L'EDITORIALE DI

Ezio Viola
Managing Director, The Innovation Group

IMMAGINARE IL FUTURO PER PREVEDERE LE CONSEGUENZE DELLE TECNOLOGIE

Alcune volte, quando si deve scegliere cosa commentare e analizzare tra gli avvenimenti e le notizie di cui solitamente tratta questa Newsletter, ci si può trovare di fronte a diverse opzioni: a volte la scelta è obbligata o molto semplice, perchè sono pochi i fatti e le notizie che davvero sono rilevanti e non si ha difficoltà a sceglierne una; altre volte capita che le possibilità siano molteplici, di notizie interessanti ce ne possano essere diverse, ma non ne emerge chiaramente nessuna ed è difficile trovare un filo rosso meno generico e banale di quello della continua evoluzione e del cambiamento che il mercato digitale e i suoi giocatori provocano. Questo è il caso suscitato da due temi forse minori trattati anche al recente G7.

Il primo è il caso di "Wannacry", sia per l'impatto e la risonanza che per la dimensione dell'attacco e la velocità in cui è stato diffuso, dove viene mostrato, ancora una volta, come la minaccia alla sicurezza di paesi, infrastutture critiche, imprese e individui può fare un salto di qualità e contemporaneamente mettere in luce come i "basics" della sicurezza (in questo caso avere dei sistemi operativi aggiornati) siano ancora poco rispettati. D'altro canto, se è vero che la cybersecurity è stata uno dei punti all'ordine del giorno del recente G7 e che il risultato su altri argomenti più strategici sia stato un freno all' apertura dei Paesi, le premesse per affrontare la cybersecurity, che si fonda sul rafforzamento della collaborazione tra enti e paesi, sono ancora molto deboli.

Sempre durante il G7, è stato affrontato il tema della tassazione dei giganti del Web.

Su questo punto, in Italia è stato annunciato il recente accordo dove anche Google, dopo Apple, deve pagare al fisco qualche centinaio di milioni di euro (circa 300) per sistemare la propria reputazione e dare "una mancia" allo Stato, cosa che fa sempre bene di questi tempi.

Questo tema si lega allo strapotere che i giganti del Web ormai hanno acquisito e rimanda alla mancanza di un sistema di regole comuni e alla necessità di sistemi fiscali omogenei tra i diversi Paesi, in primis in Europa, la cui attuazione è al di là da venire. Sappiamo che gli stra-conosciuti giganti del web (notizia recente: Uber riprende il servizio anche in Italia), si basano sul modello di ***business a piattaforma****, ossia sull'implementazione dei modelli* ***economici dei mercati multilaterali*** *basati sull'effetto rete e resi oggi più velocemente scalabili e globali dal digitale.*

Collegato al ruolo sempre più da "oligopolio" di queste aziende, è il tema della nascente e crescente ***nuova economia dei dati****: il nuovo petrolio e carburante del futuro delle economie. Lo posizione del potere e dei profitti, si sposterà sempre più verso chi saprà estrarre valore dai dati, attraverso tecnologie avanzate degli Analytics e in prospettiva di tutto l'armamentario tecnologico messo a disposizione da Cognitive Computing e Intelligenza Artificiale.*

segue alla pagina successiva >>

GIUGNO 2017

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Massimo MESSINA
Head of Global ICT, Unicredit

UniCredit

SOMMARIO

IN PRIMO PIANO
Sviluppo degli Ecosistemi e Piano Strategico Triennale
Roberto Masiero

NUMERI E MERCATI
Nuove console e realtà virtuale per il rilancio del mercato del gaming
Camilla Bellini

LA TRASFORMAZIONE DIGITALE
Open vs Closed Innovation
Francesco Manca

Un Innovativo Strumento per l'Ottimizzazione del ciclo di Produzione
Vincenzo D'Appollonio

BANCHE E FINTECH
Blockchain e Innovazione: non è solo tecnologia, bellezza!
Ezio Viola

CYBERSEC E DINTORNI
Domande e risposte su #WannaCry, il ransomware 2.0
Elena Vaciago

VOCI DAL MERCATO
La nuova direttiva UE sulla protezione del know-how riservato e dei segreti commerciali
Avv. Pierodavide Leardi

L'annuncio recente della disponibilità dei servizi di pagamento di Apple-Pay anche in Italia è l'ultima dimostrazione di come, chi possiede i dati può entrare facilmente in mercati complementari. In questo scenario le autorità regolatorie, non ultima la Consob, hanno alzato la loro voce, sbagliando bersaglio, sul possibile Far West che si potrebbe scatenare se non si regola l'innovazione tecnologica che riguarda il mondo Fintech.

Le economie di scala aumentano significativamente il valore delle aziende piattaforma globali. Questo è dovuto al potere economico insito nello sfruttamento dell'"effetto rete" che aumenta al crescere del numero dei partecipanti. Ciò si combina anche con l'"effetto Big Data", cioè con l'avere sempre più dati a disposizione, che agisce a sua volta sui partecipanti generando ancora più dati. Non per nulla, i giganti della rete hanno profitti stratosferici (25B$ solo nel primo trimestre 2017). In un sistema competitivo ora sbilanciato verso lo strapotere dei giganti del web, non si deve però fermare l'innovazione dei piccoli, ma occorre prevedere le regole… Il dominio crescente di queste aziende però non può essere limitato con l'approccio che le autorità regolatorie hanno adottato in passato, ad esempio con la minaccia di break-up, perché non funzionerebbe: non siamo ai tempi del petrolio… e in una economia di dati le catene del valore sono più "fungibili e liquide" e facilmente rigenerabili.

In questo contesto di grandi temi, e sempre richiamando fatti recenti, risultano un po' "patetici" sia la recente dichiarazione di pentimento del co-fondatore di Twitter, che ha lamentato che"Internet si è rotta", accorgendosi che il mondo non è diventato automaticamente migliore attraverso la libertà di utilizzo della rete, sia le iniziative di Facebook per bloccare il dilagare di fake news e minacce sul web.

Questi fatti recenti, ci inducono a una considerazione: ***se non sappiamo prevedere tutti gli eventi che ci aspettano e che possono arrivare dall'evoluzione della tecnologia, abbiamo forse più ampio margine per prevederne le conseguenze, se questi si realizzeranno. Alla base però della nostra comprensione deve stare la conoscenza dell'uomo e dell'animo umano****. Infatti se guardiamo questo video assolutamente straordinario disponibile su http://www.ina.fr/video/I10257139 e girato nel 1947, troviamo molte innovazioni arrivate 60-70 anni dopo: internet mobile, schermi ovunque – soprattutto a uso di intrattenimento e informazione – televisione in 3D… In questo filmato colpisce non tanto la tecnologia mostrata, quanto I comportamenti che essa provoca: una volta accettata una possibile previsione, se ne possono immaginare le conseguenze. Oggi questa capacità di pensare il futuro della tecnologia, è possibile ma le sue conseguenze potrebbero essere negative in quanto potremmo accorgerci di essere incapaci di gestirla.*

QUESTO MESE ABBIAMO FATTO COLAZIONE CON..

BLOCKCHAIN, ARTIFICIAL INTELLIGENCE E BOT: LE NUOVE BUZZWORD DEL MONDO IT

Intervista a **Massimo Messina**, HEAD OF GLOBAL ICT di UNICREDIT

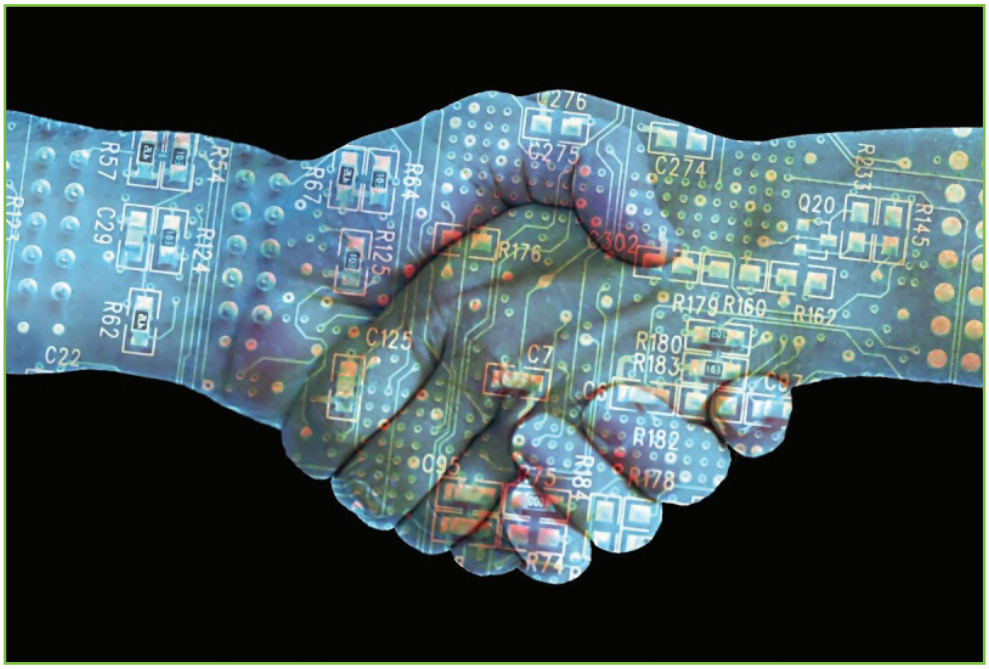
Questo mese abbiamo avuto la possibilità di approfondire con ***MASSIMO MESSINA*** *i nuovi trend e le nuove evoluzioni tecnologiche che potrebbero trasformare le aziende e i settori (non solo quello finanziario) nei prossimi anni:* ***Blockchain, Artificial Intelligence e Bot*** *sono infatti le nuove buzzword del mondo IT che – proprio secondo Messina – sono ormai dei percorsi tracciati nel panorama tecnologico mondiale, su cui occorre però ora definire servizi a valore aggiunto e nuovi modelli di business.*

Partendo proprio da uno dei temi caldi oggi per il settore Finance, quello della ***Blockchain***, questa è indubbiamente una tecnologia che sta attraversando un periodo di forte hype, ma non per questo deve essere ritenuta meno interessante: consente infatti di creare nuove situazioni di disintermediazione degli scambi e delle relazioni tra attori diversi, introducendo elementi di novità in termini di certificazione e scambio. D'altra parte, uno dei grandi potenziali della blockchain resta legato alla possibilità di utilizzare questa tecnologia combinandola con altre, le cryptocurrencies, gli smart contract, l'IoT, ecc. È infatti dall'utilizzo combinato di queste nuove tecnologie che nasceranno nei prossimi anni dei veri servizi a valore aggiunto, nei settori più differenti. E, probabilmente, la nascita di questi nuovi servizi sarà il fattore vero che porterà ad un'accelerazione nella diffusione della tecnologia blockchain.

A questo riguardo, la recente similitudine proposta dall'HBR, che paragona la blockchain al ruolo infrastrutturale e fondativo del TCP/ IP in relazione ad Internet, è sicuramente un punto di vista con cui concordare, benché forse sia più l'HTML il termine di paragone più esatto. L'HTML ha infatti democratizzato una tecnologia al tempo accessibile solo ad un numero ristretto di persone, aprendo Internet all'uso e alla combinazione di un numero diverso di tecnologie: questo è lo stesso ruolo infrastrutturale che la blockchain rischia di avere nei prossimi anni nei confronti di tutto l'IT.

Un altro tema che indubbiamente sarà iper-esposto ad analisi e dibattiti nel 2017 è quello relativo all'artificial intelligence. Questo è un termine che d'altra parte suscita ricordi legati soprattutto all'automazione e alla robotica, al Giappone degli anni '90, "limitando", o comunque specializzando, un insieme di tecnologie e di ambiti applicativi più ampi. A questo riguardo, sarebbe forse più consono adottare il temine ***Augmented Intelligence***, legando i nuovi strumenti più avanzati di analisi dei dati a quel trend iniziato diversi anni fa con la comparsa di soluzioni di business analytics, che posero per la prima volta un accento forte sul tema della datification e dell'uso dei dati in azienda per supportare i processi di decision- making. Affrontando questi temi, l'accento dovrebbe essere posto infatti non tanto sul tema della sostituzione dell'uomo nello svolgimento di task specifiche, ma piuttosto sul tema dell'affiancamento della componente "artificiale" all'attività umana: l'augmented intelligence può amplificare la capacità intellettiva dell'uomo e supportare i suoi processi decisionali, riducendo i tempi di acquisizione, processazione e analisi dei dati e delle informazioni. Questo discorso ha cominciato a diffondersi proprio da quelle soluzioni di analytics di cui si accennava poco sopra, passando poi per il machine learning e il deep learning, arrivando infine a soluzioni più evolute e complesse come quelle relative al cognitive computing. Ad oggi molte applicazioni di queste tecnologie e di questi strumenti le troviamo già nei processi aziendali e negli oggetti di uso comune, benché a questo riguardo sarà fondamentale, per la loro evoluzione, comprendere come evolveranno le policy relative alla privacy e all'uso dei dati raccolti da questi strumenti.

Infine, un altro tema di cui si sentirà discutere molto nel corso del 2017 è quello dei bot, considerati da molti le nuove app, ovvero i nuovi strumenti attraverso cui potremmo fruire dei servizi ora disponibili via applicazioni mobili. Partendo dal presupposto che quanto affermava Mark Zuckerberg alla scorsa edizione della F8 Developer Conference sia vero, ovvero che nessuno vuole installare una nuova app per ogni servizio, l'introduzione di nuovi strumenti che, partendo dal linguaggio naturale, possano semplificare la fruizione dei servizi oggi disponibili su smartphone e tablet è un evoluzione indiscutibile. Resta d'altra parte la necessità, prima di vedere effettivamente diffondersi i bot, di definire nuovi modelli di business e nuovi ecosistemi in grado di supportare la loro adozione. Ad oggi, i marketplace delle applicazioni sono infatti una sorta di meccanismo di certificazione e di garanzia delle applicazioni stesse, di test della sicurezza e della qualità di quanto reso disponibile dagli sviluppatori: non esiste d'altra parte ancora nulla di paragonabile a questo ecosistema per i bot e, finché non cominceranno ad emergere in modo strutturato modelli di business paragonabili a quelli delle app, sarà difficile valutare appieno il potenziale e il ruolo di questa tecnologia.



SVILUPPO DEGLI ECOSISTEMI E PIANO STRATEGICO TRIENNALE

Di **Roberto Masiero**, President, The Innovation Group

Questo Piano ha una duplice valenza. Una prima valenza è interna alla PA, che il Piano mira a modernizzare radicalmente, superando i silos tra le varie Amministrazioni, integrando i dati e rendendoli accessibili attraverso l'approccio "API first", mirando ad assicurare ai cittadini un vantaggio in termini di semplicità di accesso e miglioramento dei servizi digitali esistenti.

La seconda valenza è quella che Alessandro Longo chiama "**l'effetto di leva abilitante sulle aziende private**"[1]: e cioè l'effetto volano che il miglioramento di efficienza della Pubblica Amministrazione dovrebbe generare, favorendo la crescita digitale dell'economia del Paese.

Ora, tutti noi facciamo il tifo per l'Agid e per il Team per la Trasformazione Digitale; ma il tifo – come recenti avvenimenti calcistici dimostrano – da solo non basta. Vediamo quindi come queste due valenze si correlano nel piano, quali sono i principali elementi di criticità e come si possono superare.

Il Piano Strategico Triennale è un documento enciclopedico, che contiene gli obiettivi generali, quelli di dettaglio, chi deve fare che cosa e entro quando. Ora, buttare il cuore oltre l'ostacolo va bene, ma "cum juicio": ad esempio, se gli obiettivi sono tanti, in tempi così ristretti, se le competenze sono così scarse, se i comuni sono alla canna del gas e non possono spendere né per integrare i moduli standard con i loro patchwork di applicazioni legacy (è il motivo per cui sono così diffidenti rispetto all'ANPR), né –sia mai detto – per assumere, forse sarebbe il caso di definire alcune priorità fattibili in tempi ragionevoli e chiarire le risorse con cui finanziare la migrazione, specialmente dei piccoli e medi comuni.

Come rileva l'ANCI, "**deve essere chiaro che lo Stato non può prima indicarci di seguire la strada della centralizzazione dei sistemi e poi non permetterci di adeguare i nostri software per agganciarci ad essi.**" [2]

Altri osservatori hanno già puntualizzato le problematiche relative alla governabilità,alla mancanza di modelli attuativi[3], all'esigenza di forme strutturate di monitoraggio[4][5]. Sono convinto d'altronde che queste criticità siano già all'attenzione del Commissario Straordinario e dell'Agid.

Mi interessa invece soffermarmi maggiormente sull'"**effetto (del Piano come) leva abilitante sulle aziende private**".

E l'anello di congiunzione tra le due valenze sta evidentemente nella parte sugli Ecosistemi, ovvero quei settori in cui maggiormente si può vedere l'effetto propulsivo della crescita digitale alimentata dalla collaborazione pubblico-privato. E qui si evidenzia la suggestione "fuggettiana", che peraltro pervade l'intero piano, e che Alfonso Fuggetta giustamente rivendica: "**Livello strategico**: il modello (del Piano) è basato sul principio della coopetition e su ecosistemi nei quali si distingue tra fornitori di sistemi e servizi di backend ("aperti" tramite API) e sviluppatori di applicazioni e siti web (sistemi di frontend).

Il pubblico presidia principalmente il backend, aprendo ai privati il mercato dei frontend.[6]" Suggestione che tuttavia non viene declinata compiutamente nel capitolo del Piano dedicato agli ecosistemi.

Teniamo presente infatti che la percentuale di spesa della PAC + Difesa è pari al 7,9% del mercato, mentre PAL + Sanità (l'80% della spesa regionale) vale il 7,3%. Se la spesa pubblica in ICT rappresenta solo il 15% del mercato e non certamente la sua parte più dinamica – potrà rapprentare al massimo un "lubrificante" per la crescita digitale del Paese, ma la componente fondamentale della crescita dovrebbe esser data proprio da quei servizi che l'iniziativa privata dovrebbe essere stimolata a sviluppare.

Di questo invece nel Piano non si parla: si elencano diffusamente una pletora di Ministeri e di Pubbliche Amministrazioni che dovrebbero sviluppare servizi per i 12 Ecosistemi proposti, ma in nessun modo si affronta il problema di come incentivare i privati a sviluppare un ruolo trainante nello sviluppo di questi nuovi servizi. Una carenza a cui probabilmente varrebbe la pena di riflettere.

1)- Alessandro Longo, "Dal piano triennale al Paese digitale: il grande salto" http://bit.ly/2s8pYaL

2)- Luca Della Bitta, "Sostenere i Comuni in difficoltà sul Piano triennale" http://bit.ly/2rluzzY

3)- Gianluigi Cogo, "Ecco i due grandi difetti del piano triennale Agid" http://bit.ly/2rVzK0f

4)- Paolo Coppola, "Senza banca dati nazionale delle performance nulla cambierà davvero" http://bit.ly/2s8COG6

5)- Alessandra Poggiani, "Tre interventi urgenti per completare il piano triennale Ict" http://bit.ly/2s891NA

6)- Alfonso Fuggetta,"Per il modello a ecosistemi servono standard e vision" http://bit.ly/2qS59AC

NUOVE CONSOLE E REALTÀ VIRTUALE PER IL RILANCIO DEL MERCATO DEL GAMING

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

È indubbio che l'avvento dei dispositivi mobili e la diffusione del gaming online, ed in particolare delle app, abbia fatto tremare il mercato tradizionale dei videogiochi: qualche anno fa gli analisti prevedevano infatti una radicale trasformazione del mercato, in cui i player tradizionali (tra cui Nintendo, Sony e Microsoft) avrebbero rischiato di soccombere se non avessero modificato la loro strategia.

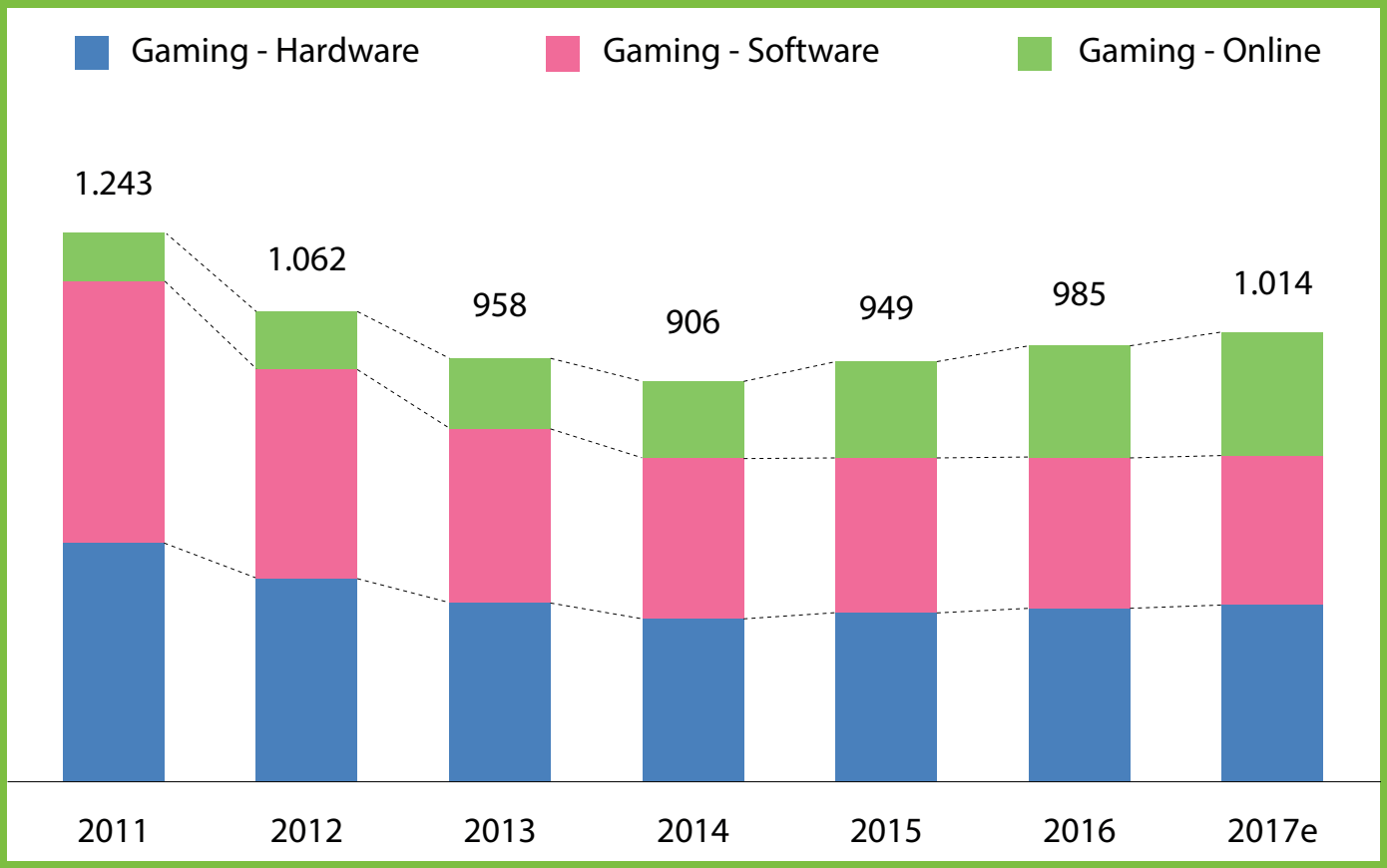
Ad oggi sembra però che i grandi player del videogioco stiano vincendo questa sfida, o quanto meno cavalcando, mostrando di essere proattivi e innovativi nel posizionamento e nella valorizzazione dei nuovi strumenti digitali. Si pensi ad esempio alla crescente attenzione per i dispositivi di realtà virtuale, o all'utilizzo delle app a fini promozionali dei canali più tradizionali: da un lato infatti il 2017 è visto come l'anno in cui la proposta commerciale dei visori e dei giochi per la realtà virtuale si consoliderà (si pensi ad esempio al recente successo riscontrato da Playstation VR o all'annuncio di Microsoft di voler definire uno standard per la diffusione dei visori VR per PC); dall'altro, la recente strategia di Nintendo di lanciare un'app per rilanciare il brand dei Pokemon anche nei canali più tradizionali, quelli del gadgeting e delle console tradizionali (ad esempio, i nuovi titoli sui Pokemon lanciati per l console 3DS).

Inoltre, il 2017 è stato e sarà un anno di annunci e di innovazioni, tecnologiche e di approccio al mercato. Si pensi al recente lancio da parte di Nintendo di Nintendo Switch, la nuova console che integra console domestica e portable per unificare e rendere continuativa l'esperienza di gioco dentro e fuori le mura domestiche; o all'annuncio da parte di Microsoft del progetto Scorpio, che verrà lanciato sul mercato a fine 2017 e che si propone come la più potente console di gioco mai progettata.

Questi annunci e trend hanno un influenza anche sul mercato italiano, che negli ultimi anni ha registrato una ripresa e che per il 2017 è previsto ancora in crescita. In particolare, il mercato del gaming in Italia, che comprende sia l'hardware sia il software e la spesa per app e giochi online, è previsto crescere nel 2017 con un tasso del 3% (contro il 3,8% dell'anno precedente), per un valore complessivo pari a poco più di un miliardo di Euro. A crescere è soprattutto il mercato dell'Online Gaming, benché anche il mercato dell'hardware (console home, console portable e accessori) segua un trend positivo.

IL MERCATO DEL GAMING IN ITALIA (MLN€, 2011- 2017E)

Fonte: TIG, 2017



OPEN VS CLOSED INNOVATION

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

Come noto con il termine Open Innovation si intende l'unione di idee interne ed esterne all'azienda, nonché dei percorsi interni ed esterni al mercato per promuovere lo sviluppo di nuove tecnologie, con l'effetto di ridurre il time to market di una innovazione. In un mercato sempre più dinamico e veloce, rifiutare o posticipare strategie digitali per la propria offerta può rivelarsi uno svantaggio significativo per le aziende; l'Open Innovation, affrontando il tema dell'innovazione in maniera più collettiva istituendo partnership e collaborazioni interaziendali, può quindi essere una soluzione al digital divide che si sta creando in un mercato fortemente tecnologico, offrendo ROI meno aleatori e finanziamenti meno ingenti, ma producendo gli stessi effetti di una digital transformation con conseguenze meno disruptive sull'organizzazione aziendale.

In concreto, i principali modelli di Open Innovation variano a seconda del contesto di riferimento e vanno da partnership aziendali con centri di ricerca, incubatori o altre aziende, a sponsorizzazioni di competizioni tra start-up ad hackaton o acquisizioni.

Ma quali sono le principali variabili che fanno propendere per un modello o per un altro? Cosa è che determina i vari gradi di apertura di una relazione di Open Innovation?

Le principali esperienze di mercato offrono le due determinanti che definiscono il grado di apertura di una azienda: il numero di partner con cui la azienda collabora e le fasi di innovazione in cui l'azienda si apre alla collaborazione. Il grado di apertura ha portato la letteratura a delineare quattro modelli:

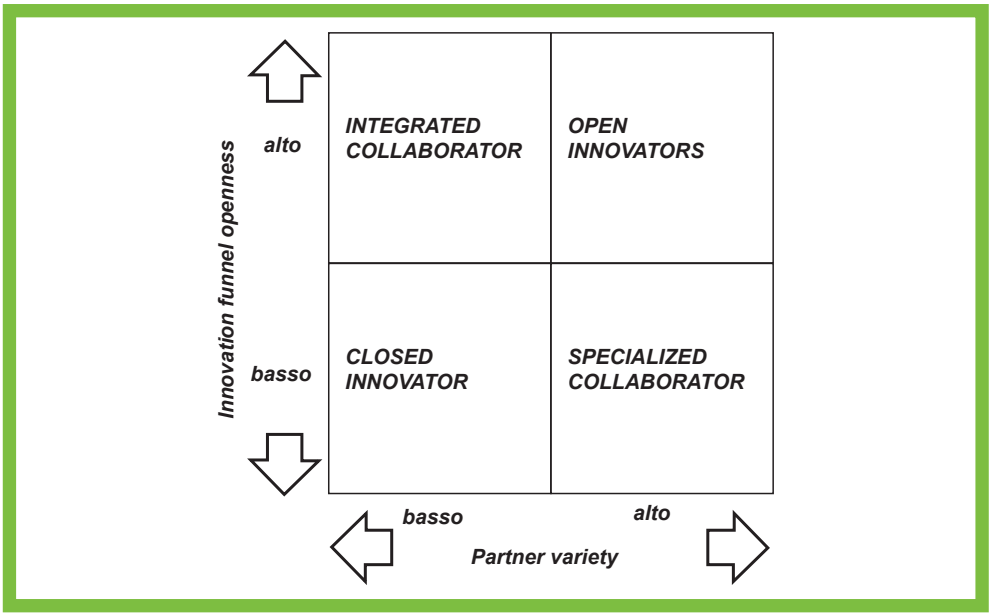
- Il modello degli innovatori chiusi è quello di coloro i quali costruiscono collaborazioni sporadiche con terzi a fini innovativi solo in fasi specifiche e circoscritte del processo di innovazione.
- La collaborazione specializzata riguarda invece le aziende che lavorano con molti partner ma circoscrivono l'oggetto delle collaborazioni ad un solo ambito del processo innovativo, come ad esempio alla fase di ideazione del prodotto.
- La collaborazione integrata corrisponde ai casi in cui la collaborazione è diffusa lungo tutto l'innovation funnel, ma le partnership collaborative riguardano solo poche selezionate imprese.
- Il modello degli open innovators è quello invece di coloro che si aprono a partnership collaborative con una pluralità di stakeolder lungo tutto l'innovation funnel.

L'innovazione più aperta necessita di una diversa mentalità e cultura aziendale rispetto all'innovazione tradizionale o chiusa: l'azienda che utilizza le innovazioni altrui per una crescita personale mette a disposizione le proprie per incentivare una crescita collettiva e facilitare una collaborazione fruttifera futura. Aprire il processo innovativo di impresa può essere quindi un'opportunità di stare al passo con i tempi, rifiutando la mentalità conservativa della maggior parte delle aziende che intende condurre l'innovazione a porte chiuse, con la prerogativa di proteggere la proprietà intellettuale e superare i confini di impresa, creando un modello di conoscenza ed innovazione disciplinato e replicabile. Open Innovation può quindi essere intesa come la sharing economy degli asset intangibili di una azienda; rifiutare questa proposta di modello innovativo è per certi versi rinunciare ad una forma di progresso tecnologico che crea valore.

Un esempio che testimonia l'efficacia di queste strategie è P&G che, riconoscendo nell'innovazione il principale driver di crescita e progresso dell'azienda, ha creato il programma connect+develop che crea una rete innovativa tra clienti, fornitori, personale interno ed agenti di innovazione esterni istituendo uno scenario di Open Innovation. Gli strumenti proposti da P&G per favorire questa connessione tra i vari nodi della rete sono incorporati profondamente nella struttura, supportati da tecnologie ICT come piattaforme web e altri software che coordinano ed aiutano il lavoro dei ricercatori e degli imprenditori tecnologici. Open Innovation è quindi riconoscere, anche da parte di una grande impresa leader in più settori, che innovare insieme è più efficace e produttivo che innovare da soli.

Sebbene i modelli di Open Innovation presentano casi virtuosi come quello di P&G, la letteratura scientifica sottolinea come nessun modello di quelli descritti sopra sia univocamente migliore degli altri e che quindi la conclusione "the more opensess, the better" può essere fuorviante se non contestualizzata. Sistemi aperti richiedono infatti anche costi oltre che vantaggi come alte capacità manageriali o situazioni in cui ci sono rapporti impari di collaborazione con più follower che effettive partecipazioni. In contesti più piccoli, circoscritti ad un unico mercato, o non inseriti in un ecosistema florido, come possono essere la maggior parte delle realtà produttive italiane, alcuni ricercatori (Lazzarotti e Manzini, 2019) suggeriscono infatti livelli intermedi di apertura (collaborazioni specializzate o integrate), come giusto compromesso tra costi e benefici.

DIVERSI GRADI DI APERTURA DELL'IMPRESA Fonte: Lazzarotti, Manzini 2009



LA TRASFORMAZIONE DIGITALE

UN INNOVATIVO STRUMENTO PER L'OTTIMIZZAZIONE DEL CICLO DI PRODUZIONE

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

Continuiamo a parlare di Industry4.0: la prima fase del nostro intervento consulenziale presso le piccole Aziende Manifatturiere, circa 25 dipendenti, che stiamo seguendo nello sviluppo di Progetti di Automazione Industriale che verranno completati entro il 2017, ha riguardato una attività propedeutica di 'ottimizzazione' del ciclo di produzione: è chiaro che ha poco senso 'automatizzare' un processo scarsamente efficiente. Durante queste attività ci siamo avvalsi, con soddisfazione, di uno strumento che riteniamo particolarmente innovativo per l'ottimizzazione operativa dei processi di produzione: AviX®, fornito dalla società olandese PQ+.

La complessità e la velocità dei processi di produzione moderni aumentano continuamente, l'osservazione "ad occhio nudo" non è spesso sufficiente per riconoscere in modo ottimale tutte le potenzialità di ottimizzazione della produzione: attraverso un'analisi video con AviX® le potenzialità di miglioramento possono essere identificate in modo puntuale e convertite in aumento concreto di efficienza.

AviX® consente un'analisi trasparente e obiettiva attraverso la registrazione del processo su video, e consente di arrivare ad ottimizzare una stazione di lavoro in soli tre passi, e di bilanciare l'intero processo con una sola ulteriore fase di analisi: l'ottimizzazione di una linea di produzione può essere realizzata in pochi giorni di lavoro, anche il ri-bilanciamento di una linea non ottimizzata a causa di variazioni di carico può essere realizzato con un semplice meccanismo di 'drag&drop'.

Lo step 1, 'Video', consiste nel riprendere i processi di produzione a video, una semplice videocamera è più che sufficiente, e trasferire il video sul computer, dove viene elaborato dal Sistema SW AviX®; le sequenze possono essere viste ed analizzate in dettaglio e ripetutamente, insieme con il personale coinvolto; le riprese video non interferiscono con l'attività in linea e l'osservazione può essere limitata a soli due o tre cicli di produzione.

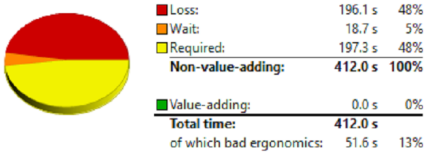
Lo step 2, 'Analisi', consiste nell'analizzare il video quadro dopo quadro, ed operazione dopo operazione; le tipologie di azioni/operazioni evidenziate sono automaticamente riconosciute e catalogate da AviX®, che ne consente la visualizzazione 'colorata' nelle categorie 'a valore aggiunto', 'necessaria', 'di attesa' e 'spreco', con un concetto di 'pull&flow'; azioni non ergonomiche sono sempre indicatrici di sprechi e quindi evidenziate in 'rosso'.

Lo step 3, 'Azioni correttive', consente di definire le azioni di miglioramento/ ottimizzazione da intraprendere, attraverso una discussione con gli esperti AviX®, insieme ai responsabili aziendali dei Cicli di Produzione, ed al personale coinvolto.

I risultati che abbiamo ottenuto sono reali e convincenti: aumento della produttività, in particolare anche nelle procedure di set-up e manutenzione; riduzione dello stock, riduzione dei tempi morti, miglioramento dell'ergonomicità e della qualità del lavoro, ma soprattutto, Personale coinvolto e motivato, attraverso la partecipazione nelle riprese, nella analisi e nello sviluppo congiunto e concordato delle azioni di miglioramento!

Secondo la nostra esperienza, possiamo dunque considerare AviX® un concreto, efficace Strumento per il Miglioramento Continuo delle Attività di Produzione per le PMI.

Step 1: VIDEO



Step 2: ANALISI

Step 3: AZIONI CORRETTIVE

BLOCKCHAIN E INNOVAZIONE: NON È SOLO TECNOLOGIA, BELLEZZA!

Di **Ezio Viola**, Managing Director, The Innovation Group

Non è insolito che le tecnologie innovative emergenti, che sono testate attraverso applicazioni prototipali in ambienti controllati, non si procedano facilmente e in modo semplice in produzione per un utilizzo sul larga scala, dove benefici e problemi sono più realisticamente messi in evidenza, analizzati e capiti. Questo è la fase in cui ci si trova per quanto riguarda le Distributed Ledger Technologies alla base della Blockchain. Ne abbiamo avuto conferma anche in un recente incontro ristretto, svolto nell'ambito del nostro Programma Fintech in preparazione del Banking Summit 2017 di Settembre (http://bit.ly/2pcK7Ie), al quale hanno partecipato esperti tecnologici, banche, startup e centri di ricerca universitari.

Alcune conclusioni dell'incontro, più che sulle potenzialità, anche disruptive, della blockchain, si sono concentrate sulle problematiche chiave che frenano l'adozione più estesa della blockchain. Esse infatti non sono prettamente quelle tecniche e tecnologiche, che esistono tuttora ma che in una prospettiva a breve-medio termine l' evoluzione tecnologica affronterà, ma quelle più articolate che riguardano data privacy , sicurezza e integrità dei dati, governance e regolazione.

Privacy e confidenzialità sono fondamentali per i servizi finanziari ma ciò è quasi in contraddizione con la trasparenza aperta che è un attributo chiave alla base del modello di blockchain puro, mentre le soluzioni di blockchain privata e permissioned stanno incorporando elementi di privacy. Fornire e garantire l'anonimato delle transazioni distribuite attraverso funzioni di encryption di crittografia avanzate è l'approccio seguito anche da molte piattaforme come Ethrereum e Monax. Cominciano a comparire anche soluzioni che permettono ai partecipanti della rete livelli differenziati di privacy, ma che portano inevitabilmente a definire il ruolo di un intermediario e/o regolatore. L'evoluzione ragionevolmente prevedibile ad oggi è un mix di soluzioni con approcci che gestiscano restrizioni all'accesso e la segregazione di dati : la soluzione non sarà solo la tecnologia, ma avranno un ruolo fondamentale anche lo sviluppo di standard e, e il coinvolgimento dei regolatori.

Sicurezza e integrità dei dati nella Blockchain sono ancora messe alla prova da vulnerabilità e minacce e l'utilizzo malevolo è ancora possibile, ma saranno affrontate dalla comunità aperta che sviluppa le tecnologie blockchain.

Ciò che è più rilevante è garantire l'integrità digitale degli asset sottostanti a catena che devono essere accessibili, protetti e validati. Le blockchain permissioned più facilmente possono sviluppare funzionalità di sicurezza e autenticazione, che sono critici per gestire asset digitali su una rete distribuita: quello che hanno fatto Ripple e R3.

L'hype che circonda oggi la blockchain non riguarda la tecnologia ma i potenziali cambiamenti dirompenti alla struttura dei mercati e delle organizzazioni economiche, delegando fiducia e trasparenza direttamente ai nodi della rete e generando potenzialmente grandi efficienze, risparmi di capitale investito , abilitando nuovi paradigmi e modelli economici di condivisione e monete digitali. Per fare ciò è fondamentale definire una governance, delle regole e nuovi requisiti regolatori. Questo è il motivo per cui tutte le banche centrali, inclusa la BCE, sono molto attive in tavoli di lavoro e con laboratori dedicati, anche se tutto ciò è poco noto. La governance di un modello distribuito come è il Distributed Ledger è ancora un fattore poco compreso, anche perché le problematiche di governance, privacy e integrazione si interconnettono. Se il modello di Governance è ad esempio basato su un meccanismo distribuito del consenso, non è definito come debba essere regolato cosi come è tuttora non determinata l'abilità di mantenere ogni singola entità responsabile.

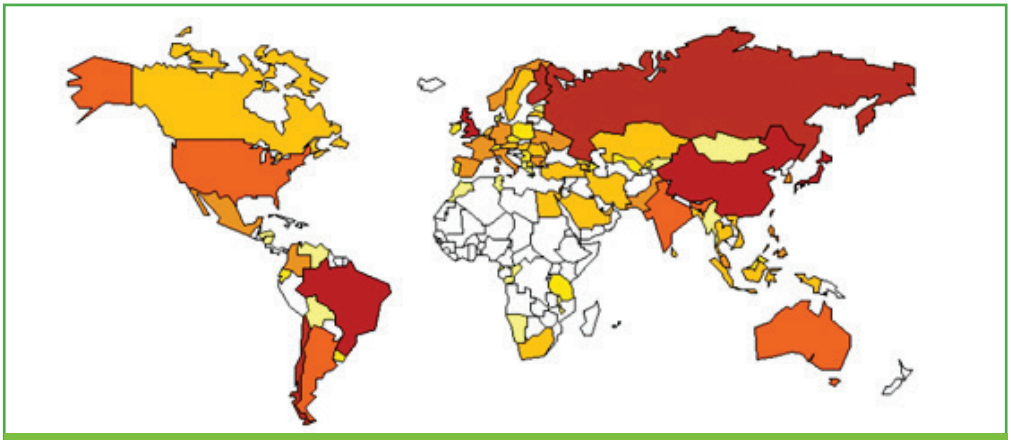
In reti permissioned, definire una governance è più semplice essendo noti i partecipanti e risulta più facile decidere chi può dettare le regole anche se alcuni trade-off e complessità possono emergere con l'aumentare delle persone coinvolte. Ciò tuttavia fa apparire la blockchain qualcosa di non molto diverso da infrastrutture esistenti, come SWIFT. E' quindi inevitabile che qualsiasi capacità di governance incorporate nella tecnologia utilizzata, debba includere valutazioni sugli aspetti regolatori esistenti nella specifica area di interesse, come nel caso dell'industria e dei servizi finanziari. L'interesse dei regolatori sulla blockchain è molto aumentato negli ultimi due anni con la continua crescita dei casi d'uso che l'industria digitale e delle start up sta realizzando. Le problematiche, gli aspetti regolatori e legali forse sono la barriera più complicata per un'adozione più larga da parte delle imprese nel medio termine. Lo sviluppo di standard e il poter indirizzare alcuni dei complessi aspetti legali che la blockchain pone (relativi a proprietà intellettuale, contratti, custodia etc.) farebbe fare un significativo passo avanti nel creare le condizioni per accelerare l'adozione della blockchain anche a livello aziendale e settoriale.

DOMANDE E RISPOSTE SU #WANNACRY, IL RANSOMWARE 2.0

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

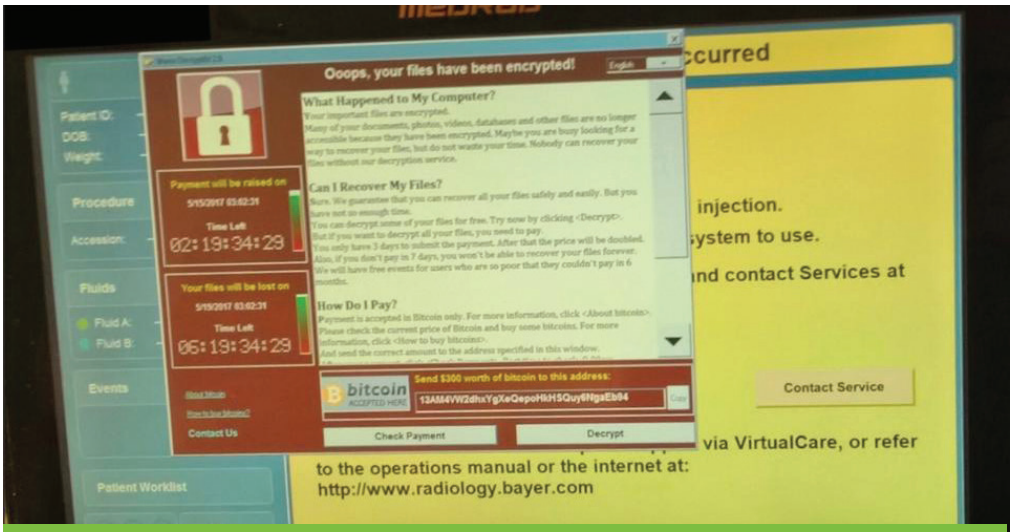
Tra il 12 e il 15 maggio scorsi, quasi ogni parte del mondo (a parte l'Africa) è stata colpita dalla diffusione epidemica di un ransomware molto potente, WannaCry (letteralmente significa "voglio piangere"), o WannaCrypt, che in tutto ha sabotato 300.000 computer PC e server in oltre 100.000 organizzazioni. Gli effetti in alcuni casi sono stati gravi. In Inghilterra, diversi enti ospedalieri dell'NHS (National Health Service), andati in tilt per l'impossibilità di accedere ai computer anche nel Pronto Soccorso, hanno dovuto dirottare i pazienti in accettazione verso altre strutture. In Germania sono saltati i display digitali delle stazioni dei treni della Deutsche Bahn: al posto degli orari dei treni è comparsa la maschera del ransomware.

Altri ad aver sperimentato gli effetti del malware WannaCry sono stati: l'operatore Telefonica in Spagna (che ha dichiarato che solo alcuni PC delle reti interne dei suoi uffici erano stati colpiti), in Italia qualche problema alle reti periferiche del ministero della Giustizia (tribunali soprattutto) e alcuni computer dell'Università Bicocca a Milano, fabbriche Renault in Francia e Slovenia e Nissan in India, il 25% dei PC della polizia indiana, Hitachi in Giappone, FedEx e alcuni ospedali negli USA (dove l'immagine del ransomware ha fatto la sua apparizione su alcuni apparati medici di radiologia di Bayer, società che ha poi dichiarato che fornirà una patch per i suoi sistemi Windows-based "presto" …). Secondo alcuni provider di soluzioni di cybersecurity, i Paesi che hanno però subito maggiormente l'attacco sono stati: Russia (dove i target sono stati numerosi, dagli operatori di telefonia, a banche, sistema ospedaliero, treni e polizia), Cina (si ha notizia di 100.000 computer colpiti nelle università, servizi di pagamento online e a una stazione di polizia), Ucraina, Taiwan, India, Brasile, Tailandia, Filippine, Armenia e Pakistan. Di sicuro si è trattato di un fenomeno globale.



HEATMAP DELLA DIFFUSIONE DI WANNACRY IL 14 MAGGIO Fonte: Symantec

IL RANSOMWARE WANNACRY SUI DISPLAY DIGITALI DELLE STAZIONI DEI TREI DELLA DEUTSCHE BAHN



IL RANSOMWARE WANNACRY SU UN SISTEMA DI RADIOLOGIA BAYER

#1 – Da dove nasce il ransomware WannaCry

Il malware sfrutta una vulnerabilità del protocollo Server Message Block (SMB) dei sistemi operativi Windows, un baco che sarebbe stato risolto se si fosse provveduto ad aggiornare Windows con un security update dello scorso marzo (la patch MS17-010). WannaCry colpisce il protocollo SMB utilizzando l'exploit dell'Nsa "EternalBlue", diventato di dominio pubblico quando lo scorso aprile una cache di hacking tool sviluppati dall'NSA sono stati esposti con

il noto leak del collettivo hacker Shadow Brokers. Questi exploit erano diretti soprattutto agli ambienti Windows (tra cui Windows XP, Windows Server 2003, Windows 7 e 8), ed era stato predetto dagli esperti di sicurezza che l'evento avrebbe potuto creare seri problemi di sicurezza, perché si tratta di sistemi operativi che continuano ad essere utilizzati pur non essendo più supportati da Microsoft con patches di sicurezza.

#2 – Tecnicamente parlando, come è avvenuto l'attacco?

Una volta entrato in una rete, il malware infettava una prima macchina, crittografando i dati e chiedendo il riscatto (inizialmente di 300 bitcoin, che diventano poi 600), e poi come un worm si propagava automaticamente ad altri computer collegati alla rete, attraverso la porta 445. Fin dall'inizio non è stato necessario alcun intervento umano, a differenza della maggior parte degli altri ransomware che arrivano tramite posta elettronica e devono quindi essere "aperti" dagli utenti.

WannaCry conteneva però anche un meccanismo "kill switch", ossia il nome di un dominio inesistente a cui il software continuava a puntare, e non trovandolo si propagava ulteriormente attraverso le reti. Un tecnico inglese, che appare su Twitter con l'account @MalwareTech, preoccupato per l'escalation dell'attacco, analizzando il codice ha scoperto velocemente un nome di dominio inesistente (http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com), lo ha registrato e in questo modo ha arrestato il processo di diffusione. La storia di come l'intervento ha fermato il malware è online. Un secondo kill switch è stato anche identificato da un ricercatore di sicurezza francese, Matthieu Suiche, che ha pubblicato i dettagli della scoperta sul suo blog. La presenza del kill switch nel codice di WannaCry, un blocco che di fatto lo "autodistrugge", potrebbe essere spiegata in 2 modi: l'autore del software malevolo lo ha previsto fin dall'inizio per poter fermare la diffusione del malware, oppure è stato previsto questo meccanismo per permettere al worm di capire se è finito dentro una "sandbox" (un ambiente protetto, utilizzato come tecnica di difesa per isolare il malware e studiarlo) e quindi bloccarsi da solo. Va detto però che il kill switch è stato osservato solo su alcune varianti del malware. Infine, è stata anche scoperta una Backdoor che WannaCry ha lasciato nei computer colpiti, una porta che potrebbe essere utilizzata in futuro dagli attaccanti per sottrarre ulteriori dati.

#3 – Istruzioni per mettersi al sicuro da WannaCry

E' chiaro, visto il funzionamento del malware, che la principale azione di difesa sta nel patchare tutti i sistemi. Oltre a questa "misura minima obbligatoria", ne vanno considerate altre comunque utili (considerando che alle reti si possono collegare chiavette USB, PC di consulenti esterni e quant'altro). Polizia Postale e CERT PA hanno immediatamente pubblicato istruzioni per prevenire i danni da ransomware WannaCry. Le misure indicate dalla Polizia Postale lato client/server sono:

- eseguire l'aggiornamento della protezione per sistemi Microsoft Windows pubblicato con bollettino di sicurezza MS17-010 del 14 Marzo 2017
- aggiornare il software antivirus
- disabilitare ove possibile e ritenuto opportuno i servizi: Server Message Block(SMB) e Remote Desktop Protocol (RDP)
- il ransomware si propaga anche tramite phishing pertanto non aprire link/allegati provenienti da email sospette
- il ransomware attacca sia share di rete che backup su cloud quindi per chi non l'avesse ancora fatto aggiornare la copia del backup e tenere i dati sensibili isolati.

Lato sicurezza perimetrale:

- eseguire gli aggiornamenti di sicurezza degli apparati di rete preposti al rilevamento delle intrusioni (IPS/IDS)
- ove possibile e ritenuto opportuno bloccare tutto il traffico in entrata su protocolli: Server Message Block (SMB) e Remote Desktop Protocol (RDP).

CERT PA ha rilasciato invece altre istruzioni anche per il riavvio di computer spenti.

#4 – Chi sono stati gli attaccanti, con quali motivazioni?

Attualmente sull'origine dell'attacco sono state fatte solo delle ipotesi: il ricercatore di sicurezza Eric Chien di Symantec ha trovato somiglianze tra il codice di WanaCrypt0r e alcuni virus del Lazarus Group, cyber criminali della Corea del Nord accusati in passato di cyber spionaggio contro la Corea del Sud, del Sony hack e del furto di 81 milioni di dollari alla Banca del Bangladesh.

Europol avrebbe invece individuato alcuni IP russi da cui potrebbe essere partito l'attacco. Al momento l'ipotesi più accreditata è che diversi gruppi di hacker si siano attivati e abbiano sfruttato la falla EternalBlue, insieme o in momenti diversi: secondo quanto riportato da Pierluigi Paganini, diversi ricercatori avrebbero individuato altro malware (e anche una botnet, Adylkuzz) che sfruttavano l'exploit EternalBlue settimane prima di WannaCry.

La motivazione più ovvia potrebbe essere quella economica, visto che WannaCry chiedeva circa 300 dollari in bitcoin per decriptare i file. Va detto poi che la difficoltà tecnica di costruzione di un malware di questo tipo è in continua discesa, con la disponibilità di strumenti (Philadelphia) molto semplificati per chi vuole cimentarsi.

#5 – La minaccia è passata o l'allerta continua ad essere alta?

Purtroppo, si stanno osservando già nuove varianti del ransomware. Sono stati pubblicati online da WikiLeaks i documenti che accertano l'esistenza di "Athena", un malware progettato dalla Cia insieme a Siege Technologies, si legge sul sito, che è in grado di "rubare i dati" all'interno dei Pc che montano il nuovo sistema operativo di Microsoft, Windows 10.

In più, Shadow Brokers ha annunciato il 16 maggio, subito dopo la diffusione del malware, che saranno rilasciati da inizio giugno nuovi zero-day ed exploit rivolti a varie piattaforme sia desktop sia mobile.

A dirla tutta, gli hacker hanno annunciato la costituzione di un Club, con la possibilità aperta solo a membri paganti di accedervi e quindi ottenere gli exploit.

In teoria chiunque potrebbe parteciparvi: il cyber crime, gli hacker state-sponsored, tecnici di società di sicurezza, investigatori e forze dell'ordine …

Infine, il CERT Croato avrebbe già individuato un nuovo worm che combina EternalBlue e altri 4 exploit sviluppati dalla NSA, "EternalRocks", potenzialmente ancora più pericoloso.

#6 – Cosa ci insegna WannaCry, la nuova generazione di ransomware

L'attacco è stato grave, ma è stato davvero un attacco, o piuttosto un evento dimostrativo? Alla fine i computer veramente colpiti non sono stati tantissimi, i bitcoin raccolti dagli hacker pochi (qualche decina di migliaia di dollari secondo chi ha controllato i conti in bitcoin su cui avrebbero dovuto girare i riscatti).

Le vulnerabilità possono oggi essere un segreto? domanda retorica.

Quanto successo ci insegna le "armi cibernetiche", sviluppate da un'agenzia di sicurezza americana, poi sottratte e diventate di dominio pubblico, con estrema velocità sono oggi in mano a chiunque: un esempio di come un segreto in ambito informatico possa facilmente diventare un "cattivo segreto", e non rimanga neanche segreto a lungo.

Continua a crescere la facilità con cui è possibile produrre un ransomware di qualità e con una User Interface avanzata (Wannacry dice passo passo agli utenti cosa devono fare per ripristinare computer e recuperare i dati! C'è perfino l'Help Desk per essere aiutati nell'impresa).

Le strutture pubbliche e private dedite a threat intelligence e information sharing dovrebbero migliorare la loro capacità di risposta: la vulnerabilità era nota, la patch disponibile da marzo, qualcuno si sarebbe dovuto attivare prima.

LA NUOVA DIRETTIVA UE SULLA PROTEZIONE DEL KNOW-HOW RISERVATO E DEI SEGRETI COMMERCIALI

Avv. Pierodavide Leardi

L'8 giugno 2016 è stata approvata la **direttiva UE 2016/943 relativa alla protezione del know-how e dei segreti industriali**. Finalmente, dopo anni di discussioni, il Parlamento e il Consiglio dell'UE hanno adottato un testo legislativo pensato per tutelare uno dei più importanti asset delle aziende impegnate ad innovare costantemente i loro prodotti e i loro processi industriali, ossia il loro **know-how**.

Lo scopo pratico della direttiva è duplice. Da un lato, si vogliono tutelare gli investimenti nell'acquisizione, nello sviluppo e nell'applicazione di know-how e **informazioni aziendali segrete**; dall'altro lato, la direttiva mira a facilitare gli **scambi di queste informazioni tra aziende**, per consentire una più facile collaborazione tra di esse a livello comunitario.

Questa direttiva delinea quindi in modo uniforme, per tutta l'UE, i requisiti di protezione e i limiti della tutela dei segreti commerciali.

Agli Stati membri è lasciata in ogni caso facoltà di prevedere una protezione più ampia per le stesse informazioni. Sarà quindi interessante vedere come la direttiva verrà recepita in Italia dato che il nostro paese garantisce una tutela particolarmente forte per questo asset aziendale.

Per raggiungere tali scopi, la direttiva si è preoccupata innanzitutto di dare una **definizione omogenea di segreto commerciale** tale da includere tutte le informazioni aziendali segrete che abbiano tre caratteristiche fondamentali: i) siano segrete; ii) abbiano valore commerciale in quanto segrete; iii) siano sottoposte a ragionevoli **misure di segretezza** da parte del loro detentore.

In questa definizione la direttiva non si discosta in modo significativo da quanto era già stato definito a livello internazionale con l'Accordo TRIPs e dalla definizione di segreti commerciali data dal nostro Codice della proprietà industriale ed intellettuale.

Tuttavia, la direttiva si preoccupa di escludere dalla protezione le informazioni c.d. trascurabili, le informazioni generalmente note o facilmente accessibili e le competenze acquisite dai dipendenti nel normale svolgimento del loro lavoro e – su un altro versante – si preoccupa di definire i casi di acquisizione, utilizzo e divulgazione di segreti commerciali che devono ritenersi leciti.

In questo modo la direttiva cerca di dare certezza e facilità di interpretazione per molti casi dubbi o di difficile interpretazione che ricorrono spesso nella pratica e di minimizzare, ove possibile, i casi di contenzioso.

La direttiva si preoccupa in particolare di prendere posizione sulle attività di ***reverse engineering*** – che insieme ai casi di sottrazione di segreti operati da ex dipendenti o ex collaboratori, sono i casi che più frequentemente danno origine a casi di contenzioso in questa materia – e stabilisce che l'acquisizione di un segreto commerciale è considerata lecita qualora il segreto sia ottenuto attraverso la osservazione, studio, smontaggio o prova di un prodotto o di un oggetto messo a disposizione del pubblico o lecitamente in possesso del soggetto che acquisisce le informazioni.

La **liceità del *reverse engineering*** è infatti un argomento molto delicato in questa materia e il limite tra lecito ed illecito è ancora attualmente dibattuto non solo in Italia.

Un'altra parte fondamentale della direttiva – prevista a favore dei titolari dei segreti commerciali – riguarda la tutela della riservatezza dei segreti nel corso dei procedimenti giudiziari.

Avviene infatti che le imprese abbiano timore a chiedere tutela giudiziale nei casi di sottrazione o di spionaggio dei propri segreti per **paura di vedere divulgati i propri segreti nel corso di un processo**, magari proprio a beneficio della loro controparte.

A questo proposito la direttiva fornisce importanti indicazioni che andranno certamente ad aggiungersi alle procedure che le sezioni specializzate nei casi di violazione di diritti di proprietà industriale già adottano per tutelare la posizione dell'imprenditore che agisce in giudizio per reagire ad un'illecita violazione dei propri segreti commerciali.

La direttiva in esame costituisce quindi un'ottima occasione per esaminare più attentamente il know-how aziendale e per prendere spunto per valorizzare e gestire in modo corretto un importante asset aziendale secondo regole che ne consentono una efficace protezione e ne garantiscono la circolazione tra aziende con i corretti strumenti contrattuali.

IL CAFFÈ DIGITALE

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

UniCredit

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