LA CENTRALITÀ DELLA RETE
PER UNA CYBER SECURITY EFFICACE
L'APPROCCIO ARCHITETTURALE PER UN'INTELLIGENCE PERVASIVA SULLE NUOVE MINACCE

AGOSTINO SANTONI

L'Ultra-broadband *fisso e mobile*, *il* Cloud Computing, *l'*Internet of Thing, *il* Big Data *e l'*Analytics *sono i principali driver tecnologici che guidano la digitalizzazione di Paesi, città, industrie e organizzazioni in tutto il mondo. È una rivoluzione di ampiezza e complessità tali che, il genere umano non ha mai vissuto in precedenza e dalla quale conseguono diverse sfide: la cyber security è una di queste e la più critica da affrontare. Le reti e le loro componenti si evolvono costantemente creando nuovi percorsi di attacco e rendendo indispensabile poter conoscere cosa si stia difendendo o si decida di proteggere, al fine di avere la totale visibilità di cosa accada in rete e di poter analizzare e collegare le informazioni in tempi sempre più ridotti. Serve l'intelligenza delle tecnologie e dei servizi, ma sono necessari anche i professionisti della sicurezza con specifiche competenze. Non è possibile capire in questa fase o prevedere come tale rivoluzione si svilupperà, ma una cosa è chiara: un'efficace risposta non può prescindere da un approccio integrato, che includa tutti gli stakeholders in campo: il settore pubblico e privato, il mondo accademico e la società civile, fino alla politica nazionale e internazionale.*

Il mondo intorno a noi sta cambiando molto rapidamente, sospinto da una trasformazione delle tecnologie in costante accelerazione. Fra queste l'It è al centro della rivoluzione che ci ha fatto entrare definitivamente in quella che chiamiamo l'era dell'*Internet of Things* (IoT), degli A*nalytics*, dell'A*utomation* e del M*achine Learning*. Oggi nel pianeta ci sono 15 miliardi di dispositivi connessi alla rete; nel 2020 questo numero crescerà a 50 miliardi e si prevede che arrivi a 500 miliardi nel 2030. Ciò implica una crescita esponenziale sia nella pervasività della connettività che nelle bande trasmissive. È una rivoluzione digitale. I dispositivi connessi genereranno uno tsunami di dati che comporterà dei mutamenti radicali nei processi di business e nei comportamenti individuali.

Le previsioni strategiche di Gartner per il 2016[1] sostengono che il futuro sarà completamente digitale, un mondo guidato dagli algoritmi e da macchine intelligenti, ovunque. I dispositivi connessi diventeranno i principali attori nelle attività quotidiane, rendendo le interazioni fra le macchine e le persone più complesse, il business più competitivo e il futuro più difficile da prevedere. Nel documento si legge che entro il 2018, il 20% del contenuto informativo rilevante per il business verrà generato dalle macchine, come i bilanci, i documenti legali, i report sui trend di mercato. Saranno assemblati proattivamente e spediti automaticamente. Sei miliardi di apparati connessi richiederanno supporto autonomamente. La realtà fisica e quella digitale non avranno più una separazione netta e le aziende dovranno rispondere a richieste di servizio in aumento da parte delle macchine come se fossero persone.

Le aziende svilupperanno un meccanismo di assistenza ai clienti fortemente automatizzato, l'intelligenza artificiale (Ai) raggiungerà un livello di sofisticazione tale per cui sarà difficile distinguere le conversazioni/interazioni uomo/macchina da quelle umane.

Entro il 2018, il 45% delle aziende che cresceranno di più sul mercato saranno quelle che impiegheranno più macchine intelligenti che dipendenti umani. Diventeranno comuni centri commerciali completamente automatizzati e aziende che offrono servizi di sorveglianza e sicurezza solo tramite droni. E questo è solo un piccolo esempio di come la digitalizzazione stia cambiando ogni aspetto della nostra esistenza. Qualunque cliente sul pianeta, senza eccezioni, che sia una piccola o media impresa, una grande corporation globale, un'azienda industriale o del settore finanziario, un service provider, un ente pubblico locale o le istituzioni principali di uno Stato, tutti si troveranno a interagire con un'infrastruttura altamente distribuita, in uno scenario in rapida evoluzione e completamente digitalizzato.

Questo processo si struttura attorno a due direttrici fondamentali: il tema P*eople Centric* e quello M*achine Centric*. Il primo è collegato ad aspetti quali il nuovo modo di lavorare o gli strumenti di collaborazione. Il secondo è più recente ed è un fattore fondamentale per la *disruption* che determinerà sui processi nei quali siamo coinvolti, tanto nella vita privata quanto in quella professionale.

Ritornando agli sviluppi correnti dell'It, cerchiamo di comprendere meglio le implicazioni derivanti dalla centralità della rete e della sicurezza, oggi e nel prossimo futuro.

1. Lawrence Orans, N*etwork and Gateway Security Primer for* 2016 (22 gennaio 2016).

Siamo giunti alla maturità del cloud e della mobilità che sono pervasivi nella nostra realtà e la digitalizzazione ci sta avviando verso una fase in cui gli elementi tecnologici predominanti sono gli *analytics*, l'automazione, il *deep* e *machine Learning*. Nel *consumer* lo vediamo ogni giorno e Google ne è un esempio con i suoi servizi che fanno ampio uso di intelligence predittiva sulle nostre abitudini e sui nostri comportamenti. Ciò che sta guidando l'era della digitalizzazione è strettamente legato ai dati. L'iperconnettività e la generazione e disponibilità dell'enorme mole di dati creata dai dispositivi non bastano, da sole, per l'innovazione: un ruolo chiave è l'estrapolazione delle informazioni (*insights*) e, al disopra di tutto, la sicurezza dell'intero ecosistema che non potrà che essere fondata su approcci olistici e architetturali.

L'evoluzione sui dati impatterà anche nell'evoluzione dei datacenter e delle applicazioni. I next-generation datacenter supporteranno un intero spettro di nuove applicazioni, non più monolitiche ma basate su micro-services, *policy driven* e realizzate su infrastrutture programmabili costruite sull'idea di piattaforme computazionali *loosely coupled*.

Ci sono oggi 22 milioni di sviluppatori nell'ecosistema delle applicazioni e nel prossimo decennio crescerà a 40 milioni; la maggior parte di loro saranno *data developers*, perché tutte le organizzazioni diventeranno strutture *data driven*. Avremo una nuova generazione di sviluppatori che scriveranno codici per estrarre informazioni dai dati. Queste applicazioni dovranno essere agili per poter continuamente essere modificate e migliorare i processi, giorno dopo giorno.

Riassumendo, l'elemento centrale nella digitalizzazione sarà l'infrastruttura (*core*), con le risorse di rete, computazionali e di memorizzazione (*storage*). Essa sarà ottimizzata per fornire agili micro-services a supporto dello sviluppo delle applicazioni di nuova generazione. Su questo elemento fondante poggiano quattro pilastri abilitanti: l'astrazione e la programmabilità, il controllo e la gestione, gli analitycs e la security. Gartner sostiene che gli architetti di sicurezza devono accettare la realtà che oggi, nel 2016, è irragionevole aspettarsi che possano costruire difese perimetrali in grado di bloccare ogni attacco o prevenire qualunque falla. Al contrario, devono adottare nuovi prodotti/servizi che abilitino la rete a essere una parte integrante della strategia difensiva, focalizzata a individuare e a rispondere agli incidenti di sicurezza.

Reti con architetture ben progettate e adeguatamente gestite rendono il lavoro degli hacker molto più difficile. Non esiste più un confine netto fra architetture di network e di security. Il tutto deve essere realizzato con schemi semplici e reso fruibile in maniera agile, con mec-

canismi avanzati di automazione. I due temi – network e security – sono intimamente interconnessi perché scompare il concetto di sicurezza limitata alla protezione perimetrale.
Una corretta strategia per la sicurezza informatica si deve basare quindi su due pilastri, entrambi essenziali: l'impiego di prodotti eccellenti (*best-of-breed*) ma anche – e soprattutto – un approccio integrato e architetturale.
All'ultima Rsa Conference (San Francisco, marzo 2016) erano presenti più di 500 aziende di security, un dato molto positivo per l'innovazione tecnologica che, al contempo, crea il grosso problema dell'integrazione di un'ampia ed eterogenea gamma di prodotti di costruttori diversi. Questo esercizio è complesso e, spesso, comporta errori che lasciano porte aperte agli hacker. In altre parole, l'innovazione di un'offerta così frammentata è resa inutilizzabile dalla complessità richiesta dall'integrazione, che aumenta esponenzialmente mentre le nuove funzionalità solo linearmente. Il risultato paradossale è che i clienti stanno diventando meno sicuri. Lo testimoniano recenti interviste ai Chief Information Security Officer (Ciso) delle maggiori aziende. Molti clienti hanno più di 10 brand diversi di security nella loro rete, alcuni arrivano addirittura fino a 100. Cisco, negli ultimi 4 anni, ha fatto un enorme sforzo di integrazione dei prodotti di security del proprio portfolio che continua a mantenere come filosofia architetturale.
Cosa succede quando i prodotti si integrano? Condividono le informazioni, consentono una visione più ampia e incentivano l'automazione degli algoritmi di analisi e delle procedure per le contromisure. Questo porta alla semplicità e quindi all'implementazione di una sicurezza veramente efficace. È inevitabile: il mercato dei vendor di sicurezza dovrà necessariamente passare verso un forte consolidamento su pochi attori capaci di proporre offerte complete e architectural-based.
Un'architettura integrata di security mette insieme la rete, gli *end-point* e il cloud. Le informazioni sullo stato della sicurezza arrivano sia dalla rete che dagli *end-point* e coinvolgono le architetture cloud. L'innovazione di Cisco nella security passa attraverso tutti gli elementi architetturali, oltre che tramite prodotti puntuali. L'aspetto cruciale dell'approccio architetturale è la visibilità: più informazioni si hanno a disposizione e più minacce si riescono a scoprire nel minore tempo possibile. L'Advanced Malware Protection (Amp) è un mercato che si misura in B$ e cresce a ritmi superiori al 20%. Cisco ha costruito una proposizione Amp molto diversa da quella di prima

generazione, caratterizzata dall'impiego di alcuni sensori che inviano le informazioni in un punto centrale per analizzare le minacce. L'approccio che suggeriamo deve essere pervasivo dell'intera infrastruttura, posizionando *cloud connector* su tutti gli elementi di rete, ovunque ci siano utenti o dati. In tal modo l'intera infrastruttura è un sensore e un *enforcer*. Quando in un punto della stessa s'individua una minaccia, le contromisure vengono apportate su tutta la rete, istantaneamente. Questa è automazione, questa è sicurezza efficace.
Un altro aspetto importante dell'architettura è la sua apertura e flessibilità. Non sappiamo quale nuova tecnica gli attaccanti utilizzeranno per violare i nostri sistemi, per cui non possiamo conoscere a priori quale nuovo schema difensivo dovremmo adottare per fronteggiare i nuovi attacchi. Per questo l'architettura deve adattarsi a frequenti cambiamenti e a tal fine basiamo la maggior parte delle soluzioni di security su progetti open source.
Quest'architettura *threat-centric* ha consentito a Cisco di ottenere il Best Security Company Award all'ultima edizione dell'Rsa conference.
Un aspetto veramente differenziante è la sua enorme capacità di *threat intelligence*: l'80% del traffico internet passa attraverso apparati di rete Cisco. Grazie alla pervasività dei propri sistemi nei mercati mondiali, ha la visibilità di più di 100Tb di informazioni al giorno. Il gruppo di security interna, chiamato Talos, trasforma questa enorme mole di dati in intelligence. Il team Talos intercetta mediamente 1.1 milioni di campioni unici di malware al giorno, esaminati per determinare se debbano essere detonati in una *sandbox* (eseguito in un sistema isolato) per analisi comportamentali più approfondite. Coerentemente con l'uso sempre più diffuso degli smartphone e delle relative applicazioni, Talos ha evidenziato un crescente trend di creazione di malware indirizzati a piattaforme mobili (circa 300.000 e 8.000 nuovi malware al mese, rispettivamente, su piattaforme mobili Android e Apple).
Le nostre sonde di web security bloccano 19.7 miliardi di Url malevoli al giorno (2.2 milioni al secondo). Per capire questo dato appieno basta confrontarlo con il numero giornaliero di interrogazioni su Google (circa 3.5 miliardi al giorno), ovvero solo con le sonde sul traffico web processano dalle cinque alle sei volte in più rispetto al numero di interrogazioni medie su Google.
Non meno impressionante è la visibilità di Talos sulle email: su 300 miliardi di email al giorno, ne blocchiamo in media l'86% (250 miliardi/giorno) che è spam. Lo spamming è uno dei vettori classici d'attacco, che avviene tipicamente mediante mail di phishing o attachment malevoli. Proattivamente Talos scrive exploits per le Common Vulne-

rabilities and Exposure (Cve) – anche queste in crescente aumento – che sono attaccabili da remoto. L'obiettivo è quello di testare in anticipo i propri sistemi, rispetto a potenziali attacchi futuri, per verificare che l'architettura di rete sia in grado di proteggere gli asset oggetto della vulnerabilità, per i quali non esiste ancora una *patch* o per quelle realtà che non hanno ancora provveduto a implementarla. Talos ha istituito un programma paritetico di partnership verso grandi aziende e istituzioni governative per contribuire allo scambio di informazioni di intelligence. Inoltre, collabora attivamente con gli attori coinvolti nella lotta al cyber terrorismo, come avvenuto di recente con riguardo al caso di Angler exploit kit (http://www.talosintel.com/angler-exposed/ [30/4/2016]).

Recentemente, l'intelligence di Talos si è arricchita con il patrimonio informativo e le straordinarie capacità di analitycs di *OpenDns*, che nasce come servizio per tradurre i nomi di domini in indirizzi Ip. Questa è una funzione fondamentale per i protocolli quali Http/s (navigazione), Ftp (file transfer) e P2p (peer to peer). Più del 2% di tutte le richieste Dns su internet, che corrispondono a oltre 50 miliardi di risoluzioni Dns al giorno e coinvolgono più di 50 milioni di utenti in internet, vengono eseguite da OpenDns.

Il malware viene tipicamente trasmesso solo dopo che una connessione internet viene stabilita. Ogni connessione inizia con la traduzione dell'host name nel corrispettivo indirizzo Ip (Dns Service). L'operazione coinvolge un database in continuo cambiamento, distribuito su milioni di server che eseguono il servizio Dns. La visibilità su queste informazioni e su quelle relative all'instradamento del traffico in internet (protocollo Bgp), entrambe in costante cambiamento, unita a sofisticati algoritmi di analisi, consente a OpenDns di individuare e isolare host malevoli prima che la loro azione di infezione sia evidenziata da strumenti di protezione tradizionali che lavorano 'a posteriori'.

Come indicato nel *Libro Bianco* sulla cyber security (https://www.consorzio-cini.it/index.php/it/labcs-home/libro-bianco) e successivamente ripreso dal *Framework Nazionale per la Cyber Security* del Cini (Cyber Security National Lab), la formazione in senso ampio deve essere parte fondamentale di ogni piano strategico nazionale sulla sicurezza informatica.

Cisco NetAcad è un'iniziativa ampia e articolata sviluppata tramite una rete di partnership globali con enti governativi, scuole, università e organizzazioni impegnate nel sociale, tra cui anche alcuni istituti di pena. I corsi sono somministrati in maniera scalabile, tramite piattaforme basate su cloud, con esercitazioni pratiche e l'obiettivo di preparare le figure professionali del futuro. Nel portafoglio corsi trovano spazio sempre maggiore i temi legati alla security sia dei sistemi informativi aziendali che del mondo industriale legato all'IoT. Dall'anno della sua fondazione il programma ha raggiunto più di 5.5 milioni di studenti, con un ritmo che cresce di circa un milione di nuovi studenti ogni anno. L'impegno di Cisco in Italia si è concretizzato con un accordo con il Governo lo scorso gennaio, che prevede una serie di investimenti strategici per il valore di 100 milioni di dollari nei prossimi tre anni. In particolare, si è convenuto con il Miur di potenziare il programma NetAcad, con un focus particolare sulle tecnologie per l'industria 4.0 e la cyber security. L'accordo prevede anche iniziative legate alla Ricerca e Sviluppo, alla collaborazione con le università italiane e alla trasformazione digitale. In tutte, la sicurezza ha un ruolo fondamentale.

Siamo giunti al termine di questo breve excursus sulla cyber security. Partiti da una panoramica sulle trasformazioni digitali legate alla quarta era dell'It, siamo approdati alle implicazioni di sicurezza di tutti gli attori coinvolti: individui, macchine e processi. Abbiamo argomentato come solo un approccio olistico e architetturale alla cyber security possa costituire una risposta efficace alle sfide poste dalle nuove minacce. Abbiamo poi validato questo concetto tramite l'esperienza del Talos team. Infine, abbiamo rimarcato come tutti, dal singolo cittadino fino alle istituzioni, passando dagli *incident team* delle aziende di ogni dimensione, abbiano il dovere di intraprendere il percorso di formazione più adeguato per definire un'esperienza sicura del nuovo mondo che ci attende

G