GENNAIO 2018

IL CAFFÈ DIGITALE

THE INNOVATION GROUP NEWSLETTER

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Antonio LA MURA
Business Development
Fintech District

INFRASTRUTTURE CRITICHE E PUBLIC SAFETY

il digitale a supporto della sicurezza

BANCHE E TECNOLOGIA

il dentro ed il fuori di una relazione "complicata"

SMART SPEAKER E ASSISTENTI VIRTUALI

cosa succede nel mondo

TIG PREDICTIONS 2018

Sommario

L'EDITORIALE

TIG PREDICTIONS 2018 ..... **2**
Roberto Masiero ed Ezio Viola

NUMERI E MERCATI

Smart Speaker e Assistenti Virtuali: cosa succede nel mondo **6**
Camilla Bellini

LA TRASFORMAZIONE DIGITALE

Servizi Digitali, User Experience e Usabilità **8**
Vincenzo D'Appollonio

BANCHE E FINTECH

Banche e tecnologia: il dentro ed il fuori di una relazione "complicata" **9**
Eleonora Porazzi

DIRITTO ICT IN PILLOLE

Internet of things/privacy e protezione dei dati **11**
Simona Cerone

CYBERSEC E DINTORNI

Cybersecurity Predictions: cosa aspettarsi nel 2018 ... **13**
Elena Vaciago

VOCI DAL MERCATO

Infrastrutture critiche e public safety: il digitale a supporto della sicurezza **15**
Camilla Bellini

Cyber threats e vulnerabilità nell'Industria 4.0 ..... **17**
Elena Vaciago

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Antonio LA MURA
Business Development,
Fintech District

Fintech District

L'EDITORIALE
TIG PREDICTIONS 2018

Roberto Masiero | Presidente, The Innovation Group
Ezio Viola | Amministratore Delegato, The Innovation Group

> Nel nostro Paese lo scenario politico post elettorale previsto dalla maggior parte degli osservatori nel 2018, può costituire l'elemento che può creare maggiore discontinuità anche sulle politiche economiche e industriali avviate e che si sono dimostrate positive

La turbolenza politica frena, la Pubblica Amministrazione ristagna, ma l'inerzia delle grandi infrastrutture e delle politiche industriali continua a far crescere il mercato ICT.

- La crescita del PIL a livello mondiale ed europeo nel 2017 continuerà nel 2018 (le ultime stime OCSE e FMI indicano un +3,5%) e in Italia la crescita prevista di 1,5 % del PIL nel 2017 è confermata anche per il 2018
- La crescita economica continua ad essere legata al boom dell'esportazioni ma sono in ripresa i consumi interni e anche gli investimenti in alcuni comparti trainati dagli impatti positivi di Industria 4.0.
- I cambiamenti di politica monetaria a livello europeo (la progressiva diminuzione del Quantitative Easing) forzerannoun'attenzione sul debito pubblico e sulle politiche di spesa pubblica dei Paesi, in particolare l'Italia.
- La politica economica e fiscale dell'attuale amministrazione USA finora sta favorendo i mercati, ma non è esclusamaggiore incertezza per il 2018,
- Altre aree di instabilità possono essere l'acuirsi di rischi geopolitici che finora non hanno avuto impatti negativi sui trend economici
- Nel nostro Paese lo scenario politico post elettorale previsto dalla maggior parte degli osservatori nel 2018 , può costituire l'elemento che può creare maggiore discontinuità anche sulle politiche economiche e industriali avviate e che si sono dimostrate positive
- Le dinamiche dei settori economici sono diversificate. Ci sono settori in crescita e/o resilienti come i settori export oriented del Made in Italy ma non solo,il settore Agroalimentare, quello della Meccanica e dei Beni Strumentali, il settore Farmaceutico, dell' Automotive e quello delle Utilities così come è tornato a crescere il settore dell'ICT. Inoltre come vedremo anche il settore bancario dopo le recenti crisi si è stabilizzato e ritornerà a crescere.

I "pilastri" della crescita nel 2017 per la trasformazione digitale del Paese si confermeranno anche per il 2018?

- IMPRESA 4.0:Prevediamo che l'impatto di Industria 4.0, come volano di investimenti e driver dell'innovazione, continuerà a dispiegare I suoi effetti: finora l'impatto è stato positivo sia lato domanda che offerta nei comparti dei beni strumentali. La questione aperta è: sono in cantiere provvedimenti abbastanza efficaci da determinare un effetto importante anche sui segmenti specifici dell'industria digitale? Ovvero: l'effetto positivo dell'incremento dell'investimento

nel digitale sui settori economici sarà tanto maggiore quanto più esso si tradurrà non soltanto in investimentiin macchine per l'automazione industriale , ma in applicazioni e servizi digitali destinati a iniettare "sangue digitale" nei processi e nei prodotti delle filiere forti del Made In Italy (vedi Prediction 9).

- Il Piano Banda Ultra Larga avrà ulteriori importanti sviluppi anche nel 2018, contribuendo a una significativa riduzione del divario infrastrutturale tra il nostro Paese e i Paesi Europei più avanzati nei prossimi 3 anni
- Prevediamo infine che la concreta attuazione dell'Agenda Digitale della PA, dopo il varo del piano triennale e dei progetti strategici (SPID, ANPR etc), potrebbe registrare un temporaneo rallentamento come effetto dell'instabilità politica per l'anno elettorale e dei possibili cambiamenti di governance. L'impatto di questi fenomeni potrebbe però essere differenziato: più pronunciato nei settori dell'Amministrazione Centrale, dove l'instabilità politica potrebbe rafforzare temporaneamente la resistenza ai processi di innovazione, meno in quei settori delle Amministrazioni Locali più aperte all'innovazione (particolarmente a livello di alcune Regioni e Aree Metropolitane).

Tutte le Predictions sono disponibili nello speciale allegato a questo numero del Caffè Digitale

> "Il Piano Banda Ultra Larga avrà ulteriori importanti sviluppi anche nel 2018, contribuendo a una significativa riduzione del divario infrastrutturale tra il nostro Paese e i Paesi Europei più avanzati nei prossimi 3 anni"

QUESTO MESE ABBIAMO FATTO COLAZIONE CON

Nasce a Milano il Fintech District, un ecosistema aperto per lo sviluppo del fintech in Italia

Intervista di **Camilla Bellini** a

Antonio La Mura, Business Development e Responsabile Fintech District

Lo scorso 26 settembre è stato inaugurato nel quartiere Isola a Milano, capitale finanziaria italiana, il Fintech District. Questa realtà, promossa da SellaLab, la piattaforma di innovazione del Gruppo Banca Sella, in collaborazione con Copernico, si propone di promuovere un ecosistema italiano (ma non solo) di banche, start up, investitori e aziende tech.

Per scoprire meglio questa nuova iniziativa, abbiamo intervistato ***Antonio La Mura****, Business Developer e Responsabile del Fintech District.*

Da dove nasce l'idea di un Fintech District a Milano? Cosa è e quali sono i suoi obiettivi? Perché una partnership con Copernico?

Il Fintech District nasce dalla volontà di creare anche in Italia, a Milano, un ambiente aperto di collaborazione, non solo commerciale ma anche tecnologica, tra start up, istituti finanziari, investitori, aziende tech, università, studi legali, etc…

In altre parole, tutto l'ecosistema che ruota intorno al mondo dei servizi finanziari in chiave high- tech.

Oggi tra le realtà che partecipano al distretto ci sono ad esempio Cisco, Digital Magics, Moneyfarm, Sardex, Satispay. Alle aziende che partecipano al Fintech District chiediamo di stillare una partnership win-win, di essere parte attiva della community e di avvantaggiarsi della rete e del know how che il distretto può offrire.

Per quanto riguarda gli obiettivi che ci prefiggiamo, li raggrupperei in quattro categorie: prima di tutto il tema del know- how, quello di sviluppare un knowledge condiviso che permei l'intera community; poi c'è tutto il tema della tecnologia e dello sviluppo di partnership tecnologiche, come ad esempio quella con Cisco; un altro aspetto molto importante, su cui stiamo alvorando molto, è quello dei capitali, dell'aggregazione di player nell'ambito degli investimenti sia in Italia sia all'estero; ed infine, ma di certo non meno importante, è l'aspetto relativo all'internazionalizzazione, all'individuazione di partnership e collaborazioni con altre realtà nostre "gemelle" in Francia, in Regno Unito e in Benelux, solo per cominciare.

In poche parole, il Fintech Distrect è una community aperta dove Banca Sella è il curatore della community, ma né determina né regola l'ingresso: è uno spazio condiviso per accelerare la diffusione del fintech in Italia.

Infine, rispetto alla scelta di stringere una collaborazione con Copernico, questa nasce dalla volontà di consolidare la costruzione di una community aperta facendo affidamento sulle competenze e l'esperienza di una realtà che oggi è leader in Italia nella gestione delle community fisiche.

La scelta di aprire a Milano un "acceleratore" dell'ecosistema fintech trasmette la vostra fiducia nelle competenze e della sensibilità del nostro Paese rispetto a questo tema.

Quali sono a vostro avviso i principali driver nella diffusione del fintech in Italia?

A nostro avviso, e da questa nostra convinzione nasce il Fintech District, il mondo delle fintech in Italia è un ecosistema molto vivo, che ha portato ad esempio alla nascita di realtà di eccellenza come MoneyFarm.

Inoltre, con la PSD2 assisteremo anche in Italia ad un'accelerazione nell'attenzione e nella sensibilità, soprattutto delle banche, rispetto a questi temi. Per quanto riguarda poi gli investimenti, anche questi cominciano ad esserci.

Tenete conto poi che, anche dal punto di vista di Banca Sella, se le aziende che promuoviamo crescono, cresce anche la banca. Certo nel complesso è una sfida, ma è anche molto stimolante e noi continuiamo a crederci.

Nello specifico, che attività vengono svolto all'interno del Fintech District?

All'interno dei vostri spazi fisici in via Sassetti 32, nel quartiere Isola, organizziamo sia eventi di networking, che consentono all'ecosistema che ruota attorno al Fintech District di conoscersi e di espandersi, sia attività di analisi e monitoraggio del mondo fintech in Italia e all'estero, che ci consentono poi di fare un match- making più consapevole tra i player dell'ecosistema.

Abbiamo inoltre dei programmi di mentorship per le start up che iniziano il loro percorso in questo mondo, così come programmi di collaborazione con gli investitori per trovare con loro le migliori possibilità di investimento. In altre parole, ancora una volta, tutte le nostre attività hanno l'obiettivo di favorire uno sviluppo sano e sostenibile del fintech in Italia.

IL MONDO DELLE FINTECH IN ITALIA È UN ECOSISTEMA MOLTO VIVO, CHE HA PORTATO ALLA NASCITA DI REALTÀ DI ECCELLENZA

NUMERI E MERCATI

Smart Speaker e Assistenti Virtuali: cosa succede nel mondo (e in Italia)

Camilla Bellini
Senior Analyst, The Innovation Group

Negli ultimi anni si è registrato, soprattutto negli Stati Uniti e più in generale nei mercati anglosassoni, un crescete interesse nei confronti degli "speaker" intelligenti per la Smart Home, dispositivi attraverso cui è possibile gestire e controllare gli oggetti connessi presenti in casa e attraverso cui si può accedere a funzionalità e a servizi digitali, dalla musica in streaming al potenziale dell'eCommerce. I primi speaker ad apparire sul mercato sono stati i dispositivi Amazon Echo (la prima generazione è disponibile dal 2014), a cui sono poi seguiti i dispositivi di Google (i Google Home, rilasciati negli Stati Uniti a partire da novembre 2016) e gli annunciati speaker di Apple, gli HomePod (attesi negli Usa e in UK nei primi mesi del 2018).

D'altra parte, al di là di questi dispositivi, che si basano sulle tecnologie di voice-recognition e virtual assistant sviluppate dai rispettivi produttori (Alexa per Amazon, Google Now per Google e Siri per Apple), sempre più aziende propongono sul mercato Smart Speaker che integrano gli assistenti vocali di terzi: basti pensare al dispositivo Invoke di Harman Kandor, il marchio della Harman International Industries (da marzo 2017 di proprietà di Samsung Electronics) specializzato in impianti audio domestici e per autoveicoli, che utilizza la tecnologia Cortana di Microsoft; o al recente Sonos One della Sonos, azienda attiva dal 2002 nel settore dell'elettronica di consumo e dei dispositivi audio, che ad oggi integra la tecnologia di Amazon Alexa, ma che si propone nei prossimi anni di integrare anche le funzionalità di Google Assistant. Altri dispositivi pronti (o quasi) a competere nel mercato degli speaker intelligenti sono poi: HP Cortana Speaker (basato su tecnologia Microsoft), Lenovo Smart Assistant (basato su Amazon Alexa) e Onkyo VC-FLX1 (anche questo basato su Alexa). C'è inoltre grande attesa per i possibili annunci di Samsung relativi al lancio di un proprio Smart Speaker che potrebbe utilizzare Bixby, possibile nuovo competitor targato Samsung degli assistenti virtuali di Google, Apple, Amazon e Microsoft.

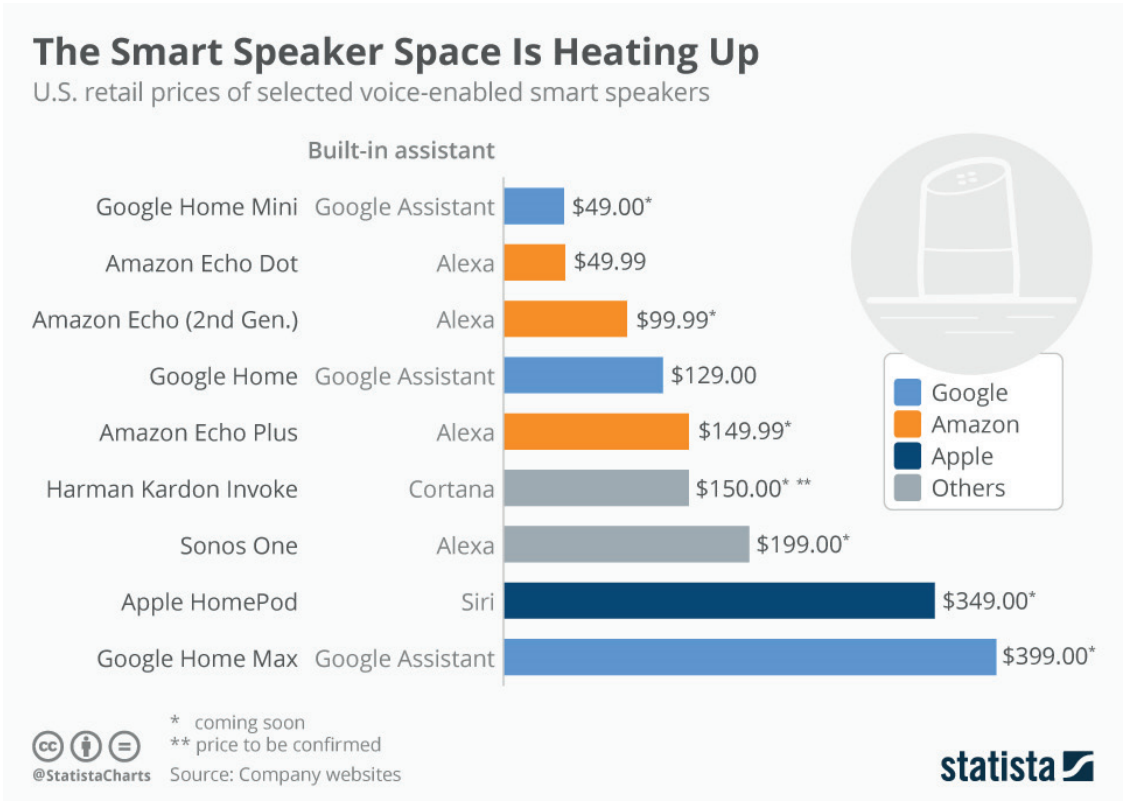
Non vanno infine trascurati i player che stanno entrando nel mercato cinese degli Smart Speaker, tra cui in primis Alibaba, che ha recentemente annunciato il lancio di un dispositivo in diretta competizione con Amazon Echo, Tmall Genie; anche Baidu ha presentato durante lo scorso CES un proprio assistente virtuale dotato di visore, mentre è probabile anche da parte di Tencent il prossimo lancio di un proprio dispositivo intelligente.

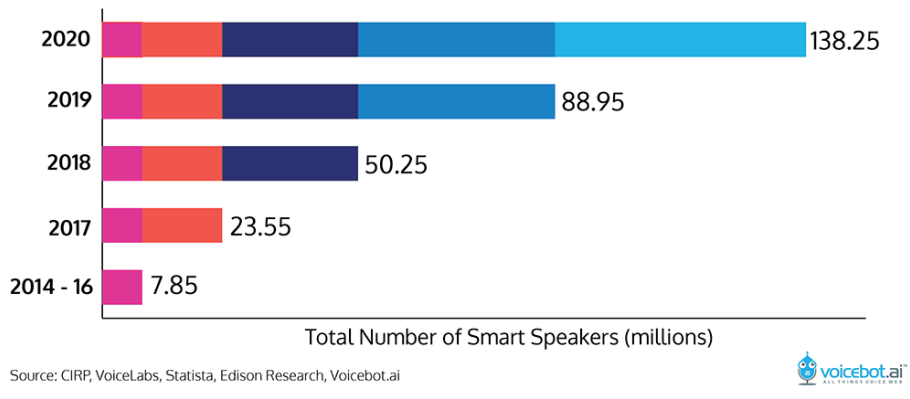
Se potrebbe dunque sembrare che il principale termine differenziante dei diversi dispositivi sia l'assistente virtuale su cui scelgono di basarsi (Alexa vs Siri vs Google), anche le scelte di differenziazione di prezzo posso influenzare la diffusione di questi dispositivi sul mercato: a fronte di un prodotto che mediamente costa $170, dispositivi presenti (o in uscita) sul mercato si suddividono in tre fasce, dai prodotti "entry

level" di Google e Amazon (Google Home Mini e Amazon Echo Dot) alla loro versione avanzata, fino ad arrivare all'annunciato speaker di Apple che esce anche in questo caso sul mercato con un premium price (secondo Statista, il prezzo sarebbe di $349),

Il numero crescente di dispositivi e di player che entrano in questo mercato, così come la crescente differenziazione dei prodotti resi disponibili, è pertanto un segnale delle elevate aspettative che vengono riservate a questo mercato e alla domanda futura di speaker intelligenti: a questo riguardo, secondo il portale Voicebot.ai, nel 2017 negli Stati Uniti la base installata di Smart Speaker era di 23,5 milioni di dispositivi, con una crescita prevista nel 2018 di circa il 113%.

Se dunque c'è grande attesa per il mercato degli Smart Speaker negli Stati Uniti, in Europa ed in particolare in Italia questo mercato in pratica non esiste ancora. La tecnologia degli assistenti virtuali necessita infatti un significativo lavoro di traduzione prima di assicurare l'ingresso di questi dispositivi in mercati non- anglofoni; per questo motivo, questi dispositivi non hanno fatto ancora il loro ingresso su mercati come quello italiano, benché da recenti indiscrezioni sembra che a breve proprio i dispositivi Amazon Echo dovrebbero arrivare anche in Italia.





LA TRASFORMAZIONE DIGITALE

Servizi Digitali, User Experience e Usabilità

Vincenzo D'Appollonio
Partner, The Innovation Group

Durante le nostre attività di Consulenza Aziendale, abbiamo spesso supportato le Aziende nella risposta a Bandi Nazionali, Regionali, Provinciali per ottenere finanziamenti in Progetti di Digitalizzazione, Internazionalizzazione, etc, attraverso le varie piattaforme digitali della PA Locale e Centrale: abbiamo sempre vissuto esperienze 'terribili', per le difficoltà di 'accesso' e le complessità di 'utilizzo' che abbiamo incontrato. Questo mi porta a fare alcune riflessioni sulla progettazione dei servizi digitali della PA. User Experience (UX) ed Usabilità sono due termini che vengono spesso confusi, ma in realtà l'Usabilità è una delle caratteristiche di una User Experience ben progettata. UX dunque significa innanzitutto progettare l'esperienza dell'utente, che deve essere il più ottimale e semplice possibile, e incontrare le sue esigenze di navigazione. Per gestire alcuni fasi critiche nel percorso dell'utente verso una conversione 'digitale', è necessario quindi semplificare al massimo i passaggi che potrebbero rappresentare degli ostacoli. Parliamo dei sette fattori della UX Digitale. 1. Utilità: è una delle caratteristiche fondamentali nella progettazione user-centred: il prodotto o il servizio deve rispondere a un bisogno dell'utente. 2. Usabilità: il prodotto deve consentire di raggiungere l'obiettivo con accuratezza e completezza (efficacia), con il minor dispendio di risorse possibile (efficienza) e garantendo un'esperienza d'uso positiva e senza intoppi e frustrazioni per l'utente (soddisfazione). 3. Desiderabilità: racchiude una serie di elementi immateriali, quali il valore e l'immagine di un brand, l'identità, l'aspetto estetico e l'emotional design. 4. Findability: Architettura dell'informazione ben strutturata. L'utente deve essere aiutato nel trovare le informazioni di cui ha bisogno, all'interno della pagina (titolo, sommario, testi, didascalie), nella navigazione trasversale (tag, link interni alle pagine), nel motore di ricerca interno. 5. Accessibilità: permettere anche a persone con disabilità di utilizzare un servizio. Anche piccole disabilità – come quelle legate, ad esempio, alle difficoltà visive che si presentano negli anziani – possono rendere frustrante l'esperienza d'uso e non permettere di raggiungere lo scopo per cui i servizi sono progettati. 6. Credibilità: connessa alla capacità di chi progetta un prodotto di risultare credibile e affidabile. Spesso gli utenti non offrono una seconda opportunità a un servizio dopo una cattiva esperienza. 7. Valore: il servizio deve produrre valore per avere successo, sia esso economico (come quello misurabile con le entrate o i profitti) o non materiale (se l'obiettivo è la gratificazione degli utenti). La UX è un orientamento olistico, che mette al centro le esigenze e i desideri degli utenti, per fare in modo che ciò che fa un'Azienda, o una Istituzione, abbia un impatto, e provochi quindi la risposta desiderata da parte delle persone. Questo implica una trasformazione culturale nella PA: "occorre pensare l'utente della PA come Cliente della PA, competendo sulla Qualità del Servizio, considerando l'intero 'percorso di fruizione' da parte del Cliente, prima, durante e dopo l'esperienza d'uso". Dare Valore alle Persone, questo deve essere l'obiettivo, la vera Innovazione: mi sento di affermare che la strada è ancora lunga.

BANCHE E FINTECH

Banche e tecnologia: il dentro ed il fuori di una relazione "complicata"

Eleonora Porazzi
Junior Analyst, The Innovation Group

La tecnologia è sempre stata una generatrice di estremi: da un lato, vi sono i suoi ferventi sostenitori, convinti che questa sia una forza inarrestabile solamente positiva; dall'altro, vi sono i tecnofobi o tecnopessimisti che vedono in lei il veicolo con cui "distruggere" per sempre l'uomo, la sua umanità e conseguentemente le sue professioni. Come spesso accade, la verità si trova nel mezzo e oscilla a volte da un lato, a volte dall'altro.

La relazione tra tecnologia e banche ha generato atteggiamenti analoghi: ad esempio, a proposito delle "fintech", che si stanno affermando sempre di più all'interno del panorama mondiale, molti ne vedono solo gli aspetti negativi o positivi, e diventa così difficile capitalizzare su quanto c'è di "buono" in questo fenomeno innovativo.

> La tecnologia è sempre stata una generatrice di estremi: a proposito delle "fintech, molti ne vedono solo gli aspetti negativi o positivi, e diventa così difficile capitalizzare su quanto c'è di "buono" in questo fenomeno innovativo

Ma quali sono (alcuni de)gli aspetti più salienti della relazione tra tecnologia e banche italiane?

Nonostante i grandi investimenti IT sostenuti di recente dalle banche (stime dell'ABI Lab parlano infatti di 8,5 Miliardi di euro investiti in tecnologia per due anni a partire dal 2014), occorre innanzitutto ricordare che, per le caratteristiche socio-culturali italiane, le banche, come altre realtà del sistema economico, sono state particolarmente restie ad adottare le nuove tecnologie.

Occorre quindi fare una breve panoramica della storia del sistema bancario italiano negli ultimi anni: infatti, nel corso del tempo sono accadute varie vicende che con la tecnologia hanno avuto ben poco a che fare.

Seppur il nostro paese sia stato impattato in maniera minore dalla crisi finanziaria avvenuta nel mercato dei mutui subprime statunitensi, nel 2008 in l'Italia (e nel mondo intero) iniziò un periodo di recessione che ha anche generato una perdita di fiducia nel sistema bancario e nei suoi attori. A questa crisi seguì la crisi del debito sovrano, che accumunò diversi paesi dell'Eurozona e che culminò con un prestito di salvataggio per la Grecia di 110 miliardi di euro, seguito poi da prestiti similari ai governi irlandesi e portoghesi.

A fronte della crescente situazione di difficoltà, nel 2014 l'Unione Europea creò il Meccanismo di Vigilanza Unico (MVU), ovvero l'ente il cui compito è quello di effettuare vigilanza prudenziale affinchè venga preservata la solidità del sistema bancario europeo.

Nonostante questo, in Italia i dissesti sono proseguiti, fino a molto recentemente, con il fallimento delle banche venete e delle quattro banche del centro italia, che ha destato molto scalpore lasciando molteplici strascichi anche nel mondo politico.

In questo quadro d'insieme, la tecnologia ha avuto un ruolo molto marginale, "nascosta" da fenomeni di altra natura che hanno tenuto i riflettori lontani dall'analisi e dalla comprensione di come la relazione della tecnologia con gli istituti finanziari si sia evoluta: quello che emerge come certo è che la tecnologia può aiutare a ridurre l'effetto delle condizioni di criticità pre-esistenti nel sistema bancario tramite una maggior efficienza sia nei confronti del suo interno che dell'esterno.

Da un lato, uno dei maggiori impulsi dati dalla tecnologia alle banche è sicuramente una miglior relazione con il cliente: infatti, oggi i canali digitali rappresentano l'80% dei punti di contatto utilizzati dai clienti ed hanno in molti casi sostituito le lunghe ore di attesa agli sportelli. L'omnicanalità rappresenta infatti l'arma competitiva con cui aumentare la fidelizzazione dei clienti, anche alla luce della relativa perdita di fiducia avvenuta a seguito delle crisi delle banche sopra citate. Più in particolare, vi sono 4 elementi che compongono la customer experience multicanale che la tecnologia abilita nelle banche: vi sono gli sportelli tradizionali, che verranno ridotti del 30% entro il 2020; vi sono gli ATM, che potrebbero però diminuire sempre più di importanza nel momento in cui si effettueranno un maggior numero di pagamenti digitali che "cash-based"; vi sono i contact center, i quali continueranno a rivestire primariamente un ruolo di supporto agli altri canali; ed infine vi è tutto quello che si può riassumere con la parola "digital", e cioè l'insieme delle tecnologie digitali (smartphone, Web, etc) che permettono di usufruire dei servizi bancari in modalità online.

Emerge, dunque, come la relazione tra banche e tecnologia possa essere tradotta in un diverso modello di relazione tra le banche ed il consumatore.

Dall'altro lato, un importante impulso dato dalla tecnologia è stato determinato dalla possibilità di rivedere ed ottimizzare i processi interni del mondo bancario: ad esempio, come riportato dai rapporti ABI Lab, attività quali la dematerializzazione, la reingegnerizzazione e l'automazione dei processi interni sono da anni all'interno delle prime 10 priorità di investimento ICT effettuato dalle banche italiane.

A questo proposito è opportuno menzionare una applicazione tecnologica particolare, ovvero quella offerta dai Big Data, il cui utilizzo da parte della banca può significare sia nuovi modi di rapportarsi con i clienti esterni, ad esempio tramite lo sviluppo di modelli previsionali sui tassi di conversione, sia un miglioramento dei suoi processi interni, ad esempio tramite un più accurato e multi-fonte processo di "scoring" per la concessione di prestiti.

Un esempio che viene spesso portato a sostegno di questo è il caso di Royal Bank of Scoltand che, tramite l'utlizzo dei Big Data, ha creato l'iniziativa "personology", in cui la banca avverte i clienti nel caso che inizino a pagare (inutilmente) per servizi già compresi nel canone bancario o quando i loro tassi di interesse sul mutuo cambiano in rialzo diventando più cari del necessario.

La relazione tra tecnologia e banche, dunque, può venir considerata come di carattere strumentale e abilitante: questo significa che la tecnologia deve essere quel mezzo che, opportunatamente declinato nelle sue svariate applicazioni, permette di migliorare la fruizione dei beni, dei servizi e dei processi bancari.

I canali digitali rappresentano l'80% dei punti di contatto utilizzati dai clienti ed hanno in molti casi sostituito le lunghe ore di attesa agli sportelli. L'omnicanalità rappresenta infatti l'arma competitiva con cui aumentare la fidelizzazione dei clienti, anche alla luce della relativa perdita di fiducia avvenuta a seguito delle crisi delle banche

DIRITTO ICT
IN PILLOLE

Internet of things/privacy e protezione dei dati

Simona Cerone
Consultant, Colin & Partners

Assistiamo, ormai con crescente frequenza, all'incremento dell'utilizzo dell'intelligenza artificiale (AI), fenomeno sintetizzabile come "macchine che riproducono le funzioni della mente umana". Una tecnologia che trova applicazione negli ambiti più eterogenei al punto tale che la loro enumerazione appare difficile, in quanto disciplina in continua evoluzione, dinamica e con ridenti prospettive per il futuro.

Un ambito di particolare interesse risulta quello sanitario, dove l'intelligenza artificiale promette, almeno per i prossimi quattro anni, di far svoltare il metodo di approccio, soprattutto con riguardo alla diagnosi della patologia.

Juniper Research stima che, entro il 2022, la spesa annuale per i sistemi di diagnosi assistita da computer (CAD) – piattaforme informatiche che supportano il medico nella formulazione della diagnosi – raggiungerà almeno gli 800 milioni di dollari a livello mondiale e che l'utilizzo dell'intelligenza artificiale per tali strumenti favorirà un risparmio significativo sui costi, perenne scommessa per la sanità, quantificato in 126 milioni di dollari.

Appare evidente come la AI, nei prossimi quattro anni, sia destinata ad avere un ruolo centrale nell'aumento di efficienza della performance del medico, non solo tramite i sistemi di diagnosi assistita da computer, ma anche mediante ulteriori tecnologie come i wearable device, le chatbox ed il monitoraggio da remoto dei pazienti.

Se molti sono perplessi e si interrogano sull'adeguatezza di cure effettuate da un robot, per altri l'intelligenza artificiale può garantire un agile accesso alle cure sanitarie anche se, è bene sottolinearlo, i CAD non hanno il compito di sostituirsi ai medici, ma quello di coadiuvarli nell'efficienza della prestazione professionale. I sistemi di intelligenza artificiale, infatti, hanno dalla loro l'innata capacità di analizzare grandi quantità di dati in poco tempo e riconoscere schemi connessi alla malattia. Ancora una volta l'analisi dei big data offre soluzioni preziose per scoprire legami tra fenomeni diversi e prevedere quelli futuri, ma a che prezzo?

I dati personali e sensibili: la tutela

La delicatezza dell'ambito di azione di tale tecnologia appare indiscutibile. Basti pensare ai dati personali che possono essere trattati con tali tecnologie.

L'articolo 9 della General Data Protection Regulation, applicabile a partire dal 25 maggio 2018, definisce "Categorie particolari di dati personali" quelli genetici e relativi alla salute il cui trattamento non risulta vietato solo a particolari condizioni tra cui "diagnosi, assistenza o terapia sanitaria".

A tale proposito desta particolare preoccupazione la recente legge Europea n° 167 del 2017, in vigore dallo scorso 12 dicembre, la quale prevede la possibilità di utilizzare, a prescindere

dal consenso e fuori dalle succitate condizioni, i dati personali sanitari a fini di ricerca scientifica o statistici.

L'utilizzo di tali dati, di cui l'interessato non ha diritto ad essere informato e ai quali non ha alcun diritto di accesso, risulta favorire principalmente multinazionali tecnologiche al fine di alimentare i sistemi di intelligenza artificiale che viaggiano mediante l'analisi di big data.

L'unica garanzia prevista dalla norma è che i dati siano anonimizzati e che sia rispettato il principio di minimizzazione dell'utilizzo.

Il Cloud computing diviene dunque il secondo protagonista di questo breve excursus.

In conformità con la normativa GDPR, in tale sistema di memorizzazione il provider assume una veste rilevante soprattutto con riferimento alle misure di sicurezza che devono essere valutate considerando la natura, l'oggetto, il contesto e le finalità del trattamento.

Un vero e proprio ribaltamento d'approccio che considera il rischio a cui sono sottoposti i dati personali, soprattutto se "particolari", intrinsecamente dipendente dalle caratteristiche del trattamento.

La GDPR prevede, all'articolo 32, che il Titolare ed il Responsabile del trattamento adottino "misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio" secondo il c.d. principio dell'Accountability, attribuendo al Titolare del trattamento il compito di una sistematica valutazione del rischio correlato al trattamento in modo da adottare misure di sicurezza adeguate alla tutela dell'interessato.

Quanto ai diritti dell'interessato, ai sensi dell'art. 82 della GDPR, "chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento".

In questo modo per l'interessato c'è sempre una cura.

CYBERSEC
E DINTORNI

Cybersecurity Predictions: cosa aspettarsi nel 2018

Elena Vaciago
Associate Research Manager, The Innovation Group

Il 2017 è stato un Annus Horribilis per la cybersecurity, con l'arrivo di alcune minacce cyber che si sono dimostrate vere e proprie epidemie (WannaCry, NotPetya) in grado di diffondersi in tempi rapidissimi attraverso i network e di dimostrare una pericolosità inusitata. I costi legati agli effetti distruttivi delle cyber-armi sono sempre più alti e l'attribuzione di questi attacchi assume sempre più spesso connotazioni geopolitiche, da "Cyber guerra fredda", come visto anche con l'ultima dichiarazione USA – UK secondo cui WannaCry sarebbe stato opera degli hacker della Corea del Nord.

Cosa potrà succedere ancora nel 2018?

Purtroppo i segnali non permettono di essere ottimisti. Le aziende dovranno concentrarsi il più possibile sull'analisi delle proprie principali vulnerabilità, oltre che adeguarsi alle numerose norme in arrivo, e contemporaneamente, con budget in crescita ma comunque sempre ristretti, dovranno prepararsi (con piani ad hoc di incident response) per essere in grado di far fronte ad eventuali emergenze. Vediamo in sintesi quali saranno le dinamiche che caratterizzeranno la Cybersecurity nel 2018.

1. **Debolezza del Fattore Umano e necessità di abbandonare l'autenticazione con UserId/password**
   Il comportamento delle persone deve oggi essere analizzato e compreso all'interno di un'architettura di sicurezza. In passato è stato fatto troppo poco per allineare tutte le persone agli obiettivi di sicurezza delle organizzazioni, e questo ha comportato un rischio via via crescente collegato a phishing, social engineering, utilizzo improprio di cloud, mobile e social network. Riconosciuto che l'errore umano, spesso non intenzionale, è la principale causa di moltissimi incidenti informativi, le aziende si stanno muovendo per correre velocemente ai ripari. Che dire … Errare humanum est, perseverare autem diabolicum. Un elemento che sarà preso maggiormente in considerazione anche dalle aziende di piccola e media dimensione nel corso del prossimo anno sarà la possibilità di autenticare le persone con meccanismi più forti rispetto alla semplice UserId/password.

2. **Ransomware: sempre più complesso e mirato.**
   La quantità di ransomware in circolazione potrebbe diminuire in futuro, ma di sicuro i nuovi "malware del riscatto" non saranno meno pericolosi. Le epidemie del 2017, prima WannaCry, poi NotePetya e BadRabbit, hanno dimostrato la capacità degli attaccanti di costruire dei ransomware estremamente virulenti, dannosi, basati su un insieme di tecniche diverse e sempre più complesse, capaci di auto-diffondersi e anche di colpire specifiche organizzazioni in modo mirato. Con un funzionamento quindi da vere e proprie cyber-armi. Assisteremo ancora in futuro a

ulteriori genesi di ransomware sempre più dannosi, che prenderanno di mira nuovi ambienti, ad esempio quelli dell'IoT.

3. **Maggiori attacchi all'Internet delle cose e alle piattaforme di Data Aggregation (es. Equifax).**
   L'adozione del paradigma IoT sta proseguendo in moltissimi contesti (case, oggetti personali, industrie, automobili, smart cities, …) ma molto spesso senza tenere in dovuta attenzione gli aspetti di sicurezza. Assisteremo quindi a nuove forme di attacco cyber, con implicazioni in alcuni casi di vera e propria Disruption, con possibili implicazioni negative per il mondo fisico e la stessa Safety delle persone.
   Un altro trend, già visto nel caso del data breach per 143 milioni di persone di Equifax, sarà quello che vedrà gli attaccanti prendere di mira chi gestisce grandi quantità di informazioni critiche (su clienti, forza lavoro, comportamenti). Pensiamo ad esempio a tutte le società che offrono servizi di marketing e intelligence, spesso basati su Big Data analytics, e al fatto che finora moltissimi dati sono stati trattati e conservati senza troppi riguardi per la privacy. Per contrastare questi rischi arriva a regime da maggio 2018 il GDPR, regolamento europeo sulla Data Protection.

4. **Il settore sanitario sempre più spesso preso di mira**
   Anche negli scorsi anni ospedali, università e centri sanitari sono stati oggetto di continui attacchi hacker: i dati sanitari delle persone possono essere un target interessante per richieste di riscatto e monetizzazione del data breach. Va considerato poi che a questo trend, destinato a proseguire fino a quando tutti non avranno al proprio interno misure severe di Data Protection, si aggiungono i rischi per sistemi medicali sempre più spesso connessi in rete: questi device spesso sono sprovvisti di procedure di patching di eventuali vulnerabilità, e sono quindi esposti ad attacchi con conseguenze potenzialmente molto gravi.

5. **Ampio dibattito in tema di Privacy**
   La linea di separazione tra ciò che è pubblico e ciò che è privato è oggi molto più sottile rispetto al passato. I comportamenti quotidiani abbassano le difese della privacy e gli stessi individui hanno oggi una sensibilità inferiore rispetto al passato sul mantenimento di riservatezza per tutto quello che è vita privata. Quando però si ha l'impressione che anche l'ultimo baluardo della privacy viene superato, per ragioni economiche di grandi corporation o da parte di spericolate operazioni di intelligence legate alla sicurezza nazionale, si ripropongono come in passato tensioni sociali, legali, politiche, che riportano in primo piano la necessità di una attenzione costante alla protezione dei diritti individuali. Questa alternanza e queste dinamiche caratterizzeranno oggi anche il dibattito politico: sempre di più si cercherà di trovare un giusto equilibrio tra le diverse esigenze, definendo la giusta demarcazione il più possibile legata al singolo contesto.

6. **Crescita degli attacchi alle Cryptocurrency**
   Le monete virtuali come i Bitcoin, Ethereum, Dash, Ripple, Litecoin e altre (anche se il Bitcoin rimane la principale valuta, come mostra lafigura), stanno attirando sempre maggiore attenzione e le valutazioni sono in grande crescita. Utilizzate da tempo come moneta di scambio dallo stesso cyber crime (ad esempio per pagare i riscatti del ransomware) oggi sono anche prese di mira dagli hacker.Ultimo caso in ordine di tempo è stato quello della piattaforma di exchange NiceHash[1] con base in Slovenia: sono stati rubati bitcoin per un valore di oltre 70 milioni di dollari (il furto sarebbe stato la frode più grande nella storia slovena). Inizialmente il sito non era raggiungibile, sembrava semplicemente un black out: solo in un secondo tempo si è saputo che i conti erano stati svuotati dagli hacker. Le indagini dell'Interpol sono in corso.
   Gli esperti di sicurezza si aspettano per il futuro che i sistemi alla base del funzionamento delle cryptocurrency saranno sempre più oggetto di attacchi, volti ad esempio ad ottenere le credenziali di accesso agli exchange o a individuare vulnerabilità nei meccanismi di tecnologie basate su blockchain.

7. **Nuovi investimenti e Budget di sicurezza in crescita**
   La crescita dei budget per la cybersecurity è stata una costante degli ultimi anni, e nel 2018 avremo ancora incrementi elevati, soprattutto per l'effetto combinato di più fattori, tra cui in primo piano l'arrivo della compliance al GDPR. La nuova norma sposterà ulteriormente l'attenzione sulle misure organizzative e tecnologiche per la Data Protection, e a cascata avrà molteplici impatti su tutto l'impianto per la sicurezza ICT. Inoltre la norma riporta in auge schemi di certificazione come l'ISO27001 o altri (ripresi anche dal Framework Italiano per la Cyber Security), in quanto solo un approccio completo ed esaustivo come questo permette di impostare tutti i controlli più efficaci, le attività di auditing e di test, le strutture e i processi organizzativi, i programmi di awareness dello staff, che sono oggi necessari sia per rispondere in modo efficace alle minacce, sia anche per essere allineati con i requisiti delle norme.

[1] Gli hacker rubano 70 milioni in bitcoin di Mauro Manzin http://ilpiccolo.gelocal.it/trieste/cronaca/2017/12/09/news/gli-hacker-rubano-70-milioni-in-bitcoin-1.16217024

VOCI
DAL MERCATO

Infrastrutture critiche e public safety: il digitale a supporto della sicurezza

Intervista di **Camilla Bellini** a
Angelo Gazzoni, Country Manager Italia, Hexagon Safety & Infrastructure

Abbiamo intervistato Angelo Gazzoni, Country Manager Italia, Hexagon Safety & Infrastructure, sul tema del ruolo delle tecnologie digitali nello sviluppo innovativo delle infrastrutture critiche di un Paese.

Nel recente rapporto "Digital Italy 2017" sul processo di trasformazione digitale del nostro Paese, che The Innovation Group ha presentato a Roma lo scorso 13 novembre, si parla del ruolo centrale delle infrastrutture critiche nel supportare tale processo trasformativo. Cosa può fare il digitale per abilitare una nuova generazione di infrastrutture critiche sempre più sicure?

Le tecnologie ICT e il digitale possono avere un ruolo centrale nello sviluppo di soluzioni che garantiscano la sicurezza e la protezione di persone, beni e infrastrutture critiche. Questo tema diventa sempre più centrale in una logica di sviluppo digitale del Paese: digitalizzare la spina dorsale del Paese, le sue infrastrutture critiche, significa tenere in conto anche degli aspetti di sicurezza che questo processo comporta. D'altra parte, benché oggi in Italia si stiano facendo significativi passi avanti in questo ambito, resta evidente il gap che ci separa dal resto dei principali Paesi dell'Unione Europea. In particolare, nel nostro Paese siamo in ritardo rispetto all'utilizzo di tecnologie digitali innovative nell'ambito della public safety. Ad esempio, oggi anche l'Italia sta cercando di adeguarsi al numero unico integrato, che però non può essere considerato un vero è proprio salto di qualità rispetto al potenziale che oggi offre la tecnologia. Si pensi al caso degli incendi in Lazio: la possibilità di affiancare alla chiamata telefonica, tradizionale canale di segnalazione, altri canali (ad esempio un applicazione in grado di veicolare anche foto e video) può diventare critico nell'ottimizzazione e nell'efficacia di intervento delle forze dell'ordine.

Un altro tema centrale è quello poi, più in generale, dell'asset management, ossia del controllo e del governo delle grandi infrastrutture critiche, come ad esempio nell'ambito delle utility e dei trasporti. In questo ambito è soprattutto l'Internet of Things che sta avendo una portata innovativa, dal momento che mette a disposizione di queste infrastrutture una rete di sensori che alimenta il patrimonio informativo alla base dell'asset management. In questo ambito ci sono oggi progetti anche in Italia, benché però manchi ancora la sensibilità per quanto riguarda la sicurezza e la gestione dell'emergenza. L'utilizzo delle tecnologie digitali per supportare la sicurezza pubblica ha inoltre anche effetti per quanto riguarda la velocità di rispristino delle funzionalità dell'infrastruttura stessa, velocità che può tradursi non solo in vantaggi in termini sociali, ma anche economici.

Qual è il ruolo di Hexagon SI nel fornire soluzioni digitali a supporto della sicurezza pubblica?

Noi, come Hexagon SI, ci rivolgiamo proprio all'ecosistema nazionale (e non solo) che si

occupa di pubblica sicurezza, dalla polizia di stato e dalle forze di sicurezza fino alla protezione civile e ai vigili del fuoco. A tutti questi attori noi offriamo soluzioni GIS che consentono di ottimizzare l'intervento, di identificare le persone da soccorrere, di localizzare le forze e le risorse in campo; in questi casi, l'input può essere una telefonata, un sms, una foto, un messaggio via whatsapp: noi facciamo in modo con le nostre soluzioni supportino questi attori nello svolgimento delle loro funzioni.

Tenete conto che noi offriamo soluzioni che supportano la sicurezza pubblica, sia che questa sia fisica o informatica. A noi piace parlare di effetto cinetico, di gestione kinetic- cybersecurity delle infrastrutture critiche: la minaccia e l'attacco informatico sono una fattispecie di criticità così come può essere un incendio o un attacco fisico alle infrastrutture critiche.

Noi siamo in grado di dispacciare risorse informatiche e fisiche, che aiutano chi gestisce la sicurezza pubblica ad affrontare in modo completo tutte le sfide che la società moderna può porre. Dagli Stati Uniti alla Nuova Zelanda e all'India, fino ad arrivare all'esperienza della gestione della public safety durante le passate Olimpiadi di Rio, Hexagon SI ha sviluppato una significativa esperienza in questi ambiti.

Avete già sviluppato progetti anche in Italia?

Abbiamo già sviluppato diversi progetti in Italia, che hanno riguardato entità e infrastrutture nazionali. Ad esempio, recentemente abbiamo lavorato con la Provincia Autonoma di Bolzano, in Alto Adige.

In particolare, abbiamo supportato la Provincia nell'assicurare ai cittadini e ai turisti assistenza in caso di emergenza, in modo rapido ed efficiente: grazie a questa collaborazione ora le agenzie di pubblica sicurezza altoatesine si basano sulla nostra soluzione I/CAD per la gestione degli incidenti, tema particolarmente rilevante in un territorio spesso frequentato da famiglie e da appassionati di attività all'aria aperta, dallo sci alle escursioni alpine. La protezione civile utilizza I/CAD per dispacciare centralmente dalla sua sala comandi a Bolzano l'attività di prima risposta.

Da questa sala comando, composta da otto postazioni, vengono processate circa 130 mila chiamate e 66 mila incidenti all'anno, che coinvolgono sia le brigate dei vigili del fuoco sia altre 306 brigate di volontari. Grazie a questa soluzione ora questo call center riesce a processare e far sì che le forze dell'ordine intervengano entro il limite dei 10 minuti, come richiesto dalla normativa nazionale.

Questo è sicuramente un esempio molto interessante e che ha supportato in modo significativo le forze dell'ordine anche in Italia.

Un altro tema centrale è quello dell'asset management, ossia del controllo e del governo delle grandi infrastrutture critiche, come ad esempio nell'ambito delle utility e dei trasporti. In questo ambito è soprattutto l'Internet of Things che sta avendo una portata innovativa, dal momento che mette a disposizione di queste infrastrutture una rete di sensori che alimenta il patrimonio informativo alla base dell'asset management.

VOCI
DAL MERCATO

Cyber threats e vulnerabilità nell'Industria 4.0

Intervista di **Elena Vaciago** a
Raoul Brenna, Responsabile della Practice Information Security & Infrastructures, CEFRIEL – Politecnico di Milano

Le vulnerabilità degli ambienti industriali che evolvono in configurazione 4.0, partendo dal classico "Industrial IoT" o SCADA/ICS, sono molteplici. Poiché le architetture sono stratificate, è opportuno adottare un approccio multilivello, che punti a scomporre le problematiche (per capirle meglio) collocandole sul corretto layer di riferimento, e poi a riconsiderarle valutando anche interdipendenze e possibili effetti a catena. La priorità oggi, se vogliamo una reale resilienza delle infrastrutture critiche (ed in generale di Industria 4.0) a livello Paese, è muoversi in fretta, come afferma **Raoul Brenna**, Responsabile della Practice Information Security & Infrastructures di CEFRIEL- Politecnico di Milano, in questa intervista con TIG.

> "INDUSTRY 4.0 INDICA LA NUOVA RIVOLUZIONE INDUSTRIALE"

Cosa si intende con il concetto Industria 4.0? quali sono le tecnologie abilitanti che lo riguardano? E perché per esso si parla di problematiche di sicurezza informatica?

Il termine Industry 4.0 indica la nuova rivoluzione industriale e ci si riferisce ad uno scenario che prevede un'interconnessione completa e globale degli impianti, dei sistemi di trasporto, della logistica e anche del personale, quindi in generale di tutto l'ecosistema intorno alle attività manifatturiere dell'azienda e idealmente della filiera in cui opera.

Le tecnologie abilitanti sono numerose (Robot collaborativi, Droni e AGV, Big data, Machine learning e Intelligenza Artificiale, Cloud Banda larga e Ultralarga, IoT e sensori), ma il risultato è quello di una fortissima focalizzazione sul "real time": dalla detection, alla data ingestion, all'elaborazione, fino all'integrazione e alla fruizione da parte dei diversi attori coinvolti di specifici insight sui processi di produzione e sui prodotti realizzati.

Ci si spinge anche a tematiche di Predictive e Prescriptive maintenance che puntano a fornire informazioni su quello che succedrà e su come gestire o evitare specifici eventi. Queste tecnologie distribuite, spesso nuove ma altrettanto spesso "legacy" e riadattate mediante retrofitting (per abilitarne la trasmissione dei dati, le comunicazioni in ambienti eterogenei e l'accessibilità worldwide) sono tutti "ingredienti" su cui il rischio cyber è potenzialmente elevatissimo e su cui la connotazione di "real time" di cui dicevo poco sopra non può che essere un'amplificazione.

Quali e quante sono le vulnerabilità degli ambienti industriali e in particolar modo quelle ereditate dal nuovo scenario di Industria 4.0, caratterizzato dall'iperconnettività a tutti i livelli?

In un ambiente industriale, specie se "evoluto" in ottica 4.0, il tema della gestione delle vulnerabilità è molto complesso, perché di fatto le troviamo a tutti i livelli: dagli ambienti per cui questi problemi sono già molto noti (come PC, client e reti ICT) ai nuovi oggetti connessi: sensoristica distribuita con connettività wireless o simili che spesso, essendo di matrice consumer, nascono con minore attenzione alla sicurezza. Pensiamo ai robot e ai droni, che possono essere oggetto di attacchi per cui diventa possibile prenderne il controllo da remoto. Inoltre entra in gioco il cloud che a sua volta presenta problematiche di sicurezza. Perfino le stampanti 3D hanno i loro problemi: si è già prefigurato un loro utilizzo malevolo che porterebbe a una produzione di prodotti con errori intrinseci.

Va poi considerato tutto il tema del collegamento della supply chain e quindi dei rischi associati all'assemblaggio di prodotti di terze parti poco sicuri, o semplicemente degli accessi privilegiati garantiti a fornitori magari non altrettanto consapevoli delle tematiche di cybersecurity.

In ambienti industriali molto "connessi", anche le tradizionali vulnerabilità dell'ICT acquistano una rilevanza particolare: si pensi al fatto che nel 2014 in Germania un accesso abusivo ad un altoforno ha avuto conseguenze molto gravi.

Una volta entrati nella rete con tecniche di phishing, gli attaccanti hanno infettato i sistemi ICS utilizzati nella produzione di acciaio e sono riusciti a prendere il controllo dei sistemi che governano l'altoforno: di conseguenza, la fabbrica ha subito gravi danni non potendo governare correttamente lo shutdown. Esistono anche cyber threats specifici per i processi industriali o di logistica, ad esempio RFID malevoli in grado di compromettere i sistemi di lettura e i database sottostanti, malware che parlano la lingua di PLC e SCADA per controllarli, impianti di produttori "furbi" in grado di intercettare il traffico nella fabbrica anche a scopo di sottrazione di Intellectual Property rispetto ai macchinari concorrenti.

Gli attacchi cyber al mondo industriale sono quindi già una realtà oggi, ma le aziende sono consapevoli di questi rischi?

Negli ultimi anni, attacchi al settore energetico, agli autoveicoli, persino al mondo manifatturiero confermano il potenziale impatto di campagne su vasta scala verso questo target e ne confermano anche l'attuale esposizione. Tecniche di phishing più o meno mirato abilitano il raggiungimento di reti e segmenti di impianti ipoteticamente isolati. La mancanza di patch in reti "office" (oltre che nelle reti di processo) ha messo in luce negli ultimi mesi come poi questo isolamento sia più teorico che pratico, e comporta la propagazione di infezioni che hanno come conseguenza estrema il blocco dell'azienda.

In Italia la sensibilità su questi temi e la percezione del rischio ci sono, almeno tra gli addetti del settore dell'Information Security. L'allineamento su questi temi, in termini di gravità percepita, può tuttavia essere solo parziale verso il business, nonostante esso sia l'Owner degli impianti di cui parliamo.

Gli attacchi agli ambienti industriali sono una realtà, accadono, però sono molto difficili da rilevare.

Quello che si misura di solito è il loro effetto, che in alcuni casi può risultare veramente molto grave, con una reazione a catena che blocca tutta la filiera, come si è visto di recente quando il malware NotPetya ha fermato le operazioni della società di spedizioni danese Maersk per settimane, con un danno economico complessivo tra i 200 e i 300 milioni di dollari. In questi casi il business percepisce il problema… ma purtroppo tardivamente.

VOUCHER
MISE 2017

Ministero dello sviluppo economico

The Innovation Group
Innovating business and organizations through ICT

Il voucher per l'internazionalizzazione del Ministero dello Sviluppo Economico è un contributo a fondo perduto a favore delle PMI che vogliono crescere sui mercati internazionali con il supporto di un Temporary Export Manager.

Anche quest'anno il MISE, Click day per invio telematico della domanda dalle ore 10.00 del 28 novembre 2017, offre la possibilità alle PMI italiane di beneficiare dei Contributi a fondo perduto, sotto forma di voucher, per l'acquisto di prestazioni consulenziali finalizzate a sostenere i processi di internazionalizzazione; la dotazione è di 26 Milioni di Euro.

I servizi consulenziali devono essere erogati esclusivamente da società di TEM accreditate dal MISE.

I contributi sono di due tipi:

a) Contributi «voucher early stage»:

€ 10 mila a fronte di un contratto di servizio di importo almeno pari a € 13 mila e con durata di almeno 6 mesi.

b) Contributi «voucher advanced stage»:

€ 15 mila a fronte di un contratto di servizio di importo almeno pari a € 25 mila e con durata di almeno 12 mesi.

Da diversi anni The Innovation Group, ora in fase di riaccreditamento per il voucher 2017 secondo le direttive del Decreto Ministeriale, è attiva in decine di progetti di consulenza per l'internazionalizzazione con le PMI, ed è in grado di occuparsi di tutta la gamma di servizi previsti e finanziabili: assistenza organizzativa, contrattuale, sviluppo di competenze, analisi e ricerche di mercato, ricerche di potenziali partner industriali e/o commerciali, identificazione e/o acquisizione nuovi clienti.

CONTATTACI PER CAPIRE COME COGLIERE QUESTA OPPORTUNITÀ!

NOTE

IL CAFFÈ DIGITALE

ISCRIVITI ALLA NEWSLETTER MENSILE!

RICEVI GLI ARTICOLI DEGLI ANALISTI DI THE INNOVATION GROUP E RESTA AGGIORNATO SUI TEMI DEL MERCATO DIGITALE IN ITALIA!

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Fintech District

COMPILA IL FORM DI REGISTRAZIONE SU

www.theinnovationgroup.it