IL CAFFÈ DIGITALE

THE INNOVATION GROUP NEWSLETTER

L'EDITORIALE DI

Ezio Viola
Managing Director, The Innovation Group

IL MERCATO DIGITALE E L'INDUSTRIA DELLE IDEE: COSA DOBBIAMO ASPETTARCI?

È uso comune trattare negli articoli di agosto/settembre di qualsiasi rivista, blog o newsletter, temi non impegnativi, di fare il punto della situazione rispetto alla prima metà dell'anno e, allo stesso tempo, di consigliare letture e approfondimenti per sfruttare al meglio i restanti mesi prima della chiusura dei bilanci e di Natale.

Seguendo questa tradizione, quindi, cercherò di fare entrambe le cose (fare il punto della situazione e fornire spunti e consigli di lettura), partendo da una breve sintesi di quanto illustrato durante il nostro recente briefing di metà anno sulle previsioni del mercato digitale in Italia: rispetto infatti a quanto presentammo mesi fa e dalla definizione del 2017 come "l'anno del crocevia" per la crescita digitale del paese, abbiamo ora rivisto stime e numeri anche alla luce dei trend e delle iniziative ("digitali" e non) del primo semestre.

Ebbene, a Gennaio presentammo una forbice di crescita possibile del mercato digitale[1] per il 2017 tra l'1,7% e il 4,7% (rispetto al 2016), una forbice dal valore stimato di circa 1,6 miliardi di euro; le possibilità di crescita, e quindi la capacità di far fruttare appieno quei 1,6 miliardi potenziali, dipendeva dall'andamento di alcuni fattori (interni ed esterni) di rischio, ma soprattutto dall'attuazione secondo i tempi prefissati dei tre piani per la crescita digitale del paese: il Piano Banda Ultra Larga, la Strategia per la crescita digitale 2014-2020 (con il recente Piano Triennale dell'AgID) e il Piano Nazionale Industria 4.0. A semestre concluso, d'altra parte, la forbice della crescita del mercato rimane, benché leggermente ridotta: la crescita è ora prevista tra un valore minimo di 1,2% e un massimo di 3,6%, pari a circa 1,3 miliardi di euro di margine potenziale di crescita per il 2017, 300 milioni in meno rispetto alle stime di inizio anno.

Alcuni dei fattori esterni di rischio e opportunità sono infatti cambiati, in positivo e negativo, rispetto ad inizio anno:

- *la paura che il 2017 fosse l'anno del "break", più che del "make", per l'Unione Europea si è allontanata;*
- *è attualmente previsto un cambio di strategia per la politica delle Banche Centrali con un aumento graduale dei tassi e la fine del quantitative easing, mentre "debito" diventerà la parola chiave per il governo dell'economia;*
- *rimane l'incognita della politica economica della nuova amministrazione negli Stati Uniti;*
- *lo scenario politico italiano si è normalizzato, il governo attuale terminerà la sua legislatura, mentre si spera che il digitale diventi un tema centrale, e non accessorio, della prossima campagna elettorale;*

segue alla pagina successiva >>

SETTEMBRE 2017

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Marco ONADO
Professore Senior di Economia degli Intermediari finanziari dell'Università Bocconi

Bocconi

SOMMARIO

- *la crescita economica prevista del PIL per l'anno in corso secondo il FMI è del 1,3- 1,4%, contro le stime di inizio anno del 0,7- 0,9%, con la ripresa (soprattutto) dei consumi, ma anche degli investimenti;*
- *alcuni settori "problematici" sembrano ora in una fase di ripresa, come ad esempio il settore bancario: da malato a convalescente per le sofferenze, ma in via di stabilizzazione dopo la sistemazione delle principali crisi bancarie;*
- *rimangono alcuni settori in crescita o resilienti: i settori export- oriented del Made in Italy (+6,6% tra gennaio e aprile), ma non solo; restano positivi l'agroalimentare, la meccanica, il farmaceutico, l'automotive e e le utilities.*

Per quanto riguarda i "pilastri" della crescita e della trasformazione digitale del paese, questi hanno avuto finora un andamento con velocità disallineate alle previsioni di inizio anno:

L'impatto di Industria 4.0 come volàno di investimenti e driver dell'innovazione è da poco iniziato, in particolare sui segmenti di spesa dell'ICT come software e servizi;

Il Piano Banda Ultra Larga prosegue, ma rimangono elementi di instabilità e di rischio legati anche a come i diversi attori pubblici e privati si stanno muovendo, in particolare nelle zone bianche e grigie;

La concreta attuazione dell'Agenda Digitale della PA, oltre al piano triennale presentato, non ha avuto una concreta accelerazione ed è ancora al palo la sua concreta attuazione: sarà fondamentale non solo l'accelerazione sui vari progetti strategici noti, ma avviare il disegno degli ecosistemi digitali delineati nel piano triennale stesso.

Se dunque gli accadimenti e i trend della prima parte del 2017 ci hanno portato a contenere il potenziale di crescita del mercato digitale italiano, questa non è l'unica "preoccupazione" che ho rispetto allo sviluppo dell'industria digitale, anzi.

Quando infatti mi capita di leggere o scrivere dell'industria digitale e di come l'innovazione e le nuove tecnologie, che via via appaiono sul mercato, vengono presentati dai vari attori, il ruolo che le grandi potenze tecnologiche e digitali vecchie e nuove (le GAFAN, un acronimo che sta per Google, Apple, Facebook, Amazon e Netflix) hanno assunto nella trasformazione della vita quotidiana, delle imprese e dei governi, molte volte mi sono chiesto se il ruolo della "Tecnologia, con la T maiuscola" non abbia ormai offuscato o preso il posto di ogni altra forma di pensiero critico, che una volta era proprio del ruolo dell'Intellettuale Pubblico.

A questo riguardo sto trovando alcuni spunti e stimoli interessanti nel libro "The Ideas Industry. How Pessimists, Partisans, and Plutocrats are Transforming the Marketplace of Ideas" di Daniel W. Drezner, professore di politica internazionale presso la Tufts University: il libro analizza come l'ascesa di una classe di super-ricchi, in particolare negli Stati Uniti, abbia determinato un profondo cambiamento nella categoria degli intellettuali, dando sempre più risalto a una nuova figura, il "Thought Leader" o "leader di pensiero". Questi sono "evangelisti", più che pensatori, e molti provengono proprio dal mondo digitale o dalle Business School.

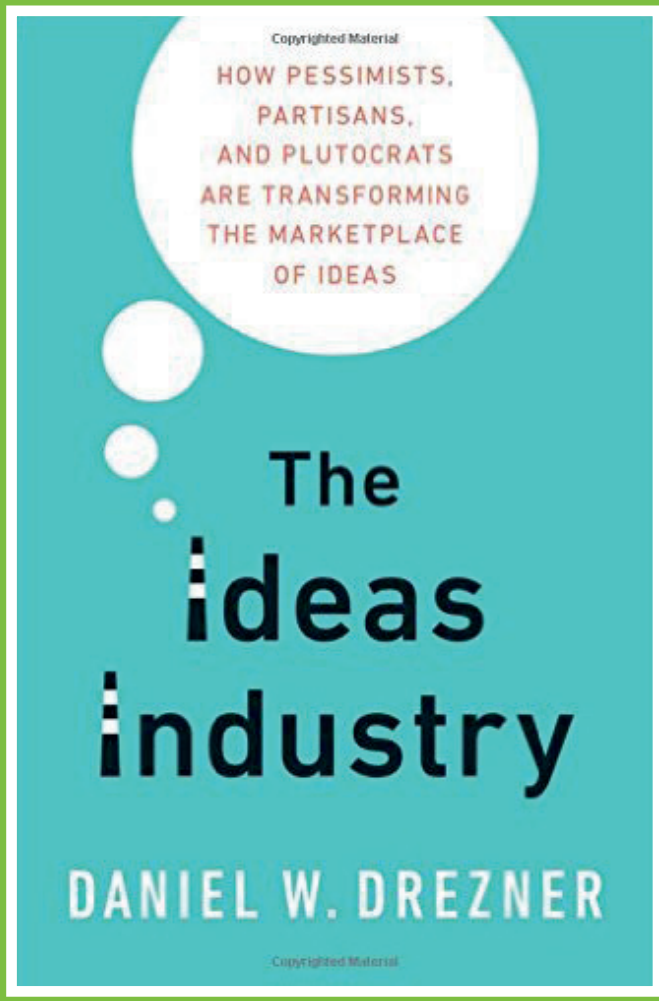
Questo nuovo tipo di intellettuale, se così lo vogliamo chiamare, più che approfondire le complessità e svolgere analisi critiche, è portatore di un profondo desiderio di cambiare il mondo e spesso considera la "Tecnologia, con la T maiuscola" come il nuovo e unico motore del cambiamento.

Di esempi noti il libro ne fa diversi e come tratto comune mostrano un legame piuttosto stretto con il denaro: le loro idee, infatti, nascono per essere destinate ad un pubblico il più ampio possibile (TED viene portato come esempio di piattaforma che consente di entrare nel circolo degli speaker ben pagati), per essere "massimizzate", attraverso una pletora di collaborazioni con riviste, libri e apparizioni televisive, convegni. Il pensiero e le idee diventano prodotti da vendere e promuovere e più sono semplici, ma provocatori, e meglio è, perché il marketing del pensiero diventa fondamentale. Tutto questo con buona pace del fatto che alcuni di questi personaggi sono stati scoperti a copiare contenuti altrui[2].

Questo modello di intellettuale, il "leader di pensiero", fa dunque sponda con la categoria dei super- ricchi ed è molto allineato anche ai valori della Silicon Valley, perché spesso condivide e si presta a sostenere tesi congeniali ai suoi abitanti. Negli Stati Uniti, infatti, alcune think thank indipendenti e riconosciute hanno già dovuto fare i conti con questa "plutocrazia delle idee", venendo a patti con essa in cambio di fondi, altrimenti vedendo assottigliarsi i finanziamenti ai propri studi. Qualcosa indubbiamente su cui riflettere.

Note:

1. Qui inteso come la somma dei mercati dell'ICT tradizionale e delle New Digital Technologies (NDT); non vengono considerati i mercati dei contenuti digitali e dell'elettronica di consumo
2. Fonte: http://politi.co/2uVWei0



QUESTO MESE ABBIAMO FATTO COLAZIONE CON..

BANCHE, CRISI FINANZIARIE E PROUST: DA DOVE RIPARTIRE PER PROGETTARE LE BANCHE DEL FUTURO?

Intervista di Camilla Bellini a Marco Onado, PROFESSORE DELL'UNIVERSITÀ BOCCONI

Se non lo facciamo subito, lunedì non avremo un'economia. Una frase tratta dal film di Curtis Hanson "To Big to Fail", con cui il presidente della FED post-fallimento di Lehman Brothers, Ben Bernanke, cerca di convincere il Congresso degli Stati Uniti ad intervenire nel salvataggio delle banche americane. Una frase che **Marco Onado, Professore Senior di Economia degli Intermediari finanziari dell'Università Bocconi**, riprende nel suo ultimo libro "Alla ricerca della banca perduta", edito da Il Mulino (2017). Una frase che il professore Onado richiama anche nel nostro recente incontro in preparazione al suo intervento al Banking Summit 2017, che The Innovation Group organizza il 21 e 22 settembre a Saint Vincent, durante il quale il professore presenterà il libro e parteciperà al dibattito sul futuro delle banche italiane.

Marco ONADO

Una frase che, d'altra parte, ben motiva e spiega la scelta di allora, ma quanto mai attuale nel caso italiano, di un intervento pubblico per sventare la minaccia di fallimento delle principali banche di investimento (e non), dal momento che, come spiega Onado, "non può esistere un'economia di mercato (o un sistema capitalistico, se si preferisce) senza le banche".

Il ruolo imprescindibile delle banche rispetto al sistema economico attuale dipende però non tanto dalla loro dimensione quantitativa, dall'ammontare del totale dell'attivo dei bilanci, che ha reso le grandi banche globali dei leviatani e che pure ha avuto (e continua ad avere) la sua rilevanza nelle scelte di intervento pubbliche; ma, piuttosto, nell'ingarbugliamento della vocazione stessa delle banche, che come più volte viene ribadito da Onado, sono passate dall'essere delle utility bank, ossia delle banche che assolvono funzioni di utilità pubblica come tipicamente sono le attività di intermediazione, a diventare delle casino bank, ossia delle banche dove la componente speculativa ha preso il sopravvento sulle altre attività: basti pensare che, come ben documenta Onado, a fine 2014 il volume delle posizioni in derivati delle banche europee ammontava a 360 trilioni di euro, mentre quello delle banche americane a 184 trilioni di dollari; numeri che, a prescindere dal modo in cui sono stati calcolati, danno evidenza del fatto che la dimensione delle attività speculative delle banche occidentali è cresciuta addirittura di due ordini di grandezza superiori rispetto all'effettiva dimensione dei loro attivi di bilancio.

D'altra parte, il discorso sulle banche oggi nel contesto dell'economia globale è ben più complesso e articolato delle sole considerazioni qui riprese e che al contrario ben vengono tratteggiate nel libro di Onado, che si propone, richiamando già dal titolo Proust e la sua Recherche, di andare alla ricerca, nel suo passato e nel suo presente, del modello di banca perduto, quella banca forse più "utile" che la globalizzazione e la corsa all'innovazione finanziaria hanno collaborato a incrinare e a confondere.

Libro che d'altra parte resta (a mio avviso volutamente) distante dai temi del digitale e dell'innovazione tecnologica, che spesso al contrario vengono visti come gli strumenti di trasformazione e risanamento delle banche.

Onado sembra al contrario rendere esplicita una cosa: che il digitale serve, e questo non viene messo in discussione; ma serve ancora di più ritrovare l'identità e la vocazione delle banche per far sì che queste ritornino a sostenere e a guidare (e non a frenare, come oggi sembra accadere) l'economia globale.

MUSK, ZUCKERBERG E IL DILEMMA DELL'AI

Di **Camilla Bellini**, Senior Analyst, The Innovation Group

Il mercato dell'Artificial Intelligence sta suscitando ormai da qualche tempo un acceso dibattito sul suo futuro e sul suo potenziale. È il mercato che forse più di altri ha assistito ad un proliferare di ipotesi, avvertimenti, scontri, annunci e rimpianti: basti pensare a Bill Gates, che quando nacque Microsoft era preoccupato soprattutto di poter perdere la possibilità di lavorare alle basi dell'AI, dovendosi occupare dell'impresa nascente. Anche nel suo piccolo, Il Caffè Digitale ha dato ampio spazio al tema nelle passate edizioni, ribadendone soprattutto il potenziale, i trend di mercato e gli attori coinvolti nella corsa all'intelligenza artificiale.

D'altra parte, in questa sede poco spazio è stato dedicato ad alcuni aspetti dell'AI che al contrario stanno infiammando il dibattito mondiale, coinvolgendo i "titani" della scienza e del digitale: da Elon Musk a Mark Zuckerberg, da Bill Gates a Stephen Hawking.

Al centro del dibattito in questo caso è la potenziale minaccia dell'intelligenza artificiale nei confronti dell'umanità e della civilizzazione.

Termini coloriti, che non sono stati scelti da chi scrive, ma che sono stati utilizzati dallo stesso Elon Musk lo scorso 15 luglio, quando è intervenuto al National Governors Association Summer Meeting a Providence in Rhode Island. In quella circostanza, il CEO di Tesla e SpaceX ha ribadito che "l'AI è un rischio fondamentale per l'esistenza della civiltà umana"[1], sottolineando la necessità di ricorrere ad una regolamentazione proattiva che mitighi il rischio della sua proliferazione, dettata inevitabilmente dalle leggi del mercato e della competizione.

L'appello di Musk, che ormai da anni dichiara la sua preoccupazione rispetto al tema, ha suscitato ancora una volta ampio clamore, accendendo il confronto tra Musk e Mark Zuckerberg, il fondatore di Facebook. Quest'ultimo, infatti, interrogato da un utente durante un suo Facebook Live[2] in merito all'affermazione sopra citata, ha dichiarato di non comprendere questi atteggiamenti negativi, anzi di ritenerli addirittura "irresponsabili": da ottimista, come lui stesso si definisce, Zuckerberg vede infatti soprattutto il potenziale di questa tecnologia, ad esempio nell'ambito dei trasporti e della sanità, due contesti in cui possono essere salvate (grazie a migliori diagnosi) o risparmiate dalla morte (evitando gli incidenti automobilistici, prima causa di decessi) molte persone.

A supporto della "preoccupazione" di Elon Musk si è schierato però già in passato Bill Gates che ha dichiarato di considerare l'intelligenza artificiale un tema critico, che deve essere maneggiato con grande prudenza per evitare che si trasformi in una minaccia reale per lavoratori, cittadini ed individui. E lo dichiara alla faccia di Eric Horovitz, capo dei Microsoft Research Lab che, al pari di Zuckerberg, trova difficile capire la posizione di Elon Musk e Bill Gates.

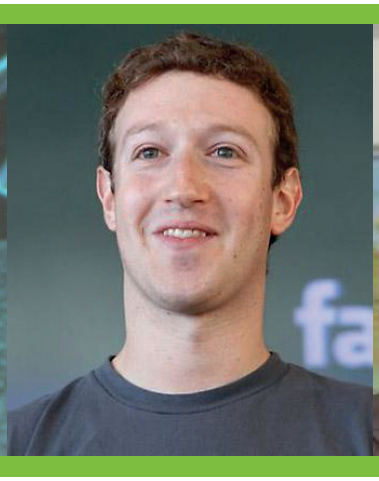
È evidente dunque che, per quanto si possa essere d'accordo con l'una o l'altra posizione, il tema dell'intelligenza artificiale non può (e non deve) passare inosservato a tutti i livelli del dibattito pubblico e delle strategie aziendali: in questo senso, positivo è proprio l'interesse dimostrato dai governatori degli Stati Uniti rispetto al tema durante l'incontro con Elon Musk, o la richiesta alla Commissione Europea, posta a inizio anno dai deputati UE, di norme per disciplinare lo sviluppo della robotica.

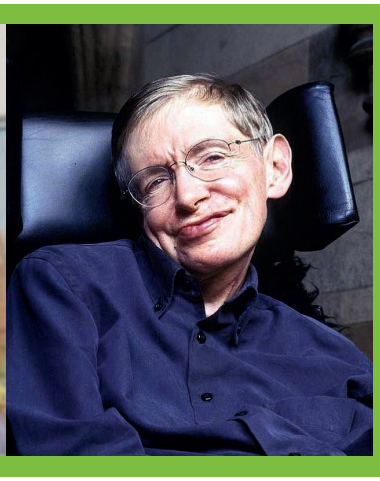
In questo senso, soprattutto in riferimento all'iniziativa europea, che è stata approvata con 396 voti favorevoli, 123 contrari, 85 astenuti, è interessante notare come l'approccio adottato, al di là del dibattito oggi tanto in voga, guarda in modo positivo alla possibilità di legiferare rispetto al tema dell'intelligenza artificiale, considerandone "le implicazioni e le conseguenze legali e etiche, senza ostacolare l'innovazione"[3].

In questo senso, l'approccio proposto dal Parlamento Europeo risponde in modo positivo alle raccomandazioni di Elon Musk rispetto alla necessità di una regolamentazione proattiva per la robotica e l'intelligenza artificiale, ma la "purifica" dell'eccessivo (a parere di chi scrive) negativismo e del pessimismo con cui viene espressa dal CEO di Tesla; e, allo stesso tempo, pone dei freni all'ottimismo del fondatore di Facebook, facendo un passo verso un processo di regolamentazione dell'AI che d'altra parte è riconosciuto come imprescindibile.

Note:

1. www.nga.org/cms/video/2017/sm/closing-plenary
2. Un servizio di Facebook che consente ad un utente di trasmettere dei video live in streaming
3. Fonte: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%20TA%20P8-TA-2017-0051%200%20DOC%20PDF%20V0//IT



LE NUOVE TECNOLOGIE PER LE EMERGENZE MEDICO-SANITARIE UN'APP SOCIALE, UNA SAPP: IL TELEFONINO, IL TUO SALVAVITA

Di **Carlo Geri**, Medici Volontari Italiani – Onlus

La Web APP "Il Telefonino, il tuo Salvavita", in Rete da ormai cinque anni, è stata definita **SAPP**, **S**ocial **APP**lication, proprio per le finalità sociali ed in un certo senso "social", che si ripromette. Ovvero di permettere il superamento dell'anonimato medico sanitario, soprattutto quando chi viene soccorso non è in grado di collaborare con i soccorritori.

Deriva dall'esperienza sul campo dell'Associazione "Medici Volontari Italiani", MVI, associazione la cui attività consiste in medicina di strada a Milano, e nel contempo la SAPP è divenuta parte integrante del Servizio del Comune: "Cittadini più Coinvolti & più Sicuri".

In questa nota si vuole descrivere come un'iniziativa proveniente dal basso ed inizialmente con finalità limitate, per non parlare delle risorse, con progressioni successive, sia tecnologiche e sia di contenuto, possa divenire un progetto rientrante nella filosofia Smart City/Smart People ed anche di Digital Transformation.

Infatti, come esiste il "Citizen journalist" ed il "Citizen scientist", grazie al digitale in tasca, si può pensare non solo al "Cittadino soccorritore", ma anche allo sviluppo di una gestione ad personam delle chiamate al **NUE, Numero Unico d'Emergenza, 112/118**. Vedremo come.

Da quanto detto, si evince che il contesto riguarda gli interventi medico-sanitari sia di "primo" che di "pronto" soccorso, in quelle situazioni internazionalmente definite con l'acronimo ICE, In Case of Emergency.

Un po' di storia:

"nel 2005, un infermiere Inglese, a seguito degli attentati nella Metro di Londra, registrò l'acronimo ICE, acronimo che ognuno di noi può memorizzare nella propria rubrica telefonica, cartacea o digitale che sia, abbinandovi un numero telefonico, permettendo così ai soccorritori, una volta arrivati sul luogo dell'intervento, di ottenere informazioni su chi viene soccorso.

Specialmente quando quest'ultimo, come già detto, non è in grado di collaborare con i soccorritori stessi."

Nel caso critico come quello appena descritto, ci si trova in una situazione di "anonimato clinico" per un lasso di tempo non prevedibile e conseguentemente in una situazione di grave rischio potenziale.

IMPOSTAZIONE DI UNA SOLUZIONE..... DIGITALE

Visto che in un intervento d'emergenza/urgenza il fattore tempo è fondamentale, sia per quanto concerne la velocità dell'intervento e sia per quanto riguarda la fruibilità delle informazioni cliniche di chi viene soccorso, le cosiddette "informazioni salvavita", ci si chiede: **come queste informazioni possano essere a disposizione del Sistema di Soccorso sin dalla chiamata al NUE, Numero Unico d'Emergenza: 112/118**?

Alcuni anni anni or sono, MVI concepì l'idea di aggiungere al numero telefonico previsto da ICE le informazioni non solo anagrafiche, ma soprattutto quelle salvavita. Fare questo in formato cartaceo era alquanto semplice, un po' meno farlo digitalmente ed allora si varò il progetto: "Il Telefonino, il tuo Salvavita".

La tecnologia di base era già disponibile, diffusa ed a costo quasi zero per questa iniziativa, si parla infatti di Smartphone e Codice QR. Mancava l'anello di congiunzione, o meglio il link, tra la tecnologia esistente ed il profilo clinico salvavita per una gestione digitale e remota di tale profilo. Questo link è stato realizzato grazie al contributo della Fondazione IBM e della Società "G 7, Soluzioni Informatiche".

In particolare, la Fondazione IBM, all'interno del Progetto "Celebration of Service" nell'ambito delle celebrazioni del suo primo centenario, ha sviluppato l'applicazione che permette di digitalizzare, tramite QR Code, il profilo sanitario, permettendo così l'uso dello Smartphone sia come repository del profilo stesso e sia come mezzo trasmissivo. E questo a seconda se si è soccorritore o si viene soccorso.

La Società "G 7 Soluzioni Informatiche" ha messo in Rete come Web APP quanto prodotto dalla Fondazione IBM, sviluppando il sito "iltelefoninoiltuosalvavita.org" e poi, nel tempo, ne ha curato la manutenzione e lo sviluppo di nuove feature derivanti dall'uso della Web APP sul territorio.

In definitiva quanto sopra permette di produrre un BADGE **(fig.1)**, contenente il numero ICE da chiamare, la foto del possessore dello Smartphone e le informazioni salvavita in formato QR Code, quindi un set di informazioni gestibile digitalmente e quindi facilmente trasmissibile via Smartphone.

IL FUTURO DIGITALE...PROSSIMO

La SAPP ha dimostrato che, utilizzando le nuove tecnologie "standard" presenti nella tasca di noi cittadini, è possibile non solo risolvere il problema dell'anonimato clinico in una situazione d'emergenza medico-sanitaria, ma anche di divenire soccorritori efficienti di "primo soccorso".

Con questa finalità è in Rete oltre alla SAPP, anche l'APP "Where ARE U?" da parte AREU – Lombardia, Azienda Regionale Emergenza ed Urgenza, che permette di inviare al Sistema di Soccorso la geolocalizzazione del luogo ove è richiesto l'intervento di soccorso, assieme ad altre feature specifiche.

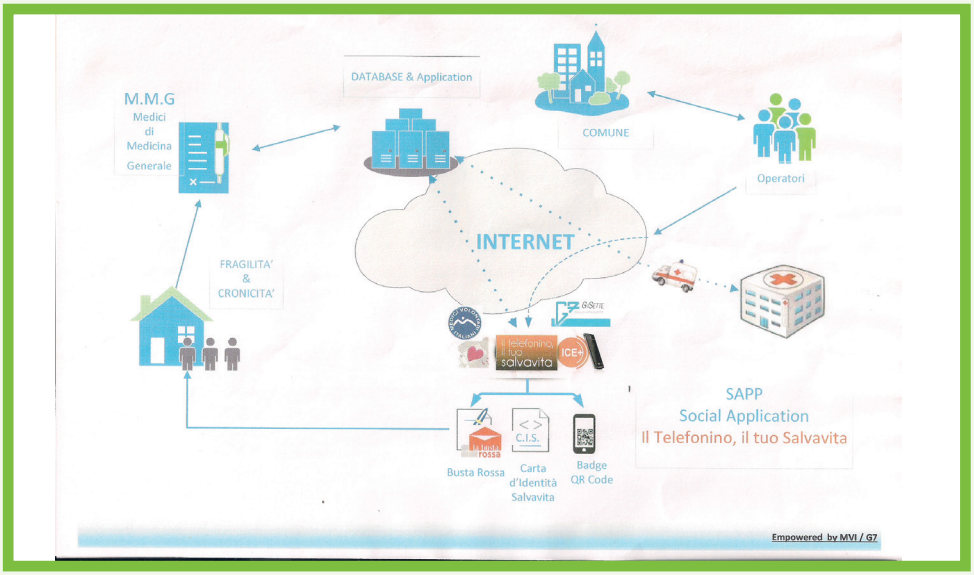
Considerando poi che le informazioni contenute nel BADGE, soprattutto quelle medico-sanitarie necessitano di sistematici aggiornamenti, pensare di mettere in cantiere un progetto come quello che si evince dallo schema allegato **(fig.2)** per lo sviluppo di un'interoperabilità sinergica e finalizzata a quanto sin qui esposto, potrebbe essere un progetto da prendere in considerazione, in quanto si ritiene che i tempi siano oltremodo maturi.

E sarebbe anche un chiaro esempio di Digital Transformation grazie alla disruption di tutti quei lacci e lacciuoli "analogici" che al momento non permettono uno sviluppo digitale più spedito.

GUARDA LE DUE FIGURE
NELLA PAGINA SEGUENTE

BADGE CONTENENTE IL NUMERO ICE DA CHIAMARE, LA FOTO DEL POSSESSORE DELLO SMARTPHONE E LE INFORMAZIONI SALVAVITA IN FORMATO QR CODE

PROGETTO: IL TELEFONINO, IL TUO SALVAVITA



IOT E FOG COMPUTING: L'INTELLIGENZA 'ACCANTO' ALLE 'COSE'

Di **Vincenzo D'Appollonio**, Partner, The Innovation Group

Il termine "Fog Computing" è stato introdotto da Cisco come nuovo modello per facilitare il trasferimento di dati wireless a dispositivi distribuiti nel paradigma della rete Internet of Things (IoT), estendendo il cloud computing ed i servizi fino ai 'bordi' della rete. Il Fog, vera e propria 'Nebbia' Informatica, si diffonde in Rete attraverso una molteplicità di 'centri di condensa' dei servizi dati, elaborazione, storage ed applicativi. Rispetto al Cloud computing, le caratteristiche distintive del Fog sono la vicinanza agli utilizzatori finali ed agli obiettivi di Business del Cliente, la distribuzione geograficamente capillare dell'Intelligenza e della Informazione in rete, la disponibilità di pool di risorse localizzate direttamente fruibili 'ai bordi' della rete, la riduzione della latenza e il risparmio di banda nel backbone, per ottenere una migliore qualità del servizio (QoS), con una superiore 'user experience' ed una maggiore ridondanza in caso di guasto.

Per questa ragione, il Fog Computing supporta al meglio il concetto di Internet of 'everyThings', in cui la maggior parte dei dispositivi utilizzati dagli Esseri Umani e dalle 'Cose' è quotidianamente collegata 'direttamente' tra di loro. Stiamo parlando di telefoni 'smart', dispositivi di monitoraggio sanitario indossabili, veicoli, dispositivi a 'realtà aumentata', piante, coltivazioni, edifici, infrastrutture, macchinari industriali, patrimonio artistico, etc.

Il Fog Computing, in estrema sintesi, offre servizi di data computing e data storage distribuiti e 'localizzati', con alta Qualità di Servizio per Applicazioni in tempo reale e streaming. Permette anche una maggiore eterogeneità in quanto consente la connessione ai dispositivi e ai router degli utenti finali: di seguito alcuni esempi di Applicazioni in Fog.

Smart Energy Grid: i collettori in Fog elaborano i dati dalle applicazioni di bilanciamento del carico energetico, quali micro-griglie, misuratori intelligenti e comandi di rilascio agli attuatori, e generano report in tempo reale. A seconda della domanda e della disponibilità di energia, i dispositivi passano automaticamente a energie alternative (vento e solare).

Smart Traffic Lights (connected vehicles): le telecamere nelle strade possono ad esempio rilevare automaticamente alcune auto in situazioni d'emergenza, come ambulanze, vigili del fuoco, e cambiare le luci dei semafori per aprire strade libere attraverso il traffico, o per identificare la presenza dei pedoni e calcolare la distanza e la velocità di un veicolo in arrivo.

Smart Farming, Reti di attuatori: gli attuatori, disposti 'ai bordi' della rete, localizzati nei territori coltivati, possono esercitare azioni fisiche, a differenza dei tradizionali sensori wireless, e controllare il processo di misurazione dei vari parametri, la stabilità e i comportamenti oscillatori, inviando avvisi e report di monitoraggio.

Smart Buildings: i sistemi di controllo wireless permettono di misurare la temperatura, l'umidità e i livelli di inquinamento in un edificio e queste informazioni vengono continuamente scambiate tra tutti i sensori per formare misure affidabili. I dispositivi e i sensori in Fog reagiscono alle informazioni raccolte e prendono decisioni, come abbassare la temperatura o rimuovere l'umidità dall'aria, creando degli edifici 'intelligenti'.

I vantaggi del Fog Computing sono dunque la riduzione significativa del flusso dei dati in rete, con conseguente riduzione della congestione, del costo di comunicazione e della latenza; l'eliminazione delle strozzature derivanti dai sistemi di elaborazione centralizzati (core computing); la maggiore sicurezza dei dati crittografati in quanto questi rimangono più vicini all'utente finale, riducendo così l'esposizione ad attacchi ostili; una migliore scalabilità derivante dai sistemi virtualizzati. In conclusione, il modello 'Fog Computing' fornisce in particolare alle Applicazioni IoT elevati livelli di scalabilità, affidabilità e tolleranza agli errori, assicurando consumi assai minori di quantità di banda.

DIRITTO ICT IN PILLOLE

SMART WORKING: IL DELICATO EQUILIBRIO TRA PRIVACY E FLESSIBILITÀ ORGANIZZATIVA

Di **Avv. Alessandro Cecchetti,** General Manager, Colin & Partners

Il mondo del lavoro sta attraversando una trasformazione epocale. Non si tratta solo – si fa per dire – di raccogliere le nuove sfide del mercato attraverso l'adozione di infrastrutture digitali di ultima generazione o di dar vita a nuove figure professionali per rispondere con rapidità e preparazione agli input dell'economia delle informazioni.

L'incessante rincorsa al cambiamento percorre infatti anche il fronte organizzativo. La formula dello smart working riflette appieno la metamorfosi culturale che stanno attraversando le imprese, complice l'implementazione di politiche basate sulla valorizzazione delle persone e la disponibilità organizzativa delle risorse favorita dall'azzeramento delle distanze fisiche grazie all'utilizzo delle tecnologie e della rete.

Lo scorso 10 maggio, con l'approvazione del Senato, il Disegno di legge sul lavoro autonomo – ribattezzato "Statuto del lavoro autonomo" – è divenuto legge, riconoscendo ulteriore dignità a questa formula, sempre più diffusa in grandi aziende e multinazionali, sebbene ancora stenti a decollare nella maggior parte delle piccole e medie imprese, dove la presenza fisica è considerata ancora essenziale per lo svolgimento dell'attività.

La prestazione lavorativa fuori dal perimetro aziendale pone una serie di questioni giuridiche inerenti le modalità di utilizzo della strumentazione informatica che caratterizza la prestazione dei subalterni "in smart working", prima tra tutti quella del controllo a distanza da parte del datore di lavoro, ma anche la tutela delle informazioni aziendali, temi questi strettamente connessi.

Sul primo punto la normativa e la giurisprudenza sono intervenute più volte nell'ottica di raggiungere un efficace equilibrio tra l'interesse legittimo del datore di lavoro nell'esercizio della propria attività imprenditoriale, e quello dei dipendenti e della loro riservatezza, disciplinato dall'art. 4 dello Statuto dei Lavoratori. Argomento, questo, riformulato poco più di un anno fa dal D.Lgs. 151/2015 (c.d. Jobs Act) con il precipuo intento di rispondere alle numerose evoluzioni tecnologiche ed organizzative connesse che hanno naturalmente caratterizzato le aziende italiane.

Due i punti più dibattuti nell'ambito della querelle. Da un lato la questione del significato di "tutela del patrimonio aziendale" che – accanto alle "esigenze organizzative e produttive" e alla "sicurezza sul lavoro" – giustifica il ricorso a "gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza", sebbene la loro installazione sia consentita solo previo accordo sindacale o di autorizzazione da parte dell'Ispettorato Nazionale del lavoro. Dall'altro lato, il che cosa si debba intendere con "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" che può far uscire l'introduzione del dispositivo tecnologico dalle autorizzazioni giuslavoristiche.

Un'ulteriore novità introdotta dal Jobs Act, è la possibilità di utilizzare le informazioni raccolte con gli strumenti introdotti in azienda alle condizioni sopra indicate per "tutti i fini connessi al rapporto di lavoro". In altre parole sarebbe possibile utilizzare tali informazioni anche per finalità di carattere disciplinare, previo necessario conferimento ai lavoratori di "adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli". La lettura congiunta di questi concetti alimenta il dibattito interpretativo sulla nuova versione dell'art. 4 dello Statuto dei Lavoratori, che è tutt'ora aperto e alimentato da una giurisprudenza a commento.

Il risvolto è anche tecnologico ed ulteriore conferma dell'attenzione sempre più alta sul tema è rappresentata dall' "Opinion 2/2017 on data processing at work" dello scorso giugno. Il documento si inserisce perfettamente nella logica "privacy oriented" definita dalla General Data Protection Regulation rinforzandone i principi. Il parere ribadisce infatti in più passaggi l'esortazione a prevedere misure di protezione delle informazioni by design e sistemi di minimizzazione dei dati e pone l'accento sull'importanza delle valutazioni di impatto piuttosto che sulla valutazione dei rischi connessi da un lato all'utilizzo di strumenti e piattaforme fuori dal perimetro di sicurezza aziendale, dall'altro al monitoraggio dettagliato dell'attività lavorativa del dipendente.

LE NEO-BANCHE DIGITALI CHE VOGLIONO "SFIDARE" LE BANCHE TRADIZIONALI

Di **Francesco Manca**, Junior Analyst, The Innovation Group

Le contingenze temporali degli ultimi anni, riassumibili in fenomeni demografici, sociali, economici e regolatori ma soprattutto le tecnologie digitali, hanno contribuito ad una tra le più grandi rivoluzioni del settore bancario degli ultimi tempi come la nascita delle Fintech. L'interrogativo è capire se la dimensione del fenomeno Fintech continuerà a crescere nel medio-lungo termine e, nello specifico, se il posizionamento nel mercato delle "challenger bank" rispetto alle banche tradizionali verrà consolidato. Negli ultimi anni si è infatti sempre più pronosticata una azione disruptive sull'attuale settore finanziario da parte delle Fintech, in realtà c'è chi pensa che in orizzonti di medio-lungo termine ci saranno due probabili scenari: alcune Fintech, ampliando la gamma dei propri servizi, verranno percepite come competitor delle vere e proprie banche tradizionali, altre invece daranno origine a modelli ibridi di collaborazione con banche tradizionali diventandone ad esempio piattaforme per i loro servizi digitali. Questa analisi si concentra sul primo scenario che vede protagoniste le nuove banche digitali, o challenger bank, definibili come istituti che fanno affidamento sul digitale come unico o predominante canale di interazione con il cliente e che stanno ottenendo (o hanno da poco ottenuto) una licenza bancaria.

Negli ultimi anni c'è stato infatti un contesto favorevole alla presenza di nuovi entranti nel mercato bancario, che ha spinto la creazione di nuove realtà che offrono servizi finanziari o che ha incentivato le stesse banche ad aprirsi al mondo digitale per non soffrire una competizione da parte di attori esterni al settore. Il contesto favorevole si concretizza in un cambiamento del profilo dei consumatori di servizi finanziari/bancari, che hanno così nuovi bisogni da soddisfare: i millennial stanno diventando i nuovi acquirenti di servizi bancari con esigenze di servizi on-demand, la diffusione pervasiva degli smartphone come mezzo di iperconnessione incentiva ulteriormente a richiedere tramite app servizi on-demand con caratteristiche di immediatezza e semplicità ed infine il cambiamento generale nel mondo occidentale che, dopo l'ultima crisi finanziaria, ha visto l'indebolimento della fiducia nei confronti del settore bancario tradizionale. Le nuove banche digitali hanno trovato così terreno fertile avendo tra i principali driver di riferimento una struttura asset light, l'offerta di prodotti semplici ed una interazione immediata e costante con il cliente. Queste neo-banche vogliono essere delle vere e proprie challenger bank e si stanno ora focalizzando su prodotti sempre più specifici del settore bancario, come prestiti, finanziamento a PMI e mutui, oltre ai servizi di money transfer che hanno da sempre caratterizzato il mondo Fintech. L'offerta è caratterizzata solitamente oltre che dal mezzo di interazione digitale, anche da una ampia flessibilità contrattuale e costi minore per andare incontro alle singole esigenze del cliente.

Alcuni esempi sono le inglesi Atom Bank e Starling Bank e la tedesca N26 Bank. La prima, che è stata tra i pionieri delle challenger bank, fornisce i suoi servizi bancari tramite app, non ha filiali fisiche e non dispone di un tradizionale outlet bancario online, caratteristiche che le permettono di abbattere gran parte dei costi fissi e di gestione a favore di una offerta con tassi di interesse favorevoli per il consumatore ed altamente competitivi per i competitor tradizionali. Atom ha acquisito la licenza bancaria nel giugno del 2015, ed è stata lanciata al pubblico nell'aprile del 2016. Attualmente ha un finanziamento venture superiore ai 200 milioni di sterline. Starling Bank ha ricevuto la licenza bancaria nel luglio 2016 e, dopo aver lanciato la sua beta nel marzo 2017, ha annunciato lo scorso giugno la sua espansione in Europa (il primo paese sarà l'Irlanda). Oltre ai servizi tipici delle challenger bank queste due banche ricorrono all'uso di tecnologie biometriche per garantire la sicurezza dei loro clienti e per aumentare l'immagine tecnologica ed innovativa delle loro aziende. N26 invece offre la proposta di banca digitale nell'eurozona; inizialmente nasce come interfaccia facente riferimento ad Wirecard, poi nel Luglio 2016, ricevendo la licenza bancaria da BaFin, è diventata autonoma con il nome N26 Bank. Attualmente è presente in 17 paesi dell'eurozona, offre tramite app l'accesso ai servizi MoneyBeam (servizio di money transfer), Mastercard e TransferWise e progetta di fornire a breve l'accesso tramite app a servizi di credito a consumo, prodotti di risparmio ed assicurativi. Queste ed altre realtà del mondo bancario saranno presenti al Banking Summit 2017 organizzato da The Innovation Group il 21 e 22 Settembre a Saint Vincent. Il successo di alcune banche digitali testimonia le grandi opportunità in questo mercato. Il terreno fertile per i nuovi entranti e la basse barriere all'entrata possono però causare grande competizione tra questi nuovi entranti e rischi di sopravvivenza nel lungo periodo o tempi troppo lunghi per raggiungere il break even point.

Il successo del mondo delle neo-banche, oltre ad essere fortemente influenzato dalle caratteristiche della loro offerta è anche strettamente vincolato dalla legislazione vigente. Vari paesi stanno agendo diversamente per regolamentare il mondo Fintech e le licenze bancarie per le neobanche. La Gran Bretagna, avendo l'esigenza di presentare proposte lungimiranti ed innovative in campo finanziario per far fronte ad un settore che impiega più di 1.2milioni di persone e produce più del 7% del valore aggiunto di tutta l'economia, presenta lo scenario più avanzato. La Financial Conduct Authority (FCA) inglese ha introdotto Project Innovative a supporto dell'autorizzazione bancaria per business innovativi che include anche una sandbox per testare nuove offerte in contesti scoperti dalle normative standard, in passato poi Bank of England ed FCA hanno formato un acceleratore di Fintech che supporta e da consulenza alle fintech per le implicazioni del processo di regolamentazione. Altri contesti innovativi internazionali sono Singapore che, data la spinta innovativa del suo settore finanziario, ha le potenzialità per essere hub di challenger bank nella regione asiatica e gli USA che dopo UK hanno il maggior numero di startup Fintech interessate a diventare neobank.

È quindi lecito pensare che nei mercati finanziari sviluppati con un'elevata penetrazione di smartphone e di retail banking, in cui la regolamentazione non offre sviluppi e o evoluzioni imminenti (Europa continentale), o in cui è ancora alta la fiducia nelle banche, nel medio periodo le challenger bank collaboreranno con gli incumbent per ripristinare la fiducia dei clienti migliorandone l'esperienza ed estendendo su di loro i vantaggi dei minori costi operativi. Al contrario, in paesi con un'elevata penetrazione di smartphone e una scarsa fiducia bancaria, o in cui la regolamentazione sarà sempre più accomodante all'istituzione di neo bank, è possibile che queste diventeranno sempre più alternative ai player tradizionali (con conseguenti effetti disruptive nel settore).

LE ULTIME EVOLUZIONI DEL RANSOMWARE: COSA INSEGNANO I CASI WANNACRY E NOTPETYA

Di **Elena Vaciago**, Associate Research Manager, The Innovation Group

Le attività malevole come virus, ransomware e APT, rappresentano un problema grave per aziende di tutte le dimensioni almeno da un paio di decenni. Quanto avvenuto negli ultimi mesi però, prima con il ransomware-worm WannaCry, poi con il worm-wiper NotPetya, mostra un'evoluzione preoccupante sia nella sofisticazione del malware, sia nella velocità di diffusione dello stesso e negli impatti procurati.

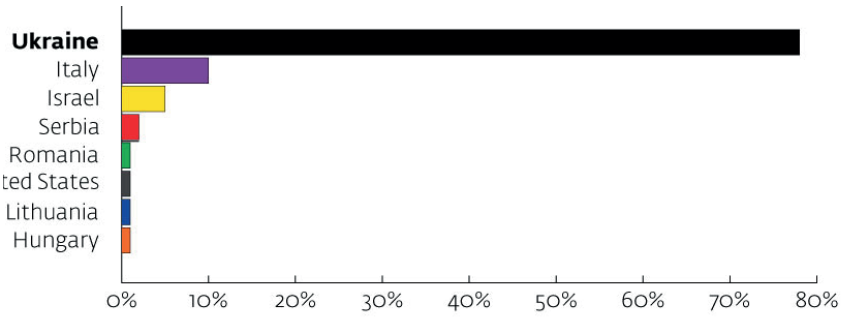
L'attacco WannaCry lo scorso maggio ha compromesso centinaia di migliaia di sistemi in pochi giorni in oltre 150 paesi, arrestando anche processi critici come quelli di ospedali, trasporti, linee di produzione industriale. Solo un mese dopo, la stessa vulnerabilità di WannaCry (e il relativo exploit NSA EternalBlue), unita ad altre tecniche, ha permesso a un nuovo attacco, identificato inizialmente come il ransomware Petya (poi si è visto che era una sua variante e ha preso altre denominazioni: NotPetya, Petwrap, ExPetr, EternalPetya, Nyetya, …) di infettare decine di migliaia di macchine in oltre 60 Paesi, arrivando perfino alla centrale di Chernobyl.

Ad essere colpiti sono stati: il gruppo pubblicitario WPP, FedEx, il gigante delle spedizioni Maersk, Nuance Communications e, forse, anche la società petrolifera russa Rosneft. Inoltre questa volta tra le vittime sono state contate numerose aziende italiane che erano invece sfuggite alla precedente diffusione del ransomware WannaCry.

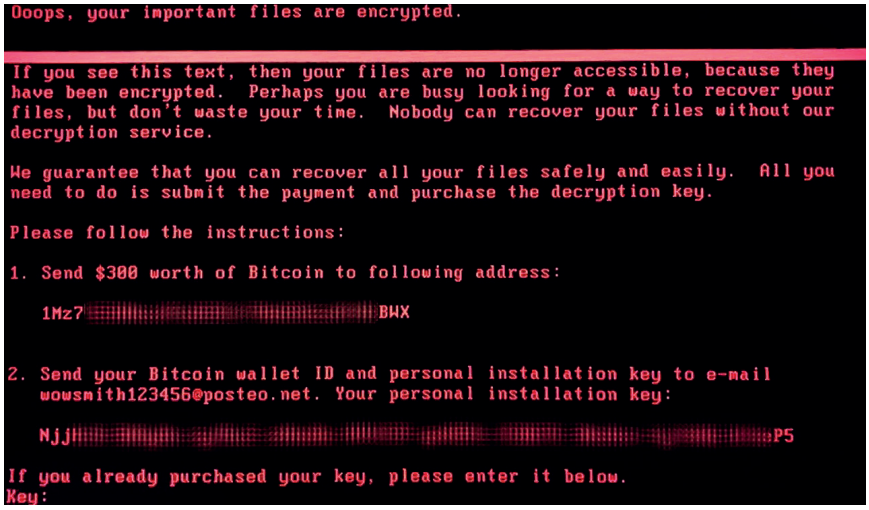
Come mostra la figura, ESET ha misurato che l'80% delle infezioni erano avvenute in Ucraina e il 10% in Italia. Una di queste, la Maschio Gaspardo di Padova, un produttore di macchine per la lavorazione del terreno con sede in Ucraina, colpita dal malware ha dovuto chiudere tre stabilimenti per diversi giorni, mandando a casa 650 tecnici e operai.

#PETYA RANSOMWARE DETECTIONS

Fonte: ESET



LA RICHIESTA DI RISCATTO



MA COSA E' SUCCESSO E COME SI E' DIFFUSO NOTPETYA?

Secondo varie fonti, gli ultimi giorni di giugno una variante del ransomware Petya (già noto dal 2016) ha colpito prima l'Ucraina per arrivare poi, in breve tempo, a molti altri Paesi, utilizzando l'exploit NSA EternalBlue (che sfrutta la vulnerabilità di Windows SMBv1) oltre che WMIC e PSEXEC per propagarsi lateralmente nelle reti colpite.

Il nuovo malware, rinominato in vari modi (lo chiameremo NotPetya), è congeniato per attaccare il file master del disco rigido (MFT) e sostituisce il Master Boot record (MBR) con un proprio codice dannoso.

Mostra la videata che riportiamo in figura per la richiesta di riscatto impedendo di fatto il riavvio del PC.

E' risultato che almeno una ventina di vittime hanno pagato il riscatto, ma ben presto **non è stato più possibile farlo**, perché la mail a cui scrivere è stata quasi subito disabilitata dal Service Provider Posteo. Anche pagando però **non era poi possibile decriptare i file**: a differenza del ransomware originario, la nuova variante NotPetya non prevede infatti nel suo codice alcun meccanismo di recovery. Per questo motivo FedEx ha ad esempio dovuto dichiarare di aver perso irrimediabilmente alcuni file. Si è trattato quindi di un wiper malware, progettato solo per fare danni: si potrebbe dire, una **vera arma cibernetica**.

La comprensione dei meccanismi di NotPetya è ancora in corso, ma al momento si hanno alcune evidenze:

1. L'attacco era **principalmente rivolto all'Ucraina**, che come detto è stato di gran lunga il Paese più colpito. L'infezione ha riguardato in questo Paese infrastrutture critiche come l'Ukrenergo, il principale provider nazionale di energia elettrica, l'aeroporto internazionale

di Boryspil, la Banca Centrale, con il coinvolgimento di POS e sportelli ATM.

2. Il meccanismo iniziale di infezione ha sfruttato un meccanismo di update software legittimo (relativo alla soluzione di tax reporting ucraina M.E.Doc) che è stato infettato con il malware. In questo modo l'update del sofware è servito come **veicolo per diffondere l'attacco**, in alternativa ad una mail di phishing o a un classico web download, potendo quindi superare le difese perimetrali tradizionali.
3. Per propagarsi internamente alle reti delle aziende colpite, NotPetya ha utilizzato strumenti Windows standard: un trend questo che secondo gli esperti potrebbe diventare **molto preoccupante** se venisse utilizzato sistematicamente in tutti i prossimi attacchi ransomware.

QUALI LE MOTIVAZIONI DIETRO L'ATTACCO?

Per come è stato condotto, l'attacco NotPetya fa pensare che non ci fosse la motivazione del guadagno, **l'infrastruttura per ricevere i pagamenti non era abbastanza resiliente**: una sola email (che è stata disabilitata dal provider Posteo in poche ore), un solo indirizzo bitcoin.

Inoltre, mentre con il ransomware Petya originario era possibile ripristinare i file criptati, il nuovo malware era di fatto un wiper, che **cancellava i file in modo irreversibile** puntando quindi a un vero sabotaggio. Gli esperti non escludono che la videata ransomware apparsa sia stata in realtà un modo per NASCONDERE alle organizzazioni colpite la reale natura e gli effettivi scopi del malware, che non limitava i suoi effetti al singolo sistema, ma puntava invece a infettare più sistemi e a sabotare le operazioni in modo più ampio.

Distraendo le persone (che si preoccupavano principalmente del pagamento), l'attacco veniva portato avanti in modo silente e più efficace.

L'attacco è stato quindi piuttosto **sofisticato ed innovativo**, soprattutto sul fronte dell'iniziale vettore di attacco (la compromissione dell'update software del programma M.E.Doc), oltre che sulle capacità di propagazione attraverso reti tra loro collegate (il malware ruba le credenziali presenti sulla macchina per provare ad accedere ad ulteriori sistemi, non va invece su Internet come WannaCry).

Il fatto che fosse così tanto mirato a sabotare servizi legati all'economia ucraina, ha fatto subito sorgere il sospetto che il **mandante fosse uno stato straniero** interessato a dimostrare le sue capacità di prendere il controllo di sistemi critici per l'operatività della nazione: l'agenzia di sicurezza Ucraina SBU ha accusato subito i servizi russi come mandanti dell'operazione. Anche FireEye, società chiamata dalla Polizia Nazionale Ucraina ad effettuare indagini forensi su dati e macchine colpite, ha trovato molte analogie con gli attacchi informatici effettuati da **Sandworm Team**, un gruppo di base in Russia che ha già colpito l'Ucraina nel dicembre 2015 e poi nel dicembre 2016 .

COSA CI HANNO INSEGNATO GLI ATTACCHI WANNACRY-NOTPETYA

1 – AGGIORNAMENTI DI SICUREZZA.

Entrambi gli attacchi sfruttano una vulnerabilità del sistema operativo windows che poteva essere risolta utilizzando patches pubbliche: una prima lezione è quindi **banalmente** che i sistemi operativi andrebbero tenuti il più possibile aggiornati. Se questo avviene nella maggior parte dei casi quando l'utente è un privato, nel caso di aziende, le operazioni di patching presentano spesso delle complessità, per cui un ritardo può essere giustificato – anche se alla luce dei fatti recenti risulta comunque rischioso. In azienda, possono però esserci delle motivazioni per cui non tutti i sistemi siano correttamente aggiornati: una delle preoccupazioni è che una volta fatto l'aggiornamento, alcuni software che girano sul sistema non funzionino più. Un altro tema è quando l'aggiornamento dovrebbe essere svolto da un fornitore esterno, che dovrebbe garantire anche per la funzionalità complessiva della macchina – ma questo requisito potrebbe non essere stato richiesto nell'acquisto iniziale del prodotto. Ancora peggio se in azienda ci sono computer che, pur funzionando, hanno sistemi operativi per cui non sono più forniti aggiornamenti di sicurezza.

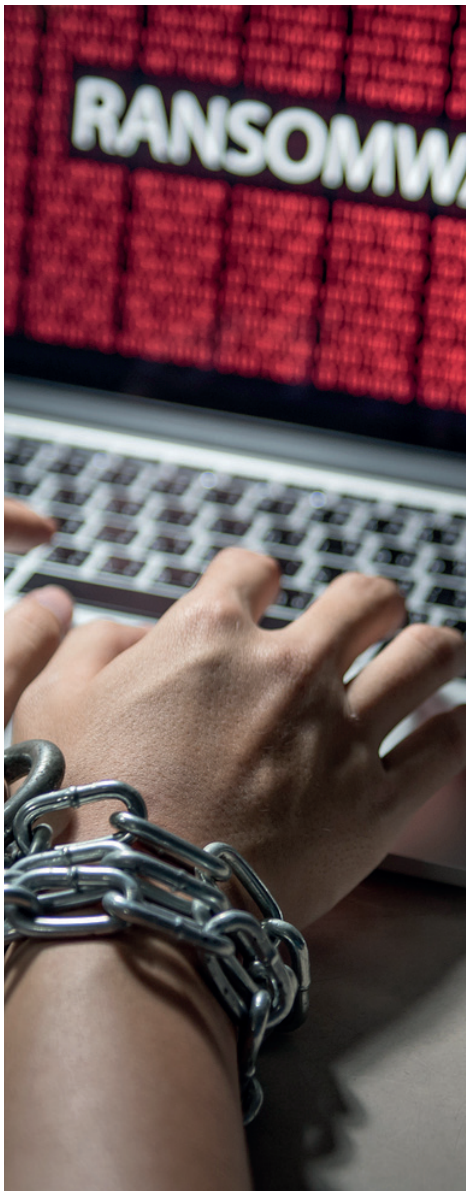
Uno studio 2017 di Spiceworks ha rilevato che 1 azienda su 2 continua ad avere macchine Windows XP in funzione (nonostante Microsoft non abbia smesso nel 2014 di fornire supporto a questo sistema): interrogati sulle motivazioni, la metà degli intervistati risponde che non ha tempo per effettuare l'upgrade; il 37% lamenta tagli al budget; un ulteriore 31% afferma che problemi di compatibilità con il software in uso frenano l'azienda ad effettuare l'upgrade …

2 – IMPATTO ECONOMICO PIU' AMPIO RISPETTO AL PASSATO.

Se inizialmente si era pensato che gli effetti di NotPetya fossero inferiori a quelli degli incidenti legati a WannaCry (che inizialmente erano stati più numerosi) è bastato poco tempo per far svanire questa illusione. Una società britannica di prodotti di consumo, la Reckitt Benckiser, ha calcolato che l'interruzione della produzione dovuta a NotPetya le è costata 110 milioni di sterline (135 milioni di dollari); il produttore di cioccolato Mondelez ha stimato un danno economico pari a 3 punti percentuali rispetto alla sua crescita del secondo trimestre. Se una volta gli attaccanti cyber violavano i dati e quindi portavano a danni legati principalmente alla gestione dei clienti o al danno di reputazione, ora, i nuovi ransomware-worm-wiper sono in grado di **bloccare la produzione o interrompere la supply chain**, con danni economici ancora più devastanti.

3 – CONCORRENZA SLEALE E SPIETATA NEL CYBERSPAZIO.

Lo scenario che si sta dipingendo con il diffondersi dei nuovi attacchi lanciati presumibilmente da Stati nemici fa ipotizzare una forma di "cyber-war economica", lanciata contro un occidente economicamente avanzato ma poco preparato sul fronte delle difese digitali, messo quindi in ginocchio e costretto a correre ai ripari stanziando investimenti rilevanti sul fronte della cybersecurity per **preservare la propria dipendenza dai sistemi digitali**. In definitiva, potenzialmente meno competitivo rispetto ad economie emergenti in cui il security-by-design diventa elemento competitivo sostanziale della nuova economia digitale.



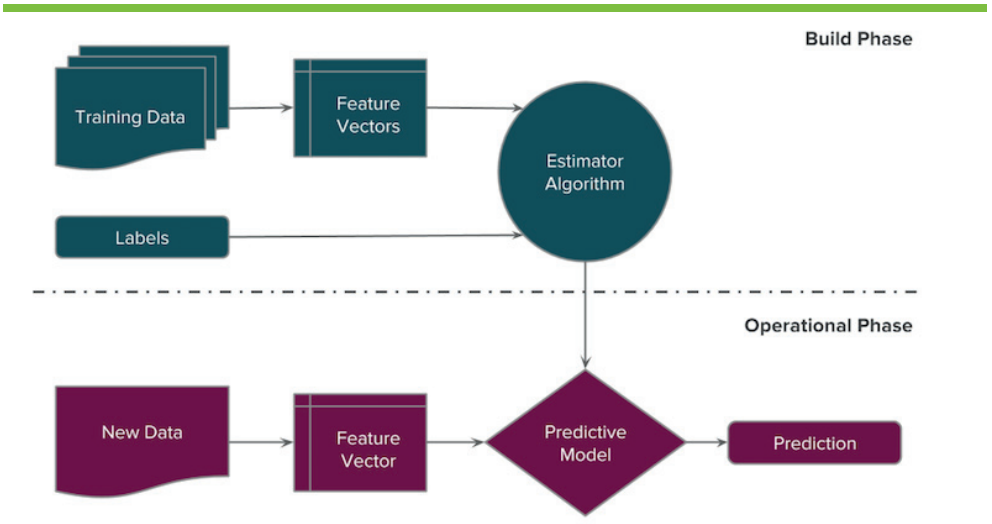
DATA CENTER DIGITAL TRANSFORMATION: LA SFIDA DI IBM

Di **Francesco Manca**, Junior Analyst, The Innovation Group

Il 14/15 Giugno si è tenuta a Londra l'edizione europea del Cloud Analyst Day di IBM. Oltre a trattare nello specifico l'offerta e i punti di forza dell'offerta Cloud di IBM, c'è stata anche l'opportunità di approfondire alcune dinamiche generali di alcuni mercati tecnologici tra cui quello dell'intelligenza artificiale (AI). Secondo le stime di The Innovation Group, le dimensioni del mercato italiano di tecnologie AI negli sono abbastanza contenute (circa 25mln nel 2017), ma è prevista una forte crescita con un CAGR del 65% nei prossimi sei anni fino ad arrivare a quasi 300mln nel 2022. In questo periodo si prevede una progressiva diminuzione della quota delle componenti software all'interno del mercato ed una crescita dei servizi, specialmente per un aumento del mercato di soluzioni API e Cloud, la cui offerta è già ampliamente strutturata. Tra i principali provider di tecnologie intelligenti tramite Cloud ed API c'è IBM con Watson: la piattaforma Cloud per servizi AI. IBM è pioniere tra i fornitori di tecnologie intelligenti su piattaforma Cloud e, come la maggior parte degli altri providers, ha investito molto nella sua offerta AI puntando sul fatto che la maggior parte di chi ha adottato tecnologie intelligenti nel recente passato continuerà a farlo, perché crede che queste saranno un "must have" per rimanere competitivi nel futuro prossimo[1]. L'interesse delle aziende per le tecnologie AI ne incentiva la ricerche che nella sola IBM hanno prodotto in pochi anni 825[1] brevetti. La maggior parte delle piattaforme di servizi AI sono in Cloud (SaaS), in quanto è una struttura che permette di offrire ed aggiornare in un unico luogo strumenti che si stanno sviluppando ed, allo stesso tempo, rendono ogni servizio molto customizzabile.

La maggior parte dei provider differenzia la propria offerta in soluzioni analytics, data visualiaztion, sistemi di text to speech, speech to text e visual recognition, tutte applicabili a contesti ed industry diversi, allo scopo di potenziare l'analisi dei dati strutturati e di codificare quelli non strutturati. Ad oggi i servizi più maturi ed efficienti sono quelli di conversazione e quindi meccanismi di text to speech e speech to text che permettono una interazione diretta tra utente e macchina. Le applicazioni più comuni sono quindi soluzioni di chatbot e virtual agent, finalizzate essenzialmente a servizi di front desk per l'interazione con il consumatore finale. Parallelamente a questi tool specifici per singole applicazioni, le piattaforme generalmente offrono anche servizi più generici, che integrano diverse tecnologie intelligenti cercando di usare dati, analizzarli, farsi domande e darsi delle risposte che possano essere rilevanti per l'utilizzatore. Sistemi di questo tipo sono ancora tra i più immaturi, ma di certo sono anche tra quelli con più potenziale di sviluppo ed utilizzo e su cui i principali vendor puntano come driver per lo sviluppo della loro offerta. IBM, ad esempio, ripone nella sua offerta Watson Discovery le maggiori aspettative di mercato e di sviluppo. Nello specifico, Discovery Service è un insieme di API che può generare rapidamente ricerche intelligenti, analisi dei contenuti, crea dati, estrae valore da dati non strutturati e strutturati in un sistema facilmente scalabile e di facile utilizzazione. I driver della domanda di soluzioni intelligenti tramite piattaforme cloud non sono però confinabili alla sola efficacia delle tecnologie, ma anche ad altre caratteristiche tecniche e funzionali. Le tecnologie intelligenti autoapprendono ed interpretano i dati tramite meccanismi di machine learning, che necessitano di un traning specifico e particolare a seconda dell'utilizzatore. Questo significa che sistemi con un training proprio e costruito sullo use case dell'utente aumentano la probabilità di avere soluzioni più efficaci; raggiunto un determinato livello si autoaddestrano ed imparano autonomamente sui dati a loro disposizione. Offrire tecnologie già addestrate per mano di altri utilizzatori, rendendono disponibile questo sviluppo tramite cloud a terzi può infatti avere effetti contrastanti: se da un alto si potenza il raggio di azione e l'efficacia della tecnologia stessa offrendole maggiori use case sui quali il sistema fa inferenza per arrivare ad una soluzione, dall'altro si possono aprire gli sviluppi tecnologici compiuti da uno specifico utente anche ai suoi potenziali competitor. Il grado di privatizzazione dei propri dati, ma soprattutto del training applicato alla tecnologia, è quindi un altro dei fattori sostanziali su cui i vari provider si differenziano: da un lato offrendo la protezione del grado di training e dall'altro garantendo un servizio sempre più dinamico ed in evoluzione. IBM ha deciso di perseguire il primo percorso, garantendo un training non condiviso, in cui il livello di efficienza varia a seconda del livello di training dell'utilizzatore, in un' ottica in cui ogni dato caricato e ogni training è di dominio privato; altri attori del mercato hanno invece optato per una scelta open e meno privatizzata, in cui ogni utilizzatore "condivide" correzioni ed algoritmi di training per una conseguente ottimizzazione del sistema. Infine è utile segnalare che la domanda di servizi AI non appare distribuita in modo omogeneo. I principali fruitori di servizi AI sono imprese di grandi dimensioni o startup; mancano all'appello le imprese medie che al momento non sembrano ancora interessate a questo mercato o, meglio, in cui domina il timore di fare investimenti troppo azzardati su tecnologie di cui riconoscono le potenzialità ma non ancora del tutto affidabili (perché non pienamente mature). Le grandi imprese identificano invece nelle tecnologie AI opportunità competitive sul piano dell'innovazione che possono permettere di guadagnare quote di mercato e/o di consolidare la propria posizione dominante; le startup tecnologiche al contrario, vedono nelle tecnologie AI la principale vena innovativa che ne giustifica l'esistenza e che può permettere l'inserimento e l'ingresso nel mercato.

1. https://www.ibm.com/blogs/watson/2016/11/leading-cognitive-charge-companies-hold-ai-patents/

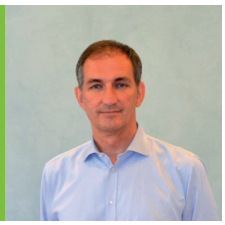


LE AUTO CONNESSE SARANNO IL PROSSIMO OBIETTIVO DEGLI HACKER?

Intervista di **Elena Vaciago** a **Giuseppe Faranda**, DriveSec

Il recente attacco ransomware WannaCry, seguito a breve da Petya o NotPetya, ha dimostrato quali sono le vulnerabilità di molteplici sistemi informativi in tutto il mondo. Ma cosa succederà quanto ad essere "presa in ostaggio" sarà la nostra automobile connessa? Qual è oggi il rischio che si corre acquistando autovetture dotate di sempre maggiore "intelligenza" a bordo? Ne abbiamo parlato con Giuseppe Faranda, Amministratore Delegato della startup italiana dedicata alla sicurezza della mobilità DriveSec.

Giuseppe FARANDA



Come si sta trasformando il business dell'Automotive e qual è oggi la maturità del mercato delle autovetture connesse?

L'industria automobilistica è oggi nel mezzo della sua più grande trasformazione da quando nel 1908 apparve il primo modello di auto per il mercato di massa. Oggi il cambiamento però non sta nel prezzo o nella catena di produzione, ma piuttosto nasce dal matrimonio tra elettronica avanzata, connettività, piattaforme software e big data intelligence: tutto questo farà nascere nuove opportunità di business e trasformerà l'esperienza d'uso dei consumatori. Se siamo ancora lontani dai veicoli autonomi, le auto connesse sono invece già una realtà: le vendite sono passate da 8 milioni nel 2015, a 30 milioni nel 2017 e diventeranno 100 milioni nel 2021. Diversi car maker, da GM a BMW, Mercedes, Volkswagen, hanno già soluzioni mature di autovetture connesse da proporre al mercato, e vedono la connettività come lo strumento per mantenere nel tempo una relazione diretta con gli acquirenti, relazione che una volta era gestita dalle concessionarie.

La connettività delle auto, tra di loro (V2V), con le infrastrutture di trasporto (V2X), con le persone (V2C), abilita nuovi business model tutti da esplorare. Quali saranno quelli più interessanti?

La tecnologia sta facendo nascere nuove opportunità diverse dalla tradizionale vendita dell'automobile. Oggi per il car maker è possibile analizzare il comportamento e lo stile di guida, e offrire al cliente servizi aggiuntivi, come una manutenzione personalizzata, vendita di software o intrattenimento. Inoltre sarà possibile rivendere i suoi dati e il geo-posizionamento ad assicurazioni e network pubblicitari, come fanno oggi Google e Facebook (con tutti i limiti che saranno imposti dalle nuove norme EU sulla privacy). Già oggi i veicoli possono produrre, tramite i sensori e le centraline a bordo, numerose informazioni rilasciate a velocità elevate, come mostra la Tabella successiva.

Examples of Data Elements Broadcasted by Vehicles

GPS Position	Steering wheel angle	Stability control status
Latitude	Acceleration set	Brake boost applied
Longitude	Longitudinal acceleration	Auxiliary brake status
Elevation	Vertical acceleration	Vehicle Size
Transmission and speed	Brake applied status	Vehicle temperature
Positional accuracy	Taw rate	Camera imaging
Transmission state	Brake status not available	Vehicle width
Motion	Brake system status	Vehicle weight
Speed	Traction control state	Radar imaging
Heading	Anti-lock brake status	Vehicle length

Il trend è così interessante che un fornitore globale del mercato automobilistico, Delphi Automotive, che conta 161mila dipendenti e 126 fabbriche in tutto il mondo, ha già acquisito 2 startup, Control-Tec, attiva nel mercato dei data analytics, e Movimento, che dispone di una tecnologia OTA (over-the-air) per update software rivolti a autovetture in movimento.

Possono poi nascere modelli di business legati allo sviluppo di servizi per la mobilità, car sharing, guida in città e noleggio, uniti a ulteriori servizi, come controllo della navigazione, gestione di flotte, diagnostica da remoto, automatic collision notification, safety, telematic & usage based insurance, fino al più evoluta guida autonoma, che a sua volta si potrà scomporre in altre alternative (guida assistita, truck platooning, ecc.). Per lo sviluppo di tutte queste opportunità alcuni car maker stanno lanciando società dedicate, come Mercedes me, Movis VW. Gli analisti di mercato dicono che entro il 2020 il mercato dei servizi di connected car potranno arrivare ai 40 miliardi di dollari all'anno.

Va aggiunto che una maggiore condivisione di informazioni delle autovetture, tra di loro e con le infrastrutture esterne, viene vista positivamente e addirittura incentivata dalle autorità pubbliche, perché potrebbe facilitare un migliore controllo del traffico, risolvere problemi di viabilità e di sostenibilità ambientale, migliorare la risposta in caso di incidenti. Negli USA il Dipartimento dei trasporti sta proponendo di abilitare comunicazioni V2V per tutti i veicoli leggeri entro il 2018, in modo da scambiare dati come velocità dell'autovettura, posizione, frenata, e il National Highway Traffic Safety Administration (NHTSA) ha pubblicato una propria proposta di regolamentazione per mettere in sicurezza queste comunicazioni.

In Europa invece, per ridurre la mortalità sulle strade, tutti i nuovi modelli di auto e furgoni leggeri dovranno essere dotati, da aprile 2018, di dispositivi di chiamata d'emergenza (eCall) simili alle attuali black box telematiche, in grado di allertare automaticamente i servizi di soccorso in caso d'incidente stradale.

Quali sono però i rischi legati ad una più ampia superficie di attacco aperta con il nuovo scenario dei veicoli connessi?

Tutti i temi della sicurezza ICT si trasferiscono al mondo automotive. In un futuro molto prossimo le automobili saranno degli oggetti in movimento costantemente connessi con gli ambienti esterni, tra di loro, con i sistemi di gestione del traffico (Traffic Management), con altre applicazioni residenti in cloud, con gli smartphone dei guidatori e viaggiatori, con smart homes e smart cities.

Per lo sviluppo di un ambiente complessivamente resiliente è importante,

in questo momento, avere una visione il più possibile ampia e onnicomprensiva della situazione. E come mostra la figura successiva, ripresa da un'analisi di CBInsights, le macchine saranno oggetti sempre più complessi da tenere sotto controllo.

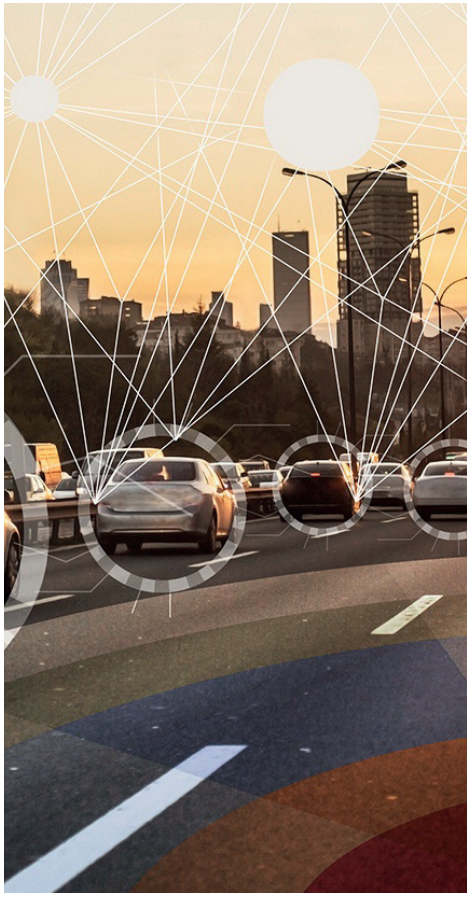
I punti di vulnerabilità di un'auto connessa sono molteplici, e alcune di queste vulnerabilità sono già note: il sistema di intrattenimento collegato a Internet, trasmissioni non crittografate via reti esterne, Bluetooth, access point WiFi, porte USB, problemi del software in APP per smartphone rivolte ad esempio all'apertura della vettura.

I ricercatori di sicurezza hanno già dimostrato come sia possibile hackerare le centraline presenti nelle autovetture (ad esempio entrando attraverso la porta dei sistemi di On Board Diagnostic, OBD-II, collegandosi tramite reti Bluetooth, WiFi o da smartphone), e prenderne il controllo, come nel caso degli attacchi andati a segno per la Jeep Cherokee e per la Tesla.

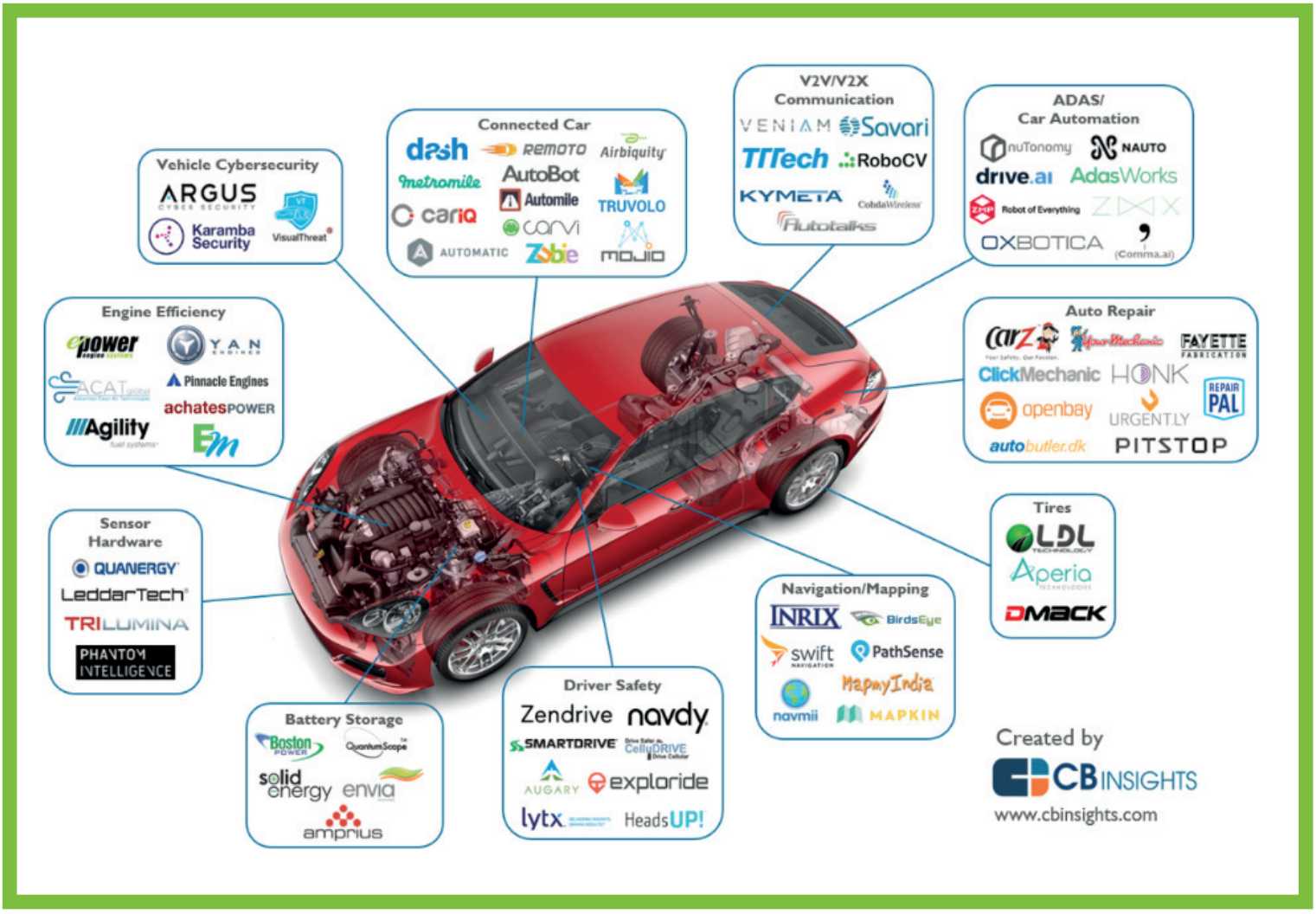
Un'ulteriore complessità è data dal fatto che bisognerà preoccuparsi a breve di mettere in sicurezza parchi circolanti di decine di milioni di vetture, con età diverse (in media 10 anni) e capire come far convivere generazioni di tecnologie diverse.

Mentre per la Functional Safety esistono già metodi e metodologie per valutare la resistenza dei sistemi di ausilio alla guida o per i sistemi di guida autonoma, dal punto di vista della cybersecurity, non esiste una normativa di riferimento e i vari OEM ci stanno lavorando in modo indipendente, senza una condivisione delle problematiche, collaborando con società esterne a cui delegare attività di VA/PT. Con l'incremento delle comunicazioni e dei punti potenzialmente vulnerabili dovrà essere rivisto l'attuale approccio alla cybersecurity: un elemento importate sarà poter aggiornare il firmware delle centraline over the air (FOTA, SOTA). Per poter essere aggiornate dovranno però essere dotate di maggiore memoria, con extra costi e quindi la necessità di ripensare i business model.

In definitiva, la sicurezza cyber deve diventare una priorità, dal disegno del veicolo fino a quando il guidatore sale in macchina e oltre: bisognerà mettere in sicurezza ogni aspetto della vasta superficie d'attacco di una Connected car, abilitando i corretti livelli di sicurezza e connettività di volta in volta.



UNBUNDLING THE AUTOMOBILE



NOTE

IL CAFFÈ DIGITALE

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Bocconi

iscriviti alla nostra **Newsletter** mensile per restare in contatto con noi!

Riceverai articoli dei ricercatori di **The Innovation Group**, aggiornamenti sul piano **Eventi**, informazioni sulle **Ricerche** e i **White Paper**, Inviti e promozioni riservate.

COMPILA IL FORM DI REGISTRAZIONE SU

www.theinnovationgroup.it