che rientra nella ritessitura del delicato nesso corpo - mente, avvicinandosi alla meravigliosa armonia che caratterizza l'essere umano, apre la strada a una disciplina nuova. Tanto che non è più corretto parlare di Robot o di intelligenza artificiale, perché siamo di fronte a tecnologie biomimetiche che cercano di riprodurre l'essere più perfetto che esiste in natura: l'essere umano. In questo percorso difficile e impegnativo c'è spazio per le competenze più disparate, mentre si sta attuando una profonda rivoluzione delle discipline e dei saperi tradizionali, che credevamo immodificabili.

Qualche hanno fa Giuseppe Longo in un celebre saggio ha cercato di definire il profilo del "Simbionte", di fatto una ibridazione tra l'homo sapiens e l'homo technologicus. Al di là di questa immagine per alcuni aspetti suggestiva per altri inquietante, quali sono i livelli di interazione tra uomo e macchina e cosa dobbiamo aspettarci da questa necessaria ma anche difficile convivenza, che sollecita analisi e riflessioni di varia natura: epistemologica, filosofica, sociologica oltre che tecnico ingegneristica?

I ricercatori che operano in questo campo si trovano dentro un incrocio fittissimo di relazioni. Studiano di fatto biomeccanica con i medici, il sistema nervoso con i neuroscienziati, si intendono di computer scientist e si misurano con i matematici da un lato e con gli ingegneri per affrontare questioni di *material scientist*. Serve padronanza in discipline che vanno dalla medicina alla chimica, alla fisica, dal momento che stiamo provando proviamo a far dialogare un corpo e una mente artificiale. Per non parlare delle implicazioni filosofiche, epistemologiche ed etiche che entrano in gioco. Avremo delle macchine che sono in grado di guidare, e che seguiranno criteri e regole. Nel caso in cui si verifica un guasto meccanico, ai freni per esempio: la macchina chi salverà: il pilota, i pedoni, il bambino che magari si trova col papà in auto. Un individuo agisce seguendo l'istinto di conservazione della specie, la macchina farà un veloce calcolo e sceglierà lo scenario potenzialmente meno dannoso. Sarà il calcolo probabilistico a farla decidere, non eiste infatti una componente ormonale in uno strumento artificiale. Ma la macchina robot sarà in grado di fare la scelta giusta? Se ha deciso per una opzione violando una regola per salvaguardarne un'altra, ha commesso un reato e quindi deve essere perseguibile. Non esiste però un codice civile penale differenziando che possa chiamare in causa un sistema non biologico, in grado di commettere un reato. Non stiamo parlando di uno scenario fantascientifico, ma di qualcosa che comincerà a interessare la nostra quotidianità, su cui il anche il diritto sarà chiamato a fare dei passi avanti per reggere il vento dell'innovazione.

Diritto e tecnologie: la nuova frontiere

I rapporti tra diritto e nuove tecnologie aprono territori realmente molto difficili da tracciare. Sapremo venirne a capo?

Non abbiamo altra scelta. Bisogna prendere atto che non c'è più la separazione tra discipline umanistiche e scienze esatte. Gli intellettuali devono sedersi a un unico tavolo e parlare in maniera aperta con scienziati e ingegneri di tutti i rami del sapere fisi. Anche la ricerca spaziale dovrà essere coinvolta: un giorno gli uomini migreranno su altri pianeti, non è solo una faccenda che può appassionare gli astrofisici, perché ad essere coinvolti saranno sociologi, storici, antropologi, giuristi. Saremo infatti chiamati a concepire nuove forme di società, una diversa trama dei rapporti umani. Quando l'umanità apre un versante inesplorato di conoscenza il corso dell'evoluzione cambia marcia, in quel momento tutte le discipline sono chiamate a contribuire al "salto" di paradigma. Per questo credo che l'intuizione di Giuseppe Longo, cui la sua domanda si rifaceva, è quanto mai attuale e pertinente.

Il mondo del lavoro risentirà gli impatti più forti del cambiamento in atto. In un recente intervento apparso su un quotidiano nazionale diceva molto opportunamente che non sarà certo facile trasformare un operaio in esperto di coding e auspicava un nuovo patto sociale per educare il cittadino a muoversi in un nuovo orizzonte delle opportunità. Significa che dovremo abituarci all'idea che l'automazione sottrarrà posti di lavoro o esistono delle contromisure adeguate?

La paura che l'automazione sottragga posti di lavoro è assolutamente giustificata e comprensibile. Occorre dire che se vogliamo continuare a crescere secondo modelli economici dominanti, il rischio che le macchine possono distruggere i lavori di routine esiste. Il fenomeno come è noto non è inedito. La differenza rispetto al passato sta nella velocità con cui la rivoluzione si sta attuando. Telefono e motore a scoppio hanno dato all'umanità un tempo significativo, che abbiamo sfruttato per abituarci, Adesso tutto è successo nel giro di dieci anni. Difficile riuscire a riconvertire un lavoratore che ha perso il posto aggiornando con estrema rapidità le sue competenze. Quando parlavo di patto sociale mi riferivo essenzialmente al fatto che oggi tutte le componenti devono impegnarsi per trainare la società nel suo complesso verso livelli più alti di competenza e preparazione. Occorre creare una catena diffusa di *continuus learning*, una società capace di parlare a tutti i livelli della scala sociale per rendere la gente consapevole di quello che sta avvenendo.

Potremmo definire questa sua proposta usando il celebre scritto del Premio Nobel Ilya Prigogine che auspicava una "Nuova Alleanza", traducibile oggi in un patto educativo che veda finalmente schierati in una logica collaborativa le agenzie della formazione, la scuola, e perché no la politica e persino i sindacati e i corpi intermedi?

Un progetto di vasta portata dovrebbe essere messo in atto. La fase eccezionale che stiamo vivendo richiede misure eccezionali. La tecnologia diffusa non deve essere un tabù, una scatola nera che i più ignorano. Nelle nostre aule si continua a insegnare con la giusta attenzione e rigore materie come l'italiano, il latino, dovremmo però allargare la soglia di impegno a discipline che vanno dall'informatica al *coding*, perché il nuovo alfabeto dell'universo digitale è sostanziato da questi mattoni del sapere.

Formazione e sicurezza sono le sfide da vincere

La formazione e il trasferimento tecnologico rimangono le leve strategiche, più utili per sfruttare al meglio le opportunità legate a questa grande rivoluzione. Dovranno mutare anche i criteri di recruiting seguiti fino ad oggi per individuare i profili richiesti da un mercato in continuo divenire?

Quando svolgiamo un'attività di recruiting dovremmo tenere conto della tipologia di attività svolte dal profilo che ci interessa. Se il nostro candidato non ha avuto la possibilità di fare un mestiere che, lo ha "obbligato" ad aggiornarsi continuamente, dovremo fare in modo di stimolarlo a riaprire l'orizzonte dell'apprendimento con le giuste metodologie. Nella società digitale è facile per tutti noi diventare "dinosauri" perché l'obsolescenza delle conoscenze è molto rapida. Se non diamo spazi di studio e di approfondimento attuando processi di *lifelong learning* anche dentro le aziende rischiamo di emarginare miliardi di persone. Non innaffiare un capitale umano di tale portata non possiamo permettercelo, direi di più: nessun paese civile se lo può permettere se vuole stare al passo con i tempi.

A proposito di consapevolezza. Cybersecurity Trends è la rivista della Fondazione GCSEC di Poste Italiane che ha come mission la diffusione di una equilibrata cultura del digitale e dell'uso della rete in tutte le fasce della popolazione. Sotto lo specifico profilo della sicurezza, l'automazione, la catena di montaggio robotizzata e più in generale le applicazioni della robotica in ambiti delicati come la medicina e l'assistenza socio-sanitaria sono trasformazioni organizzative e di processo che presentano fattori di rischio?

L'aspetto più delicato della rivoluzione che abbiamo cercato di tratteggiare e che riguarda i profili di *governance* del rischio, riguarda la gestione delle banche dati, che vengono immagazzinate e rielaborate dalle macchine intelligenti. Basta pensare all'enorme quantità di dati che riguardano la sanità, che incrociati con le importanti capacità predittive e previsionali di cui disponiamo possono dare tutto il percorso futuro della vita di un individuo. Le conseguenze di tutto questo sono facilmente immaginabili, sul piano della discriminazione ma anche del controllo che ne deriva. Il fenomeno è pericoloso, la preoccupazione maggiore risiede nel fatto che i detentori di questo enorme magazzino di informazioni sono player privati. E' questo il tema vero che chiama in causa le autority, gli stati, e più in generale l'etica e il diritto alla privacy e alla riservatezza.

Come si vede la frontiera tra filosofia, diritto, etica, rispetto della persona è tutta da ripensare e da aggiornare. La sfida è appena cominciata. La rivoluzione che stiamo vivendo ha bisogno che le menti più avvertite e responsabili si facciano portavoce di una riflessione globale. Il mondo sotto i nostri piedi sta cambiando non possiamo assistere a tutto questo da spettatori passivi, perché saremmo condannati a un declino certo e ìrreversibile. ■

Virtual Security Analysts

Autore: Uday Veeramachaneni

Il settore della sicurezza ha fatto un ottimo lavoro nel creare rumore e aspettative intorno al tema del "Machine Learning" o "Intelligenza Artificiale".

Le industrie del settore sostengono che il problema stia nelle regole, troppi attacchi non identificati e troppi falsi allarmi e pertanto le tecnologie di Machine Learning rappresentano la soluzione a queste tipologie di problemi.

PatternEx, ad esempio, sta lavorando su questa tematica. Umani e computer devono collaborare per identificare i modelli di cyber attacco che sono in evoluzione nascosti fra i nostri dati. Il segreto è comprendere come le macchine e gli esseri umani possano collaborare e istruirsi a vicenda per combattere in modo efficace le minacce emergenti.

Il Machine Learning funziona senza regole e può intercettare attacchi che sfuggono all'analisi tradizionale. Ma cosa risolve? Quali sono i compromessi?

BIO

Uday Veeramachaneni è il co-fondatore e CEO PatternEx, la cui idea è di utilizzare l'intelligenza artificiale per accelerare il rilevamento e l'analisi delle minacce nel dominio della sicurezza delle informazioni. Uday ha conseguito un master in economia e informatica e utilizza la sua esperienza per sviluppare sistemi di apprendimento automatico che aiutano le aziende a proteggere i propri dati. Uday si è occupato della gestione prodotti e soluzioni per alcune delle migliori aziende nel settore della sicurezza e delle infrastrutture come Citrix e Riverbed, inoltre ha lavorato presso start-up e grandi aziende tra cui Juniper Networks e Motorola.

Per spiegare questo in dettaglio, è utile organizzare l'universo del Machine Learning in tre distinte tipologie utilizzate nel settore della sicurezza:

1. Unsupervised Machine Learning
2. Static Supervised Learning
3. Active Supervised Learning

Unsupervised Machine Learning

La maggior parte di ciò che sentiamo essere pubblicizzato come "rilevamento avanzato delle minacce" è l'apprendimento automatico senza supervisione o semplicemente il rilevamento di anomalie. Questo approccio è ampiamente usato in molti domini per organizzare i dati e trovare valori anomali in quei dati. Nella sicurezza informatica, l'Unsupervised Machine Learning analizza il log o il pacchetto dati e cerca di trovare valori anomali nei dati. Ciò ha senso perché la stragrande maggioranza dei comportamenti online è legittima e i comportamenti dannosi potrebbero essere anomali.

Sfortunatamente, le relazioni tra le imprese e i loro dipendenti, partner, fornitori e clienti sono estremamente complesse. I comportamenti variano ampiamente e ciò che sembra essere un'anomalia potrebbe invece rivelare della normale attività.

Ad esempio, potresti venire a sapere che c'è una sottrazione di dati in Ucraina per poi scoprire che c'è un appaltatore legittimo che lavora lì per una divisione diversa.

La promessa dell'Unsupervised Learning è attenuata da una sfumatura importante che illustra il difetto logico in questo approccio: la definizione di

(Continua a pagina 31)

PSD2 e sicurezza. Blockchain quali scenari possibili?

Autori : Luca Faramondi, Francesco Leccese, Francesco Peverini

La data del 13 gennaio 2018 è ben evidenziata sul calendario di chiunque interagisca, più o meno direttamente, con il mondo bancario. Poco più di un mese ci separa dall'entrata in vigore della direttiva 2015/2366/UE anche nota come PSD2. Le maggiori innovazioni introdotte da tale normativa sono ben note: da una parte vi è l'introduzione di nuovi soggetti all'interno del mercato, dall'altra troviamo l'introduzione di nuovi strumenti di autenticazione per l'accesso ai sistemi di pagamento elettronici.

Per quanto riguarda l'innovazione che verrà introdotta in risposta ai nuovi parametri di sicurezza per l'avvio di una transazione elettronica, molte aziende hanno già iniziato ad adottare numerose soluzioni ben collaudate e che rispondono pienamente ai vincoli introdotti dalla PSD2. Inoltre, il crescente numero di sistemi di sicurezza intrinsecamente previsto nei nuovi smartphone, tablet e computer ben si coniuga con i vincoli che a breve saranno introdotti.

È infatti l'introduzione dei nuovi soggetti nel mercato, AISP (Account Information Service Provider) e PISP (Payment Initiation Service Provider), a destare maggior preoccupazione in chi è responsabile dell'adeguamento dei servizi bancari nei termini richiesti dalla nuova normativa.

Il compito principale dell'AISP è quello di "collettore di informazioni" provenienti da fonti differenti al fine di elaborare e mostrare un report dettagliato dei dati ottenuti dalle diverse fonti.

Dal punto di vista del cliente, un esempio di servizio offerto dall'AISP, potrebbe essere la presentazione di un report statistico circa l'utilizzo di tutti i suoi conti, non necessariamente ospitati dalla stessa banca.

Il PISP, invece, occupa la posizione di canale di comunicazione tra il cliente e la banca, erogando un servizio di interfacciamento necessario a dare l'input alla transazione da eseguire.

In entrambi i casi, sia quello di acquisizione delle informazioni da parte dell'AISP, che quello di avvio della transazione mediante PISP, emerge la necessità di rendere accessibili, a servizi forniti da terze parti, i dati che fino ad oggi sono stati custoditi, gestiti ed aggiornati solo ed unicamente dalla banca proprietaria.

Possiamo dunque affermare che la nuova direttiva causerà necessariamente un'evoluzione dell'attuale sistema bancario trovando un nuovo equilibrio in cui le banche perderanno il ruolo centrale ed autoritario attualmente ricoperto. Allo stesso tempo nasceranno numerosi servizi, gestiti da terze parti, a cui ogni cliente potrà affidare il ruolo di tramite o gestore delle proprie informazioni bancarie.

Questo nuovo futuro equilibrio non si differenzia dall'attuale scenario solo per la presenza di nuovi soggetti del mercato ma comporta un riassetto dell'attuale aspetto organizzativo oltre che infrastrutturale.

Se da una parte l'avvento dell'introduzione della PSD2 sembra rappresentare un serio problema di business dovuto alla perdita del legame diretto tra istituto bancario e cliente, dall'altra può rappresentare l'occasione per un nuovo design della catena di servizi coinvolti nei pagamenti.

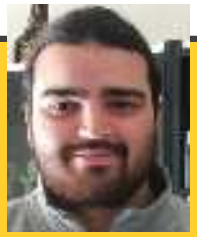
Tale occasione consiste nella possibilità di importare nuove tecnologie e nuovi strumenti proponendo un'acquisizione di conoscenze da altri settori, non necessariamente affini a quello bancario, al fine di costituire le fondamenta del nuovo quadro di riferimento.

Lo scopo di questo articolo vuole essere quello di descrivere tali tecnologie affrontando tematiche la cui validità scientifica è indiscussa e che allo stesso tempo rappresentano temi caldi ampiamente dibattuti.

La prima proposta consiste nell'introduzione della distributed ledger technology come strumento di archiviazione delle transazioni bancarie. Progetti come BitCoin, Ripple ed Ethereum, sono solo alcuni esempi di progetti circa l'applicazione di distributed ledger in ambito economico-finanziario. Le proprietà di replicazione e preservazione dell'integrità dei dati rappresentano i due grandi vantaggi introdotti da tale sistema rispetto alle attuali implementazioni di registrazione delle transazioni bancarie.

BIO

Luca Faramondi, Ph.D. Ricopre attualmente la posizione di assegnista di ricerca presso il laboratorio di Sistemi Complessi e Sicurezza del Campus Bio-Medico di Roma. I suoi interessi di ricerca sono nel campi dell'identificazione delle vulnerabilità di sistemi distribuiti, dei cyber physical systems e dei problemi di ottimizzazione. Autore di varie pubblicazioni scientifiche, nel 2014 è stato finalista per il "CIPRNet Young Critis Award". La sua tesi è stata premiata come miglior tesi di laurea nel campo delle infrastrutture critiche dall'Associazione Italiana esperti in Infrastrutture Critiche (AIIC) nel 2016. Nel 2017 ha ottenuto il titolo di dottore di ricerca in Ingegneria Informatica ed Automazione.



BIO

Francesco Peverini, Dottore in Matematica. Ha conseguito il titolo di laurea magistrale il 28 Aprile 2017 presso l'Università degli Studi di Perugia. Il suo lavoro di tesi, in ambito crittografico, ha riguardato la costruzione pratica di un innovativo Secret Sharing Scheme. Attualmente collabora come stagista presso GCSEC, occupandosi di uno studio riguardo le possibili vie di implementazione della Blockchain e delle nuove tecnologie crittografiche in ambito PSD2.

BIO

Francesco Leccese, Dottore in Matematica. Ha conseguito il titolo di laurea triennale il 25 Febbraio 2015 presso l'Università degli Studi di Perugia. E' laureando magistrale in Matematica per la Sicurezza Informatica con una tesi di stampo crittografico incentrata sulle Curve Ellittiche applicate nella Blockchain. Attualmente collabora come stagista presso GCSEC, occupandosi di uno studio riguardo le possibili vie di implementazione della Blockchain e delle nuove tecnologie crittografiche in ambito PSD2.

Il secondo suggerimento nella ridefinizione del framework, supportato da numerose pubblicazioni, va di pari passo con l'adozione dello standard open banking. Lo sviluppo di open API per la fruizione di servizi erogati dalle banche ben si sposa con l'introduzione dei nuovi attori inseriti e definiti dalla PSD2 come erogatori di servizi per il cliente.

L'ultimo aspetto innovativo proposto riguarda l'utilizzo di tecniche crittografiche che stanno prendendo sempre più piede nell'ambito del cloud computing. Tali strumenti assumono fondamentale importanza nel momento in cui, come richiesto dalla PSD2, servizi gestiti da terze parti richiedono l'accesso parziale a documenti e dati di proprietà di altri attori al fine di analizzarli senza necessariamente disporre di un accesso completo.

La Blockchain Technology

La Blockchain Technology è una delle strade fortemente battute al fine di integrare nuove caratteristiche di sicurezza nel sistema di salvataggio delle transazioni.

Una Blockchain rappresenta una struttura dati composta da blocchi concatenati nel rispetto di vincoli di integrità delle informazioni contenute in essa. Ciò significa che se si intende corrompere un dato registrato in un blocco, l'intera struttura risulterebbe compromessa evidenziando il tentativo di corruzione. Per definizione, la Blockchain consiste in una serie di copie di tale struttura che viene condivisa, replicata e sincronizzata da entità distribuite geograficamente sul territorio.

Il processo di aggiornamento dei dati all'interno di questo tipo di struttura è descritto dai seguenti passaggi semplificati. Nel momento in cui viene eseguita una nuova transazione essa viene registrata in un blocco di informazioni che sarà inviato a tutti i nodi della rete per essere validato, cioè per effettuale un controllo circa la bontà delle informazioni aggiunte. Raggiunto il consenso tra i nodi della rete in merito all'integrità dei dati, tale informazione viene aggiunta da ogni nodo alla propria copia locale delle Blockchain mantenendo aggiornato ed allineato lo stato della propria copia rispetto agli altri nodi.

Tra le tematiche che vanno affrontate per poter adottare tale tecnologia è necessario far luce su chi detiene l'autorità sulla gestione dei dati e su chi può utilizzarli. Nella sua concezione iniziale la Blockchain nasce come una struttura decentralizzata che non necessita di una Certification Authority definita. Risulta quindi evidente che, come precedentemente anticipato, l'utilizzo di questa tecnologia non propone solo una riprogettazione infrastrutturale ma comporterebbe anche una revisione gestionale ed organizzativa dell'attuale mercato.

Molti sono gli studi che cercano di trovare il modo di adattare questo strumento nel contesto della PSD2, cercando di risolvere problemi come la diminuzione dei tempi di accesso ai dati, l'utilizzo di tecniche crittografiche per la salvaguardia dei dati e l'individuazione dei possessori delle chiavi di accesso alle informazioni custodite nei blocchi.

Crittografia Omomorfica

La natura di intermediatore di PISP ed AISP porta come diretta conseguenza la necessità di definire come i Third Party Providers (TPPs) possano consultare e gestire nella maniera più sicura possibile i dati custoditi dagli istituti bancari. Un utile strumento matematico, la crittografia omomorfica, lavora in tal senso

permettendo uno scambio di informazioni tra client e server basato su una comunicazione sicura. Più precisamente la crittografia omomorfica può essere vista come una scatola capace di elaborare dati crittografati sconosciuti di e fornire il risultato esatto di operazioni eseguite sui dati, nonostante non si abbia una chiara visione dei dati originali. Attualmente lo studio di tale tecnologia è di forte interesse nell'ambito del Cloud Computing ma suggerisce una via concretamente percorribile per rispondere alle problematiche di accesso ai dati di una possibile richiesta effettuata ad un AISP. Attraverso l'applicazione di algoritmi basati sulla crittografia omomorfica l'AISP potrebbe essere in grado di calcolare il saldo totale di più conti bancari senza conoscere il dato non crittografato dei saldi di ciascun conto.

OpenAPI e Web Services

La prima richiesta della PSD2 alle banche è quella di poter permettere ai nuovi TPPs di accedere ai dati custoditi dagli istituti bancari al fine di erogare i propri servizi.

In realtà l'Open Banking da anni sta remando in questa direzione, proponendo l'istituzione di servizi web al fine di promuovere l'interazione tra le banche.

La più classica struttura di un servizio web prevede la realizzazione di un servizio locale residente sui server di un'istituzione al quale è possibile interfacciarsi attraverso l'utilizzo di una interfaccia rappresentata dalle open APIs. Da una parte, chi eroga il servizio mostra pubblicamente un elenco di strumenti utilizzabili, diffondendo con il grado di sicurezza desiderato l'accesso a tali prodotti. Dall'altra parte, chi usufruisce di tali servizi ottiene l'accesso, secondo quanto deciso dalla policy dell'erogatore, e le informazioni circa l'utilizzo degli strumenti messi a disposizione tramite il servizio web. Allo stesso tempo ogni dettaglio implementativo ed ogni informazione parziale necessari per l'erogazione del servizio restano invisibili al richiedente.

Conclusioni

Gli argomenti trattati nascono in concomitanza di uno studio che mira alla ricerca di percorsi percorribili e scientificamente sostenuti le cui caratteristiche suggeriscono una sorta di complementarietà con le tematiche legate all'introduzione dei TTPs previsti dalla PSD2. ■

Virtual Security Analysts

(In seguito a pagina 28)

"anomalia" non è la definizione di "malevolo". Confondendo i due si finisce per trattare moltissimi falsi positivi.

Static Supervised Learning

A differenza del l'Unsupervised Machine Learning, lo Static Supervised Learning riceve gli input dagli esseri umani per creare modelli. Pensiamo ai modelli di Supervised Learning come a sistemi che "pensano" come gli umani e apprendono nel corso del tempo. I data scientists raccolgono feedback dall'uomo, poi formano un modello con quel feedback, impiegandolo poi in produzione. Questo processo di apprendimento spesso richiede mesi o addirittura anni a seconda di quando e dove vengono integrati i nuovi feedback umani.

Questo tipo di modello funziona in ambienti statici in cui ciò che stiamo cercando di prevedere non ha grosse variazioni. Ma "statico" non descrive il mondo della sicurezza informatica. La realtà legata al mondo della Cybersecurity è caratterizzato da dinamismo: una realtà nella quale l'attaccante modifica continuamente i suoi comportamenti per riuscire ad attaccare il sistema. Realtà nella quale gli attaccanti cambiano tecniche e comportamenti molto più velocemente di quanto i modelli di apprendimento supervisionati possano essere preparati.

Come è possibile, pertanto, aggiornare i modelli in tempo reale?

Active Supervised Learning

Per portare l'intelligenza artificiale nel dominio della cybersecurity, l'Active Supervised Learning risulta essere l'approccio ottimale. L'apprendimento attivo è un modo per formare modelli di Supervised Learning in tempo reale, senza procedere con milioni di esempi che devono alimentare le macchine per la formazione.

L'Active Supervised Learning offre la promessa di un apprendimento supervisionato con un periodo di training delle macchine veramente ridotto.

Il sistema coinvolge continuamente gli analisti per imparare da loro e creare nuovi modelli di Supervised Learning. Chiamiamo questi modelli Virtual Analyst perché sono in grado di distinguere tra schemi di comportamento malevoli e normali con grande precisione, come un analista umano.

Il termine Virtual Analyst implica anche che dobbiamo pensare a come integrarli nei nostri processi di sicurezza. Dispiegati correttamente, possono fornire enormi benefici ad un'organizzazione per migliorare la sua capacità di difesa e possono agire, inoltre, come sistemi di early warning. ■

Fake News – Cosa sta succedendo?

Autore : Gianluca Bocci

La comunicazione ha subito nel tempo un continuo mutamento; all'inizio era basata su semplici gesti, poi arrivarono le parole e dunque, i primi sistemi di scrittura. Ma è con lo sviluppo della stampa e a seguire con altre invenzioni come il telegrafo, il telefono, la radio e la televisione, che ebbe inizio la divulgazione delle informazioni e della conoscenza su larga scala, al punto da influenzare profondamente e rapidamente lo sviluppo sociale di diverse generazioni.

BIO

Gianluca Bocci, laureato in Ingegneria Elettrica presso l'Università La Sapienza di Roma ha conseguito un Master Universitario di 2° livello presso l'università Campus Bio-Medico di Roma in "Homeland Security - Sistemi, metodi e strumenti per la Security e il Crisis Management". Attualmente è Security Professional Master nella funzione Tutela delle Informazioni di Tutela Aziendale, nella direzione Corporate Affairs di Poste Italiane. Certificato CISM, CISA, Lead Auditor ISO/IEC 27001:2013, Lead Auditor ISO/IEC 22301:2012, CSA STAR Auditor e ITIL Foundation v3, supporta le attività del CERT e del Distretto Cyber Security di Poste Italiane; in tale ambito ha maturato una pluriennale esperienza nella sicurezza delle applicazioni mobili, anche attraverso attività di ricerca e sviluppo realizzate con il mondo accademico. Precedentemente, presso importanti multinazionali ICT, in qualità di Security Solution Architect, ha supportato le strutture commerciali nell'ingegneria dell'offerta tecnico-economica per Clienti di fascia enterprise, con particolare riferimento ad aspetti di Security Information and Event Management, Security Governance, Compliance e Risk Management.

In queste circostanze la politica è, "quasi sempre ed ovunque", intervenuta per disciplinare il corretto utilizzo dei mezzi di comunicazione, con l'obiettivo d'impedirne l'abuso e di conseguenza tutelare i cittadini, le imprese pubbliche e private, nonché lo Stato stesso. Un salto quantico nella trasformazione dei processi comunicativi avviene però con l'avvento delle tecnologie digitali e in particolare con l'uso dei computer e delle reti dati; strumenti questi, inizialmente utilizzati dalle forze militari e dalle comunità scientifiche e in seguito dalle grandi organizzazioni e singoli cittadini, negli ultimi anni anche in un regime di completa mobilità. Di fatto la rete ha definitivamente abbattuto ogni sorta di barriera spazio-temporale, consentendo di accedere a qualunque tipo d'informazione e a un numero illimitato di servizi, tra cui quelli per lo sviluppo delle relazioni sociali; ne sono un esempio, le chat, i blog, i forum e i social network[1]. La rete ha dunque permesso, in uno spazio "libero", di andare oltre i modelli tradizionali della comunicazione, consentendo alle persone, da una parte, di essere sempre e comunque informate sui fatti grazie ad un patrimonio informativo dalle dimensioni infinite e sempre aggiornato, e dall'altra, di condividere esperienze, opinioni e sensazioni personali, diventando per la prima volta dei veri e propri *"contributor"* dell'informazione. Purtroppo però la rete in questi ultimi anni, rispetto a quella *"libertà"* tanto decantata, ha fatto emergere alcuni nuovi problemi e in particolare quello dell'attendibilità delle informazioni che possono essere alterate e\o manipolate (le c.d. *fake news*), al punto da generare disinformazione, indipendentemente dal fatto che sia accidentale (*misinformation*) o intenzionale (*disinformation*); disinformazione che può essere utilizzata per le più diverse ragioni come, ad esempio, influenzare l'opinione pubblica, istigare all'odio, danneggiare l'immagine di aziende, offendere e\o minacciare le persone e molto altro ancora. Adottare delle regole per avere un'informazione di qualità in rete sta dunque diventando un'esigenza sempre più impellente.

Alcune iniziative per la prevenzione e il contrasto delle fake news

Per rendersi conto della dimensione del fenomeno basta poco; inserendo in un qualunque motore di ricerca frasi come "bufale in rete", "le più grandi fake news in rete" e parole chiavi similari, si trova di tutto su quanto è "apparentemente" accaduto e raccontato dalla rete. Il quotidiano "La Stampa", con un articolo pubblicato online[2], riferisce testualmente: *"Il 2016 passerà alla storia anche come l'anno in cui siamo entrati nell'epoca delle post-verità. Quello delle 'bufale' non è un fenomeno nato negli ultimi 12 mesi, ma in quest'arco di tempo sempre più siti, blog e account hanno cominciato a proliferare sul web incessantemente per lucrare sulle 'fake-news', ma anche solo per generare odio e malcontento".* C'è in pratica di tutto, dai fantomatici sismologi intervenuti in rete per parlare dei complotti che le istituzioni avrebbero architettato pur di non pagare i danni ai cittadini in riferimento agli ultimi terremoti che hanno colpito l'Italia centrale, al finto e già defunto Umberto Eco che avrebbe, attraverso le sue dichiarazioni, cercato d'influenzare il referendum abrogativo del Dicembre dello scorso anno; a seguire le false dichiarazioni di politici e ancora sulle origini della meningite e di come questa è stata veicolata in giro per il mondo e poi ancora di tutto e di più sulle scie chimiche, i microchip impiantati sotto la pelle degli uomini per il controllo delle mente, fino a tutti i falsi che hanno incessantemente accompagnato Donald Trump e Hillary Clinton durante la loro campagna elettorale per le presidenziali americane. Proprio su quest'ultimo punto è tornata, poco prima dell'estate, Hillary Clinton con un suo intervento presso il Wellesley College. Senza mai riferimento al proprio avversario, che poi ha vinto, la Clinton ha fatto alcune interessanti affermazioni: *"Vi state laureando in un momento in cui sta avvenendo un assalto totale alla verità e alla ragione. Basta connettersi per 10 secondi ai social media per venirne colpiti direttamente in faccia"*[3] e *"Nei prossimi anni, vi confronterete con fiumi di troll, sia online che di persona, impazienti di dirvi che non avete nulla di sensato da dire o nulla di significativo con cui contribuire alla società, potrebbero anche arrivare a definirvi una donna maligna (nasty woman)".* Il problema delle fake news deve essere però d'interesse anche per le aziende, in particolare quelle maggiormente esposte da un punto di vista mediatico, dal momento che una falsa dichiarazione potrebbe avere delle ripercussioni sulla loro reputazione, come è recentemente accaduto a Sturbuck[4]. La domanda sorge dunque spontanea, cosa si può fare per arginare questo fenomeno? Da come si stanno muovendo alcuni Stati e organizzando i grandi *"big"* della rete, sembra che i margini di manovra passano per diversi tipi d'intervento, alcuni di natura legislativa, altri di natura tecnologica. In Francia e in Germania sono state avviate alcune iniziative per verificare l'attendibilità delle informazioni, con l'obiettivo di rimuovere quelle false; ad esempio, in

> *C'è in pratica di tutto, come il finto e già defunto Umberto Eco che avrebbe, attraverso le sue dichiarazioni, cercato d'influenzare il referendum dello scorso anno.*

Germania è recentissima l'entrata in vigore di una legge che obbligherà i social network con oltre due milioni di utenti, a rimuovere contenuti che incitano all'odio (hate speech), pubblicano pagine false e offensive, espongono minacce, e così via. L'attuazione della legge sarà garantita da circa cinquanta dipendenti del ministero della Giustizia che controlleranno l'applicazione della norma. La legge, in vigore dal mese di Gennaio 2018, presenta un impianto sanzionatorio che, valutato e applicato dallo

stesso ministero, nel peggiore dei casi prevede multe di 50 milioni di euro. La Francia per tutelare i propri elettori durante la recente campagna elettorale per l'elezione del nuovo presidente della Repubblica, ha incaricato una società di fact-checking di segnalare a Facebook la presenza di notizie false. Anche in Gran Bretagna, dopo il referendum sulla Brexit, la Commissione Media ha avviato un'inchiesta sul tema. In Italia, nel mese di Febbraio, attraverso un'iniziativa parlamentare, è stato presentato e annunciato dalla Senatrice Adele Gambaro[5]

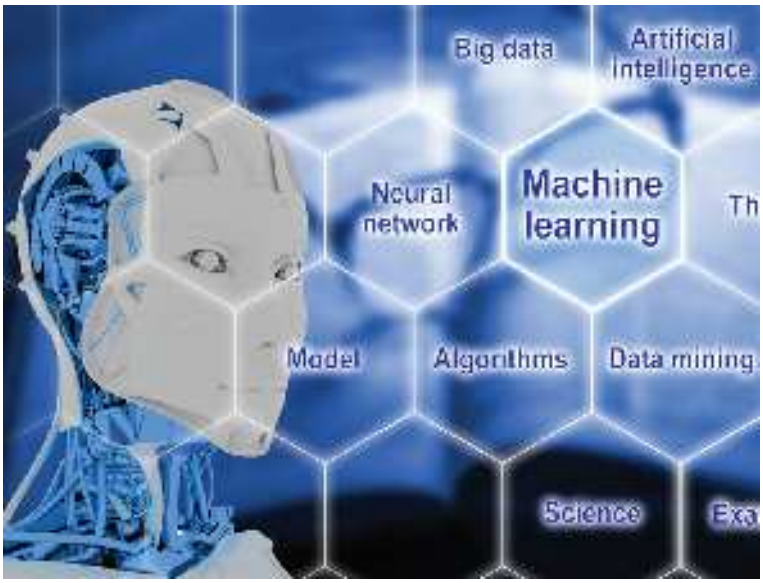
- Atto Senato n°2688 (XVII Legislatura) - il primo disegno di legge contro le false notizie e l'istigazione all'odio in rete; il disegno di legge assegnato alle commissioni riunite 1ª (Affari Costituzionali) e 2ª (Giustizia), è stato pensato in linea con gli indirizzi presentati nella risoluzione 2143 (2017) *"I media online e il giornalismo: sfide e responsabilità"* approvata il 25 Gennaio 2017 dall'Assemblea Parlamentare del Consiglio d'Europa. Anche l'Unione Europea, con la neo-commissaria al digitale Mariya Gabriel, sta prendendo posizione nei confronti delle fake news, avviando già nelle prossime settimane una consultazione pubblica per individuare un approccio equilibrato, a tutela della libertà di espressione di chiunque. I big della rete stanno invece cercando di capire quali sono esattamente le responsabilità che hanno nella gestione delle informazioni e in particolare quelle false; al riguardo, è stato fatto un esercizio per tentare di comprendere la natura dell'informazione a proposito della sua attendibilità. Non vi è dubbio che ci siano alcune informazioni palesemente false, la cui origine ha il solo scopo di monetizzarle. Attraverso notizie sensazionali e link che permettono il re-indirizzamento verso pagine web che non hanno nulla a che vedere con i contenuti presentati in quella da cui si era partiti, l'utente è indotto a "cliccare" su pubblicità varie, consentendo al gestore del sito di guadagnarci (c.d. click-baiting). Spesso la pubblicazione di questo tipo d'informazione contrasta con la politica dei principali social che provvedono a rimuoverla; analogamente per tutte quelle che sono palesemente in contrasto con le leggi nazionali e internazionali, perché ad esempio fonte di diffamazione. L'area a cui si è fatto appena riferimento è ben definita, al punto che gli stessi social non hanno grandi difficoltà nell'intervenire. C'è però un'area grigia in cui è difficile agire e per la quale si corre il rischio di limitare la libertà altrui; basta pensare a quelle informazioni che pur distorcendo la realtà, sono comunque il frutto di opinioni personali che, se pur criticabili, sono espressione di una libertà di pensiero che deve essere comunque e sempre garantita. Da questo punto di vista è facilissimo che possa generarsi rumore di fondo, solo per fare un esempio basti pensare ad un confronto che nasce sulla base di studi scientifici che, a loro volta, sono smentiti da altri studi scientifici. E' chiara dunque la difficoltà d'intervenire da parte di un gestore di piattaforma social, ogni qualvolta che si trova difronte a informazioni che, pur in contrasto con la realtà dei fatti, mancano di elementi oggettivi che ne giustificano la rimozione, essendo in ultima analisi il prodotto di un confronto democratico. L'idea sostanziale di Facebook per prevenire e contrastare le fake news, è quella di coinvolgere chi dell'informazione ne ha fatto una professione, oltre allo sviluppo di strumenti adeguati per facilitare il compito di chi è preposto al controllo. Basandosi su queste premesse, il programma di Facebook si articola nei seguenti punti:

- coinvolgere i professionisti dell'informazione - testate giornalistiche, stampa, e cosi via - per ottenere consigli e suggerimenti su come migliorare la piattaforma social e pubblicare\raccogliere in generale informazioni che la rendano una fonte affidabile;
- rimuovere tutte le informazioni false che, opportunamente segnalate dagli utenti, includono link che rimandano a siti web che trattano tutt'altro rispetto al post originale e presentano contenuti pubblicitari; particolare attenzione è rivolta allo sviluppo di nuovi strumenti software che, sfruttando tecniche di Machine Learning, facilitano l'identificazione delle false notizie, che comunque devono essere sempre verificate prima della eventuale rimozione. C'è, infatti, ancora un elevato rischio di segnalare falsi positivi, almeno fino a quando queste tecnologie non saranno sufficientemente mature;
- rimuovere gli account di fantasia segnalati dagli utenti, per creare relazioni tra persone reali, ben identificabili che, di conseguenza, sono maggiormente responsabilizzate rispetto a quanto pubblicano; in questo modo si tende a limitare il fenomeno dell'hate speech e del cyberbullismo. Anche in questo caso si stanno sviluppando strumenti che sfruttano il Machine Learning e si sta potenziando il team che, prese in carico le segnalazioni degli utenti, provvedono alla verifica e all'eventuale rimozione degli account;
- fornire all'utente una serie d'informazioni aggiuntive rispetto a quella d'interesse, in modo tale che possa rendersi conto se si è imbattuto in una notizia falsa o alterata. Alla fine del 2016 in Francia, Germania, Stati Uniti e Olanda, sono state avviate una serie di sperimentazioni basate sul coinvolgimento delle c.d. fact checking organizations. Quando un utente ritiene che una notizia sia falsa, la segnala al social che a sua volta la inoltra alla fact checking organization (non necessariamente una sola) e attende l'esito dell'analisi. Se è dimostrato che si tratta di un falso, la notizia non è rimossa ma contraddistinta come potenzialmente *"disputed"*. Da quel momento, ogni utente è reso consapevole che quella notizia è stata contestata e valutata e, se vuole, può approfondire i motivi che hanno indotto il social, se pur indirettamente, a qualificarla in quel modo. In aggiunta si stanno potenziando i c.d. articoli collegati (related articles) attraverso i quali sono messi a disposizione degli utenti link che rimandano a pagine che trattano lo stesso tema e dunque consentono di approfondire la notizia d'interesse.
- avviare campagne di sensibilizzazione, ad esempio attraverso il coinvolgimento delle scuole, per fornire consigli utili a migliorare il senso critico e dunque a individuare le notizie false.

In generale emerge dalle precedenti considerazioni che c'è un grande fermento intorno a questo tema e che ancora molto c'è da fare, sia da un punto di vista normativo, sia tecnologico; ad esempio sfruttando sempre di più i metodi di apprendimento automatico, ma anche rendendo maggiormente consapevoli gli utenti nel valutare le informazioni.

Conclusioni

L'intelligenza artificiale è la scienza che rende le macchine intelligenti e l'apprendimento automatico, anche chiamato Machine Learning dall'inglese, è un modo per renderle tali. In particolare, attraverso le



tecniche di Machine Learning, si conferisce ai sistemi la capacità di imparare autonomamente affinché poi, possano svolgere compiti anche complessi, senza necessariamente programmarli. Gli algoritmi di apprendimento dopo molteplici cicli di esecuzione dovrebbero, infatti, sviluppare una conoscenza empirica dei problemi, per valutare e riconoscere le informazioni. Il Machine Learning è utilizzato per molteplici scopi, nell'ambito della sicurezza, per il riconoscimento facciale, per identificare immagini illegali, rilevare lo spam, individuare potenziali frodi e nei sistemi anti-terrorismo; si tratta chiaramente di una lista non esaustiva delle possibili applicazioni. Per alcune specifiche applicazioni, il Machine Learning è però ancora immaturo, anche se la comunità scientifica sta cercando di porvi rimedio e gli investimenti stanno via via crescendo nel tempo; è proprio il caso della fake news e della loro individuazione. Addirittura per alcuni non è chiaro se l'apprendimento automatico possa ritenersi una soluzione adeguata nel breve termine, sempre in riferimento alle fake news. Ciò che si può affermare con ragionevole certezza, indipendentemente dal grado di maturità delle tecniche appena menzionate, è che si tratta di un problema che non può essere affrontato con le sole tecnologie, ma occorre assolutamente il coinvolgimento delle persone. Del resto è evidente a chiunque che, il contenuto di un messaggio può assumere molteplici significati andando oltre quello di ogni singola parola. Gli attuali strumenti di apprendimento automatico restituiscono risultati interessanti quando devono individuare dei "pattern", meno se devono entrare nel merito del significato di un'informazione, soprattutto quando presentano contenuti che tendono alla satira, all'umorismo o all'esagerazione. Rilevare automaticamente una fake news può pertanto essere veramente un compito arduo se pensiamo al problema in termini semantici; analogamente se pensiamo al fatto che ogni volta occorre stabilire qual è l'informazione di riferimento da assumere come base di certezza. Si tratta di una grande sfida per la quale, da una parte c'è la consapevolezza che la strada da percorrere è ancora lunga, dall'altra si sa che un grande sforzo deve arrivare dalla comunità scientifica e dalle imprese, anche attraverso l'attuazione di programmi di ricerca scientifica e industriale e lo sviluppo sperimentale. Tutto ciò sfruttando le tante possibilità offerte dai programmi di finanziamento resi disponibili sia a livello comunitario, sia nazionale. ■

1 Le chat consentono di comunicare con le persone in tempo reale, i forum sono utilizzati per sostenere discussioni dove non tutti i partecipanti sono online nel medesimo istante. I social network, sfruttando una caratteristica peculiare del c.d. Web 2.0, ossia la possibilità di interagire con la rete, sono delle vere e proprie piattaforme di aggregazione delle persone; come piazze virtuali favoriscono lo sviluppo di relazioni attraverso la condivisione d'informazioni, opinioni, immagini e link. In altre parole, i social network, offrono la possibilità a chiunque di partecipare alla "discussione" di qualunque genere e tipo.
2 http://www.lastampa.it/2016/12/31/societa/le-pi-grandi-bufale-del-X3Zin44VLpSL9mq9JBcmWP/pagina.html
3 http://america24.com/news/hillary-clinton-contro-le-fake-news-paragona-trump-nixon
4 http://www.businessinsider.com/fake-news-starbucks-free-coffee-to-undocumented-immigrants-2017-8?IR=T
5 http://www.senato.it/leg/17/BGT/Schede/Ddliter/47680.htm

Robot e rivoluzione 4.0 Verso l'economia delle idee

Gli scenari del cambiamento : Intervista VIP a Stefano Venturi, AD Hewlett Packard Enterprise

Stefano Venturi

Autore: Massimiliano Cannata

"Appuntamenti come SINNOVA servono ad attrarre capitale, idee, talenti. Territori come la Sardegna sono ricchi di capitale umano, che dobbiamo sfruttare per mettere in moto l'economia delle idee, che sarà il risultato tangibile della rivoluzione digitale, che stiamo vivendo. Siamo alla vigilia di un nuovo grande Rinascimento, importanti opportunità si potranno aprire se sapremo raddoppiare il nostro impegno nella ricerca, lanciare un'autentica *call for action* del sistema educativo finalizzata ad adeguare preparazione e profili alle richieste di un mercato che sta cambiando. Sgombrare il campo da inutili paure sarà determinante: l'automazione non toglierà lavoro, se sapremo costruire un ecosistema aperto al futuro e soprattutto capace di promuovere i "ribelli dell'innovazione".

Stefano Venturi *Corporate Vice President* e amministratore delegato Hewlett Packard Enterprise in Italia, fa il punto sulle sfide della nuove era digitale. Lo abbiamo incontrato a margine del *keynote speech* che ha tenuto a SINNOVA, la tre giorni che si è tenuta a Cagliari dal 5 al 7 ottobre, voluto da Sardegna Ricerche e gestito dalla *Smeralda Consulting*. L'evento promosso da Valter Songini, responsabile della comunicazione di Sardegna Ricerche, organizzato e gestito da Smeralda Consulting, ha polarizzato l'attenzione di istituzioni e imprese, facendo registrare un boom di visitatori (più di ottomila persone). Magica e affascinante la location: l'ex manifattura tabacchi, un luogo di rilevanza storica, radicato nella memoria collettiva del popolo sardo, oggi rivitalizzato e trasformato in una piattaforma relazionale hi-tech, proiettata sulle rotte virtuali di un sistema capitalistico che sta mutando pelle.

L'intervista

Dott. Venturi Industria 4.0 Evoluzione o rivoluzione, questo il tema del suo intervento di Cagliari. Come dobbiamo intendere questa dicotomia?

Negli ultimi venti anni abbiamo sperimentato una rivoluzione senza precedenti. E' cambiato il mondo. Il primo profondo salto di continuità è avvenuto a metà degli anni novanta con l'avvento del world wide web, non di Internet che era uno strumento già conosciuto da smanettoni e super esperti. Con il web alla portata di tutti muta lo scenario di riferimento, perché scatta una prima grande fase di disintermediazione. E' questa la parola chiave che il paradigma digitale porta con sé.

Cosa vuol dire esattamente?

Vuol dire che molti dei passaggi legati al vecchio mondo industriale non esistono più, semplicemente perché non sono più necessari. Ci ricordiamo forse più della guida monaci, degli annuari SEAT, degli elenchi telefonici? Sembra preistoria a parlarne. Oggi accediamo all'informazione in qualsiasi luogo e momento. Chiunque può guardare al mondo e cercare le cose che gli servono. Si è creato un flusso orizzontale che investe anche i cittadini e i professionisti che hanno ormai acquisito un potere enorme, con il risultato che molte lobbies si sono viste espropriate del monopolio del sapere. Sono così cominciati a nascere ambiti di business prima inimmaginabili.

La bolla a cavallo del 2000 e l'esplosione delle dot com sembrava aver arrestato la grande fascinazione del virtuale sgonfiando di fatto i bagliori della new economy. Invece?

Invece è accaduto che dopo quella grave crisi è arrivata un secondo grande rivolgimento, collocabile a metà del 2000 con l'irruzione dirompente dei social network e con l'apparizione, nel 2007 del primo *smart phone*. La

correlazione di questi due fattori ha innescato un cambiamento straordinario disintermediando l'accesso tra le persone. Si comincia a parlare di *social innovation*, la comunicazione non corre più dall'alto verso il basso, ma si crea un flusso orizzontale, rispetto a cui tutti possono essere protagonisti.

Quali sono i riflessi di queste fenomenologie che stanno incidendo sulla vita relazione e sugli stili di vita?

Sono enormi e non ancora tutti studiati a fondo. A partire dall'attività di marketing oltre, più in generale, alle iniziative di comunicazione che sono ormai per definizione bidirezionali. Non a caso si parla di era partecipativa. Milioni di persone hanno ormai imparato a parlarsi tra loro, con contenuti multimediali in un piazza virtuale. Per sviluppare nuovi prodotti le aziende lavorano in collaborazione con i propri target di clienti, mettendo in campo delle autentiche *call for ideas*, dei concorsi di idee finalizzati a migliorare la qualità dei servizi.

Ha ragione Derrick De Kerckhove quando parla di dimensione omeopatica del web, per tratteggiare la dimensione della nostra quotidianità?

Sicuramente. La terza rivoluzione digitale, che poi coincide con la quarta del mondo industriale, è caratterizzata dalla convergenza di quattro forze e sarà un autentico tornado, perché oltre ad essere più forte delle precedenti scardinerà il tradizionale bilanciamento dei poteri economici.

I vettori del cambiamento e la "macchina di Turing"

Possiamo tratteggiare i lineamenti di questi "vettori" del cambiamento?

L'Internet of things e gli open data, che sono a mio giudizio fattori complementari, saranno il primo vettore. Ciascun individuo al pari degli oggetti è leggibile da un sensore che registra qualsiasi movimento. Gli open data sono il serbatoio enorme di informazioni, che se messo a disposizione per esempio dalla PA agli utenti diventa un asset di condivisione della conoscenza di straordinaria potenzialità. A questi due fattori vanno aggiunti i *Big Data Analytics*, che implicano una capacità interpretativa. Grazie ai progressi delle scienze matematiche e allo sviluppo di specifiche abilità combinatorie siamo in grado di individuare percorsi di senso anche se messi di fronte a una quantità enorme di in formazioni. L'immensità del bosco, insomma, non ci spaventa, perché sappiamo trovare i sentieri di riferimento per orientarci.

I robot che posto occupano in questo processo evolutivo?

Siamo al terzo grande catalizzatore del cambiamento. Parlerei di intelligenza artificiale, che qualcuno erroneamente fa rientrare nel grande capitolo dei Big Data Analitics. Con l'apporto dell'IA siamo in grado di leggere fenomeni complessi. Aspetto che diventa decisivo per collegare fatti ed eventi, orientare le scelte strategiche, fornendo input all'organizzazione aziendale e al sistema produttivo nel suo insieme. La diffusione dei robot, anche in ambiente domestico rappresentano il volto più eclatante di questo salto qualitativo, che vede l'automazione uscire dal "recinto" della fabbrica per entrare nelle nostre case e per cambiarci la vita. Vi è poi la quarta forza il *Cloud*, strumento che ci consentirà di abbattere la soglia di accesso alla potenza elaborativa dando linfa all'ECONOMIA DELLE IDEE, che è e sarà il motore delle grandi trasformazioni anche in futuro. La logica *dell'open source*, la società dell'accesso che si amplia, le nuove frontiere della mobilità facilitata da *app* sempre più capillari sono tutti elementi che stanno imprimendo un'accelerazione straordinaria all'innovazione.

BIO

Stefano Venturi è Corporate Vice President e Amministratore Delegato di Hewlett Packard Enterprise in Italia. In questa posizione, che ricopre da Dicembre 2011, Venturi ha la responsabilità di guidare le attività dell'azienda e di indirizzarne la crescita nel mercato italiano.
Formatosi in Olivetti dal 1979 al 1984, Venturi è rientrato in Hewlett-Packard come Amministratore Delegato dopo essere cresciuto all'interno dell'azienda dal 1984 al 1991. In seguito, Venturi ha ricoperto il ruolo di Country Manager di Wyse Technology Italy, Managing Director EMEA South in Sun Microsystems, Amministratore Delegato di Cisco in Italia per 13 anni e, sempre in Cisco, di Vice President Europe per il Public Sector per i successivi 2 anni.
Venturi è Presidente della American Chamber of Commerce in Italy e membro del Consiglio di Presidenza di Assolombarda Confindustria Milano Monza e Brianza, con delega "Attrazione Investimenti e Competitività Territoriale", nonche' membro dell'Advisory Board Investitori Esteri di Confindustria.
Venturi ricopre, inoltre, il ruolo di Vice Presidente di Assinform con delega all'Education ed è Consigliere Incaricato e membro del Consiglio di Presidenza di Confindustria Digitale con l'incarico di Presidente dello Steering Committee "Competenze Digitali".

A proposito di robotizzazione e di intelligenza artificiale, siamo di fronte a un rischio o a un'opportunità?

In Europa, secondo uno studio della Commissione, assisteremo alla creazione di 700.000 nuovi posti di lavoro entro il 2020 nei settori ad alta tecnologie e fino a 450.000 nuove figure professionali (high-tech leader) con competenze multidisciplinari (digitali, materiali, manifattura additiva, biotecnologia, nanotecnologia e fotonica). Se sapremo governare il cambiamento, anziché subirlo, avremo una grande opportunità da cogliere. Per poterne sfruttare appieno le potenzialità dobbiamo riuscire a posizionarci tra gli *early adopters* di queste tecnologie, utilizzare l'accelerazione che offrono per colmare l'attuale gap, ad esempio approfittando della spinta offerta dagli incentivi del piano Industria 4.0 per innovare il settore manifatturiero. Rimane ovviamente decisivo promuovere formazione e aggiornamento di lavoratori e aziende sui temi legati alle nuove tecnologie.

Nel suo intervento ha accennato a un invecchiamento della cosiddetta "macchina di Turing": significa che nascerà o è già nata una nuova generazione di computer?

Di fatto sta già nascendo: stiamo lavorando nei nostri HPE Labs ad un progetto chiamato *The Machine* con il quale puntiamo a realizzare un nuovo paradigma denominato *Memory-Driven Computing*, un'architettura appositamente creata per l'era dei Big Data. Lo scorso maggio abbiamo presentato un prototipo dotato di 160 terabyte (TB) di memoria, sufficienti per lavorare simultaneamente con otto volte i dati contenuti in tutti i volumi conservati presso la Libreria del Congresso statunitense, ovvero circa 160 milioni di libri. Finora non era mai stato possibile memorizzare e manipolare data set di queste dimensioni all'interno di un sistema single-memory.

Avremo dunque disponibile una grande quantità di memoria. Come verrà usata?

Sarà possibile, ad esempio, lavorare contemporaneamente con tutte le cartelle cliniche digitali di ogni persona sulla Terra; ogni dato presente all'interno di Facebook; ogni spostamento dei veicoli a guida autonoma di Google; ogni data set prodotto dalle esplorazioni spaziali – e tutto nello stesso momento, ottenendo risposte e scoprendo nuove opportunità a velocità senza precedenti. Mentre il progetto procede, stiamo già inserendo le innovazioni tecnologiche nei prodotti che attualmente commercializziamo. Grazie ad esempio a soluzioni software-defined come HPE Synergy riusciamo a costruire infrastrutture così intelligenti da adattarsi a qualsiasi carico di lavoro e fornire servizi alla in maniera estremamente veloce ed efficiente.

Il sistema Italia di fronte alla rivoluzione digitale

Come vede il "sistema Italia" di fronte a questa grande rivoluzione che alcuni studiosi definiscono la "terza digitale" e la "quarta per il mondo industriale"?

Le classifiche internazionali, come il Global Information Technology Report 2016 del WEF, vedono l'Italia in ritardo nel percorso di digitalizzazione. Siamo però tra i paesi che stanno recuperando più velocemente posizioni e abbiamo delle eccellenze importanti, aziende e persone. Dobbiamo capitalizzare questo valore, imparare a fare sistema e investire in modo significativo nell'innovazione, consapevoli che la trasformazione digitale può permettere al nostro Paese di recuperare competitività a livello globale. Qualcosa sta già cambiando, a partire dalla consapevolezza del fenomeno, si cominciano a vedere i primi effetti del piano Industria 4.0, recentemente rilanciato dal Governo sotto il nome di Impresa 4.0, che prevede interessanti spunti in tema di incentivi e sgravi fiscali anche per la formazione e il trasferimento tecnologico. Diventa fondamentale puntare sulla riqualificazione dei lavoratori, formandoli con le necessarie competenze digitali e implementando processi di *Life Long Learning*.

Quali sono le regioni e i contesti territoriali italiani più permeabili all'innovazione?

La trasformazione digitale impatta su tutti i settori e ogni azienda deve imparare a sfruttare le potenzialità offerte dalle nuove tecnologie per innovare ed innovarsi. Nell'ultimo anno abbiamo realizzato in collaborazione con i nostri partner 19 HPE Innovation Lab distribuiti in 9 regioni italiane, con l'obiettivo di portare l'innovazione vicino a dove sono le aziende clienti, a portata delle PMI sul territorio. Si tratta di centri di competenze dove le aziende e le PA locali possono entrare in contatto con le tecnologie e sviluppare progetti ad hoc. Abbiamo già realizzato diversi eventi e incontri mirati, ottenendo un riscontro molto positivo dalle realtà aziendali che vi hanno preso parte.

Rimanendo alle nostre latitudini, ritiene che SINNOVA e appuntamenti simili possano contribuire a rilanciare il Mezzogiorno in questa grande partita da cui dipende il futuro della nostra economia?

Credo che eventi come quello organizzato a Cagliari siano importanti soprattutto, ma non solo, per il Mezzogiorno, un'area del nostro Paese dove si sente forte il bisogno di confronto, condivisione, contaminazione. È da questi incontri e dai processi che vi prendono forma che nascono idee e collaborazioni: quella che chiamiamo Open Innovation e che prevede l'apertura del processo di innovazione alla filiera aziendale e alla collaborazione tra Start Up e aziende consolidate. Più in generale, eventi in grado di promuovere questi incontri, la cultura dell'innovazione e le opportunità offerte dalle nuove tecnologie sono indubbiamente un incentivo e un acceleratore verso un percorso di rilancio della nostra economia.

I ribelli dell'innovazione

Allargando l'angolo di visuale, possiamo provare a individuare i mercati che conquisteranno la leadership in questo nuovo articolato scenario?

Quando si sparigliano le carte grandi opportunità possono nascere per tutti, quindi anche per l'Italia a patto di lavorare sulla formazione. Sappiamo, da studi molto recenti, che il 15% degli occupati nel nostro paese dovrà nel giro di pochi anni, abituarsi all'Idea di dover cambiare lavoro. A fronte di questo inutile piangersi addosso, occorre invece far scattare un grande piano nazionale, che metta al primo posto gli investimenti in ricerca che vanno raddoppiati. Allo stesso tempo occorre far partire un vero mercato del Venture Capital. Abbiamo molte start up ma sono poche quelle realmente di rottura. Abbiamo invece bisogno che si facciano strada i RIBELLI DELL'INNOVAZIONE, capaci di trasformare anche le idee apparentemente più irrealizzabili in ricchezza reale.

Dalla sua analisi appare chiaro che non è finita qui l'era dei rivolgimenti. Dobbiamo dunque aspettarci ancora altri scossoni?

La manifattura additiva, la stampa 3D è l'esempio più noto. L'industria meccanica avrà degli impatti importanti, solo per citare un caso esempio. Produrre un motore o semplicemente un ricambio costerà lo stesso in

qualsiasi parte del mondo, perché potrà essere realizzato ovunque. Le fonderie ricavavano per sottrazione la forma dalla materia, oggi tutto questo non servirà più. Sarà determinante mettere in campo competenze multidisciplinari, per progettare un'automobile, gestire i processi di qualità e assemblare i pezzi. Chi invece si era concentrato sulla produzione delle sottoparti, verrà disintermediato perdendo spazi di mercato e quindi potere. Tutto questo comporterà un riequilibrio della *supply chain*, della logistica, fino alla stessa gestione dei ricambi, che non ha precedenti.

Nulla sarà come prima c'è da pensare?

Pensiamo alla manutenzione predittiva, per cui si potranno riparare i guasti prima che avvengano, alle macchine che non avranno piloti, allo sviluppo dei droni di nuova generazione che si incroceranno con l'intelligenza artificiale garantendo servizi a valore aggiunto nei campi più svariati: dalla mobilità, alla salute. Nuove tecnologie di visualizzazione trasformeranno i nostri orologi in strumenti utili anche per i portatori di disabilità. Insomma il mondo viene riscritto dalla tecnologia, nulla sarà prestabilito, si potrà reinventare tutto.

Un'ultima sollecitazione riguarda il contesto in cui Lei opera. Su quali progetti state puntando per diffondere la cultura digitale?

Grazie all'impegno dei dipendenti HPE che prestano il loro contributo volontario, finanziato dall'azienda fino a 12.100 ore l'anno (dati relativi al FY16), stiamo realizzando diversi progetti mettendo a disposizione le nostre competenze per diffondere la cultura digitale in tutte le fasce d'età. Con l'iniziativa **CoderDojo** insegniamo a bambini e ragazzi, dai 7 ai 14 anni, a sviluppare il pensiero computazionale utilizzando le basi del coding. La serie di incontri **Safe2Web** ha invece come obiettivo mettere in guardia e insegnare ai giovani a proteggersi dai potenziali pericoli della rete, grazie a un uso consapevole di Internet e dei social.

Quali opportunità si apriranno in concreto per i giovani?

Attraverso un protocollo siglato con il MIUR, abbiamo poi lanciato il nostro percorso di Alternanza Scuola-Lavoro, **FabLab@HPE**, con cui i ragazzi che frequentano gli ultimi 3 anni delle scuole secondarie di secondo grado imparano, attraverso il coding, a capire, controllare e sviluppare metodologie per risolvere i problemi e cogliere le opportunità offerte dalla società e dal mercato del lavoro. Il protocollo prevede inoltre la realizzazione, da parte dei giovani coinvolti e con il supporto dei nostri tutor, di FabLab all'interno delle scuole che partecipano al programma, promuovendo così un circolo virtuoso che coinvolge anche gli studenti delle prime e seconde classi. Siamo anche tra le aziende di Assolombarda promotrici di **ABCDigital**, un'iniziativa che vede il coinvolgimento dei ragazzi delle superiori, incentivati con dei crediti formativi, nell'insegnare agli over 60 l'uso dei tablet, di Internet e dei principali servizi digitali, utili a ridurre il Digital Divide. Per dare un'idea della portata del nostro impegno, basti dire che l'iniziativa CoderDojo ha coinvolto lo scorso anno 850 ragazze e ragazzi, Safe2Web 900, mentre i partecipanti ai FabLab@HPE sono stati circa 2000. ■

La IV rivoluzione industriale e i nuovi dubbi aml-etici

Autore: Viviana Rosa

Macchine che parlano ad altre macchine, che imparano e agiscono senza alcuna necessità dell'intervento dell'uomo: siamo nel regno dell'"Internet of Things", il punto in cui il mondo fisico e quello virtuale collidono. Il futuro è già qui, ma è fondamentale che alla rivoluzione tecnologica corrisponda una rivoluzione culturale consapevole e un'adeguata attenzione alle implicazioni etiche.

Visto che il progresso non si può e non si deve fermare, con buona pace dei "luddisti", cosa dobbiamo fare? Cogliere le opportunità e minimizzare i rischi, indicando delle linee guida che preservino anche le future implicazioni morali e sociali. Le applicazioni del "Machine Learning" sono innumerevoli: sicurezza, intrattenimento, elettrodomestici, energia, salute. Dalla domotica, che consente risparmi economici e di tempo, alle Smart Cities: con soluzioni per risolvere i problemi delle città, come il risparmio energetico o i flussi di traffico, dall'Industrial IoT che consente aumento della produzione, abbattimento dei costi e una maggiore personalizzazione, agli Smart Stores che forniscono shopping personalizzati, esperienze originali fatte su misura per ogni cliente, alle automobili che si guidano da sole. A prima vista potrebbe sembrare uno scenario futuribile, in realtà molte persone interagiscono, in modo più o meno consapevole, ogni giorno con sistemi basati sul Machine Learning come per esempio i

sistemi di riconoscimento delle immagini usate sui social media oppure di riconoscimento vocale degli assistenti virtuali o i sistemi che raccomandano prodotti o servizi usati nei negozi online e per promuovere contenuti sui social media. Viviamo in un mondo in cui l'informazione sta diventando la moneta corrente, il nuovo petrolio, una risorsa per supportare la nuova rivoluzione industriale. Un fattore chiave per l'economia digitale i cui benefici sono autoevidenti, ma quali sono i rischi? La Machine Learning è lo strumento che consente di dare un significato ai dati, di estrarre informazioni che hanno un valore e questo pone nuove sfide per la gestione di questa tecnologia. Se da una parte abbiamo la possibilità di salvare vite, grazie a nuove e più accurate diagnosi, così come di aiutare gli insegnanti con attività su misura che facilitino l'apprendimento, di supportare sistemi di trasporto intelligenti e facilitare nuove scoperte in campo della fisica, dell'astronomia

BIO

Viviana Rosa ricopre il ruolo di Commercial Director in BSI Group Italia, azienda nella quale entra nel 2010, e per la quali si occupa della strategia commerciale e marketing oltre che dell'introduzione di nuovi prodotti nel settore della Sicurezza e del Risk Management. Durante la sua carriera professionale, per diversi anni, ha ricoperto ruoli di rilevanza internazionale seguendo importanti progetti di comunicazione, marketing e vendite per realtà di svariati settori, instaurando solidi rapporti con gli stakeholder di riferimento, comprese le amministrazioni pubbliche e gli enti governativi. Laureata in Lingue e Letterature Straniere presso l'Università Cà Foscari di Venezia ha ottenuto una specializzazione post laurea in Multimedia Content Design presso la Facoltà di Ingegneria di Firenze e ha studiato Foundation of Management a Londra presso l'ILM - Istituto di Leadership Management.

e delle neuroscienze, vista la capacità di analizzare grandi quantità di dati; dall'altra è opportuno interrogarsi, di fronte ad un cambiamento di scenario epocale, sui cambiamenti per la società e sulle conseguenze sociali ed etiche. La capacità di accedere ai dati diventa sempre più importante, e chi accede per primo può trarne vantaggi significativi, dunque sarà necessario gestire le fonti dei dati in maniera strategica. Un altro rischio etico potrebbe essere quello di nuove asimmetrie di potere in cui gli individui rinunciano volontariamente alla propria privacy in cambio di maggiore efficienza, convenienza o accessi a servizi. E' notizia di questi giorni (http://www.bbc.com/news/world-asia-china-34592186) che nel 2020 in Cina partirà un Social Credit System che darà un voto alle persone in base alla loro reputazione online e i cittadini che offriranno i loro dati avranno notevoli vantaggi come prestiti e tasse più basse. I ricercatori dovranno considerare i futuri potenziali utilizzi dei dati e costruire il più ampio consenso che sia eticamente accettabile, riformulando i tradizionali concetti di privacy e di consenso. I dati, infatti, vengono usati in modo sempre più dinamico e combinati in modo innovativo creando maggiori informazioni: con un considerevole aumento dei rischi per la privacy. In merito a questa tematica il Parlamento Europeo ha approvato la nuova legislazione in materia di protezione delle informazioni (EU GDPR) che dovrà essere applicata entro il 25 maggio 2018. Il nuovo regolamento definisce importanti responsabilità legali per le organizzazioni che raccolgono, conservano e processano dati e include ulteriori misure per proteggere le informazioni dei cittadini. Viene introdotto il principio di Privacy by Design che riconosce l'importanza fondamentale dell'integrazione, della protezione delle informazioni e della gestione della privacy. BSI (British Standards Institution) lavora con le aziende per identificare le potenziali minacce o violazioni all'attuale regolamento. Nel campo dell'Intelligenza Artificiale, il rapporto uomo-macchina solleva un numero considerevole di domande sulle possibili conseguenze a livello sociale. Le persone sono favorevoli all'utilizzo di robots in situazioni che possono essere pericolose o difficili per l'uomo, ma lo sono molto meno se il ruolo dell'automa diventa di maggior rilievo, soprattutto per la paura di perdere il contatto umano. Le preoccupazioni principali sono legate alla paura che i robot possano causare danni, al timore di essere rimpiazzati dalle macchine, di fare esperienze spersonalizzanti, di esser costretti a restringere le scelte e la libertà dell'individuo, principalmente alla paura di perdere il controllo. La paura di perdersi in vere e proprie "bolle", micro mondi creati da una sempre maggiore personalizzazione delle informazioni proposte all'utente tali da ridurre il suo orizzonte conoscitivo e da minare la consapevolezza di differenti prospettive. Nel giro di pochi decenni le nuove tecnologie potrebbero conferire all'uomo capacità fisiche e cerebrali potenzialmente illimitate, grazie all'interazione tra AI e biotecnologie. Il rischio potrebbe essere quello di trovarci di fronte ad un "superuomo" disumanizzato. L'uomo rischia cioè di "ridursi" semplicemente alla somma delle proprie estensioni artificiali come afferma Michael Bess, docente di storia alla Vanderbilt University che si occupa dell'impatto culturale delle nuove tecnologie. (https://aeon.co/ideas/why-upgrading-your-brain-could-make-you-less-human). Come gestire, dunque, l'interazione uomo-macchina? Come combinare al meglio l'intelligenza umana e i sistemi di AI così che possano lavorare insieme in modo efficace e sicuro? Dando delle linee guida che tengano in considerazione tutti gli aspetti.

Questa è la direzione seguita dai nuovi standard, sviluppati per coprire i diversi aspetti legati all'interazione uomo-robot, sia dal lato della sicurezza

fisica delle persone che li utilizzano, sia con un impronta etica.

Sul primo **a**spetto due esempi sono dati dagli standard ISO 10218-1: 2011 e 13482:2014.

Lo standard ISO 10218-1: 2011, attualmente in aggiornamento, specifica i requisiti e le linee guida per una progettazione sicura, le misure di protezione e le informazioni per l'uso dei robot industriali: descrive i rischi di base associati ai robot e fornisce requisiti per eliminare o ridurre adeguatamente i rischi associati a tali pericoli.

La norma ISO 13482:2014 'Personal care robot safety' specifica i requisiti e le linee guida per la progettazione intrinsecamente sicura di robot abilitati a fornire servizi alla persona, quali robot che compiono attività domestiche (trasporto di oggetti, pulizia, recupero oggetti), che forniscono assistenza all'essere umano (apparecchi per alzarsi da una sedia o dal letto, per entrare o uscire da una doccia) o che aiutano il trasporto di persone all'interno di spazi definiti (casa, edifici pubblici).

Dall'esigenza di dare una definizione anche dal punto di vista "etico" è nata invece la BS 8611 *"Ethics design and application robots"* che mette in evidenza come i rischi etici abbiano implicazioni di portata più ampia rispetto ai pericoli fisici. L'utilizzo di robot e tecniche di automazione rende i processi più efficienti, ma è fondamentale che le questioni etiche e i rischi come la disumanizzazione o la dipendenza dai robot siano identificati e indirizzati. Con questo standard vengono date le linee guida per trattare questo nuovo ambito. BS 8611 è stato sviluppato grazie ad un approccio collaborativo a cui hanno contribuito professionisti di vari settori: dagli esperti di ingegneria, robotica e sicurezza, agli scienziati, ai filosofi ed esperti di etica. Questa metodologia si rivela fondamentale affinché nessun aspetto venga sottovalutato. ■

---

https://www.istockphoto.com/it/foto/code-of-ethics-in-technology-gm817338718-132203337

https://www.istockphoto.com/it/foto/human-and-robot-shaking-hands-gm856484032-141097391

La grande sfida delle minacce interne. Perennemente incomprese, sottostimate, mal riportate od ignorate.

Autore: Vassilios Manoussos

Le "Data breaches" nelle notizie

Data breaches, attacchi cyber, intrusioni cyber sponsorizzate da Stati e minacce di una cyber guerra sono ormai diventati temi costanti dei media generalisti. I cittadini ne sentono parlare sempre di più, ma quali insegnamenti ne traggono in realtà?

BIO

Vassilis Manoussos è esperto consulente in forensica digitale, CEO di Strathclyde Forensics e consigliere presso il Security Circle di Glasgow.
E' anche Professore Associato alla Edinburgh Napier University ed alla Cyber Academy. Vassilis ha una grande esperienza nelle investigazioni digitali forensi, nell'audit dei rapporti della polizia e nella consulenza in cyber security. E' spesso invitato come VIP speaker da conferenze internazionale, tavole rotonde e corsi universitari.
Vassilis Manoussos può essere contattato a : vassilis@ForensicsExperts.co.uk

I casi che fanno le "breaking news" sono sempre le brecce spettacolari, quelle dell'ampiezza di Talk-Talk, SONY o Yahoo. Infatti, ad attirare l'attenzione sono i grandi numeri, una costante dell'attuale giornalismo. Ma questi casi non sono che la punta dell'iceberg. Sono casi troppo grandi per essere nascosti, spesso troppo difficili da gestire e da contenere rapidamente. Sono quelli che ci stupiscono semplicemente per la quantità: Yahoo! col suo miliardo di indirizzi email compromessi; Talktalk e la perdita dei dati privati e bancari di 157,000 utilizzatori o ancora BUPA (un'azienda dell'industria della sanità, la più grande fonte di brecce attuale) coi suoi 500,000 dossier persi. Seguono poi, per il Regno Unito, la NHS (National Healthcare System), la Tesco Bank e Three Mobile, solo per citare alcuni esempi.

Il problema sottostante è che questi sono affari colossali che operano in settori molto regolamentati quali le telecom, la finanza e la sanità, dove le leggi e le normative già in vigore sulla protezione dei dati obbligano le vittime a pubblicare le brecce e di notificare l'incidente a tutte le persone compromesse, nascondendo così i casi più piccoli di brecce, leak e hack di dati. In verità, le grandi ditte saranno sempre bersagli di primo grado, mentre i piccoli affari non lo sono per forza. Le piccole e medie imprese, al contrario, hanno la tendenza a perdere di propria mano dati importanti, perché non hanno implementato un processo adeguato quanto minimo di sicurezza oppure non hanno offerto le adeguate formazioni al loro staff. Le PME ed i micro-business spesso non sanno dove sono archiviati i loro dati e spesso, non sono quindi nemmeno al corrente che vi è stata una breccia od un leak fino al giorno in cui vengono direttamente impattate – ad esempio quando qualcuno usa le loro informazioni per estrarre denaro dai loro affari, completando i dati rubati con azioni di *phishing* oppure di *social engineering* per mandare in porto il reato.

Molto spesso, le PME perdono i loro dati per causa di una parte terza: un vendor, un cliente, o persino un'agenzia governativa. Le tipologie dei *data breaches* sono variabili, dalle più semplici alle più critiche. Nella loro forma più semplice, una breccia può provenire dallo skimming di emails da agende di contatti. Ad esempio, personalmente posseggo un certo numero di indirizzi di email professionale, che uso per scopi diversi. Quello che usavo per comunicare con clienti esistenti o potenziali è diventato rapidamente un ricevitore di spam, di fatto non avevo reso pubblica questa mail su un website ed i miei firewall e software di sicurezza sono ottimali. Nello stesso tempo, nessuno degli altri 30 indirizzi email che posseggo è stato vittima di spamming. L'indirizzo che si ritrovò inondato di spam è quindi stato trovato nelle agende dei computer di clienti e contatti che non avevano una sicurezza adatta. Il risultato? La mia mail

divenne comune in numerose liste di spam usate da criminali e neppure i miei filtri speciali facevano più fronte. Ho finalmente dovuto annullare quel conto ed aprirne uno nuovo.

Questo esempio sottolinea un leak indiretto, con risultati che sia cittadini che ditte patiscono ben troppo spesso. Ovviamente, qui parliamo della parte più bassa dell'insieme dello spettro delle brecce, che personalmente considero più un disturbo che un rischio reale che mi prende di mira personalmente. Ma se ad essere nello stesso modo attaccato fosse il device di un contrattante o di un consulente, potrebbe finire con l'aprire brecce verso informazioni molto più sensibili e le conseguenti perdite finanziarie dirette.

Cosa rivelano i numeri

Le statistiche sui data breaches sono variabili secondo le fonti, ma la minaccia sembra essere consistente ed in crescita, avendo come vittime predilette i governi ed i sistemi di sanità.

Secondo **Gemalto** ed il loro sito **BreachLevelIndex**[1], nel 2016 si è raggiunto il record di 1,378,509,261 files[2] compromessi da 1,792 brecce. L'unico aspetto positivo è che 4.2% dei dati rubati erano criptati, cioè praticamente senza nessun valore per i loro nuovi "proprietari". L'aspetto preoccupante invece è che **solo 4.2% dei dati erano criptati**, e che per di più nel 52.2% delle brecce il numero esatto dei dati compromessi è classificato come *"sconosciuto"*.

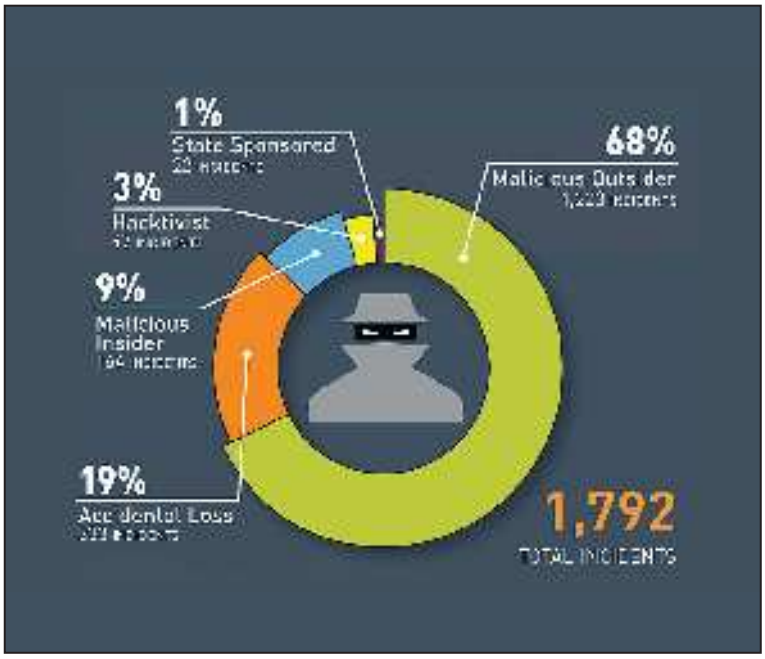


Immagine 1. ***Data breaches*** **secondo la provenienza**
(fonte: breachlevelindex.com)

Se veniamo ora alle grandi strutture, il rischio proviene spesso dall'esterno del perimetro di sicurezza: come ben vediamo nell'immagine 1, più dei due terzi delle brecce sono state orchestrate dall'esterno[3]. Ciò nonostante, un significativo 28% rimane attribuito ad insiders e a perdite accidentali. La combinazione di questi due fattori costituisce la minaccia interna che deve fronteggiare qualsiasi ditta.

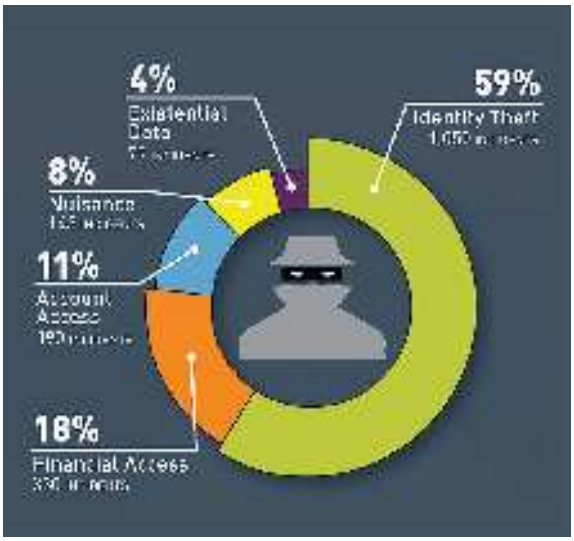


Immagine 2. ***Data breaches*** **secondo le tipologie**
(fonte: breachlevelindex.com)

La maggioranza dei *data breaches* è costituita da furti di identità, il rischio più grave per le ditte ed i loro clienti. Non è quindi una sorpresa vedere che i dati delle aziende e degli enti attivi nella sanità sono diventati il primo obiettivo dei cyber criminali.

La minaccia dall'interno

Con quasi il 28% dei leaks e delle brecce provenienti dall'interno delle strutture vittime, ha un senso affermare che il mondo degli affari ed i CISO in particolare dovrebbero iniziare la loro difesa iniziando a ridurre in modo drastico questo tipo di minaccia.

Nell'Info Security Magazine, leggiamo che una stima di quasi il 63% delle ditte sono state colpite da un *"old school data leak"*: la stampante. Si valuta pure che tra il 10 e il 18% dei leaks interni risultano da documenti, che contenevano informazioni fondamentali del business, stampati e caduti in mano a semplici impiegati o a contrattanti. Il rischio si estende poi ai documenti che sono forniti alle istituzioni statutarie (ad esempio le autorità di finanza, gli enti regionali o anche le autorità di tutela del medio) che non usano triturare o distruggere correttamente i documenti ricevuti una volta trattati. Questa percentuale è già ampia di per sé, se consideriamo che si tratta di ecosistemi *corporate* che generalmente posseggono stampanti in rete che richiedono un login per stampare, lasciando quindi una tracciabilità dell'atto *in sine*.

Nelle PME, le stampanti in rete spesso non richiedono all'utilizzatore delle credenziali per stampare e poi recuperare la copia cartacea. Quindi la sola soluzione d'inchiesta su di una breccia da stampante si rivela essere un'investigazione digitale forensica sistematica (e spesso tanto costosa quanto disturbante), un fattore che spinge

ancora di più le piccole imprese ad essere le vittime principali del *"leak-by-printing"*.

Ma la taglia conta davvero?

Benché la risposta a questa domanda sia spesso affermativa, se veniamo alla sicurezza dei dati la nostra risposta è definitivamente «no!». Non conta quanto grande o piccola sia un›azienda: le sue risorse digitali sono la ricchezza di tutti i suoi stakeholder.

La maggioranza delle piccole aziende e di quelle familiari non hanno impostato un sistema di sicurezza permanente dedicato alla protezione delle loro risorse digitali. Sono spesso convinti che una breccia non succederà loro, perché non sono dei bersagli finanziari od industriali importanti. In verità, purtroppo, sono proprio le PME che subiscono sempre di più cyber crimini dovuti a *leaks* o ad impiegati sleali. Nel giugno 2013, il *leak* dei documenti della NSA ad opera di Edward Snowden ha fatto il giro del mondo. Snowden ha semplicemente aggirato protocolli di sicurezza antiquati ed ha utilizzato il suo accesso altamente privilegiato per copiare dei documenti confidenziali del governo americano su di un flash drive. Lavorando da Honolulu, distante parecchi fusi orari dalla centrale dei server della NSA situata a Fort Meade, ha creato una breccia nella sicurezza statunitense usando solo poche e semplici azioni. La domanda per le PME è quindi semplice: se la NSA ha potuto essere derubata da un impiegato… che pensate che possa succedervi?

La vera minaccia...

Si sa bene ormai che nel caso delle piccole imprese che non destano l'interesse dei criminali per scatenare un attacco in piena regola, la minaccia è sia interna, sia causata da un malfattore che fa uso dell'ingegneria sociale. La grande maggioranza dei casi che ho esaminato recentemente vedeva persone ingannate e spinte a pagare le loro fatture su "nuove coordinate bancarie" ricevute generalmente via email. Questo tipo di minaccia può provenire sia da interni che da esterni, allo stesso tempo. La minaccia interna è palese: trattasi di un impiegato che desidera fare soldi facili, che è sleale oppure che è semplicemente scontento del suo lavoro.

Esiste anche una minaccia "semi-interna": il personale IT. Molte ditte, quando crescono e necessitano l'istallazione di una rete, scelgono di affidarne il compito ad una ditta esterna, che ne assicurerà la buona gestione. Non è una scelta pessima, anzi vi sono ditte legittime e con ottima reputazione ad offrire questo tipo di servizi. Però si corre il rischio che se qualcosa va storto dall'esterno, il cliente ne subirà le conseguenze. In una recente investigazione, abbiamo verificato che una ditta di supporto IT di Glasgow ha subito le dimissioni di alcuni membri del suo staff, ma nessuno ha pensato di cambiare le loro credenziali ed i loro login presso i server dei clienti, impedendo agli ex-impiegati di accedervi. Anche se questo non è stato un gesto intenzionale, trattasi di una grave mancanza di professionalità da parte della ditta.

È stato un incidente...

Gli incidenti accadono, ma è importante essere preparati ad affrontarli. Il maggior problema nell'uso dell'informatica e del net è che tutti possono accedervi. Si potrebbe presupporre che un professionista con educazione universitaria (ad esempio un medico o un avvocato) sa quello che fa. Giusto? Ebbene.... no. La maggioranza dei professionisti del mondo giuridico, ad esempio, non hanno avuto una minima formazione all'uso del computer, del cloud o della sicurezza del loro PC. Al meglio hanno avuto formazioni corte per imparare ad usare al meglio un software specifico (ad esempio management dei casi ed esperienza pratica nello scrivere documenti in Microsoft Word e poi mandarli via email. Ma ciò non significa che abbiano la minima idea di come i computer, i file Word o le email funzionino. E qui sorge un problema. Non permetteremmo a nessuno senza la dovuta formazione di eseguire un intervento, ma diamo la nostra fiducia a professionisti senza formazione che si occupano di gestire dati personali nostri, della nostra famiglia o dei nostri affari.

Il 16 marzo scorso, l'ICO (Information Commissionaire's Office) del Regno Unito ha sanzionato un avvocato con una multa di £1,000[4] per aver perso documenti sensibili. L'avvocato lavorava su questi documenti sensibili di un suo cliente da casa. Ha usato un computer comune, quello a cui aveva accesso anche suo marito, ed ha dimenticato di criptare i documenti secondo le norme in vigore. Non vi sono state evidenze che il marito leggesse i suoi documenti. Un giorno però, lui decise di fare un upgrade di software. Pensò che sarebbe stato utile archiviare nel cloud tutti i documenti di sua moglie, ma scelse un servizio che archiviava i documenti rendendoli accessibili ai motori di ricerca e scaricabili senza password. Sui 725 documenti caricati, solo 15 erano indicizzati e secretati, ma 6 di loro contenevano informazioni ultra-confidenziali pertinenti alla Corte della Protezione Sociale e delle Famiglie. Il leak di soli 6 documenti ha coinvolto direttamente e indirettamente circa 200-250 persone, inclusi bambini ed adulti vulnerabili.

Il leak è stato certamente uno sbaglio e nessuno insinuò che sia stato fatto intenzionalmente, da lì la somma modesta della multa. Ciò nonostante, l'avvocato avrebbe dovuto saperne di più, su quanto esiste sulle linee guida chiare redatte sia dall›ordine degli avvocati, sia dalle Corti e le ha ignorate.

Il GDPR arriva...

Il nuovo Regolamento europeo sulla protezione dei dati (GDPR) è in corso e tra meno di sei mesi scatta la scadenza della sua implementazione obbligatoria.

In una recente ricerca (eseguita soprattutto sulle *Freedom of Information Requests*) ha dimostrato che un gran numero di ditte e di enti governativi

non ce la faranno a rispettare questa scadenza. Secondo la Law Society (U.K.) solo 54% delle ditte sono fiduciose di essere pronte, ovvero quasi metà del business crede che non riuscirà ad adempiere gli obblighi sino alla data dell'entrata in vigore del regolamento. Peggio, 24% delle ditte non hanno nemmeno iniziato a pianificare le operazioni necessarie per essere conformi.

La situazione si rivela ancora peggiore quando si viene agli enti pubblici locali. Secondo l'ICO[5]:

Immagine 3. Dati dell'ICO su enti locali e GDPR
(fonte: iconewsblog.org.uk)

I risultati delle ricerche[6] sul livello di preparazione degli enti locali è preoccupante. Queste strutture gestiscono un'enorme quantità di dati su tutti i cittadini che vivono, lavorano, hanno una proprietà o una ditta nella loro giurisdizione.

Il GDPR sarà una tappa unica per la sicurezza e la privacy dei dati negli affari, con la sua nuova caratteristica, quella della *"privacy by design"*.

Le ditte devono affrettarsi ad assicurarsi che hanno eseguito tutto quello che è ragionevolmente possibile per mettere in sicurezza l'integrità dei dati personali in loro possesso e per farne buon uso quando è necessario. In poche parole, ogni azienda deve imparare ad essere diligente. La nuova legislazione ha previsto multe pesantissime e gli esperti dell'industria scommettono che le prime grandi strutture che non saranno conformi potrebbero diventare degli esempi, venendo loro applicate le penalità massime (o vicine ai massimi previsti). È perciò essenziale poter dimostrare che si è stati diligenti, che i processi sono operativi, che vi sono audit regolari e che si possiede un'assicurazione cyber. Questi sono tutti parametri che ridurranno la responsabilità di un'azienda in caso di perdita di dati.

Epilogo

Il mondo degli affari deve capire quanto le sue risorse digitali ed i dati sensibili in suo possesso sono importanti non solo per le loro operazioni di business. Sono importanti per tutti i stakeholders, nonché per tutti quelli che potrebbero essere lesi nel caso che vengano resi pubblici dati sensibili.

Le aziende devono sbarazzarsi della mentalità del *"ciò non capiterà a me"* o *"siamo un business troppo piccolo per interessare qualcuno"*. La vittimologia di oggi comporta organizzazioni di tutte le dimensioni, da proprietari individuali a liberi professionisti, da ONG a multinazionali.

Le aziende devono iniziare a ripianificare la loro cyber sicurezza e la loro conformità col GDPR, perché non sono due lavori a sé stanti. Al contrario, sono direttamente connessi e se vengono eseguiti correttamente ed in modo sincrono, il risultato finale sarà di rendere il business più efficiente e più funzionale e nello stesso tempo, aumentarne il valore.

A titolo indicativo, proponiamo una lista dei punti sui quali dovrebbe focalizzarsi qualsivoglia ente o azienda:

- Investire in software di cyber security di base (anti malware e firewalls);
- Investire (se necessario) in software di Data Loss Prevention e di Data Loss Detection;
- Investire in formazioni per tutto lo staff, sui principi ed i processi di base della sicurezza dei data;
- Capire ed implementare la *Data Security* e la *Privacy by design;*
- Eseguire audits regolari delle IT Policies e della conformità dei software e hardware;
- Prepararsi per essere conformi al GDPR;
- Preparare un piano di risposta agli incidenti;
- Preparare un piano di Disaster Recovery;
- Formare ed allenare regolarmente, con simulazioni di attacchi, il Response Team;
- Elaborare un piano di controllo dei danni (con un avvocato ed un PR);
- Avere un contratto con una ditta o un professionista di Retainer of Digital Forensics che potrà investigare ogni tipo di incidente immediatamente dopo la sua scoperta.

Prevenire è sempre molto meno costoso che riparare le conseguenze di un disastro. ■

1 http://breachlevelindex.com
2 http://breachlevelindex.com/assets/Breach-Level-Index-Report-2016-Gemalto.pdf
3 http://breachlevelindex.com/assets/Breach-Level-Index-Infographic-2016-Gemalto-1500.jpg
4 https://ico.org.uk/media/action-weve-taken/mpns/2013678/mpn-data-breach-barrister-20170316.pdf
5 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/03/ico-survey-shows-many-councils-have-work-to-do-to-prepare-for-new-data-protection-law/
6 https://iconewsblog.org.uk/2017/03/20/information-governance-survey/

Le conseguenze di una cybersecurity mal compresa e mal gestita: un sistema malato destinato all'implosione!

Intervista VIP con Marc German, Business Diplomat e esperto in criminalità informatica

Marc German

autore: Laurent Chrzanovski

Laurent Chrzanovski: Descriva il Suo percorso.

Marc German: Ho debuttato nella mia carriera internazionale, trent'anni fa, nel quadro dei mercati di compensazione. Ho effettuato numerose missioni all' Estero in regioni che non avevano delle relazioni normalizzate con l'occidente quali l'URSS e come Consigliere di società francesi fui molto presto interessato da ciò che non si definiva ancora come intelligenza competitiva. Da allora ho iniziato numerosi partenariati industriali e commerciali, nell'ambito delle opportunità consecutive alla caduta del Muro di Berlino.

Più di recente, nel 2008, in una pratica di prospettiva, ho fondato il gruppo di riflessione strategica *"Reflextrat"*, dedicato appunto al successo e alla diffusione delle imprese innovanti sui mercati emergenti operando simultaneamente a sradicare delle cattive pratiche in seno alle imprese e alle istituzioni.

Laurent Chrzanovski: Come è arrivato ad interessarsi alla cyber-sicurezza?

Marc German: Poiché oggi tutto è informatizzato e passa da internet, cosciente delle nuove sfide legate alla sicurezza dei progetti informatici sempre più complessi, allora auditore della Cattedra di Criminologia al CNAM, mi sono focalizzato sulla lotta contro la cyber-sicurezza.

Laurent Chrzanovski: Quali aspetti della cyber-sicurezza La preoccupano oggi?

Marc German: La qualità del source-code è il primo livello della sicurezza informatica. In effetti un errore nel codice che provoca una

disfunzione dell'applicazione si chiama un bug, è un errore che si vede e che si può correggere, è solamente costoso; in compenso un errore nel codice, che non provoca disfunzioni e non si vede si chiama una breccia, ed è quest'ultimo il vero incubo delle imprese e delle amministrazioni poiché può costare molto di più …

Ma questa non è che la parte tecnica della cyber-sicurezza che richiede una risposta tecnica, ci sono poi delle sfide comportamentali che sono molto più complicate poiché, come sempre, in materia di protezione e di sicurezza il comportamento umano è l'anello debole, è quindi imperativo sradicare le cattive pratiche.

Laurent Chrzanovski: Come giudica lo stato della presa di coscienza nelle imprese in cui Lei è stato /è attivo?

Marc German: Le imprese e le amministrazioni capiscono oggi che devono uscire dalla dipendenza dei grandi player – Microsoft, Oracle e

SAP – che producono attrezzature alle quali esse devono adattarsi e che sono poco performanti, poco affidabili e molto costose.

Oggi, certe tecnologie di rottura sperimentate permettono di creare in modo agile degli strumenti specifici che rispondono a dei nuovi modelli economici permettendo, per esempio, all'informatica delle imprese di non essere più un fattore di costi, ma una fonte di profitti.

Laurent Chrzanovski: e nel campo nel quale Lei si muove in generale?

Marc German: La mancanza di "igiene comportamentale" degli utilizzatori finali persiste in modo drammatico. Si può utilizzare un software su un terminale e una rete altamente sicura, se l'utilizzatore vi ricarica il suo telefono personale o il suo tablet, rende fragile di fatto l'insieme creando un punto di accesso… La moda del BYOD è un fenomeno aggravante.

Laurent Chrzanovski: quali sono secondo Lei le poste di resilienza del 4.0

Marc German: La capacità delle imprese e delle amministrazioni di premunirsi dai diktat dei principali editori dei soft e di ERP di ogni genere ritrasmessi da società di servizio il cui 70% del volume di affari è costituito dalla manutenzione. I primi forniscono delle soluzioni che non lo sono, poiché i bisogni funzionali specifici delle imprese non sono integralmente coperti, sono allora gli utilizzatori finali che devono adattarsi a degli strumenti inadatti al loro business. I secondi, che

BIO

Specialista in diplomazia aziendale e in prospezioni di affari, Marc German gestisce di numerose reti internazionali nel quadro di partnerships industriali. Specialista del rischio legale e della gestione di crisi, ha fondato nel 2008 il gruppo di riflessione strategica "reflextrat", specializzato nel successo e nella visibilità di ditte novatrici sui mercati emergenti. Questo think tank a sviluppato servizi performanti a continuazione dei lavori della Scuola Francese di Prospettiva del CNAM, istituzione mondialmente riconosciuta per la sua capacità di decriptaggio di problematiche complesse per meglio capire l'avvenire. Pioniere dell'intelligenza in competitività, da più di 30 anni Marc German conduce missioni sul terrreno, in Francia e all'estero, con l'obbligo costante di portare risultati. Ha così partecipato alla creazione, al lancio e allo sviluppo di diverse aziende di successo in settori molto diversi (aeronautica, difesa, energia, internet..). Dopo essere stato consigliere di società francesi nel quadro delle opportunità consecutive alla caduta del Muro di Berlino, ha dato inizio a numerosi partenariati industriali e commerciali, assicurandone la coordinazione tra gli attori istituzionali, le ditte private e le personalità scientifiche, politiche e mediatiche.

Precursore della diplomazia aziendale, creativo riconosciuto per fornire soluzioni, Marc è intervenuto durante tutte le tappe importanti dei vari mercati a seconda dei bisogni specifici dei suoi clienti, governativi o privati (partnerships contro-intuitivi, finanziamenti innovanti, offsets, soluzioni asimmetriche...), curando sempre l'eradicazione di 'bad practices' al seno delle stesse aziende o instituzioni.

Auditore della Cattedra di Criminologia del CNAM, è un partigiano dell'aggiunzione della nozione di "crimine economico" nel Codice Penale, ricoprendo nei regolamenti e nel diritto francese un campo ben più ampio di quello compreso ora e includendo persino la difesa dei piccoli azionari...

Dal 2010, Marc è tresoriere dell'Associazione Francia-Medio Oriente della Legione d'Onore.

Nel 2014, osservando i nuovi challenge europei legati alla safety ed alla security di progetti informatici semprre più complessi, Marc ha creato una ditta di servizi per accompagnare l'evoluzione digitale, specializzata nell'uso di breaking technologies, agili soprattutto nella creazione di software dotati dei più alti standard di qualità, al servizo dei grandi gruppi industriali e delle amministrazioni statali.

hanno un modello economico fondato sulla vendita del "giorno/uomo", si accontentano indelicatamente delle insufficienze dei primi poiché il loro benessere è assicurato dalla consegna dei soft inoperanti: meno tutto questo funziona, più immagazzinano dei patrimoni in manutenzione. Il peggio è che né le amministrazioni, né le imprese sono alla fine proprietari di questi oggetti informatici porosi, inadatti e dispendiosi.

La sfida principale di resilienza del 4.0, è la promozione delle tecnologie di rottura che permettono di produrre in modo agile dei mezzi specifici totalmente adattati ai mestieri. Queste tecnologie esistono, non solo esse consentono di uscire dal funesto modello economico "giorno/uomo" contro prestazioni virtuose "a forfait" ma che permettono anche di avere una informatica al servizio del loro mestiere e non il contrario.

In materia di comportamento, si tratta di mettere l'accento su delle formazioni adattate e soprattutto di responsabilizzare gli utilizzatori finali… Una lunga strada!

Laurent Chrzanovski: quali campi della sicurezza del mondo digitale Le sembrano particolarmente sottovalutati in rapporto ai comportamenti fisici?

Marc German: In materia di comportamento fisico, il problema è innanzitutto endogeno, il "nemico" è prima di tutto all'interno.

Laurent Chrzanovski: chi dovrebbe assumere la cultura di difesa digitale nelle imprese e sotto quale forma a Suo avviso?

Marc German: C'è una responsabilità trasversale, sotto l'egida del "padrone", poiché si tratta di una minaccia sui processi vitali dell'amministrazione o dell'impresa.

Laurent Chrzanovski: Perché secondo Lei l'Europa ha per troppo tempo ignorato la nostra transizione al digitale e le nuove poste in gioco di sicurezza per rapporto alle grandi potenze?

Marc German: Gli europei mancano di visione e di pensiero strategico e fanno fatica a definire in modo appropriato il male al quale sono confrontati, ciò che è vero in materia di terrorismo lo è altrettanto in materia di cyber-sicurezza. Gli slittamenti semantici o l'inversione del senso delle parole snaturano il pensiero.

Senza esserne la replica, il cyber è la trasposizione informatica del mondo reale. Così, la cyber-criminalità non è una nuova forma di criminalità, è la trasposizione della criminalità classica al cyber; i criminali adattano semplicemente il loro modo di azione a ciò che è al tempo stesso un nuovo mezzo, un nuovo vettore e un nuovo terreno di gioco.

Laurent Chrzanovski: è ancora possibile in un continente in pace dal 1945 instaurare di nuovo uno spirito di vigilanza senza farsi tacciare da big-brother o da guerrafondaio?

Marc German: Non si tratta di adottare una postura politica opportunista come risposta ad una moda, la capacità di resilienza è una vera sfida strategica.

Laurent Chrzanovski: perché si è così poco sensibili alle buone pratiche dei nostri vicini in seno all'UE quando quest'ultime hanno fatto le loro prove e si reinventa l'acqua calda in ogni paese? Mancanza di conoscenze? Ego politico?

Marc German: L'insieme degli attori del mondo dell'informatica considera la cyber-sicurezza prima di tutto come un nuovo mercato portatore di crescita economica e di guadagni finanziari, tutti si sono precipitati in ciò che considerano come un nuovo Eldorado.

Ora, come ho affermato in precedenza: meno tutto ciò funziona, più i problemi perdurano e più questi stessi attori si rimpinzano. In Francia più che altrove il sistema è tanto marcio quanto chiuso a chiavistello… Le carriere-tipo dei dirigenti superiori dell'informatica li vedono passare indifferentemente dal mondo dei software a quello dei servizi, alla DSI dei grandi gruppi è il regno dei conflitti di interesse, della cooptazione sfrontata e della grande spartizione fra amici… Si tratta di un vero crimine economico, ecco quindi la faccia nascosta della cyber-criminalità, la più pericolosa e la più costosa, poiché sono le amministrazioni, le imprese e finalmente i contribuenti che pagano la fattura.

Questo sistema prevaricatore è destinato all'implosione! ■

Il fattore umano nella cyber security

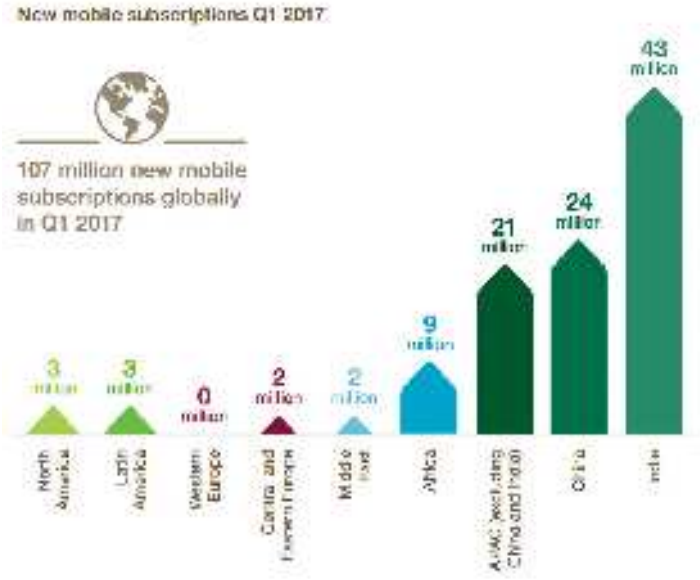
autore: Nicola Sotira

Analizzando i numeri che riguardano la rete il fattore immediatamente è che il miliardo sia un suffisso che caratterizza ogni argomento ad essa relato. IOT, dati, mobile, esporranno sempre il suffisso miliardi, numeri che saranno sempre più grandi; uno scenario che cambierà tutto nel nostro approccio tradizionale e nella cultura di Internet.

Il numero che ha catturato la mia attenzione è quello che ci svela il numero di utenti di Internet nel mondo, stimato a di 3,8 miliardi (1) su una popolazione mondiale di 7,5 miliardi. Un numero che sta crescendo ogni anno ed è connesso all'aumento della mobilità e al numero di abbonamenti alla rete dati, principalmente, LTE. Dando un'occhiata all›ultimo report mobile di Ericsson, possiamo notare che nel primo trimestre del 2017 c'è stato un incremento pari a 107 milioni di nuove utenze mobile, raggiungendo così quota 7,6 miliardi (2). Leggendo tra le righe del report è anche evidente la banda larga mobile spinge la crescita delle iscrizioni in tutte le regioni in cui i nuovi consumatori, spesso, stanno acquisendo la loro prima esperienza su Internet attraverso reti mobili e tramite smartphone. I numeri nel report ci dicono chiaramente che i dispositivi mobili costituiranno la nuova piattaforma di accesso alla rete e che l'aumento di utenti Internet è strettamente collegato a questa crescita. Ritornando al numero della popolazione internet stimata in 3,8 miliardi possiamo spingerci in una affermazione po› più forte ora! Avremo un numero crescente di vulnerabilità, qualcosa come 3,8 miliardi? Osservando tutti i principali incidenti sembra ormai sempre più evidente la correlazione con gli errori umani, l›uso improprio della tecnologia digitale. Forse la mancanza di conoscenza? Quando il lavoro o i sistemi diventano più complessi aumenta la possibilità di errore umano. Quindi, non ci si può stupire che l›errore umano sia responsabile di oltre un terzo delle violazioni dei dati (3).

Trasformazione Digitale

Nel suo ultimo libro, Alec Ross, ex consigliere di Obama e Hillary Clinton, parla di come la tecnologia digitale possa avere un effetto di spinta nell'economia di un Paese. Il digitale trasformando ogni aspetto della nostra vita cambierà drasticamente l'economia, cosa che Ross riassume così: "La terra era la materia prima per il mondo basato sull'agricoltura, le risorse minerarie per quello industriale, così i big data sono la materia prima su cui si basa e su cui sarà sempre più basata l'economia mondiale (4) ". La trasformazione digitale promette di cambiare il volto delle nostre aziende e di tutti i settori industriali, ma, essere digitali richiede grandi cambiamenti per cui semplicemente investire nelle ultime tecnologie non basta. Le organizzazioni devono cercare di progettare nuovi scenari di business, rivedere i modelli operativi, attrarre e promuovere talenti digitali.



Siamo pronti a questo cambiamento? Siamo in grado di misurare la conoscenza del digitale nella nostra organizzazione? Pensiamo che sia un compito difficile da attuare?

Nel caso avessimo qualche dubbio su questa rivoluzione tanto profetizzata, non potremmo ignorare il fatto che tutte le aziende che hanno pienamente attuato questo processo abbiano avuto successo migliorando la redditività, la produttività competendo e vincendo anche contro i colleghi nativi digitali.

Un cambiamento che richiede persone e conoscenze, non è solo questione di implementazioni di Intelligenza Artificiale o di Big Data.

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.

Il Cyber Theater

Nella terra promessa del digitale dobbiamo tenere a mente che lo scenario sta diventando sempre più complesso. Entro il 2020 Cisco stima che il 99% dei dispositivi sarà connesso, stiamo parlando di più o meno di 50 miliardi di dispositivi, e questo significa che ci troveremo in uno scenario dove anche i nodi periferici avranno capacità computazionali e dati. Tutti contesti dove parlare ancora di perimetro, in cui organizzare la difesa è storia antica, i nuovi confini sono rappresentati dai dati.

Prima di andare con la nostra immaginazione fino al 2020, possiamo provare a fare un esercizio sull'anno che sta arrivando, il 2018 quando la PSD2 entrerà in campo. PSD2 sta per *Payments Services Directive,* la Direttiva UE sui servizi di pagamento che, in poche parole, afferma che le banche non hanno la proprietà delle informazioni dei loro clienti, ma è il cliente stesso a possederle.

Risultato? Le banche dovranno fornire l›accesso, tramite API, a terze parti. Il cliente potrà decidere se fornire l›accesso ad agenti di borsa, contabili, gestori di finanze o App, e la banca dovrà consentirne l›accesso. Parlando di App, significa che presto saremo in grado di utilizzare una terza parte per gestire e controllare il nostro conto bancario, trasferire denaro e pagare. Possiamo facilmente immaginare che in un breve periodo saremo in grado di pagare il nostro conto tramite Facebook, Google o Apple. Ma, ancora di più, potremo scaricare software di terze parti per gestire il nostro banking online senza dover creare un account separato al di fuori della nostra banca. Le banche stanno cercando di studiare strategie e modelli di business per mantenere il loro mercato, ma ancora una volta ci serve una riflessione sugli utenti. Siamo pienamente preparati per questo cambiamento? Siamo assolutamente sicuri che tutti gli utenti conoscano l›impatto reale in termini di sicurezza? Il numero di App scaricate da market non ufficiali è significativo insieme al numero di smartphone *jailbreakati* o *rootati*.

Siamo completamente certi che i consumatori abbiano una reale comprensione dell'impatto che tale comportamento provochi nello scenario descritto in precedenza? Di certo le banche stanno applicando misure di sicurezza più forti e la PSD2 provvede un framework di sicurezza che incrementa le misure di sicurezza, ma ancora il comportamento umano e la conoscenza sono fondamentali per prevenire frodi e danni.

Scenario che ci metterà poco a diventare più sofisticato, perché in futuro le macchine entreranno nel processo digitale di pagamento. I processi Machine to Machine (M2M) saranno la naturale evoluzione di questo percorso che, semplificando e automatizzando i processi, richiederà all'utente una specie di *codifica della fiducia*. Ci fideremo delle cifre visualizzate dal sul display del nostro cellulare quanto ci fidiamo dei soldi che abbiamo nel nostro portafogli oggi? Questo perché i nuovi contesti digitali porteranno sempre di più verso una valuta di 0 e 1, non più banconote in tasca.

Questa evoluzione di scenari e trasformazione di processi richiede un cambiamento culturale, una mentalità digitale che le organizzazioni e il governo devono affrontare, un divario culturale che dobbiamo recuperare tanto velocemente quanto i passi della tecnologia in questi anni. Naturalmente, nel futuro teatro digitale ci aspetteranno molti scenari complessi, come veicoli autonomi, robot e molto altro ancora in un mondo sempre connesso. Tornando al presente possiamo vedere già cambiamenti introdotti tramite social network e mobile. Nelle organizzazioni, ci troviamo di fronte a un fenomeno crescente di BYOD che spesso viene sottovalutato riguardo al problema della sicurezza. Questi dispositivi sono accessi a banda larga presenti nelle nostre organizzazioni, con dispositivi in cui le persone condividono informazioni aziendali e personali senza, a volte, una chiara comprensione del potenziale rischio.

Quanti utenti condividono la loro posizione perché hanno una reale necessità di farlo? Quanti dispositivi di tracciamento inviano dati sensibili e posizioni nelle nostre organizzazioni? Quanti manager sanno che un telefono cellulare in una riunione strategica potrebbe essere pericoloso? E potremmo continuare con il cloud e l'utilizzo che stiamo facendo di software che forse stanno condividendo i nostri dati con il nostro permesso, permesso che spesso molti utenti ignorano vista la semplicità con le quali si accettano le clausole di installazione.

Il comportamento umano nel digitale

Una lettura interessante in questa area è il libro "Psychology of the Digital Age: Humans Become Electric" di John Suler. Suler è Professore di Psicologia presso la Rider University, riconosciuto a livello internazionale come esperto nel settore emergente della *cyberpsicologia*.

Nel libro Suler spiega che le persone tendono a pensare al cyberspazio come un luogo immaginario senza vere frontiere, uno luogo da non prendere troppo sul serio (5). Leggendo il libro potreste realizzare qualcosa che i laboratori hanno già evidenziato, le persone agiscono nel cyberspazio in un modo completamente diverso da quello che usano di solito nel mondo fisico.

Si rilassano, si sentono più disinibiti, si esprimono più apertamente e la stessa differenza di comportamento riguarda i temi della sicurezza.

I ricercatori hanno definito questo comportamento *"effetto disinibizione"*. Abitudine pericolosa che può causare problemi, in questo contesto le persone tendono a condividere cose molto personali, rivelano emozioni segrete, paure, desideri e abbiamo visto, in alcuni attacchi di ingegneria sociale, anche una password e informazioni riservate.

Diversi studi sugli utenti dimostrano la diversa percezione del rischio da parte degli utenti nello spazio digitale. I laboratori Felt e Wagner, ad esempio, hanno esaminato il comportamento degli utenti con alcune app che prendono decisioni sull'accesso al dispositivo e i propri dati.

Il risultato è stato che quando le azioni richieste riguardavano perdite finanziarie erano più attenti, mentre quando l›azione era reversibile il livello di difesa si abbassava. Differenze sostanziali anche nel comportamento tra uomo e donna, e le persone, di 50 anni di età, classificati più a rischio rispetto alle persone sotto i 30 anni.

Altro studio interessante è stato condotto da Garg and Camp (7) sulla percezione dei rischi online come, per esempio, virus, phishing e furto d›identità. Risultato? Quando i rischi possono essere facilmente confrontati con i rischi conosciuti nel mondo fisico vengono meglio compresi e quindi presi in considerazione.

Sicurezza know how

Come descritto, siamo in uno scenario più complesso dominato da nuove tecnologie in cui la sicurezza deve essere più che una semplice riflessione. Capiamo chiaramente che dobbiamo spostare l'attenzione difendere a mettere in sicurezza il dato ovunque sia presente, dai dispositivi sino al cloud. Ma che dire del sapere delle persone sulla cultura della sicurezza. Come abbiamo scritto sopra, diversi studi dimostrano che il comportamento umano e la percezione della sicurezza nello spazio informatico sono diversi e spesso rischiosi. Comportamenti rischiosi che ci causano problemi e aumentano l'esposizione delle organizzazioni. A causa della complessità e al fine di aumentare le capacità di cybersecurity abbiamo bisogno di un piano per migliorare la consapevolezza su questo tema.

Un piano di formazione che deve coinvolgere scuole, consumatori e dipendenti delle organizzazioni. Educare i giovani nelle scuole sul rischio e sull'uso responsabile degli strumenti digitali nel cyber spazio aiuterà una nazione a prepararsi per il futuro, con l'ovvio di creare una pipeline di talenti, poiché sappiamo che la carenza di competenze per le organizzazioni è ancora uno dei problemi aperti.

Uno di questi programmi sui ragazzi è stato avviato in Inghilterra dove verranno offerte lezioni di sicurezza informatica a ragazzi di 14 anni e più, un progetto sperimentale che offre formazione di quattro ore a settimana su questo argomento. Un uso responsabile e sicuro degli strumenti digitali e dei dispositivi di rete è un must per qualsiasi utente, e dato che l›approccio tecnologico è sempre più precoce, è bene iniziare il percorso educativo verso la consapevolezza a partire dalla scuola.

La formazione e gli strumenti devono essere adattati in base all›età e alle esigenze dei destinatari, è possibile sviluppare progetti e programmi volti a promuovere un›adeguata conoscenza del mondo digitale con cui i bambini e i giovani interagiscono; un altro ottimo esempio è disponibile on-line con l›iniziativa code.org, organizzazione no profit americana.

Le organizzazioni dovrebbero condurre campagne di sensibilizzazione che coinvolgano dipendenti e clienti, questi programmi dovrebbero concentrarsi sull'incoraggiare una modifica del comportamento digitale sia in ufficio che a casa. L›obiettivo è che le persone siano in grado di comprendere e seguire le policy provenienti dall›organizzazione, prevenire e segnalare incidenti e contribuire alla condivisione delle informazioni.

Conclusioni

La trasformazione digitale richiede un ecosistema sicuro per offrirci il massimo vantaggio. Ma dobbiamo anche colmare il divario culturale creato da questi strumenti.

L'aumento delle misure di sicurezza e la realizzazione di un'architettura digitale sicura e resiliente devono essere priorità per tutti i paesi e devono essere priorità nelle agende dei governi. Oltre a questo abbiamo bisogno di un piano di formazione e sensibilizzazione a partire dalla scuola, l'innovazione è un percorso che deve essere preparato per formare il DNA digitale della nuova generazione.

Riferimenti

.1 source WeAreSocial 2017

.2 Ericsson Mobility Report 2017

.3 2017 State of Cybersecurity from Ponemon Research Group

.4 The Industries of the Future - Alec Ross

.5 Psychology of the Digital Age: Humans Become Electric - John Suler

.6 Felt, A., Egelman, S., and Wagner, A survey of smartphone users' concerns. Proceedings of Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM 2012), ACM Press.

.7 Vaibhav Garg and Jean Camp. End user perception of online risk under uncertainty. IEEE Proceedings of HICCS 2012. ■

Sicurezza dei robot industriali: rischi, vulnerabilità e attacchi

Politecnico di Milano e Trend Micro FTR hanno analizzato il mondo dell'Industry 4.0 rivelando rischi, pericoli e le possibili contromisure.

Autore: Federico Maggi,
Trend Micro

I robot industriali possono essere compromessi, alterando in maniera decisiva la normale funzionalità dei sistemi industriali e minando la sicurezza del personale. Questo è uno dei risultati di una delle mie ultime ricerche, realizzata in collaborazione tra Politecnico di Milano e Trend Micro FTR, **"Rogue Robots: Testing the Limits of an Industrial Robot's Security,"** presentata il 22 maggio 2017 alla prestigiosa conferenza accademica "IEEE Symposium on Security and Privacy" a San Jose (CA) e anche il 25 luglio al principale evento industriale di cybersecurity, "Black Hat Briefings" a Las Vegas (NV).

La ricerca ha avuto origine dalla collaborazione tra il laboratorio di sicurezza e architetture (NECST, Ing. Davide Quarta, Ing. Marcello Pogliani, Ing. Mario Polino supervisionati dal Prof. Stefano Zanero) del Dipartimento di Elettronica, Informazione e Bioingegneria del Politecnico di Milano e il team FTR di Trend Micro, rappresentato dal sottoscritto.

La ricerca conferma lo spirito pioneristico dell'eccellenza accademica italiana e di Trend Micro, da sempre precursore nell'esplorare i nuovi grandi temi legati alla tecnologia e alla sicurezza, e dimostra per la prima volta come i robot industriali possono essere compromessi. La nostra analisi suggerisce anche una strategia per affrontare in tutta sicurezza l'avventura della quarta rivoluzione industriale.

I robot nell'Industry 4.0

I robot rappresentano un elemento sempre più critico del nostro tessuto industriale. Questo li rende un bersaglio potenziale sia per gruppi cybercriminali in cerca di guadagno, sia per stati che vogliono colpire l'operatività di un avversario.

(Continua a pagina 54)

BIO

Federico Maggi è Ricercatore di minacce con il team di Ricerca Prospettica di Trend Micro (FTR), una élite di ricercatori la cui missione è combattere i criminali informatici e esplorare il futuro delle tecnologie emergenti, cercando di prevedere e prevenire rischi e minacce emergenti alla sicurezza.
Prima di entrare in Trend Micro, è stato Assistant Professor presso il Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB), Politecnico di Milano in Italia, dove ha co-diretto il gruppo di sicurezza dei sistemi presso il Laboratorio NECST. Collabora con diversi gruppi di ricerca (ad esempio, UCSB, FORTH, NEU, Stony Brook, KU Leven e RHUL), e ha tenuto diverse lezioni e conferenze come relatore in sedi e scuole di ricerca internazionali. Svolge anche la funzione di revisione o organizzazione di comitati di conferenze rinomate.

Sicurezza adattiva e HuMachine® Intelligence per proteggere il business dalle minacce next-gen e minimizzare i danni

Autore: Morten Lehn,
General Manager Italy di Kaspersky Lab

BIO

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

In vent'anni di attività nel mondo della sicurezza, Kaspersky Lab ha maturato una notevole esperienza, che indica come gli attacchi, non solo quelli mirati, siano sempre più compositi e difficili da rilevare.

C'è bisogno d'implementare una strategia olistica costante, che non trascuri nulla e che sia la fusione di tre fattori fondamentali: big data, apprendimento automatico e la competenza degli analisti.

Il termine big data non dovrebbe essere preso alla lettera, come se si trattasse di una vasta gamma di informazioni conservate da qualche parte. Non è solo un database; si tratta di una combinazione di tecnologie che consentono l'elaborazione istantanea di grandi volumi di dati al fine di estrarre informazioni di threat intelligence. In questo caso, con il termine "data" ci riferiamo a tutti gli oggetti, sia che essi siano innocui, totalmente dannosi o potenzialmente utilizzabili per scopi dannosi.

Ci dedichiamo alla sicurezza informatica da più di 20 anni, e in tutto questo tempo abbiamo analizzato un gran numero di oggetti. Tutte le informazioni in merito sono conservate al sicuro nei nostri database. E quando parliamo di "oggetti", ci riferiamo non solo ai file o a parti di codici, ma anche a indirizzi Web, certificati, esecuzione di file log per applicazioni legittime e non. Tutti questi dati non solo vengono catalogati con etichette come "pericoloso" o "sicuro", ma sono immagazzinate anche informazioni sui rapporti tra gli oggetti: da quale sito web il file è stato scaricato, quali altri file sono stati scaricati dal sito e così via.

KSN è il nostro servizio di sicurezza su cloud. Una delle sue funzioni è quella di bloccare rapidamente le minacce più recenti per il cliente. Allo stesso tempo, permette a tutti i clienti di partecipare alla crescente sicurezza globale inviando su cloud metadati anonimi sulle minacce rilevate. Studiamo ogni minaccia rilevata da vari punti di vista e aggiungiamo le sue caratteristiche nel nostro database delle minacce. Fatto ciò, i nostri sistemi possono rilevare con precisione non solo quella minaccia, ma anche quelle simili. Quindi, la nostra raccolta riceve dati aggiornati in tempo reale.

Delineare cosa sia l'apprendimento automatico e come viene utilizzato in Kaspersky Lab non è un compito facile. Innanzitutto va detto che usiamo un approccio multilivello. Gli algoritmi di apprendimento automatico vengono utilizzati in diversi sottosistemi e a diversi livelli.

Ogni giorno i nostri sistemi ricevono centinaia di migliaia di oggetti che hanno bisogno di un'analisi tempestiva e di categorizzazione (etichettare un oggetto come

pericoloso o meno). Già più di 10 anni fa sapevamo che non avremmo potuto farcela senza automazione. Il primo compito era capire se un file sospetto assomigliasse a uno dannoso che già avevamo. E qui entrava in gioco l'apprendimento automatico: abbiamo creato un'applicazione che analizzava tutti i nostri dati salvati e, quando veniva aggiunto un nuovo file, i nostri analisti venivano informati su quale fosse l'oggetto più simile al nuovo arrivato.

È divenuto subito chiaro che sapere se un oggetto fosse simile ad altri dannosi non era abbastanza. Avevamo bisogno di una tecnologia che permettesse al sistema di dare un verdetto in maniera indipendente. Così abbiamo costruito una tecnologia basata su alberi di decisione. Addestrata sulla nostra vasta raccolta di oggetti dannosi, la tecnologia rilevava una serie di criteri, specifiche combinazioni che potevano servire come indicatori che definiscono senza ambiguità un nuovo file come pericoloso.

Seguendo il nostro principio di sicurezza multilivello, i nostri modelli matematici vengono anche utilizzati per il rilevamento dinamico. In effetti, un modello matematico è in grado di analizzare il comportamento di un file eseguibile proprio durante la sua esecuzione. È possibile costruire e formare il modello secondo gli stessi principi applicati ai modelli matematici di rilevamento statico, utilizzando invece i log file di esecuzione come "materiali di allenamento". Tuttavia, c'è una grande differenza; in condizioni reali, non possiamo permetterci di aspettare finché il codice termini l'esecuzione. La decisione dovrebbe essere presa dopo aver analizzato un minimo di azioni. Attualmente, un progetto pilota di questa tecnologia, basata sull'apprendimento profondo, sta dando ottimi risultati.

Gli esperti in apprendimento automatico concordano sul fatto che non importa quanto intelligente sia un modello matematico, un essere umano sarà sempre in grado di superarlo, soprattutto se la persona è creativa e può dare un'occhiata a come funziona la tecnologia, o se c'è tempo a disposizione per eseguire numerosi test ed esperimenti. Per questo motivo, prima di tutto, ogni parte del modello deve essere aggiornabile; in secondo luogo, l'infrastruttura deve funzionare perfettamente; e terzo, l'essere umano deve controllare il robot. Ecco qui sono tutti e tre i casi.

Circa 20 anni fa, la nostra squadra di Anti-Malware Research (AMR) operava senza l'ausilio di sistemi automatici. Oggi, la maggior parte delle minacce vengono rilevate da sistemi formati dai nostri ricercatori. In alcuni casi, il sistema non può dare un verdetto inequivocabile oppure pensa che l'oggetto sia dannoso, ma non può ricollegarlo a nessuna famiglia conosciuta. Quindi, il sistema invia un avvertimento ad un analista AMR in servizio, fornendo una serie completa di indicatori in modo che l'analista possa prendere la decisione finale.

All'interno al nostro AMR c'è un gruppo di ricerca specifico chiamato Detection Methods Analysis Group, che è stato creato nel 2007 per lavorare specificamente sui nostri sistemi di apprendimento automatico.

Ultimo ma non meno importante tassello dell'approccio olistico sono i nostri analisti raggruppati nel Global Research and Analysis Team (GReAT). I ricercatori di questa squadra indagano le minacce più complesse: APT, campagne di cyberspionaggio, i maggiori focolai di malware, ransomware e le tendenze cybercriminali nascoste ma presenti in tutto il mondo. La loro competenza unica sulle tecniche, gli strumenti e gli schemi di cyberattacchi ci consente di sviluppare nuovi metodi di protezione che possono fermare anche gli attacchi più complessi. ■

Sicurezza dei robot industriali: rischi, vulnerabilità e attacchi

(In seguito a pagina 52)

Parlare di attacchi informatici che coinvolgono i robot fa immediatamente pensare ai film di fantascienza. La realtà però è così lontana, almeno concettualmente: i sistemi robotici nell'industria sono infatti un ingranaggio vitale nei processi manifatturieri e presenti in ogni settore, dai produttori di chip in silicio alle catene di produzione di autovetture, passando per vetrerie o industrie alimentari, per esempio. Le stime parlano che nel 2018 il numero di robot nelle fabbriche di tutto il mondo sarà di 1.3 milioni ed il trend sarà sempre più in crescita. I robot sono un fondamentale fattore abilitante per l'Industry 4.0, una nuova era di innovazione che automatizza e rende più intelligenti le fabbriche e che potrebbe trasformare la società nello stesso modo in cui il motore a vapore ha cambiato il corso della storia nel XVIII secolo.

Nel report spieghiamo come, dal momento in cui questi sistemi diventano sempre più intelligenti e interconnessi, cresce la loro superficie di attacco. Alcuni robot possono addirittura essere raggiunti direttamente da Internet, per il monitoraggio e la manutenzione a distanza. Purtroppo, questo nuovo ecosistema emergente è caratterizzato però da software di vecchia generazione, basato su sistemi operativi vulnerabili, librerie non sempre aggiornate (o non aggiornabili!), scarso o scorretto utilizzo di crittografia, sistemi di autenticazione deboli, con credenziali predefinite che non possono essere cambiate facilmente. Combinando vulnerabilità di queste classi, trovate durante la ricerca, abbiamo dimostrato l'esistenza di 5 attacchi specifici dei sistemi robotici industriali, che vanno ad esempio dalla violazione dei minimi requisiti di sicurezza fisica, fino all'introduzione di micro difetti negli oggetti manipolati dal robot.

Da qui, gli scenari di attacco sono svariati: creazione di danni fisici, sabotaggio di prodotti, esfiltrazione di segreti industriali, fino alle richieste di riscatto avanzate dall'aggressore in cambio di rivelare in quali unità di prodotto egli ha silenziosamente introdotto micro-difetti (e.g., automobili, aerei, medicinali). Per tutelarsi è necessario un approccio e uno sforzo olistico che richiede il sostegno e la partecipazione di tutti gli stakeholder, inclusi i vendor di security e gli sviluppatori di software e questo va oltre il migliorare semplicemente la qualità dei software embedded.

La strada è ancora lunga, ma ricerche di questo genere aiutano a dare un segnale e a sviluppare un'Industry 4.0 sicura. ■

Il fenomeno del deep web

La rivoluzione digitale e le nuove sfide della sicurezza

"La rete è il mondo rifatto con i materiali della comunicazione. Con l'avvento dei ***digital*** media niente sarà come prima. Una nuova categoria dell'essere si mescolerà alla dimensione tradizionale, modificando le relazioni interpersonali, le abitudini, gli atteggiamenti individuali e i comportamenti collettivi. Ancora non sappiamo le conseguenze che scaturiranno dalle enormi potenzialità che la multimedialità porta con sé".

La citazione del filosofo francese Pierre Levy richiamata da Gian Maria Fara, Presidente dell'Eurispes autore della prefazione al saggio di Livio Varriale (*La Prigione dell'umanità*, Minerva Edizioni) tra poco in libreria, può essere utile a innescare una riflessione sulla pervasività di Internet che ha ormai travalicato le originarie finalità comunicative, modellando radicalmente l'universo del lavoro e i ritmi della quotidianità. Viviamo, infatti, tutti dentro il web come in una dimensione omeopatica. Dall'industriale al digitale, stati società e imprese su scala globale, stanno sperimentando un profondo salto di paradigma: il capitale intangibile e giacimenti di know-how grazie ai nuovi strumenti dell'Ict sono, infatti, per la prima volta disponibili su fonti potenzialmente aperte a tutti. Connettività diffusa, Big Data, Internet delle cose, Cloud Computing sono tutti strumenti che oltre a mutare i processi organizzativi e produttivi stanno incidendo profondamente sugli equilibri della società contemporanea. Basti pensare che il 90% dei dati disponibili è stato creato negli ultimi due anni, che i social network permettono già a miliardi di persone di esprimere e comunicare le proprie idee in tutto il mondo alla velocità di un click e che nel 2020 il numero di device connessi alle reti si prevede potrà toccare quota 80 miliardi.

Il lato oscuro della Rete

Esiste infatti un lato oscuro della rete che va sotto la definizione di *"deep web"*, la "fogna dell'universo parallelo" che nasconde illeciti e atroci nefandezze, che mette in guardia gli specialisti della sicurezza. "Questa altra faccia della luna ha il profilo sinistro di una nera regione dell'illecito, in cui si commerciano armi, si spacciano sostanze stupefacenti, si effettua cyberspionaggio, si fanno circolare medicine fuorilegge, vi si esercita la pedo- pornografia e ogni forma di prostituzione fisica e, quel che è peggio intellettuale". La parte cosiddetta clear della rete è solo la punta dell'iceberg, una briciola infinitesimale, rispetto a un sommerso crescente, ormai popolato da siti che fanno riferimento a banche, governi, imprese multinazionali, cellule terroristiche, hacker senza scrupoli. Un esercito organizzato, una macchina criminale che si alimenta con scientifica e diabolica rapidità. I fatti più recenti della cronaca hanno dimostrato l'urgenza di questo fenomeno. Il recente ed eclatante caso di *"Wannacry"* come è noto ha inaspettatamente scandito una sorta di *"Day after digitale"* senza precedenti che ha messo a nudo le vulnerabilità della *digital society*. L'Europa e non solo l'Italia si è scoperta impreparata rispetto a un evento che ha evidenziato l'ingenuità e l'impreparazione degli utenti, mostrando la delicatezza di sistemi pubblici che non hanno ancora maturato una omogenea visione del rischio. "Persino l'ultimo recente alert riguardante un software obsoleto capace di mettere a rischio i segreti dell'esercito rendendo vulnerabile gli apparati della difesa può dare l'idea della posta in gioco. Camminiamo tutti su un terremo di seta, sospesi su un baratro in cui potenza tecnologica e fragilità vanno a braccetto. La pericolosa espansione del *deep web* rende ancora più fosco il quadro fin qui tratteggiato, facendo comprendere l'importanza che dovrà assumere una *governance* del rischio multilivello, adeguata a sventare minacce sempre più sofisticate. Tutto questo comporterà investimenti crescenti nella formazione di nuove figure professionali. Il *security manager* avrà l'arduo compito di "tutelare" la trasmissione di una mole crescente di dati e informazioni. Dovrà essere messa a sistema una capacità di gestire pianificazioni, policy e processi, particolarmente complessi. Sempre più rilevanza avranno i Big Data, che richiederanno ai professionisti della security competenze specifiche di Data Analyst.

Tra immunizzazione e adattamento

Lo studio di Varriale dimostra infine, con dovizia di dati, come governance della sicurezza e governance dei sistemi complessi, siano ormai termini che si intrecciano. In un mondo caratterizzato dalla instabilità dove è venuta meno la cultura del controllo, la classe dirigente dovrà in fretta comprendere che le tradizionali strategie di governo dei processi evolutivi della scienza e della tecnologia risulteranno sempre meno efficaci. Sarà decisivo mettere in campo capacità strategica e intuizione nell'intercettare i segnali del cambiamento. L'esperienza più recente insegna che l'azione di contrasto al cyber crimine non potrà risolversi in una risposta meccanica agli attacchi esterni, bisogna piuttosto mettere in atto delle policy che sappiano interpretare i processi "carsici" dell'infezione, che allignano nel "sottosuolo" del *deep web*.

In conclusione non sembra inopportuno appropriarsi della metafora biologica utilizzata dal linguista e antropologo Gian Paolo Caprettini: *"la sicurezza di domani si fonderà sul delicato equilibrio tra due processi: immunizzazione e adattamento. Gli attacchi provengono dal mondo esterno e il soggetto – individuo, stato o impresa che sia - non dovrà fare altro che mettere in moto gli anticorpi per assicurarsi la sopravvivenza. Ma gli anticorpi non sono altro che una rielaborazione di informazione a livello genetico".*

Risulterà decisivo ritrovare un equilibrio tra due forze antagoniste che agitano l'*homo-tecnologicus*: una spinta centrifuga che lo ha portato e lo porta a conquistare lo spazio uscendo da sé e una forza centripeta che lo induce fatalmente a ripiegarsi a chiudere i ponti con l'esterno, a vivere nella "schiavitù volontaria" di apparati che ne limitano continuamente la libertà. La rete potrà essere un meccanismo di compensazione, la valvola potente che può consentirgli di recuperare i contatti perduti con la vita delle città contemporanee o si trasformerà in una soffocante e subdola prigione? Intanto reale e virtuale si continuano a mescolare nel flusso del web, amplificando la circolarità di un processo esistenziale e psicologico, che rende difficile ogni tentativo di orientamento. Probabilmente dovremo aggiungere un ulteriore significato al termine sicurezza, individuabile nell'esigenza di riequilibrare il rapporto tra l'io e il mondo, tra il "corpo elettronico" e le risorse di creatività di cui ciascuno è originale portatore. ■

web for your business
swiss webacademy

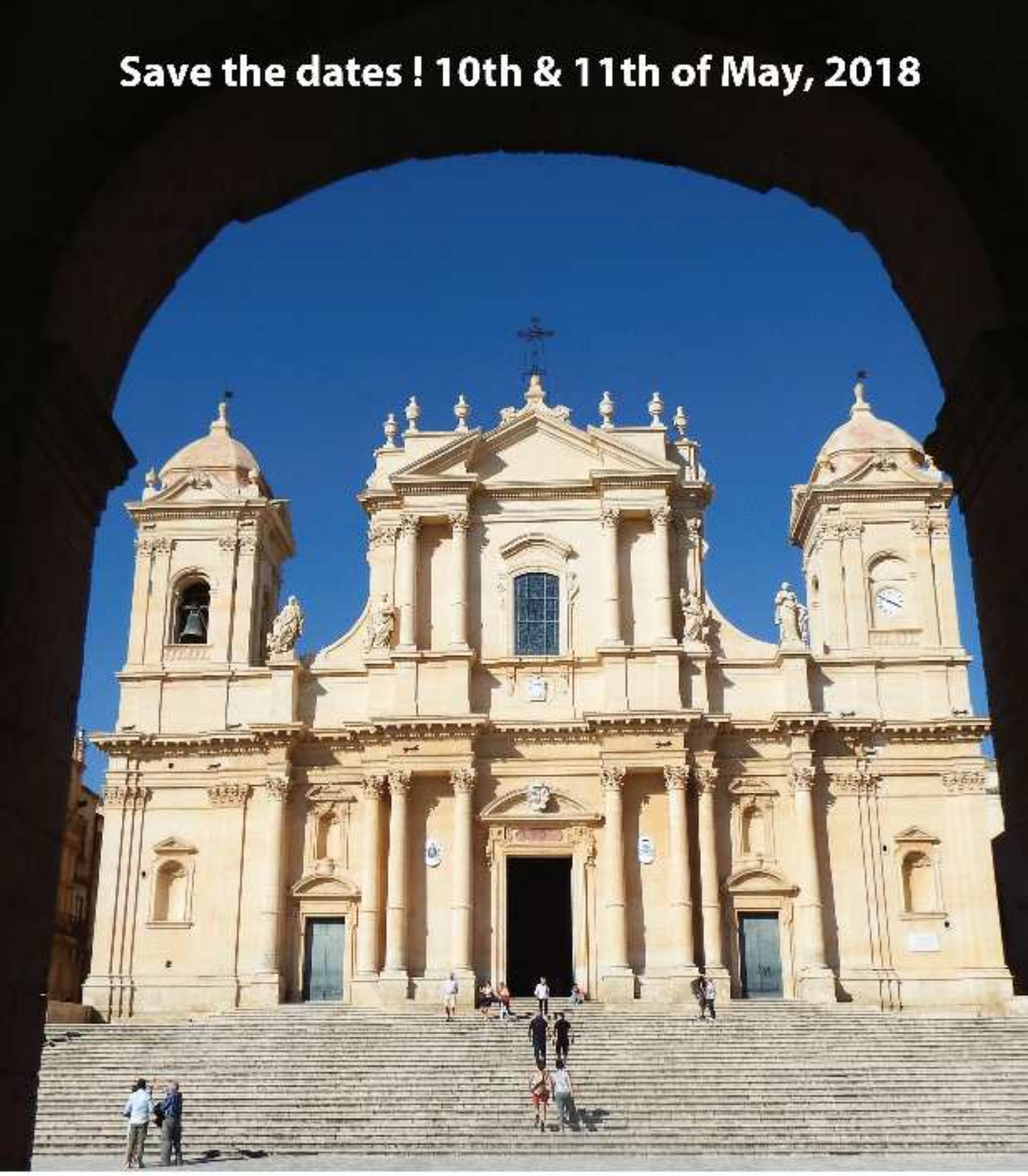
CYBERSECURITY ROMANIA
CONGRESS
SIBIU

CYBERSECURITY SWITZERLAND
CONGRESS
PORRENTRUY

CYBERSECURITY MEDITERRANEAN
CONGRESS
NOTO

3 Specific Ecosystems
3 Public-Private Dialogue Platforms

Save the dates ! 10th & 11th of May, 2018



Cybersecurity-Mediterranean at Noto, Sicily

organized by:

CYBERSECURITY MEDITERRANEAN
- CONGRESS -

CITTA' DI NOTO
PATRIMONIO DELL'UMANITÀ

web for your business
swiss webacademy

www.cybersecurity-mediterranean.it

ICS FORUM
Industrial CyberSecurity

MILANO, 30 gennaio 2018
Grand Visconti Palace

PRESS

Sicurezza industriale, è il momento di agire

I cyber attacchi stanno causando alle imprese perdite economicamente rilevanti e a farne le spese sono sempre più spesso le strutture manifatturiere. Basti pensare che il danno causato alle imprese del settore industrial / manufacturing ammonta, secondo un recente studio di Accenture, in media a oltre 10 milioni di dollari l'anno.

Anche i più recenti dati del Rapporto Clusit confermano che da gennaio a giugno 2017 gli attacchi informatici sono cresciuti dell'8,35% rispetto allo stesso periodo del 2016 e che l'Europa sta diventando uno dei bersagli preferiti del cyber crime.

Nonostante il tema della cyber security nell'industria stia diventando sempre più una priorità e le aziende stiano procedendo nei loro percorsi di digital transformation, manca ancora in Italia una cultura diffusa su queste tematiche: le aziende, soprattutto le micro e piccole imprese, non sono preparate né a difendersi né a reagire ai cyberattacchi.

L'evento

Di questi temi si parlerà a Milano, il prossimo 30 gennaio, a ICS Forum, l'evento organizzato da Messe Frankfurt Italia dedicato non soltanto a chi opera nel settore della sicurezza informatica, ma anche e soprattutto a chi con questi temi deve, suo malgrado, confrontarsi ormai quotidianamente in azienda: dai tecnici dei reparti produttivi fino ad arrivare al top management delle imprese manifatturiere.

"Messe Frankfurt Italia organizza da diversi anni eventi dedicati al mondo manifatturiero e delle utilities, tra cui una serie di tavole rotonde per promuovere la Cultura 4.0", sottolinea Francesca Selva, Vice President di Messe Frankfurt Italia. "Parlando con le tante imprese che abbiamo incontrato nel corso di questi appuntamenti abbiamo colto l'esigenza di un evento che offrisse formazione e informazione sul tema della sicurezza industriale. È un'iniziativa che troverà poi un seguito anche a maggio, in occasione della prossima edizione di SPS Italia a Parma, dove la Cyber Security sarà uno dei pilastri del Percorso Digital Transformation".

A presiedere ai contenuti del Forum è uno Steering Committee del quale fanno parte esperti provenienti da università, aziende utilizzatrici, associazioni patrocinanti, realtà che sviluppano soluzioni di automazione, aziende fornitrici di tecnologie IT, integratori di sistemi, aziende specializzate nella fornitura di soluzioni per la sicurezza dei sistemi, società di servizi e consulenza.

"Oggi i temi della OT Security e della Continuità Operativa sono di estrema importanza nello sviluppo dei piani di innovazione e digitalizzazione in ottica Industria 4.0 e Utility 4.0, sia quindi nei contesti tipici del manufacturing che nelle infrastrutture per erogazione di servizi essenziali", spiega Enzo Maria Tieghi, presidente dello steering comittee di ICS Forum. "Per questo sono convinto che un evento come ICS Forum sarà un appuntamento di assoluto interesse per chi deve confrontarsi con il tema della Industrial Cyber Security, cioè la protezione da rischi informatici di reti e sistemi di

Messe Frankfurt Italia
info@italy.messefrankfurt.com
www.messefrankfurt.it
Tel. +39 02 880776.1
Fax +39 02 72008053

Contatti
press@icsforum.it

PRESS

Nel corso della giornata, alla quale sarà possibile partecipare gratuitamente registrandosi all'indirizzo https://www.eventbrite.it/e/biglietti-ics-forum-37758435497, saranno offerti ai partecipanti non soltanto informazioni generali sul tema, ma anche indicazioni concrete per aiutare le imprese a passare dalla teoria alla pratica. Si parlerà del rapporto tra Cyber Security e Digital Transformation, degli impatti sulla proprietà intellettuale e sulla gestione della privacy, anche in vista della prossima entrata in vigore del regolamento GDPR, di normative, di gestione del rischio negli impianti industriali. Saranno inoltre presentati dei casi aziendali, al fine di fornire degli esempi di come aziende di diversi settori e dimensioni stanno affrontando questo argomento.

"Un tema chiave per il successo della transizione digitale nell'industria è legato alla sicurezza dei dati sensibili che si possono ottenere dalle macchine di una linea produttiva", spiega Marco Vecchio, segretario di ANIE Automazione, una delle associazioni che ha concesso il patrocinio alla manifestazione. "In particolare, al fine di creare valore aggiunto dalla enorme quantità di informazioni che si raccolgono, risulta strategica la relazione che si instaura tra costruttore di macchine e utilizzatore finale il quale dovrebbe sempre più affidarsi al suo fornitore per l'analisi di questi preziosi dati. Questo passaggio è tanto tecnologico quanto culturale ancora di più nel nostro Paese vista la struttura industriale tipicamente basata sulle PMI".

Partner dell'evento

ICS Forum ha ricevuto il patrocinio di AgID (Agenzia per l'Italia Digitale), A.I.PRO.S. (Associazione Italiana Professionisti della Sicurezza), ANIE Automazione, ANIMA (Federazione delle Associazioni Nazionali dell'Industria Meccanica varia e affine), ANIPLA (Associazione Nazionale Italiana Per l'Automazione), Assintel (Associazione nazionale imprese ICT), Assolombarda – Confindustria Milano Monza Brianza, Clusit (Associazione Italiana per la Sicurezza Informatica), Commissione Europea, Confindustria Digitale e Fondazione GCSEC (Global Cyber Security Center).

Informazioni essenziali su Messe Frankfurt
Messe Frankfurt è il più grande operatore al mondo specializzato nell'organizzazione di fiere, congressi ed eventi dotato di un proprio polo fieristico. Con più di 2.300 collaboratori dislocati in circa 30 sedi consegue un fatturato annuo di circa 647 milioni di euro. Messe Frankfurt ricorre a una profonda interconnessione con i vari settori e a una rete di distribuzione internazionale per servire in maniera efficiente gli interessi commerciali dei suoi clienti. Un'ampia gamma di servizi, onsite e online, garantisce ai clienti in tutto il mondo un livello di qualità costantemente elevato e flessibilità nella pianificazione, organizzazione e realizzazione della loro manifestazione. Il ventaglio di servizi offerti spazia dall'affitto del polo fieristico all'allestimento degli stand, dai servizi di marketing al personale e alla ristorazione. La sede principale della Società è a Francoforte sul Meno. Gli azionisti sono la Città di Francoforte, che detiene il 60 percento, e il Land Assia con il 40 percento. Ulteriori informazioni sono disponibili al sito: www.messefrankfurt.com | www.congressfrankfurt.de | www.festhalle.de

Messe Frankfurt Italia
info@italy.messefrankfurt.com
www.messefrankfurt.it
Tel +39 02 880776.1
Fax +39 02 72008053

Contatti
press@icsforum.it

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

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/

ICS FORUM
Industrial CyberSecurity

MILANO
30 GENNAIO 2018
Grand Visconti Palace

CYBER-SMART MANUFACTURING

CULTURA E TECNOLOGIE PER L'INDUSTRIA CONNESSA E PROTETTA

PER INFORMAZIONI
espositori@icsforum.it
visitatori@icsforum.it

www.icsforum.it

In collaborazione con
INNOVATION Post
Nuove tecnologie e industria digitale

Organizzato da
messe frankfurt