

DIRECTION Reportec 93

SOLUZIONI SERVIZI E TECNOLOGIE ICT

CLOUD COMPUTING A PORTATA DI MANO

TECHNOLOGY

Sempre più IoT nel futuro di PTC

INTERVIEW

Qlik e Vodafone per la data security nell'Automotive

TRENDS & MARKET

Le aziende rinnovano le reti per supportare la digitalizzazione

START UP

Ribes Tech: innovazione che nasce dalla Ricerca pubblica

SECURITY
& BUSINESS

SPECIALE

Identità e accesso alle applicazioni alla base della Digital Transformation

CYBER ATTACK

Quali sono le principali minacce per l'Internet of Things?

SOLUZIONI

La security fabric di Fortinet orchestra i firewall



Questa volta
siamo noi
a chiedere aiuto
a voi.

Fai un'offerta per una nuova ambulanza.

Servizio emergenza/urgenza 118 - auto medica - trasporto ammalati - trasporto organi - corsi di formazione di primo soccorso per aziende e per la popolazione - stazionamento ad eventi di massa - spettacoli e manifestazioni sportive - 37 sezioni in tutta la Lombardia - 100 anni storia.

Questo è quello che possiamo offrirti, tutti i giorni 365 giorni all'anno. Adesso tocca a te.

DONACI IL TUO 5 x mille: C.F. 03428670156, oppure puoi fare una donazione detraibile
(IBAN It43u0326801603000866949890)

Visita www.crocebianca.org e scoprirai come poterci aiutare.

Direction Reportec
 anno XIV - numero 93
 mensile novembre-dicembre 2016

Direttore responsabile: Riccardo Florio
 In redazione: Giuseppe Saccardi,
 Gaetano Di Blasio, Paola Saccardi,
 Daniela Schicchi
 Ha collaborato: Gian Carlo Lanzetti
 Grafica: Aimone Bolliger
 Immagini da: Dreamstime.com

Redazione:
 via Marco Aurelio, 8 - 20127 Milano
 Tel 0236580441 - fax 0236580444
 www.reportec.it
 redazione@reportec.it

Stampa:
 A.G. Printing Srl, via Milano 3/5
 20068 Peschiera Borromeo (MI)

Editore:
 Reportec Srl, via Marco Aurelio 8,
 20127 Milano

Presidente del C.d.A.: Giuseppe Saccardi
 Iscrizione al tribunale di Milano
 n° 212 del 31 marzo 2003
 Diffusione (cartaceo ed elettronico)
 12.000 copie

Tutti i diritti sono riservati;
 Tutti i marchi sono registrati e di proprietà
 delle relative società.

FOCUS ON

Un mercato dinamico che continua a crescere	4
I servizi di cloud integration	8
Le previsioni di VMware per le applicazioni cloud-native	10
Il cloud fa breccia anche nel mercato finanziario	12
Integrazione ibrida tra risorse in cloud e locali	14
La fattura diventa smart e si sposta nel cloud	15
Cloud, agilità e disponibilità dell'IT il focus del 2017	17

INTERVIEW

Qlik e Vodafone per la data security nell'automotive	20
---	-----------

TECHNOLOGY

Sempre più IoT nel futuro di PTC	23
D-Link: 30 candeline e 18 anni in Italia	26
Il supermercato Coop del futuro	28
Zebra lancia i palmari professionali Android	32
Pure Storage e Cisco: infrastruttura scalabile	34
Teorema fa crescere l'innovazione	41

START UP

Ribes Tech: innovazione che nasce dalla Ricerca pubblica	30
---	-----------

TRENDS & MARKET

Le aziende rinnovano le reti per supportare la digitalizzazione	36
--	-----------

Un mercato dinamico che continua a crescere

Il cloud computing ha aiutato molte imprese a trasformarsi negli ultimi cinque anni, ma gli analisti concordano sul fatto che il mercato stia entrando in una seconda fase, sia per quanto concerne i servizi cloud pubblici sia per quelli di tipo "private" realizzati e mantenuti all'interno dei data center aziendali.

Nel 2017 il mercato cloud dovrebbe aumentare il livello di accelerazione soprattutto a seguito della crescente esigenza delle imprese di ottenere efficienza nel processo di scalabilità delle loro risorse di calcolo.

Il cloud sempre più presente nel mondo enterprise

Una delle tendenze da aspettarsi per il 2017 è un progressivo spostamento di risorse enterprise nel cloud. Uno dei trend "nuovi" è che le aziende di livello enterprise che dispongono di budget importanti, grandi data center e applicazioni complesse si stanno progressivamente indirizzando verso il cloud anche per ospitare le applicazioni che attengono al loro core business. Già oggi diverse aziende utilizzano applicazioni enterprise all'interno di Amazon Web Services (AWS) lasciando percepire che i CIO sono, in qualche modo, diventati

meno restii di qualche tempo fa in relazione all'hosting di software critico all'interno di modelli di cloud pubblico. Molte aziende hanno spostato in AWS applicazioni aziendali, quali SAP, e ci si può aspettare che questa tendenza continuerà mano a mano che i CIO faranno sempre più affidamento sui provider di servizi "public cloud".

Architetture iperconvergenti a supporto del cloud ibrido

Nonostante la crescente apertura dal punto di vista generale non tutti i CIO sono disposti ad accettare i rischi associati nell'affidare i dati loro o dei loro clienti al public cloud. Va detto però che anche i servizi private cloud sono onerosi e complessi, poiché richiedono virtualizzazione avanzata, standardizzazione, automazione, accesso self-service, monitoraggio delle risorse e così via.

L'esigenza di coniugare efficienza, scalabilità e semplicità sta alimentando l'affermazione di infrastrutture iperconvergenti che promettono un approccio pre-integrato alle risorse di elaborazione e memorizzazione per aiutare le aziende a utilizzare le loro implementazioni cloud in modo

Prosegue il processo di diffusione del cloud e tra i trend per il 2017 si prospetta una maggiore affermazione nel mondo enterprise. Si affacciano anche nuove tecnologie e servizi mentre l'accelerazione delle infrastrutture iperconvergenti promette di avere un forte impatto come elemento abilitante per soluzioni cloud di tipo ibrido

più veloce. Questo tipo di approccio potrebbe rapidamente trasformarsi nella piattaforma infrastrutturale predefinita su cui costruire la parte privata di un cloud ibrido. Per il 2017 è quindi lecito aspettarsi una crescente attenzione intorno alla iperconvergenza, anche se va osservato che la disponibilità di soluzioni complete richiede ancora un po' di tempo: attualmente i sistemi iperconvergenti rappresentano componenti utili per creare infrastrutture cloud di base ma, per lo più, restano ancora piattaforme fondamentalmente standard a supporto della virtualizzazione e non riescono ancora a esprimere tutte le potenzialità necessarie per fornire ciò che le aziende hanno bisogno dal cloud.



La tecnologia dei Container influenzerà il cloud e la sua gestione

I Container sono una tecnologia emergente che permette agli sviluppatori di gestire in modo efficiente il codice sviluppato per applicazioni cloud. La società di analisi americana Forrester prevede che entro la prima metà del 2017 i Container Linux saranno già disponibili in tutte le principali piattaforme cloud pubbliche e private. Questo porterà gli sviluppatori a utilizzare direttamente queste tecnologie, sfruttandole per costruire i propri stack con cui alimentare lo sviluppo di micro-servizi. L'avvio di un

nuovo paradigma di questo tipo significherà però affrontare nuove sfide e le aziende dovranno cimentarsi con nuovi requisiti in termini di sicurezza, monitoraggio, archiviazione e problematiche di rete mano a mano che i Container saranno rilasciati in produzione in modo massiccio.

Più fornitori di cloud per una stessa azienda

Nel passaggio al cloud è importante assicurarsi di non stare scambiando un'infrastruttura legacy per un'altra. Per questo motivo, nella progettazione dei propri servizi cloud, le aziende devono poter contare su un livello di flessibilità tale da consentirgli di adottare diverse piattaforme o fornitori di cloud alternativi rapidamente e con il minimo impatto per i servizi esistenti.

Lo spostamento di dati nel cloud non implica che un'organizzazione debba prendere precauzioni per la protezione dei dati, ma significa assumersi la responsabilità di richiedere al fornitore di servizi di predisporre i livelli appropriati di protezione delle informazioni, misura e controllo per garantire la sicurezza. Il trend a cui si sta assistendo è che le aziende stanno diventando molto più accorte nel modo di valutare potenziali fornitori di cloud, preoccupandosi (diversamente da quanto accadeva in passato) di trovare verifiche indipendenti sulla loro

capacità e analizzando in dettaglio le loro policy per la sicurezza dei dati e la governance. Questo trend sarà rafforzato ancora di più alla luce delle prossime normative GDPR e dell'esigenza di predisporre una definizione scritta di tutte le policy e le procedure di sicurezza dei dati che potranno essere richieste da un auditor.

Nuovi servizi cloud per risolvere problemi specifici

Il fatto che le aziende utilizzino più provider cloud alimenta l'introduzione di nuovi servizi di integrazione per la gestione e il monitoraggio di tutti i servizi di cloud contratti da un'organizzazione.

Per rendere il cloud ibrido funzionante, inoltre, le aziende necessitano di una funzione di audit per garantire che il servizio rimanga sempre conforme alle aspettative, con un servizio indipendente di monitoraggio (gestito sia internamente sia attraverso una terza parte indipendente) in grado di verificare che il provider fornisca i livelli sottoscritti contrattualmente. Questo sta portando allo sviluppo di un nuovo ruolo: il broker di servizio di cloud, con il compito di provvedere sia a definire i servizi necessari a un'azienda sia a determinare il modo più appropriato per fornirli, gestirli e renderli sicuri. La crescita del cloud porterà necessariamente allo sviluppo di nuove applicazioni, la cui portata è limitata solo



dall'ingegno e la visione di fornitori di servizi; mentre alcuni saranno destinati a mercati di nicchia, altri affronteranno problemi comuni. Tra quelli che appartengono a quest'ultima categoria, uno dei servizi in più rapida crescita nel 2017 è probabile che sarà la gestione delle patch (tra cloud pubblico e attrezzature on-premise) che consente di rimuovere il sovraccarico amministrativo sulle funzioni IT, assicurando che i sistemi si mantengano costantemente conformi alle policy e sicuri e in grado di rispondere alle vulnerabilità zero day.

Altri servizi che si stanno affacciando comprendono identity management as a service, già in uso in diverse istituzioni governative e servizi di data protection in grado di fornire backup, ripristino, garanzia di conformità attraverso tutti i dispositivi utilizzati dagli utenti aziendali e tutti i dati cifrati memorizzati sul cloud pubblico.

L'uso di cloud ibrido favorirà anche la diffusione di servizi di monitoraggio delle performance del cloud attraverso molteplici provider, per i quali si è già trovata una sigla: CMaaS, acronimo di Cloud Monitoring as a service. I CMaaS forniscono l'integrazione sia con i servizi public cloud (per esempio Office 365, Salesforce, Huddle, Google Apps) sia con i servizi IaaS e PaaS (per esempio Microsoft Azure, AWS, Google App Engine). ✨

I servizi di cloud integration

L'esplosione di servizi e applicazioni basati su cloud offre ai vendor e alle aziende un'opportunità per ripensare al modo in cui integrare applicazioni e database. Tradizionalmente, le aziende hanno utilizzato software on-premise per collegare e sincronizzare le applicazioni o spostare, trasformare o unire dati tra sistemi o i propri uffici. Ma se le applicazioni e l'elaborazione dei dati vengono spostati nel cloud, l'integrazione software legata a un data center aziendale non ha più molto senso. Per questo motivo, una pluralità di vendor, sia affermati sia emergenti, sta vendendo servizi di integrazione basati su cloud.

Un segmento importante del mercato PaaS

In sintesi un servizio di cloud integration è una piattaforma cloud-based, multi-tenant, progettata per supportare i flussi di lavoro legati all'integrazione tra e attraverso le fonti di dati e le applicazioni in esecuzione sia nel cloud sia in un data center aziendale (vale a dire on-premise).

Alcuni fornitori di servizi di cloud integration supportano anche applicazioni mobili, servizi di gestione delle API, gateway B2B, servizi di trasferimento

Nuove offerte di servizi e nuove opportunità di business nascono dall'esigenza di integrare dati e applicazioni tra il cloud e le implementazione on-premise

di file e ambienti big data.

La società di analisi americana Gartner chiama collettivamente questo tipo di soluzioni "integration Platform as a Service" indicandoli con la sigla iPaaS. Sempre secondo Gartner, questi servizi generano il secondo più importante segmento del mercato complessivo PaaS (che vale oltre 1,5 miliardi di dollari). Oltre agli attori di livello enterprise, Gartner individua decine di fornitori di piccola dimensione indirizzati verso mercati di nicchia o consumer. Senza dubbio, il numero di fornitori di servizi di integrazione cloud aumenterà mano a mano che crescerà il numero di applicazioni cloud (che già oggi sono stimate in oltre 3mila, con più di 6mila servizi), accelerando la domanda di servizi di integrazione.



Strumenti di progettazione e flussi di lavoro

In generale, i servizi di integrazione cloud forniscono un ambiente di progettazione grafica (desktop o basato sul cloud) che utilizza un'interfaccia di tipo drag & drop e che riduce al minimo la necessità di codifica o di "scripting". Nei casi d'uso più semplici o quando è disponibile un modello precompilato, questo consente anche agli utenti business che non dispongono di competenze di sviluppo di creare flussi di integrazione senza dover ricorrere al supporto dell'IT. Questi flussi di lavoro possono spostare o sincronizzare i dati tra e attraverso le applicazioni, nonché convalidare e trasformare i dati lungo il loro percorso. I servizi di integrazione cloud possono anche essere utilizzati per orchestrare processi end-to-end; inoltre, la maggior parte di essi prevede uno spazio di memorizzazione per i metadati per archiviare i flussi di lavoro di integra-

Tradurre i dati in un formato comune

La maggior parte dei servizi di integrazione cloud offrono adattatori pacchettizzati per una miriade di applicazioni cloud, così come per molti sistemi on-premise. Gli adattatori acquisiscono dati da un sistema (fonte) e lo passano a un motore di integrazione runtime, che può operare in locale o da remoto in un centro di hosting cloud, che mappa i dati e li "traduce" in un formato omogeneo prima di passarli al sistema di destinazione. Molti fornitori di servizi offrono kit di sviluppo che consentono all'utilizzatore finale di creare adattatori personalizzati per sistemi nuovi o non ancora supportati.

zione e le statistiche di runtime e questo facilita lo sviluppo in team nonché il riutilizzo e le attività di monitoraggio e gestione da remoto. Molti fornitori di servizi di "cloud integration" pubblicano i prezzi sui loro siti Web, offrono prove gratuite e prevedono modalità di pagamento basate su canoni mensili o annuali anziché sull'acquisto di licenze perpetue. Poiché le piattaforme di integrazione sono eseguite nel cloud e non in un data center aziendale, è lecito aspettarsi che sia previsto anche il supporto di funzioni di provisioning e scalabilità dinamiche, la possibilità di aggiornamenti automatici e che siano messi a disposizione dell'utilizzatore finale una serie di tool basati su Web per il monitoraggio, l'amministrazione e la gestione delle prestazioni e della fatturazione. *

Le previsioni di VMware per le applicazioni cloud-native

Il vendor ha introdotto le tecnologie per le applicazioni cloud-native nel 2015 con il lancio di vSphere Integrated Container (VIC) e della piattaforma Photon e, da allora, l'interesse intorno a questo modello emergente di sviluppo di applicazioni è costantemente cresciuto

Il 2016 è stato l'anno dei container, con i nuovi progetti open source promossi dai più importanti player di mercato, compresa VMware, che ha lanciato vSphere Integrated Containers come progetto open source. L'infrastruttura cloud-native su container sta vivendo un momento chiave e VMware prevede che il 2017 sarà caratterizzato dai seguenti trend.

di aziende sta già sperimentando l'utilizzo di sistemi operativi leggeri e funzioni di virtualizzazione in moderne CPU per avviare in modo trasparente una Virtual Machine per ogni container che viene "lanciato". Questo approccio potrebbe, potenzialmente, aumentare l'isolamento e la sicurezza dei container senza aggiungere alcun ulteriore sovraccarico e VMware ritiene che ci sarà grande fermento intorno a questa idea il prossimo anno.

Kit Colbert,
CTO, cloud
platform
business unit
di VMware



Più virtualizzazione nei container

I container di oggi si basano su tecnologie integrate nel kernel di Linux, tra cui gruppi di controllo per isolare i container l'uno dall'altro sulla macchina host. Tuttavia, un certo numero

Le tecnologie di "container persistence" arriveranno in produzione

Finora, la maggior parte dei container sono "senza stato": in altre parole, i dati all'interno del container vengono distrutti quando l'istanza del

container si chiude e qualsiasi stato di applicazione deve essere conservato in un database esterno o con un altro servizio storage. Ciò è in gran parte dovuto all'immaturità delle tecnologie di "container persistence" disponibili oggi sul mercato. Tuttavia, con l'avvento di nuove funzionalità come PetSets di Kubernetes, di tecnologie come quelle di PortWorx e con Docker volume driver for vSphere, VMware è convinta che si avrà presto un aumento dei livelli di maturità per le tecnologie di "container persistence" che permetterà finalmente di iniziare a vedere i container in produzione.

In forte aumento le soluzioni per la sicurezza dei container

La sicurezza dovrebbe essere in cima ai pensieri della maggior parte degli utenti di container, poiché questa tecnologia porta con sé un'ampia gamma di problemi legati alla security. Le immagini container possono includere le vecchie versioni di library con vulnerabilità di sicurezza. I container Linux condividono un kernel e hanno, quindi, un limite di protezione e la sicurezza dei container in rete è ancora agli inizi.

C'è però uno spiraglio positivo: con i container sempre più in produzione, le aziende chiederanno soluzioni di sicurezza per garantire che le applicazioni critiche e i dati non siano eccessivamente esposti. A tale riguardo VMware ha sviluppato NSX e altre aziende stanno lavorando su come



affrontare questa domanda lasciando prevedere interessanti sviluppi nei prossimi 12 mesi.

Un crescente successo per Pivotal Cloud Foundry

Nel corso degli ultimi anni le tecnologie container hanno conquistato la scena sul mercato. Nel frattempo, la piattaforma applicativa cloud-native open source Pivotal Cloud Foundry (PCF) è rimasta in silenzio costruendo una vasta base clienti di sviluppatori e operatori cloud-native. PCF ha superato la soglia dei 200 milioni di dollari nel 2016, a dimostrazione di una crescita forte e continua. Il framework Spring Boot di Pivotal è cresciuto a un tasso elevatissimo, superiore a 2,5 milioni di download al mese, alimentando l'interesse per PCF come il runtime di produzione. Il 2017 è prevedibile che sarà l'anno in cui PCF raccoglierà i frutti del lavoro fatto finora. *

Il cloud fa breccia anche nel mercato finanziario

Secondo una ricerca commissionata da Colt il settore del capital market sta mostrando crescente interesse verso i servizi cloud-based

I servizi cloud si stanno facendo strada all'interno del settore del mercato di capitali come dimostra una ricerca condotta dalla società di ricerca e consulenza Celent e commissionata da Colt, società che fornisce servizi on-demand di rete e di comunicazione alle aziende. La ricerca, dal titolo "Il cloud diventa maggiorenne nel Capital Market" ha mostrato un atteggiamento più morbido e interessato verso il cloud negli ultimi 12-18 mesi, grazie a una maggiore consapevolezza in merito alla sicurezza, alla stabilità e all'affidabilità delle soluzioni basate su questa tecnologia, come emerge dalle risposte degli intervistati.

Andrea Deli, Client Director South Region, Capital Markets Colt ha dichiarato: «Le pressioni del mercato stanno

portando le aziende a concentrarsi sui propri punti di forza, affidando le funzioni tecnologiche agli specialisti. Non è quindi una sorpresa scoprire che il cloud sta crescendo nei mercati di capitali, aiutando le imprese ad affrontare le pressioni normative e di costo, permettendo loro al contempo di concentrarsi sul core business».

La ricerca promossa da Colt evidenzia come i principali fattori che guidano l'adozione del cloud siano quattro: l'aumento della regolamentazione (per esempio MiFID II, Dodd-Frank); la pressione sui costi; l'incertezza macroeconomica (per esempio Brexit o l'economia cinese) e l'ascesa del "financial technology".

Queste sfide che le aziende si trovano ad affrontare richiedono una maggiore agilità nell'infrastruttura che le soluzioni cloud possono offrire. Anche la necessità di adattarsi alle continue normative in evoluzione, così come la proliferazione di applicazioni per il trading e la necessità di collegarsi rapidamente a molteplici fonti di liquidità, rappresentano degli aspetti che i servizi cloud-based possono aiutare a gestire più facilmente.

Sempre secondo la ricerca questi fattori si possono manifestare in modo diverso nel settore di mercato in

questione a seconda che si consideri il lato acquisti o quello delle vendite. Dal lato degli acquisti, soprattutto nelle imprese di dimensioni più piccole, si evidenzia una maggiore apertura verso modelli basati sul servizio. Le soluzioni hosted vengono, invece, impiegate per la maggior parte dei sistemi, compreso il trade management. I fondi di investimento sono interessati in particolare a ottenere velocemente dati sull'analisi del mercato e, a tal fine, il modello cloud risulta molto attraente.

Nell'ambito delle vendite, invece, si tende a focalizzare l'attenzione sul mantenimento del controllo dei sistemi. Non manca, tuttavia, il desiderio di esplorare soluzioni che diano vita a modelli di distribuzione migliori e a un modello di costo variabile inferiore. Molte aziende avrebbero già implementato tecnologie di cloud privato per le loro risorse chiave spostando le applicazioni meno sensibili sul cloud pubblico.

A tal proposito risulta che, mentre c'è maggiore consenso in merito allo spostamento di dati non-core e non proprietari in un ambiente cloud, il trasferimento di funzioni di front office e di informazioni proprietarie o relative ai clienti è rimasto indietro. Di fatto, l'adozione di soluzioni basate su cloud è diversa anche se si considerano le diverse funzioni aziendali. Tra gli ostacoli che, invece, le aziende devono superare prima che l'adozione del cloud diventi estesa vengono citate la collocazione dello storage



dei dati, la responsabilità del rischio e l'inerzia organizzativa.

Secondo Brad Bailey, Research Director di Celent, gli ostacoli verso l'adozione del cloud «non si basano più sulla diffidenza verso la tecnologia, ma su come implementare con successo una soluzione che sia conforme alle normative, e queste preoccupazioni sono comuni a tutte le soluzioni tecnologiche, siano cloud-based o no. In molti casi il cloud pubblico è ora più sicuro rispetto ai sistemi on-premises; le istituzioni stanno cambiando il loro atteggiamento da "mai" a "come" abbracciare il cloud».

Secondo quanto dichiarato dalla ricerca, il settore del capital market avrebbe la necessità di migliorare la connettività per supportare soluzioni cloud più sicure e, per questo motivo, l'accesso al cloud dedicato o privato risulterebbe più adatto alle esigenze di questo mercato poiché offrirebbe una maggiore velocità e una minore latenza oltre alla garanzia di una migliore sicurezza. *

Integrazione ibrida tra risorse in cloud e locali

Cresce l'offerta di servizi per realizzare soluzioni che collegano il mondo cloud e on-premise. Tra le soluzioni disponibili anche la piattaforma di Talend

La cloud service integration costituisce una generazione di offerta nativa per il cloud relativamente nuova che abilita l'integrazione ibrida tra sorgenti di dati o applicazioni disponibili localmente e in cloud, che viene identificato come uno specifico segmento di mercato indicato con la sigla iPaaS (integration Platform as a Service). Questo tipo di servizi si pone l'obiettivo di coniugare i vantaggi offerti dal cloud e dal modello SaaS per progetti quali l'integrazione di big data, il data warehousing, analytics e reportistica su scala enterprise.

A queste esigenze si indirizza anche Talend, azienda di software che ha sviluppato Talend Integration Cloud, una piattaforma di integrazione del cloud sicura e gestita fornita come

servizio, che permette di spostare in modo rapido e semplice i carichi di lavoro dall'ambiente on-premise al cloud.

Talend Integration Cloud

Talend Integration Cloud consente di automatizzare il provisioning di integrazione dei big data su Amazon Web Services Redshift ed EMR rendendo così questi progetti più abbordabili economicamente. Tramite la generazione di codice nativo (che sfrutta l'ambiente di parallelismo massivo di Hadoop e la velocità di Apache Spark e Spark Streaming) Talend Integration Cloud consente di eseguire i processi di integrazione con un rapido tempo di risposta e un utilizzo efficiente delle risorse. È anche possibile espandere le funzioni di analytics tramite componenti avanzati di machine learning per effettuare attività di segmentazione, di previsione, di classificazione e analisi relative alla base clienti.

«Le soluzioni di Cloud Service Integration sono tipicamente articolate sotto forma di connettori e azioni - spiega Massimo Tripodi, sales country leader di Talend Italia -. I primi si usano per la connessione ad applicazioni e sorgenti di dati nel cloud e on-premise, implementando la chiamata al servizio ed elaborando i contenuti di input/

output. La soluzione di Talend fornisce connettori precostruiti, oltre a un ambiente di sviluppo che consente di creare connettori nativi alle applicazioni senza bisogno di implementare dei servizi Web personalizzati. Le azioni di integrazione forniscono un ulteriore controllo sui dati: verifica della qualità dei dati, conversione in formati diversi.

A queste si affian-



cano ulteriori attività per gestire, unire o ripulire i dati. TIC prevede anche funzionalità di amministrazione e monitoraggio per controllare eventuali perdite di dati, errori, pianificare l'esecuzione dei processi o fornire assistenza nella configurazione di ambienti e modelli».

I servizi di cloud integration di Talend prevedono il supporto per MapReduce e l'integrazione Hadoop per abilitare l'implementazione di data warehousing, analisi o big data. Consentono di predisporre interfacce utente personalizzabili e differenziate in funzione del diverso tipo di utenza e offrono i vantaggi che caratterizzano ogni soluzione basata su progetti open source.*

La fattura diventa smart e si sposta nel cloud

Da Wolters Kluwer un applicativo in cloud pensato per PMI e “Partita Iva”

Wolters Kluwer Tax and Accounting Italia ha sviluppato Fattura SMART, una soluzione cloud pensata per le esigenze di dematerializzazione delle PMI italiane e degli studi professionali alle prese con la

dematerializzazione del processo di fatturazione, invio e conservazione dei documenti contabili.

Un processo che si prevede in rapida accelerazione anche a seguito dell'entrata in vigore grazie a gennaio 2017

Cloud, agilità e disponibilità dell'IT il focus del 2017

Albert Zammar,
vice president SEMEA
di Veeam Software



In aumento l'esigenza di agilità del business e di availability dell'IT. I suggerimenti di Albert Zammar, vice president SEMEA di Veeam

L'esigenza di rapidi tempi di reazione al mutare del contesto di business, l'accorciarsi dei cicli produttivi, applicazioni sempre più proiettate nel cloud e virtualizzate, hanno portato al centro dell'attenzione dei manager di linea e di conseguenza dei manager IT il tema della business continuity, corollario obbligato all'esigenza della disponibilità di dati e servizi.

L'Availability, sia dei dati che dei servizi, osserva Albert Zammar, Vice President SEMEA di Veeam Software, nel corso del 2016 si è di conseguenza affermata come un concetto con crescente rilevanza nello scenario tecnologico e nel vasto ecosistema

di cui è parte.

I casi di perdite di dati derivanti da interruzioni di business, sia di natura fraudolenta

che a causa di malfunzionamento o disastri ambientali, hanno ulteriormente evidenziato la necessità di poter avere un accesso ininterrotto alle informazioni e ai servizi critici, in particolare quelli di tipo on-demand. Interruzioni di servizi e relativi danni economici anche di ampia natura, con profondi impatti anche sui servizi sociali verificatesi in ambito internazionale e nazionale, quest'ultimi in ambienti ospedalieri e aeroportuali, suggeriscono ai responsabili aziendali, osserva Zammar, di focalizzarsi in efficaci adeguamenti dell'IT.

Adeguamenti che permettano di assicurare un'erogazione interna o a terzi dei servizi che costituiscono il proprio portfolio, sia al fine di evitare perdite economiche anche gravi, riduzione del fatturato, disaffezione dei clienti o la riduzione di reputazione del proprio marchio.

Ma quali sono i temi chiave da considerare che Zammar suggerisce di porre al centro della propria agenda nei prossimi mesi? Per soddisfare le aspettative di clienti e partner sono fondamentalmente quattro.

Il confluire di cloud pubblico, privato e ibrido

Solo qualche anno fa, il pensiero di espandere un'infrastruttura di data center verso il cloud ibrido-pubblico era il più delle volte ritenuto uno sforzo inutile, per la connettività, la sicurezza e un insieme di sorprese sconosciute a cui si riteneva si sarebbe andati incontro.

La realtà ha fugato molti se non tutti i dubbi, legittimi o prudenziali, ed ora il mercato è pronto all'adozione di architetture di cloud ibrido sia per le infrastrutture che per le applicazioni. Molte aziende hanno già intrapreso questa strada con risultati positivi, ma è prevedibile che nel 2017 questo avverrà ancora di più in quanto le imprese possono trovare nel cloud un modo rapido per migliorare la loro agilità e affidabilità operativa, assicurando che i dati e le applicazioni siano disponibili in qualsiasi momento e fruibili da qualsiasi luogo.

Infrastrutture software-defined

Il concetto di architettura a livelli e di separazione tra piano di controllo e piano fisico è di lunga data e risale agli albori prima della commutazione telefonica digitale e poi,



con il modello OSI, del networking a commutazione di pacchetto e delle grosse reti internazionali. Ora è approdato nell'IT.

È oramai universalmente assodato che il data center software-defined costituisce un grande trend degli ultimi anni, conseguenza della impetuosa diffusione della virtualizzazione. Eseguire le applicazioni in un ambiente virtualizzato comporta diversi vantaggi per l'azienda e facilita la costruzione di un'infrastruttura IT più efficiente, affidabile e flessibile, semplificando allo stesso tempo la gestione di tempo e risorse.

Con l'evoluzione delle aziende bisogna aspettarsi l'incremento delle richieste ai vendor di fornire software e servizi che soddisfino le aspettative della prossima generazione di innovatori.



Sicurezza: anticipare gli hacker

È inutile cullarsi nei sogni. La realtà è che nel 2017 le minacce informatiche, come l'incremento de botnet e malware e in particolare dei ransomware, tormenteranno ancora la vita e le notti degli IT manager.

Durante il 2016, mantenere l'availability è stata una delle esigenze prioritarie per l'azienda, alla luce dei numerosi attacchi ai servizi DNS che hanno provocato interruzioni dell'attività delle imprese e dei loro servizi nei momenti più delicati. La realtà è che con l'aumento dei nuovi servizi digitali aumenteranno anche gli attacchi hacker. Le aziende dovranno aumentare la sicurezza sui dati end-to-end, sul backup e sul ripristino per assicurare che i loro servizi rimangano sempre disponibili ai partner ed ai clienti.

Più dati, più business

Quello dei dati, di come raccogliarli, conservarli, proteggerli e fruirne è uno dei temi più caldi che si prospettano per l'anno iniziato. Il dato di fatto è che i data center odierni, e ancor più quelli futuri, conterranno sempre più dati sia mission-critical che con finalità di archivio.

Che si tratti di un afflusso di dati derivanti dall'Internet of Things, da sistemi aziendali sempre più complessi, o da crescenti quantità di set di dati già esistenti, la conclusione è ovvia, osserva Zammar: i dati sono destinati ad aumentare.

Il lato positivo della cosa è che questo fenomeno sarà un bene per le imprese che cercano di affinare le proprie analisi avanzate per migliorare le operazioni esistenti e fornire nuovi servizi ai propri clienti.

In sostanza, le aziende saranno in grado di acquisire sempre più insight sui dati che hanno salvato e ciò le aiuterà a prendere decisioni migliori e ad affinare la propria strategia di business.

L'aspetto da considerare è però che per le aziende che si affidano ad analisi avanzate prima di effettuare operazioni, il downtime non solo diminuisce l'abilità di confrontarsi con i clienti e fornitori, ma ostacola anche un processo consapevole di decision-making.

Le aziende devono quindi puntare sul mantenimento dei sistemi mission-critical che sostengono le loro analisi.



Qlik e Vodafone per la data security nell'automotive

Esperti di settore, clienti e partner di Qlik, hanno avuto modo di incontrarsi e confrontarsi durante la giornata milanese di Visualize Your World, l'evento annuale firmato dall'azienda che, in soli due mesi, ha toccato oltre trenta città in America, Asia Pacifico, Europa, Medio Oriente e Africa. Qlik sviluppa l'omonima piattaforma di visual analytics centrata sull'utente e, attraverso un'offerta di soluzioni basate su cloud e on-premise, l'azienda americana fornisce servizi che spaziano dal reporting all'analisi visuale self-service, fino alle analitiche guidate, integrate e personalizzate, indipendentemente da dove risiedono i dati. L'evento ha avuto come pro-

L'IoT avanza e conquista anche le auto. Antonio Carlini, head of architecture & process optimization di Vodafone Automotive illustra le novità per la gestione sicura dei dati acquisiti a bordo degli autoveicoli



Antonio Carlini, head of architecture & process optimization, Vodafone Automotive

tagonisti esperti di settore, partner e clienti di Qlik tra cui Vodafone Automotive. Nell'attuale contesto orientato all'IoT, gli autoveicoli sono sempre più spesso dotati di sistemi in grado di acquisire e gestire

dati relativi al guidatore e alle modalità di guida. Vodafone Automotive è una tra le aziende che stanno sviluppando soluzioni per garantire una gestione ottimizzata e sicura di questi dati grazie anche alle soluzioni di Qlik.

Antonio Carlini, head of architecture & process optimization di Vodafone Automotive, delinea un quadro di quelle che saranno le novità in tema di sicurezza e gestione dei dati acquisiti a bordo.

Quale strategia adotta Vodafone Automotive per tutelare al meglio i dati dei propri clienti e sfruttarli in modo proficuo?

La tematica è affrontata con la piena consapevolezza che deve coprire l'end-to-end del servizio. All'interno del Gruppo siamo, infatti, la società specializzata nella co-

pertura di servizi telematici per l'automotive, spaziando dall'elettronica installata a bordo delle vetture a tutto ciò che è più strettamente legato alla tematica delle Telco e, di conseguenza, alla trasmissione del dato fino all'elaborazione dello stesso. Il tutto con lo scopo di costruire un insieme di servizi in grado di poter soddisfare le esigenze di aziende automobilistiche, compagnie assicurative e gestori di flotte.

Un livello di copertura che, dunque, si estende a tutto tondo?

La sicurezza deve coprire l'intero ciclo del dato. A partire dalla sicurezza stessa del mezzo. Questo, perché noi gestiamo dati di localizzazione e dati che attestano il comportamento tenuto dal guidatore dell'auto. Tutti elementi fondamentali per le compagnie assicurative e i gestori di flotte che sono in grado di parametrare tariffe e servizi in base ai dati raccolti da Vodafone Automotive.

Chi guida viene informato di tale monitoraggio?

Certamente. Viene sempre messo al corrente ed è lui che ci autorizza, con la sot-

toscrizione di un modulo di privacy, a raccogliere, elaborare e fornire i dati raccolti alle società esplicitamente indicate.

In relazione all'IoT quali sono le direzioni di evoluzione?

Le evoluzioni, in tal senso sono molte. Basti pensare che l'auto reca a bordo dati ai quali, spesso, non pensiamo. Banalmente la rubrica telefonica o i contenuti multimediali che vengono sincronizzati con l'auto. Tutto questo fa emergere tematiche delicate, come la gestione e i diritti legati a questi contenuti. A breve, inoltre, sarà possibile caricare e utilizzare altri contenuti, come messaggi mail o altre forme di collaboration "on board". Proprio per questo, il sistema di trasporto dell'informazione è uno dei punti di forza di Vodafone, che collabora, da tempo, con organismi internazionali a difesa della community. Nello specifico, usiamo una connettività machine-to-machine che, per come è realizzata, è in grado di offrire una serie di misure cautelari a tutela della trasmissione dei dati che sono di gran lunga superiori alla normale connettività dati per l'utenza consumer.

A livello di elaborazione dati, quali garanzie potete offrire?

Noi prevediamo segregazione del dato per le diverse tipologie di elaborazione e tutte quelle misure che garantiscono la sicurezza di accesso al dato attraverso autenticazioni, autorizzazioni, securizzazione dei canali b2b e trasmissione del dato verso i partner business che vogliono integrare i loro dati con quelli elaborati da noi. Tutti questi aspetti sono stati oggetto di policy specifiche, che regolamentano tutte le operazioni: dall'analisi, allo sviluppo fino alla "veritazone" del dato. La soluzione è operativa nei nostri data center, quindi è offerta come soluzione in cloud, interamente gestita da Vodafone con tutte le relative certificazioni - delle quali siamo dotati - per garantire il servizio offerto.

Quindi è fondamentale predisporre un sistema di collaborazione fattiva tra le diverse figure coinvolte nel processo?

Corretto. È necessario che tra Vodafone, la casa automobilistica e la compagnia assicurativa sussista una collaborazione che possa

portare a una gestione condivisa dei dati per la parte di competenza di ciascuno e per i fini che ogni attore, che interviene nel processo, desidera conseguire.

Qual'è lo stato dell'arte relativo alla scansione antivirus e all'aggiornamento del sistema operativo della vettura?

L'aumento dei dati presenti sulla vettura richiede e richiederà presto un aggiornamento sempre più frequente, proprio come quello che siamo abituati a fare con l'antivirus sul computer. Dovrà diventare una pratica frequente per garantirci la

dovuta sicurezza. Dal punto di vista operativo, gestire la sicurezza, significa implementare le policy aziendali. Sicurezza gestita, per un'azienda come la nostra, è tutta l'intera collaborazione che si ha, anche, con gli organismi internazionali come gli enti regolatori e le forze di sicurezza, visto che come azienda gestiamo una rete di security operation center che ha un'ampia diffusione territoriale. Siamo presenti in oltre 40 Paesi e, in ciascuno di questi, abbiamo accordi locali con le forze dell'ordine territoriali per gestire le tematiche legate alla sicurezza dell'auto.

C'è una sfida vinta di recente o un obiettivo tra le priorità, a breve termine, di Vodafone Automotive?

Diciamo che una sfida, già in parte vinta e un obiettivo dei prossimi mesi, è quello di portare in un numero significativo di Paesi - prevalentemente europei - una gamma di servizi in grado di coprire tutti i segmenti di business di questo mercato.

Oggi, infatti, siamo presenti in quarantaquattro Paesi, ma in modo disomogeneo. Il nostro obiettivo è quello di riuscire a coprire uniformemente car maker, compagnie assicurative e gestori di flotte aziendali. ❁



SPECIALE

IDENTITÀ E ACCESSO ALLE APPLICAZIONI ALLA BASE DELLA DIGITAL TRANSFORMATION

Per il secondo anno di seguito, la società di ricerca Gartner rileva un calo a livello mondiale nelle vendite di dispositivi mobili, in termini di unità, prevedendo un periodo di stagnazione, destinato a durare almeno per i prossimi cinque anni. Fanno eccezione i device di fascia alta, i cosiddetti "premium ultramobile", ma la realtà è che il boom dei dispositivi mobili sembra essere finito, anche perché, agli analisti, non convincono gli sviluppi sul fronte dei wearable, considerati da Gartner poco più che gadget di cui ci si annoia rapidamente. I device mobili, pur in un mercato di sostituzione, restano il tramite principale per la digital transformation, il cui fronte dell'innovazione si sposta sul software e sui servizi..

pag. 8

CYBER ATTACK

LE PRINCIPALI MINACCE PER L'INTERNET OF THINGS

Il Threat Analysis Report promosso dagli F5 Labs in collaborazione con Loryka, evidenzia come le armi più recenti utilizzate dai cybercriminali si basino sull'esplorazione delle debolezze nell'utilizzo di Internet. L'Internet delle cose (IoT) fornisce un ambiente in cui i sistemi e le appliance sono integrati sempre più, senza discontinuità.

pag. 6

SOLUZIONI

LA SECURITY FABRIC DI FORTINET ORCHESTRA I FIREWALL

Le imprese non presentano più il tradizionale perimetro aziendale protetto dai firewall come ultimo baluardo. Attraverso il framework Fortinet Security fabric, l'azienda di sicurezza fa evolvere la logica dell'integrazione estendendo a tutti i sistemi di sicurezza le capacità di protezione centrali e le informazioni d'intelligence per rispondere all'evoluzione della digital economy.

pag. 16

IN QUESTO NUMERO:

OPINIONE

pag. 2

- L'importanza dell'accesso

CYBER ATTACK

pag. 3

- La cyber security nel 2017

pag. 6

- Quali sono le principali minacce per l'Internet of Things?

SPECIALE

pag. 10

- Identità e accesso alle applicazioni alla base della Digital Transformation

pag. 14

- L'application security al centro della protezione aziendale

SOLUZIONI

pag. 16

- La security fabric di Fortinet orchestra i Firewall

pag. 19

- Raiffeisen sceglie Vasco per il banking online sicuro

Tutti concordano sulla centralità delle identità digitali nella lotta alle violazioni informatiche. È ormai chiaro, infatti, che i danni maggiori sono quelli causati dagli attacchi mirati, la maggior parte dei quali cominciano con una e-mail di spear phishing finalizzata a ottenere delle credenziali di accesso e con quelle entrare nel sistema per poi proseguire l'attacco con ulteriori fasi.

L'importanza di controllare gli accessi è sottolineata anche nelle previsioni dell'RSA Conference Advisory Board, un insieme di massimi esperti sulla sicurezza, che vedrebbe di buon occhio l'eliminazione delle password, considerate appunto uno dei maggiori punti deboli in molte organizzazioni. Ma il vero anello debole sull'accesso è rappresentato dall'Internet of Things o Everything che dir si voglia: una quantità potenzialmente devastante di dispositivi privi di una sicurezza seria, che possono facilmente essere inseriti in una botnet, consentendo attacchi DDoS immisurabili. Proprio il controllo degli accessi è indicato dagli esperti come la strada principale per cercare una soluzione o, quantomeno, metterci una pezza. A tal proposito, sarà il patching il vero protagonista in tema di IoT nel 2017. Per i suddetti motivi abbiamo dedicato l'intero speciale all'Identity e Access Management, aperto da una sintesi dello studio: "The Security Imperative: Driving Business Growth in the App Economy", realizzato a livello mondiale da Coleman Parkes per conto di CA Technologies.

Innanzitutto qualche buona notizia che riguarda proprio il nostro Paese, protagonista, per una volta di molti record europei proprio in tema di sicurezza. Sembra che la consapevolezza dei rischi stiamo aumentando e con essa l'idea che la sicurezza possa aiutare lo sviluppo del business, fosse solo perché aumenta la reputazione delle imprese.

Occorre comunque cambiare l'approccio, come avvisano i responsabili di F5 Networks e quelli di Fortinet, dei quali analizziamo le ultime soluzioni, non a caso, con un accento sulla protezione dell'accesso, delle applicazioni e delle identità.

Security & Business 40 novembre-dicembre 2016

Direttore responsabile:
Gaetano Di Blasio

In redazione:
Riccardo Florio, Giuseppe
Saccardi, Paola Saccardi,
Daniela Schicchi

Grafica: Aimone Bolliger

Immagini: dreamstime.com
www.securitybusiness.it

Editore: Reportec srl
Via Marco Aurelio 8
20127 Milano
tel. 02.36580441
Fax 02.36580444
www.reportec.it

Registrazione al tribunale
n.585 del 5/11/2010

Tutti i marchi sono
registrati e di proprietà
delle relative società

L'Advisory Board della RSA Conference azzarda alcune previsioni sull'anno a venire che porterà alcune evoluzioni sul fronte organizzativo di Gaetano Di Blasio

Todd Inskip, Principal e Commercial Consulting at Booz Allen Hamilton, in preparazione del prossimo appuntamento con l'RSA Conference, previsto a metà febbraio a San Francisco, ha sollecitato i membri dell'Advisory board della manifestazione (RSAC), di cui fa parte, per fornire alcune chiavi di lettura sugli eventi che hanno caratterizzato il 2016 e che "oscurano" il 2017 e formulare delle previsioni sull'immediato futuro.

Cyber War

Sotto i riflettori le elezioni statunitensi, che hanno portato sulla ribalta le serie problematiche legate alla potenza della rete come cassa di risonanza ed efficace strumento d'ingerenza nelle vicende di nazioni straniere.

Senza Donald Trump, l'attacco a Yahoo avrebbe monopolizzato il dibattito sulla sicurezza informatica e, invece, il primo membro dell'RSAC Board a esprimersi, Dmitri Alperovitch, cofondatore e CTO of CrowdStrike, sottolinea come la campagna per le presidenziali sia stata combattuta con il massiccio ricorso alle intrusioni informatiche.

Un segno dei tempi, certo, ma anche il prodromo



di un nuovo fronte di battaglia, più violento perché nascosto. Secondo Alperovitch la "Cyber War" porterà gli attacchi informatici sempre più nell'occhio del ciclone, diventando uno strumento come altri e innescando meccanismi di risposta che non potranno, o non dovrebbero, rimanere confinati nel "cyber-spazio", ma allargarsi a comprendere interventi diplomatici, modifiche legislative, azioni economiche. Al riguardo, Ed Skoudis, fondatore di Counter Hack, evidenzia come hacker e politici si siano sempre scontrati, ma anche che i partiti guardano con interesse alle potenzialità dell'hackeraggio" come strumento d'opposizione politica. Se in passato erano gli eserciti ad accrescere il Cyberwarefare, oggi

sono le organizzazioni politiche a cercare risposte nel deep blue.

Per questo afferma, Skoudis, è necessario che le organizzazioni siano più consapevoli dei rischi che corrono sulla rete e su come contrastarli, così pure su come affrontare false campagne, pro o contro qualcosa, realizzate impiegando bot e troll. Ma al tempo stesso gli organi politici andrebbero sottoposti agli stessi regolamenti imposti a tante altre organizzazioni, prime fra tutte quelle aziendali. Non a caso, in Italia, l'orientamento politico è già considerato un dato sensibile, secondo il Garante della Privacy. Anche le organizzazioni governative dovrebbero considerare di espandere la protezione dei dati a settori apparentemente meno strategici, anche in previsione del boom sui big data, che rischiano di diventare sia uno strumento per gli attacchi sia una miniera di dati da rivendere.

La sicurezza che arriva nei CDA

Il lato positivo, sostiene Wade Baker, un consulente indipendente, cofondatore di Cyentia Institute, è che questi attacchi e la loro eco mediatica aumentano la cultura sulla sicurezza, più degli attacchi alle grandi organizzazioni. Il che è importante perché il consulente ritiene che non solo queste minacce continueranno, ma coinvolgeranno sempre più anche le piccole e medie imprese e i consumatori. Peraltro, Baker concorda che le grandi imprese sono quelle verso cui si concentreranno gli attacchi su larga scala, che, sfruttando il supporto dei DDoS, potranno portare a danni oltre il miliardo di dollari.

Le piccole e medie imprese subiranno attacchi "adeguati" alle loro possibilità: le organizzazioni cyber criminali, infatti, sempre più sapranno calcolare il limite del danno, come per il ransomware, nei cui attacchi il riscatto, non a caso, è quasi sempre abilmente fissato a una cifra leggermente inferiore al costo di ripristino.

Non a caso ci si aspetta che il 2017 possa essere l'anno in cui diventerà "normale" che i rapporti sugli attacchi informatici arrivino nei consigli di amministrazione.

Ma sarà necessario andare oltre, perché, sottolinea Inskeep, «ogni responsabile della sicurezza informatica informa il proprio cda con messaggi e vie di comunicazione differenti, mentre sarebbe opportuno arrivare a una qualche forma di standardizzazione, anche per dare un chiaro e immediatamente comprensibile scenario della situazione relativa alla sicurezza e ai rischi informatici».

L'Internet of Things e il controllo degli accessi

L'Internet delle Cose sarà sempre più un tema centrale per la sicurezza tanto che Benjamin Jun, Ceo di HVF Labs, avverte: «Un giorno ci volteremo a guardare gli attacchi DDoS del 2016 nello stesso modo in cui oggi guardiamo gli attacchi di defacement protagonisti a fine anni Novanta».

Jun precisa: «Il proliferare di dispositivi d'ogni genere, l'uso di connessioni senza un pairing WiFi manuale (pensate a un utilizzo di AirDrop per qualsiasi collegamento) e i danni fisici, che potrebbero

derivare da un guasto a un dispositivo, rendono estremamente accidentata la strada dell'IoT. Non basterà ricorrere al patching dei dispositivi».

I piccoli firewall e router installati in case e uffici di tutto il mondo sono a rischio e, secondo Jun, la soluzione deve concentrarsi sul controllo dell'accesso. È d'accordo Wendy Nather, Research Director di Retail Cyber Intelligence Sharing Center, che paragona il rischio a una catastrofe nucleare: «Stiamo andando verso un "botnet fallout", reso possibile dall'impressionante numero di dispositivi IoT che potranno essere inseriti in una botnet e dall'incapacità dei consumatori ad aggiungere sicurezza nei loro device».

Eventuali interventi legislativi potranno, forse, essere efficaci solo nel lungo periodo, dopo che i danni alla collettività renderanno chiaro a produttori e consumatori quanto sia importante la sicurezza informatica.

Già nel 2016 si sono misurati attacchi DDoS record, ma andrà solo peggio, secondo Skoudis e dopo ogni attacco si dovrà intervenire sui dispositivi per "carrozzarli": «Il 2017 sarà l'anno dell'IoT "Total Recall"».

Nuove generazioni

Alperovitch vede positivo, pronosticando che un lento progressivo cambiamento si sta verificando da tempo in molte organizzazioni, in particolare le Fortune 500, ma altre seguono l'esempio. Un cambiamento che vede le imprese cambiare l'approccio alla sicurezza e dismettere soluzioni legacy ormai obsolete. Un cambiamento filosofico, afferma

Alperovitch: «Le imprese non pensano più a se saranno attaccate, ma a quando ciò accadrà»

Questo porterà probabilmente a strategie di incident response, ma, intanto, si osserva l'adozione di soluzioni per la sicurezza di nuova generazione, basate sul machine learning e sull'advanced behavioral analytics.

Un passo avanti nella sicurezza sarebbe, secondo alcuni, a cominciare dalla Nather, l'eliminazione delle password, troppe delle quali sono deboli e causa dei principali problemi. Ma tutto l'RSA Conference Security Board concorda che nel 2017, che nel 2017, anche se qualcuno tenterà, nessuno riuscirà a eliminarle.

Dei cambiamenti, invece, ci saranno sul fronte del DevOps. «Molte delle figure responsabili della sicurezza usciranno dagli incarichi vincolati alle logiche del DevOps e torneranno a ruoli operativi tradizionali», sostiene Jun, spiegando: «Gli sviluppatori avranno ancora responsabilità enormi per la sicurezza, ma il deployment della sicurezza richiede osservazione, messa a punto dei sistemi e rilevamento, compiti che sono svolti meglio dai ruoli tradizionali delle operation. Aiuterà, inoltre, una maggiore standardizzazione della terminologia e dei profili professionali. Mentre, dal punto di vista tecnologico, un supporto alla sicurezza arriverà dai nuovi ambienti virtualizzati e dal Software Defined Networking o, più in generale, da strumenti di sicurezza automatizzati che consentiranno anche a tecnici non esperti di sicurezza di monitorare i rischi sui sistemi in produzione.

QUALI SONO LE PRINCIPALI MINACCE PER L'INTERNET OF THINGS?

Il Threat Analysis Report fa luce sulle dinamiche sfruttate dagli hacker

di Paul Dignan, global technical account manager di F5 Networks

Gli oggetti nella nostra vita sono sempre più complessi; l'aumento dei dispositivi intelligenti e la crescente dipendenza dalle applicazioni porta oggi i criminali informatici a sfruttare sempre più le vulnerabilità online. Nel recente Threat Analysis Report promosso dagli F5 Labs in collaborazione con Loryka, appare evidente come le armi più recenti utilizzate dai cybercriminali si basino sull'esplorazione delle debolezze nell'utilizzo di Internet e come solo l'intelligent data science, oggi, possa permettere di comprendere le dinamiche dei nemici online e aiutare le aziende a superare in astuzia il crimine informatico.

L'Internet delle cose (IoT) fornisce un ambiente in cui i sistemi e le appliance sono integrati sempre più, senza discontinuità. La produzione diventa sempre più intelligente e le nostre abitazioni contengono, ormai, beni di consumo sofisticati che ci aiutano a gestire la nostra vita di tutti i giorni. Molti però si dimostrano estremamente vulnerabili alle frodi online.

*Paul Dignan,
global technical account
manager di F5 Networks*

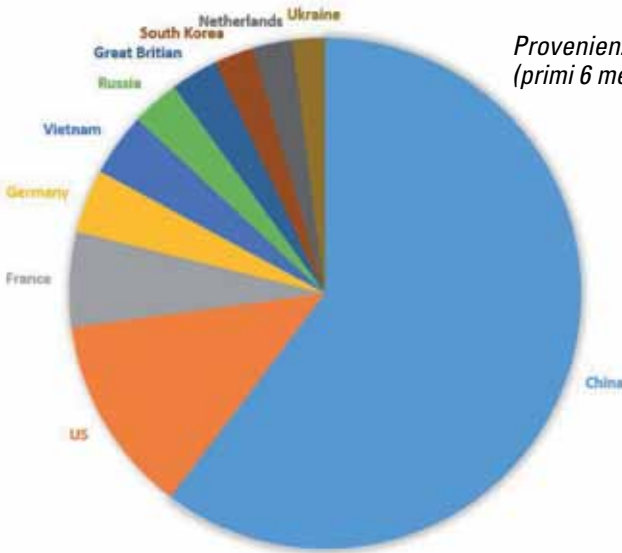


Sfruttare le debolezze

Il Threat Analysis report mette in evidenza che qualsiasi dispositivo connesso online è soggetto a debolezze e presenta vulnerabilità che possono essere sfruttate. Appare preoccupante come i dispositivi e i software dell'IoT non siano mai stati progettati pensando alla sicurezza; se da una parte i produttori degli oggetti IoT affrontano fin dall'inizio una concorrenza forte, cercando di assumere un ruolo guida sul mercato, la sicurezza da loro è spesso affrontata semplicemente come un ripensamento, una soluzione a posteriori, che rende quindi i dispositivi connessi a Internet strumenti ideali al servizio degli hacker. Entrando nello specifico nell'analisi delle minacce, non sorprende notare come i Paesi leader nel mondo come Stati Uniti, Canada e molti membri della UE, continuino a rappresentare gli obiettivi monetari più interessanti per gli hacker in virtù della solidità delle proprie realtà finanziarie.

Per questo motivo, il malware oggi si rivolge, in primo luogo, al settore finanziario, aumentando in modo significativo le sue varianti dopo il rilascio di Zeus, un pacchetto malware Trojan horse che nel 2011 venne eseguito su diverse versioni di Microsoft.

Provenienza degli attacchi telnet "brute force" verso dispositivi IoT (primi 6 mesi del 2016)



Un'altra tendenza riscontrata nel report è l'utilizzo degli attacchi Telnet-based, che stanno diventando sempre più popolari tra gli hacker. Telnet, un protocollo TCP/IP per l'accesso remoto ai computer, che consente a un amministratore o a un altro utente di accedere a computer di qualcun'altro da remoto. Gli esperti di data science hanno conteggiato 2.174.216 attacchi Telnet in sei mesi, provenienti da una vasta gamma di indirizzi IP. Le scansioni Telnet sono un vettore di attacco in forte crescita con un incremento del 140% da luglio 2015 al 2016.

Tenere il passo con gli hacker

L'immagine stereotipata di un criminale incappucciato, forse, è solo un mito; il profilo degli hacker catturati varia da individui solitari a piccoli gruppi i cui interessi spaziano dalle frodi finanziarie, al furto di identità fino agli attacchi di tipo "ransom". Comprendere il comportamento degli hacker e mantenere le aziende aggiornate sulla tecnologia è fondamentale per ridurre l'impatto del crimine informatico. L'analisi dei laboratori F5 Lab comprende dati in tempo reale, per svelare l'attività dei "cattivi virtuali" e smascherare il malware impiegato, in modo da mitigare gli attacchi rivolti alle organizzazioni.

Gli specialisti di sicurezza sono come dei medici dei dati, che a partire dai dati sono in grado di diagnosticare i problemi attraverso un monitoraggio rigoroso degli eventi e delle minacce.

I dati sono il gioiello incastonato nella corona nell'economia application-driven e rappresentano quindi l'obiettivo principale degli hacker. In questo contesto, è interessante notare che il Threat Analysis Report ha evidenziato come alcune botnet IoT di recente abbiano attaccato diverse agenzie di stato degli Stati Uniti sfruttando 52mila indirizzi IP univoci. Se il commercio è diventato sempre più rapido e digitale, è il mondo virtuale a divenire un fattore importante per la gestione delle risorse aziendali. Per i criminali informatici, tuttavia, gli ambienti multipli e i big data rappresentano un incentivo a sfruttare le debolezze nella sicurezza dei dispositivi IoT e nelle infrastrutture di sicurezza di un'organizzazione. Pertanto, gli esperti devono tenere le minacce sotto stretta osservazione e mantenersi in prima linea nello sviluppo di prodotti che rafforzino la sicurezza, le prestazioni e la disponibilità delle applicazioni, in modo che le aziende possano accedere in modo sicuro al cloud in qualsiasi momento. Un ultimo aspetto deve essere ricordato: l'IoT e la sicurezza delle applicazioni stanno cambiando profondamente lo scenario di rischio. La sicurezza online di un'azienda oggi si basa sulla capacità di unire persone preparate e tecnologie intelligenti. Entrare nella mente di un hacker comporta soluzioni di intelligent qualificate ed esperti di data science in grado di aiutare gli utenti e le aziende a evitare di essere raggirati.

SPECIALE

IDENTITÀ E ACCESSO ALLE APPLICAZIONI



ALLA BASE DELLA DIGITAL TRANSFORMATION

La spinta innovativa si concentra su applicazioni e servizi digitali: cresce l'app economy e migliora la sicurezza, soprattutto in Italia secondo Coleman Parkes

di Gaetano Di Blasio

Per il secondo anno di seguito, la società di ricerca Gartner rileva un calo a livello mondiale nelle vendite di dispositivi mobili, in termini di unità, prevedendo un periodo di stagnazione, destinato a durare almeno per i prossimi cinque anni. Fanno eccezione i device di fascia alta, i cosiddetti "premium ultramobile", ma la realtà è che il boom dei dispositivi mobili sembra essere finito, anche perché, agli analisti, non convincono gli sviluppi sul fronte dei wearable, considerati da Gartner poco più che gadget di cui ci si annoia rapidamente.

I device mobili, pur in un mercato di sostituzione, restano il tramite principale per la digital transformation, il cui fronte dell'innovazione si sposta sul software e sui servizi.

È qui che la sicurezza gioca un ruolo fondamentale, anche in considerazione del fatto che il furto delle identità è tipicamente il primo passo negli attacchi mirati e/o dei cosiddetti Advanced Persistent Attack (APT).

Proprio in Italia, peraltro, si registra una crescita della consapevolezza sui rischi alla sicurezza, registrata dallo studio "The Security

45%



le aziende italiane che hanno registrato una diminuzione delle violazioni di dati

88%



i manager italiani per i quali la sicurezza incentrata sull'identità è cruciale per il business aziendale

Imperative: Driving Business Growth in the App Economy", realizzato a livello mondiale dalla Coleman Parkes per conto di CA Technologies.

La sicurezza aiuta la crescita aziendale

La ricerca ha interessato manager e responsabili della sicurezza in Italia, dove, tra le nazioni dell'area Emea (Europe, Middle East e Africa), viene osservato un primato: la maggior riduzione delle violazioni dei dati negli ultimi dodici mesi. Più precisamente, la quota di aziende italiane che hanno registrato tale diminuzione è stata il 45%.

Secondo i dati concernenti l'Italia, estrapolati dai manager di Ca Technologies, il 67% delle imprese italiane intervistate ha adottato un approccio predittivo e/o proattivo per contrastare le violazioni. Anche questo è un dato superiore al resto del campione e principale fattore del primato. Quest'approccio, infatti, costituisce un presupposto fondamentale per realizzare una strategia di sicurezza informatica incentrata sull'identità digitale.

Proprio quest'ultima rappresenta il nuovo perimetro aziendale, in un contesto caratterizzato da mobility, hybrid cloud, aziende distribuite e supply chain integrata, il vecchio concetto di perimetro legato alla protezione della rete non corrisponde al rischio per la sicurezza: secondo dati relativi agli Stati Uniti diffusi da F5 Networks, il 72% degli attacchi è

indirizzato verso identità e applicazioni. Gli italiani sembrano averlo capito, visto che la larga maggioranza di loro (l'88%, cioè la percentuale più alta fra tutti i Paesi Emea) ritiene che la sicurezza incentrata sull'identità sia cruciale per il business aziendale. Ma non solo, perché, sempre secondo l'indagine realizzata dalla Coleman Parkes, la maggior parte dei responsabili italiani intervistati sostiene che la sicurezza informatica non possa limitarsi a salvaguardare i dati e l'infrastruttura a supporto del business, ma debba anche servire a instaurare fiducia nella relazione tra aziende e clienti, elemento essenziale per guadagnare competitività ed espandere il giro d'affari nell'odierna application economy.

In particolare, il 91% delle aziende italiane interpellate (percentuale record in EMEA) ritiene che



91%

le aziende italiane per le quali la sicurezza deve proteggere e nello stesso tempo abilitare il business

66%

le aziende che hanno riferito di una maggiore fidelizzazione dei clienti grazie alla maggiore sicurezza

la sicurezza deve proteggere e nello stesso tempo abilitare il business. Inoltre, il 92% degli intervistati (seconda percentuale più alta dopo il Regno Unito) afferma che la sicurezza è un elemento cruciale per tutelare il marchio e che può fungere da importante leva competitiva.

L'attenzione verso l'esperienza digitale, anche e soprattutto mutuata dalle tecnologie mobile, è dimostrata da altri dati, come l'85% (altro record in Emea) dei soggetti intervistati per i quali la sicurezza non deve creare ostacoli o influire negativamente sull'esperienza dell'utente, o, ancora, il 60% dei rispondenti che afferma di utilizzare indicatori quali customer experience, customer satisfaction e customer retention, crescita del fatturato e copertura digitale per misurare l'impatto della sicurezza

sul business aziendale. Chi sta investendo in sicurezza ottiene risultati in termini di business. Lo dimostrano altre risposte raccolte dagli analisti della Coleman Parkes:

- Il 76% del campione ha realizzato un ampliamento della copertura digitale grazie a una migliore implementazione della sicurezza;
- Il 69% ha rilevato un miglioramento della customer experience;
- Il 66% ha riferito di una maggiore fidelizzazione dei clienti;

Inoltre, i responsabili aziendali italiani hanno anche osservato che le iniziative messe in campo nell'ambito della sicurezza informatica hanno contribuito a far aumentare del 35% i ricavi da nuove fonti di business e hanno portato un incremento del 31% nell'efficienza operativa, del 34% nella produttività dei dipendenti e del 33% nella customer satisfaction.

L'importanza di una strategia basata sull'identità

Sono tre i principali fattori cui le organizzazioni del nostro Paese attribuiscono il "record" sul calo delle violazioni: il primo (citato dal 50% dei rispondenti) consiste nella crescita degli investimenti in security; il secondo (41%) è rappresentato dalla maggiore concentrazione delle procedure di sicurezza sulle



92%

i manager italiani che ritengono la sicurezza un elemento cruciale per tutelare il marchio e un'importante leva competitiva

85%

i manager italiani per i quali la sicurezza non deve creare ostacoli o influire negativamente sull'esperienza dell'utente

aree a rischio elevato, quali identità e accessi privilegiati; il terzo (35%) riguarda l'implementazione di nuove funzioni di security specifiche per mobile device e app.

Per lo sviluppo della protezione aziendali, però, la chiave di volta messa in luce da questa ricerca è che per i manager l'obiettivo non è la sicurezza, ma l'interazione con i clienti e la fiducia degli stessi.

Come sottolineano i responsabili di CA, una strategia di sicurezza incentrata sull'identità digitale consente di evitare che le procedure di protezione alterino l'interazione tra azienda e utenti. Questo approccio richiede l'implementazione di controlli adattivi per la gestione delle identità e degli accessi e l'adozione di controlli proattivi e predittivi per la prevenzione e

l'individuazione delle violazioni di dati. In base allo studio, il 24% delle organizzazioni italiane intervistate avrebbe già messo in atto sistemi di controllo di tipo adattivo, il 15% dichiara di aver adottato strumenti e processi di tipo predittivo e il 52% riferisce di utilizzare strumenti proattivi, che analizzano in profondità e reagiscono in tempi reali a eventi e incidenti.

È peraltro possibile riassumere in 7 passi il raggiungimento di una "buona" maturità in termini di sicurezza basata sull'identità:

1. Considerare l'identità digitale come nuovo perimetro aziendale.
2. Trattare la sicurezza come fattore abilitante del business.
3. Instaurare rapporti di fiducia nell'interazione digitale con clienti, partner, fornitori e dipendenti
4. Tutelare le esperienze, non solo i dati.
5. Adottare un approccio adattivo per la gestione delle identità e degli accessi.
6. Agire in modo proattivo e predittivo.
7. Non rinunciare mai alla sicurezza in favore della velocità.

60%

i manager che affermano di utilizzare indicatori quali customer experience, customer satisfaction e customer retention, crescita del fatturato e copertura digitale per misurare l'impatto della sicurezza sul business aziendale

Il ROI dell'identity management

Secondo gli analisti della Coleman Parkes, un elevato livello di adozione della sicurezza incentrata

76%

le aziende che hanno realizzato un ampliamento della copertura digitale grazie a una migliore implementazione della sicurezza

69%

le aziende che hanno rilevato un miglioramento della customer experience grazie alla maggiore sicurezza

sull'identità si ripaga, oltre che con una flessione delle violazioni di dati, anche con un incremento dei ricavi.

Per dimostrarlo, gli autori della ricerca hanno esaminato gli attuali assetti per la sicurezza delle organizzazioni (nell'area Emea) in tre ambiti specifici relativi all'identità: esperienza degli utenti finali, gestione identità/accessi, violazioni di dati. In questo modo hanno realizzato un modello di maturità, classificando i soggetti intervistati in base al livello di utilizzo: avanzato, base o limitato.

La maggior parte dei partecipanti (68%) sono risultati "basic", soprattutto su aspetti essenziali, quali la gestione delle password, il Single Sign-On e alcune funzioni di analisi e reportistica. Il 19% è risultato ascrivibile alla categoria Advanced, poiché in grado di applicare capacità quali la sicurezza adattiva e l'analisi comportamentale e di fornire supporto uniforme alla sicurezza multicanale.

Secondo gli analisti, gli utenti "avanzati" in Emea hanno realizzato miglioramenti significativi rispetto agli utenti Basic negli ambiti della customer experience, dell'operatività aziendale e della security. In particolare, precisano gli autori del report:

- gli utenti avanzati hanno registrato un miglioramento del 34% nella crescita del fatturato e dei nuovi ricavi, contro un 29% degli utenti Basic;

- il 93% degli utenti Advanced, rispetto al 75% degli utenti Basic, ha osservato una maggiore customer retention;
- l'89% degli utenti Advanced ha rilevato un miglioramento della customer experience, contro il 66% degli utenti Basic;
- il 34% degli utenti Advanced ha registrato una riduzione nel numero di violazioni di dati, rispetto al 24% degli utenti Basic.

Metodologia

Coleman Parkes ha intervistato 1.770 responsabili aziendali e IT (fra cui oltre 100 CSO e CISO) di grandi aziende provenienti da 21 Paesi e appartenenti a 10 settori industriali. La raccolta e l'analisi dei dati è stata eseguita nel periodo tra maggio e settembre 2016. Coleman Parkes Research Ltd., costituita nel 2000, esegue su scala mondiale ricerche di mercato incentrate sull'azione. L'azienda offre un servizio completo che prevede l'indagine e la consulenza su tutti i mercati, con una particolare specializzazione per la ricerca business-to-business incentrata su IT, tecnologie e comunicazioni. Per maggiori informazioni, consultare il sito www.coleman-parkes.co.uk.

L'APPLICATION SECURITY AL CENTRO DELLA PROTEZIONE AZIENDALE

Secondo F5 il 72% degli attacchi mira all'identità digitale degli utenti e alle applicazioni, ma il 90% degli investimenti in sicurezza si focalizza sulla protezione di un perimetro che non c'è più

di Gaetano Di Blasio

La sicurezza informatica è tradizionalmente basata sulla protezione del perimetro aziendale, ma quest'ultimo non esiste più o, più precisamente, non è più definibile come un confine tra un esterno insicuro e un interno dove sistemi e dati sono al sicuro. Maurizio Desiderio, country manager di F5 Networks, lo spiega chiaramente tracciando le attività quotidiane di un information worker, che accede alla propria mail e a una serie di applicazioni come cita, per esempio, il dirigente, Office e SharePoint, Dropbox, Concur, ServiceNow, Workday, Webex. Solo alcune delle quali appartenenti alla categoria del cosiddetto "shadow IT", cioè non controllate dall'IT aziendale.

«Tutte attività che non richiedono alcun accesso al perimetro di rete aziendale», continua Desiderio, che poi aggiunge: «Viviamo in un mondo application centric», mostrando i risultati tratti da una recente ricerca svolta negli Usa, secondo la quale oltre il 54% delle aziende utilizza in media più di 201 applicativi. Il 31% conferma di adoperare anche un numero superiore alle 500 applicazioni. I dati sono relativi a 406 rispondenti,

estrapolati da un campione di 3000 interviste in tutto il mondo. Aldilà della rappresentatività statistica, il dato qualitativo è poco confutabile e appare coerente con altre analisi che certificano il massiccio utilizzo di strumenti "esterni" all'azienda, come i device mobili spesso usati con pratiche BYOD (Bring Your Own Device) o il cloud.

«Tutte le aziende, a prescindere dal settore merceologico, erogano servizi tramite applicativi. Le applicazioni sono il cuore dell'azienda e la rappresentano in termini di brand e reputazione sul mercato», evidenzia il manager e il pensiero non può che andare alle app protagoniste della cosiddetta digital transformation.

I processi aziendali, compresi quelli rivolti verso l'esterno, per esempio nelle relazioni con la clientela, si basano sulle applicazioni, che, quindi, «devono essere sempre disponibili, veloci e sicuri», afferma ancora il country manager di F5.

I cyber criminali, hanno da tempo compreso che non è necessario bucare un firewall o eludere un IPS (Intrusion Prevention System), ma può essere più

*Maurizio Desiderio,
country manager di F5
Networks*



Le protezioni integrate di F5



facile ottenere le credenziali di accesso o sfruttare vulnerabilità degli applicativi.

Secondo dati in possesso di F5 solo il 25% degli attacchi informatici è rivolto verso il tradizionale perimetro della rete aziendale, mentre ben il 72% delle minacce mirano alle identità digitali e alle applicazioni per guadagnare un “comodo” accesso. Ciononostante, il 90% degli investimenti per la sicurezza informatica è dedicato alla protezione del perimetro.

Uno squilibrio che va corretto con un cambio d’approccio, spiega Desiderio dopo aver così introdotto l’azienda: «F5 Networks è stata fondata nel 1996. Nel 2015 ha registrato un fatturato di 1,92 miliardi di dollari e annovera tra i suoi clienti aziende di fama mondiale, comprese le prime 10 telco e le prime dieci case automobilistiche».

Di fatto una specialista “storica” di Internet che oggi propone un set completo di soluzioni per la protezione, integrate in un sistema di controllo unico, ideato per fornire l’accesso sicuro di ogni utente, con ogni dispositivo, a qualsiasi applicazione, ovunque essa risieda, spiega il country manager.

Questo comprende soluzioni realizzate grazie alla collaborazione con Microsoft per Azure, come, per esempio, il servizio F5 SharePoint Online, che rende sicuro l’uso di SharePoint da mobile, poiché la directory rimane in azienda e tutto il resto è gestito nel data center di F5.

Come detto, la sicurezza proposta da F5 si concentra

sulla protezione dell’identità e delle applicazioni. Per la prima è necessario poter effettuare controlli incrociati, per esempio sulla posizione dell’utente e sul tipo di dispositivo che sta utilizzando. C’è, ovviamente, differenza se quest’ultimo dispone o meno di un sistema biometrico o di altre funzioni per una strong authentication. Anche la “salute”, cioè lo stato d’aggiornamento del dispositivo, richiede considerazioni adeguate.

Le principali funzionalità comprendono identity e access control, e SSL inspection.

Sul fronte applicativo, F5 dispone di un’ampia gamma di funzionalità, perché non è sufficiente proteggersi solo dalle vulnerabilità. Per questo il portfolio F5 comprende firewall, Web Application Firewall, sicurezza del DNS (spesso preso d’assalto con gli attacchi DDoS), Web Fraud protection.

Come s’intuisce, concentrarsi su accesso e applicazioni sembrerebbe portare a trascurare i controlli tradizionalmente legati al perimetro, come l’antimalware, ma permette di arrivare a controllare il livello 7 della “vecchia” pila OSI. Significa anche realizzare le protezioni nel data center aziendale e anche nel cloud, quando si ha a che fare con l’hybrid cloud, ormai la condizione predominante presso le imprese.

LA SECURITY FABRIC DI FORTINET ORCHESTRA I FIREWALL

Le aziende senza perimetro e alle prese con le nuove minacce devono cambiare approccio aggiungendo intelligenza per una protezione integrata e distribuita

di Gaetano Di Blasio

Le imprese non presentano più il tradizionale perimetro aziendale protetto dai firewall come ultimo baluardo. Attacchi mirati e minacce avanzate hanno mostrato nuove strade per introdursi in azienda con tecniche spesso semplici, che sfruttano la complessità di infrastrutture per la sicurezza obsolete. Occorre un approccio integrato, secondo la visione di Fortinet. I responsabili di quest'ultima pongono l'accento sulle diverse normative imposte da organi nazionali e internazionali, sottolineando come queste comportino spesso lo sviluppo di architetture complesse, che rischiano di essere meno sicure. La soluzione proposta dalla società statunitense si chiama Security Fabric, dove fabric significa "tessuto", spiega Antonio Magoglio, senior manager Systems Engineering Italy. Si tratta di una "fitta trama" che unisce tutti i dispositivi di sicurezza, mettendoli in comunicazione.

Si parla da tempo di sicurezza integrata, ma non sempre soluzioni basate sul best of breed riescono realmente a "lavorare insieme", soprattutto laddove i sistemi SIEM (Security Information Event Manager) devono integrare più console, perdendo la capacità d'intervenire in tempo reale.

«Il mercato della sicurezza vede rallentare la propria crescita, ma noi continuiamo ad aumentare le nostre quote di mercato grazie a un ampliamento del portfolio, anche tramite acquisizioni, ma soprattutto grazie all'integrazione delle soluzioni garantita dall'unità del sistema operativo», afferma Filippo Monticelli, regional director Italy & Malta di Fortinet.

Il framework Fortinet Security fabric evolve la logica dell'integrazione estendendo a tutti i sistemi di sicurezza le capacità di protezione centrali e le informazioni d'intelligence, «per rispondere all'evoluzione della digital economy, che comprendono quelle globali provenienti dai sistemi sparsi nel mondo attraverso il cloud e quelle locali, generate per esempio dalle funzioni di sandboxing e a loro volta distribuite nel cloud», aggiunge Magoglio. In un'impresa moderna senza perimetro, questo significa distribuire immediatamente tutte le funzioni di sicurezza sull'intera rete, orchestrando le attività dei firewall in tutte le sedi aziendali.

Fortinet Security Fabric è compresa nel FortiOS, il sistema operativo dei firewall Fortinet e non presenta costi aggiuntivi, ma semplicemente usata,



*Filippo Monticelli,
regional director Italy &
Malta di Fortinet*

spiega ancora Madoglio, che sottolinea come il framework sia aperto, cioè in grado d'integrare anche soluzioni di terze parti, e scalabile.

Fortinet Enterprise Firewall si basa sulla fabric

Fortinet Enterprise Firewall è una soluzione che opera in sinergia con Fortinet Security Fabric e che abilita una difesa immediata, reattiva e intelligente contro malware e minacce emergenti. Congiuntamente, i due prodotti permettono di realizzare la struttura portante di una robusta infrastruttura di sicurezza della rete aziendale.

Quando Enterprise Firewall rileva un evento lo segnala a Fortinet Security Fabric, che determina quali informazioni dovranno essere condivise in tutta l'azienda. Per esempio, se in una determinata area vengono rilevati dei malware, Security Fabric condivide informazioni di Threat Intelligence con il resto dell'infrastruttura aziendale. Analogamente, quando viene definita una policy in una sezione, Security Fabric la applica contestualmente all'intero dominio.

Per non penalizzare le prestazioni, le funzionalità di personalizzazione flessibile del firewall consentono di adattare la condivisione di quanto connesso alla sicurezza con le esigenze specifiche di un particolare punto dell'organizzazione. Tutti i dispositivi firewall della soluzione Fortinet Enterprise Firewall sono interconnessi tramite Security Fabric.

L'interconnessione ha il duplice scopo di fornire una protezione più efficace e allo stesso tempo di semplificare la distribuzione delle soluzioni per la sicurezza, riducendo l'esigenza di predisporre più punti di intervento e di definire un numero maggiore di security policy.

In pratica, ai fini operativi Fortinet Enterprise Firewall è una soluzione che, tramite un'unica piattaforma, un unico sistema operativo per la sicurezza di rete, una gestione delle policy unificata e una singola console di gestione, fornisce una sicurezza di rete end-to-end atta a garantire una elevata protezione contro le minacce avanzate e gli attacchi mirati.

Le funzioni della soluzione Enterprise di Fortinet

FortiGate Next-Generation Firewall è, come evidenziato, una soluzione con cui Fortinet si è prefissata di perseguire l'obiettivo di assicurare un'elevatissima protezione dalle minacce più avanzate, con prestazioni ultraveloci ma senza per questo rinunciare alla semplicità operativa.

La piattaforma, che opera avendo alle spalle i FortiGuard Labs, fornisce un'ampia serie di servizi integrati. Tra questi: Stateful firewall, intrusion prevention, application control, gestione e autenticazione delle identità di utenti/dispositivi, antimalware, sandboxing, Web filtering, IP reputation, SSL Inspection, VPN IPsec/SSL, networking (LAN, WAN, Wi-Fi), gestione e reporting.



*Antonio Madoglio,
senior manager Systems
Engineering Italy di Fortinet*

Singola console di gestione

Indipendentemente dalla posizione o dalla piattaforma (hardware, virtualizzata, cloud pubblico o ibrido) di distribuzione dei dispositivi Fortinet Enterprise Firewall, la visibilità e il controllo della sicurezza della rete avviene tramite un unico sistema operativo, il FortiOS. Quest'ultimo provvede a consolidare tutti i servizi di rete forniti dalla soluzione e a dare una visibilità a 360° del traffico che sulla rete da una singola console di gestione. Il responsabile, con un solo clic, ha la possibilità di prendere visione del traffico con un'analisi che permette di esplorare cosa avviene per la singola applicazione, il tipo di minaccia, un particolare dispositivo, una determinata nazione e altri parametri di selezione.

Parimenti, per quanto concerne le policy, i responsabili della sicurezza hanno la possibilità di prendere visione del traffico di rete e impostare policy consolidate che includono controlli di sicurezza granulari. Ai fini operativi e del controllo diventa possibile:

- Identificare migliaia di applicazioni diverse con l'ausilio dell'Application Control.
- Impostare policy granulari per diversi tipi di utenti, tramite le funzioni di gestione delle identità incluse nel FortiGate e grazie alla integrazione con AD/LDAP, RADIUS, Exchange e altre fonti.
- Identificare i tipi di dispositivi, con relativi sistemi operativi, usati in rete, senza la necessità di ricorrere a specifici agenti o prodotti aggiuntivi.

- Accelerare i tempi di risposta agli incidenti tramite avanzati strumenti di visualizzazione.
- Ridurre il carico di lavoro amministrativo tramite il supporto di un'ampia gamma di servizi di sicurezza di livello enterprise.

Architettura integrata a elevate prestazioni

Le elevate caratteristiche funzionali e le prestazioni di FortiGate gli derivano dall'essere basato su FortiASIC, un'architettura integrata dedicata che permette di disporre del throughput estremamente elevato e della bassa latenza che lo caratterizzano. L'elevata capacità elaborativa fornita dai processori FortiASIC dedicati permette di effettuare ispezioni approfondite del traffico di nuova generazione e di consolidare sulla medesima piattaforma più funzioni di sicurezza. Agli Asic dedicati si affianca un'architettura software che sfrutta l'elaborazione parallela dei percorsi in modo da ottimizzare le risorse hardware e software ad alte prestazioni che gestiscono il flusso dei pacchetti, in modo da massimizzare le capacità di throughput e ridurre al minimo la latenza.

La famiglia di appliance FortiGate include poi un insieme di piattaforme flessibili che possono essere distribuite sul perimetro, come Next Generation Firewall (NGFW), sul perimetro del data center, come Firewall per data center (DCFw), presso i segmenti interni (ISFW) o presso i siti remoti di aziende distribuite.

RAIFFEISEN SCEGLIE VASCO PER IL BANKING ONLINE SICURO

La grande banca retail della Svizzera implementa la tecnologia Cronto per fornire il massimo livello di protezione contro gli attacchi nel banking online

di Giuseppe Saccardi

Vasco Data Security International ha annunciato che Raiffeisen Switzerland ha implementato la sua tecnologia Cronto per proteggere le transazioni dei clienti di e-banking. Raiffeisen, tra i maggiori gruppi bancari della Svizzera, sta implementando le soluzioni di Vasco per rendere sicure le operazioni di banking online dei suoi 3,7 milioni di clienti. La banca sta sostituendo la scheda di matrici precedentemente utilizzata per la sicurezza delle transazioni. Cronto di Vasco è una soluzione di autenticazione e firma delle transazioni, basata sulla tecnologia PhotoTAN, che consente alle banche di difendersi da attacchi hacker. Un codice a barre criptato composto da punti colorati viene visualizzato sullo schermo del PC del cliente. Il cliente utilizza la fotocamera del proprio telefono cellulare o di un dispositivo palmare prodotto da Vasco per catturare il codice a barre che viene immediatamente decodificato per visualizzare i dettagli della transazione, verificabili così dall'utente.

Gli utenti possono scegliere se utilizzare un'app mobile installata sul proprio smartphone o un dispositivo hardware DIGIPASS con tecnologia Cronto dotato di

Nuova nomina in Vasco

Vasco Data Security, società specializzata in soluzioni digitali, tra cui identità, sicurezza e produttività aziendale, ha annunciato che Scott Clements, in precedenza Executive Vice President e Chief Strategy Officer di Vasco, è stato nominato Presidente e Chief Operating Officer.

Clements è entrato in Vasco nel 2015. In precedenza era in Tyco, dove era stato Presidente dell'area di business Retail Solutions, del valore di un miliardo di dollari, e Chief Technology Officer della società.

una fotocamera integrata per eseguire la scansione del codice a barre colorato. «Grazie alla tecnologia PhotoTAN, nessun cliente ha mai subito la manipolazione di un pagamento», ha dichiarato Thomas Etter, Head of E-banking di Raiffeisen Switzerland. «Inoltre, il feedback dei clienti è stato molto positivo, il che è della massima importanza per noi perché abbiamo sempre all'equilibrio tra praticità per gli utenti e sicurezza». Scott Clements, Presidente e COO di Vasco Data Security ha commentato: «La frequenza e la sofisticatezza degli attacchi nel banking online continua ad aumentare, causando problemi per le banche e i loro clienti. La tecnologia Cronto offre il meglio di entrambi gli aspetti: il più alto livello di sicurezza e la massima comodità d'uso».

SICUREZZA COSTANTE, INTELLIGENTE

E PUOI AVERLA SUBITO.

Le tue aree di vulnerabilità aumentano. I contenuti si moltiplicano.

I cybercriminali sono sempre più scaltri.

Fortinet offre una singola infrastruttura di sicurezza intelligente che protegge la tua rete dalle minacce attuali e future.

Visita www.fortinet.it per maggiori informazioni.

FORTINET®

Sicurezza senza compromessi

Sempre più IoT nel futuro di PTC

L'azienda di software aggiorna il portfolio prodotti, si sposta progressivamente verso un modello di licenza ad abbonamento e sigla un accordo con VMware

La convergenza tra mondo fisico e digitale apre opportunità di business che alimentano la "vision" di PTC, azienda di software pioniera nello sviluppo di soluzioni CAD 3D di tipo parametrico e tra le prime a proporre soluzioni per il Product Lifecycle Management (PLM) basate su Internet. Attualmente l'offerta CAD rappresenta circa il 65% del fatturato di PTC mentre il restante 35% è legato al PLM che è il settore in maggiore crescita. L'azienda sta progressivamente aggiornando e ampliando la propria offerta con soluzioni in grado di rispondere alle più moderne tendenze tecnologiche quali IoT, realtà aumentata e virtuale. Inoltre, PTC si prepara ad affrontare il 2017 in Italia con un rafforzamento sulle componenti del servizio e della customer care. L'introduzione della nuova figura del market manager permetterà all'azienda di comprendere meglio le

Stefano Rinaldi, senior vice president Western Europe Region di PTC



esigenze dei propri clienti e di reagire in modo più rapido alle richieste del mercato, mentre attraverso la presenza di un "journey specialist" PTC si propone di fornire un supporto per guidare i propri clienti nel percorso di programmazione e realizzazione dei propri piani di investimento e nel perseguimento degli obiettivi di business. Novità anche sul versante del canale di vendita, improntato a un modello di tipo ibrido con il rafforzamento delle attività di "co-selling" in cui PTC affiancherà i propri partner nelle operazioni di vendita. L'ampliamento del portfolio di prodotti determinerà anche una corrispondente estensione della base di partner in particolare modo su mercati verticali quali la realtà aumentata.

Spostamento verso un modello ad abbonamento

PTC sta anche spostando progressivamente l'approccio di licensing dei propri software verso modelli ad abbonamento, con l'idea di favorire la scalabilità e rispondere in modo più puntuale alle esigenze dei propri clienti e favorire un più rapido ritorno sull'investimento. Il modello ad abbonamento nel 2015, anno del suo avvio, interessava il 17% delle licenze dei prodotti software dell'azienda e nel 2016 ha rappresentato circa la metà del fatturato di PTC;

gli obiettivi per il 2017 sono di portare la formula in abbonamento al 65% per arrivare nel 2018 a una quota del 85%.

Creo 4.0: funzionalità per un CAD all'altezza delle nuove sfide

Il CAD resta un caposaldo dell'offerta di PTC che, con il recente lancio di un'offerta in modalità Software as a Service, si apre sempre più anche verso il mondo delle PMI.

Il prodotto simbolo del CAD 3D di PTC è Creo di cui è stata appena rilasciata la

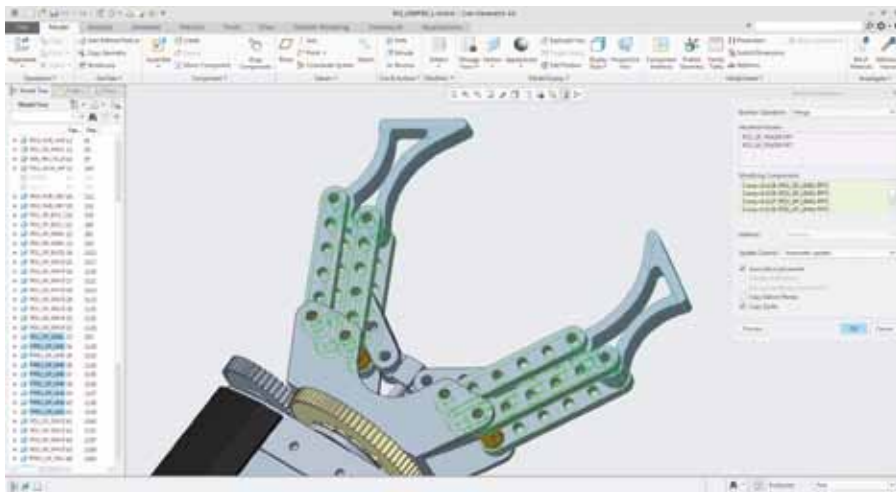
processo di progettazione i dati provenienti da sensori collocati nel mondo reale per predisporre strategie di progettazione finalizzate alla connettività e all'IoT.

La nuova release del software abilita la progettazione per l'additive manufacturing consentendo di ideare, ottimizzare, convalidare ed eseguire la verifica della stampabilità all'interno di un unico ambiente.

Per le applicazioni di realtà aumentata Creo 4.0 permette di riutilizzare i dati CAD per creare facilmente esperienze visive di progettazione coinvolgenti e informative sfruttando la realtà aumentata.

Infine, Creo 4.0 permette ai progettisti di implementare l'MBD riducendo la dipendenza dai disegni 2D, diminuendo gli errori risultanti da informazioni inesatte, incomplete o male interpretate, guidando e istruendo i progettisti nella corretta applicazione delle informazioni sul dimensionamento e sulle tolleranze geometriche.

«La realizzazione del potenziale dell'IoT non si limita all'ottenimento di maggiori dati sull'utilizzo, bensì mette nelle condizioni di



Creo 4.0

versione 4.0 che prevede nuove funzionalità per l'Internet of Things, l'additive manufacturing, la realtà aumentata e il "model based definition" (MBD). Creo 4.0 permette di introdurre nel

poter utilizzare, affinare e analizzare i dati per progettare in modo più efficace e intelligente - ha osservato Stefano Rinaldi, senior vice president Western Europe Region di PTC -. Creo 4.0 permette di sostituire le ipotesi con dati reali per migliorare le decisioni di progettazione; tutto questo, unito alla definizione basata su modelli, consente ai progettisti di ottenere una definizione digitale più completa del prodotto. Oltre ad aumentare la produttività, le novità di Creo 4.0 aiutano a sfruttare l'IoT lungo il percorso di progettazione digitale».

Un accordo con VMware per l'IoT

A rafforzare ulteriormente la posizione di PTC nel mercato IoT giunge la collaborazione con VMware che entrerà a far parte del programma ThingWorx Ready. L'obiettivo della partnership è quello di combinare l'esperienza di VMware nella gestione dei dispositivi e il suo nuovo software per l'IoT denominato Liota, con la piattaforma di application enablement e gli strumenti di

PTC Navigate: 70mila contratti in nove mesi

Nel 2016 PTC ha lanciato PTC Navigate, una soluzione per il mercato del PLM (Product Lifecycle Management) in grado di sfruttare il Web per integrare dati, processi, sistemi aziendali e persone che interagiscono con l'intero ciclo di vita di un prodotto, dall'ideazione, alla progettazione, alla produzione, alla vendita, all'assistenza, fino al suo trattamento di fine vita. Navigate è stata pensata per modificare radicalmente le modalità di accesso alle informazioni rappresentando il prodotto con la più rapida crescita di tutta la storia dell'azienda, con 70mila contratti venduti nei primi nove mesi di commercializzazione.

Questa soluzione disaccoppia il cosiddetto "system of record" dalla componente di visualizzazione e costituisce il primo esempio della capacità di PTC di sfruttare la piattaforma tecnologica dell'Internet of Things denominata PTC ThingWorx. ThingWorx funge da infrastruttura di piattaforma e da strumento di raccolta dati in grado di consentire alle aziende di creare in maniera efficace soluzioni e offerte su larga scala e su misura per i propri settori e aree di competenza. Utilizzando ThingWorx le applicazioni Navigate possono comprendere dati operativi "live" provenienti da prodotti intelligenti e connessi e, in combinazione con Windchill, consentono di superare la rigida suddivisione della gestione del ciclo di vita dei prodotti con un modello di Universal Data Access (UDA) che mette a disposizione in modo semplice i dati di prodotto a tutti i soggetti interessati, non solo agli specialisti.

analisi ThingWorx al fine di consentire agli sviluppatori di soluzioni IoT di accelerare il time to market e di creare nuovi prodotti e servizi compatibili con ThingWorx in tempi rapidi. ❁

D-Link: 30 candeline e 18 anni in Italia

Innovazione, coraggio e futuro. Questi sono alcuni degli ingredienti che hanno decretato un trentennio di successi per D-Link.

Parola di Stefano Nordio, suo vice president

Un orgoglio che fa, giustamente, mostra di sé, quello che ha ispirato le parole di Stefano Nordio, vice president D-Link Europe, in occasione dei festeggiamenti del Gruppo che ha spento le sue prime 30 candeline di attività sul mercato. «30 anni, dei quali 18 passati in Italia» - ha dichiarato Nordio - che ha aggiunto: «Un viaggio impegnativo, quello italiano. Diciotto anni che non sono stati solo uno scorrere del tempo, ma anche un susseguirsi di prodotti, tecnologia e di costruzione di reti all'avanguardia per tutti i target che volevamo raggiungere» Molti successi che sono stati raggiunti anche, e soprattutto, grazie a partnership importanti, come quella siglata, di recente, con Silicon Lab. Una collaborazione che unisce le competenze di D-Link nella

progettazione e nella fabbricazione di dispositivi di rete consumer, la sua conoscenza del mercato e il suo affermato ecosistema di prodotti per la smart-home "mydlink home", con il know-how di Silicon Labs nello sviluppo di semiconduttori e di moduli innovativi, sfruttando tecnologie essenziali per la rete wireless della casa connessa e dell'Internet of Things, come ad esempio ZigBee, Thread, Bluetooth a bassi consumi e rete wi-fi.

Numeri che fanno la differenza

Un quadro ancora più preciso è quello che ha delinato Luigi Salmoiraghi - sales & marketing director Southern Europe & UKI - che ha dichiarato: «Spesso, il successo, arriva quando riesci a fare le cose che fanno in molti, ma con modalità nuove. Questo è stato il nostro approccio. Voler avvicinare, a tutti i costi, le reti alle persone». Fatta questa premessa, si spiegano con semplicità i risultati emersi da una ricerca condotta da D-Link, con la quale, l'azienda, ha voluto perlustrare quali fossero le vere richieste ed esigenze del mercato e dei consumatori. Sono stati coinvolti, nell'indagine, 20 paesi, per un totale di circa 8500 rispondenti di età

Stefano Nordio, vice president D-Link Europe



compresa tra i 20 e i 50 anni di età, su un questionario composto da 18 domande.

La sicurezza: questione fondamentale

Non ci sono dubbi su un risultato che ha fatto da padrone in tutta la survey: avere una casa sicura e protetta è la principale ragione che spinge gli europei a utilizzare e acquistare tecnologie per la smart home.

La ricerca ha dimostrato che il motivo principale per l'acquisto di prodotti smart home è quello di rendere la propria casa un posto più sicuro. La sicurezza si conferma, quindi, il bisogno primario raccogliendo oltre il doppio delle preferenze rispetto all'obiettivo del risparmio economico.

Se guardiamo, infatti, alla wish list dei consumatori europei, videocamere di sorveglianza e sensori di movimento raccolgono il 37% delle intenzioni d'acquisto per l'anno in corso (il 23% dei rispondenti intende acquistare una videocamera di sorveglianza e il 14% sensori di movimento), mentre le smart plug sono indicate come prioritarie dal 25% degli intervistati.

La sicurezza è la risposta più comune anche per gli scenari sui quali la smart home dovrebbe concentrarsi e sviluppare automazioni: ad esempio, gli europei sognano di poter uscire di casa senza doversi più preoccupare di controllare se le finestre sono rimaste aperte e, oltre un terzo, indica come prioritaria la comodità di non dover più alzarsi per spegnere le luci di casa o scendere a controllare la porta di ingresso prima di addormentarsi.

Per contro, solo il 13% degli intervistati crede che la smart home debba portare beneficio all'intrattenimento domestico, nonostante la forte crescita dei servizi di streaming on demand di musica e film. Insomma, quasi un terzo degli intervistati vorrebbe semplicemente rendere automatizzata la propria casa e circa 1 su 10 vorrebbe dispositivi smart per monitorare il proprio animale domestico, mentre si è fuori casa o avere un occhio in più per controllare che i bambini non si facciano male e siano al sicuro.

Il terzo aspetto emerso in modo massiccio dalla survey riguarda la difficoltà, che gli utenti avrebbero, a

causa dell'esistenza di numerose app per la smart home. Troppe e ciascuna con un compito diverso. Questa frammentazione non piace ai consumatori europei - che vorrebbero poter gestire tutta l'automazione e la sicurezza domestica da una sola app, direttamente dallo smartphone/tablet.

Integrazione futura

Bisogna, dunque, guardare avanti e pensare a un sistema di interazione tra le diverse soluzioni. Interoperabilità che possa andare a generare un ecosistema gestito da una sola app, per esempio, alla quale poter collegare anche dispositivi di produttori diversi, come sta accadendo, oggi, tra D-Link e le serrature Yale Smart Living.

A tale scopo esiste già, IFTTT un insieme di regole che permette a più dispositivi, di produttori diversi, di creare procedure automatiche, con i differenti prodotti. Esistono già 200 regole, create dai consumatori che funzionano correttamente, e non solo con device D-Link. Sono questi i meccanismi che permettono di gestire agevolmente una vera e propria casa smart. ✨

Il supermercato Coop del futuro

Dall'esperienza di Expo 2015 nasce a Milano un nuovo punto vendita governato dalle tecnologie digitali e pensato per testare

Coop lo ha battezzato "il supermercato del futuro" ed è questa la scritta che trova spazio sotto l'insegna con il logo del punto vendita inaugurato il 6 dicembre a Milano, all'interno dello spazio Bicocca Village.

Su un'area di circa 1000 metri quadrati, si sviluppa un supermercato con 6mila prodotti in cui la componente visuale regna in ogni angolo grazie alla presenza di oltre 100 monitor interattivi. «Non intendiamo realizzare i punti vendita Coop in questo modo - ha precisato Marco Pedroni, presidente di Coop Italia -. Questo punto vendita

è per noi un laboratorio da cui trarre esperienze da utilizzare in altri store. Una sperimentazione non solo nei confronti del consumatore ma anche delle modalità di gestione. Non è un supermercato tradizionale e non è ancora un "non supermercato", ma un progetto ibrido all'insegna dell'innovazione e di cui siamo molto orgogliosi».

All'interno del "supermercato del futuro" la customer experience viene esaltata da soluzioni digitali interattive che forniscono un'esperienza immersiva e coinvolgente. Molti prodotti sono esposti

su banchi sovrastati da schermi interattivi, dotati di un sistema di rilevamento a infrarossi, dove è sufficiente indicare con un gesto della mano il prodotto, per vedere rappresentate sullo schermo una serie di informazioni su provenienza, caratteristiche nutrizionali, controindicazioni per allergie e così via.

Altri prodotti sono disposti su scaffali verticali affiancati da schermi touch screen da cui è possibile accedere a informazioni dettagliate sui prodotti ed effettuare ricerche filtrate in base alle specifiche esigenze del

consumatore. Le etichette sono tutte digitali garantendo un aggiornamento rapido dei prezzi, abilitando modelli di gestione del ricambio e del magazzino più efficienti, riducendo possibili errori e aprendo la strada a innovative opportunità di marketing. L'esperienza di acquisto si conclude con casse self service interamente automatizzate, utilizzabili sia con contanti sia con carte di pagamento. Il "supermercato del futuro" di Coop ospita al suo interno anche lo spazio ristorazione

Una soluzione nata dall'esperienza di Expo

Il nuovo punto vendita è figlio dell'installazione di Coop all'interno di Expo Milano 2015 per la quale erano state sviluppate una serie di soluzioni tecnologiche dallo studio Carlo Ratti Associati (diretto da Carlo Ratti, professore del MIT). Grazie allo sfruttamento di queste sinergie l'investimento complessivo, che si aggira tra i 4 e i 5 milioni di Euro, non è risultato solo sostenibile,

luogo in cui sono presenti un cinema multisala da 18 sale, una grande palestra con oltre 8mila iscritti, numerosi ristoranti. Inoltre, sorge in prossimità dell'Università Bicocca dove studiano 30mila studenti ed è attorniato da diverse realtà aziendali.



le innovazioni da introdurre in altri punti vendita



Fiorfood Cibo & Incontri e offre il servizio gratuito Coop Drive che fornisce la possibilità di ordinare la spesa online e ritirarla dopo due ore in negozio nell'area dedicata al parcheggio senza scendere dalla propria auto.

ma decisamente inferiore rispetto all'apertura ex novo di un punto vendita di analoga metratura. La collocazione è stata scelta in un'area differente rispetto al tradizionale centro commerciale. Bicocca Village è, infatti, un

«Prevediamo di avere circa 2mila presenze al giorno - ha continuato Pedroni -. Intendiamo entrare in sintonia con il target che frequenta il Bicocca Village che è costituito da famiglie, studenti e dipendenti aziendali, mettendo loro a disposizione un luogo di incontro, condivisione e di trasparenza in cui la user experience è resa estremamente semplice».

La realizzazione è frutto della collaborazione con Avanade, una joint venture tra Accenture e Microsoft: Accenture ha curato l'infrastruttura mentre le soluzioni sono basate sulla piattaforma cloud Microsoft Azure.*

Ribes Tech: innovazione che nasce dalla Ricerca pubblica

Dalle competenze e dalla ricerca dell'Istituto Italiano di Tecnologia, nasce una start up che stampa su sottili fogli di plastica celle fotovoltaiche per alimentare il mondo degli oggetti smart

L'Istituto Italiano di Tecnologia (IIT) è una realtà completamente statale nata nel 2006 con l'obiettivo di promuovere l'eccellenza nella ricerca di base e in quella applicata e favorire lo sviluppo del sistema economico nazionale. L'IIT è governato da una fondazione che segue modalità operative simili a quelle di un'azienda privata e oggi vanta uno staff di circa 1470 persone, un laboratorio centrale a Genova, dieci centri di ricerca nel territorio nazionale (a Torino, due a Milano, Trento, Roma, due a Pisa, Napoli, Lecce, Ferrara) e due "outstation" all'estero (MIT

eHarvard negli USA).

La produzione dell'IIT a oggi vanta oltre 6990 pubblicazioni, oltre 130 progetti Europei e 11 ERC, più di 350 domande di brevetto attive, 14 start up costituite e altrettante in fase di lancio. All'interno di un contesto tecnologico di così alto spessore scientifico nascono opportunità e innovazioni anche in settori quali l'Internet of Things.

Una sorgente di energia a basso costo e pulita per l'IoT

È il caso di Ribes Tech, start-up costituita a Marzo 2016 nata da una collaborazione tra il Center for Nano Science and Technology dell'Istituto Italiano di Tecnologia e OMET, azienda di Lecco specializzata nella produzione di macchine rotative per la stampa. L'unione tra queste due realtà ha portato alla realizzazione di moduli fotovoltaici in plastica utilizzabili come sorgente di energia in ambito domotica, smart city e Internet of Things, in sostituzione o in supporto delle batterie.



Lo staff di Ribes Tech

I materiali conduttori e semiconduttori hanno la proprietà di poter essere sciolti in opportuni solventi per formare inchiostri speciali e questi inchiostri sono stati utilizzati all'interno di processi standard di stampa rotativa per depositare la cella fotovoltaica su un substrato plastico.

I moduli fotovoltaici sviluppati da Ribes Tech sono pellicole sottili, flessibili e molto leggere (poche centinaia di grammi al metro quadrato) che vengono stampate in grandi volumi su fogli di plastica a basso costo. I moduli fotovoltaici possono essere fabbricati in forme e colori differenti, adattandosi alle esigenze di design degli oggetti in cui possono essere integrati. La tecnologia si basa su materiali semiconduttori organici ovvero polimeri speciali in grado di condurre la carica elettrica e quindi di assumere un comportamento conduttivo o

semiconduttivo. Sfruttando materiali polimerici questi moduli non includono sostanze tossiche o materiali rari come avviene per altre tecnologie fotovoltaiche e, inoltre, risultano compatibili con i metodi di smaltimento e riciclaggio tipici dei materiali plastici.

Applicazioni industriali già pronte e altre in fase di studio

Le applicazioni industriali indirizzate a brevissimo termine sono di integrare pannelli fotovoltaici in plastica per alimentare etichette elettroniche di supermercati, piccoli dispositivi di localizzazione indoor (iBeacon), reti di sensori di temperatura per la domotica e sistemi di monitoraggio diffusi. In questi campi Ribes Tech ha realizzato diversi prototipi e si prepara alle prime produzioni a partire dal 2017. In futuro le potenzialità della tecnologia potrebbero consentire di sostituire le modalità costruttive dell'elettronica tradizionale, realizzando sistemi completi



interamente plastici che permetteranno applicazioni fino a oggi impensabili. Per esempio, un'etichetta stampata potrebbe trasformarsi da oggetto statico in elemento dinamico (costituito da una cella fotovoltaica, un circuito elettronico e un display elettrocromico) in grado di modificare le informazioni riportate su di essa: un logo statico potrebbe lampeggiare quando l'oggetto è illuminato, la data di scadenza potrebbe essere adattata a seconda delle condizioni di conservazione e di utilizzo oppure un'informazione potrebbe mutare in seguito all'apertura della confezione. Per questa idea Ribes Tech ha già depositato una domanda di brevetto. ✨



Zebra lancia i palmari professionali Android

Nel settore professionale si stanno diffondendo dispositivi che tendono sempre più a una convergenza tra le funzionalità specifiche delle attività di business e la familiarità e semplicità che arrivano invece dal mondo consumer.

È il caso dei dispositivi della nuova serie TC5 di Zebra Technologies che ha annunciato, di recente, due nuovi computer touch, TC51 e TC52, che nell'estetica assomigliano a un comune smartphone, ma con una resistenza e caratteristiche di classe enterprise e la gestibilità di un dispositivo a uso aziendale, ma soprattutto la novità è che sono equipaggiati con il diffuso e conosciuto sistema operativo Android (Android 6.0 Marshmallow).

Con questi device la società sta dimostrando il costante impegno verso la creazione di soluzioni innovative e orientate alle esigenze dei

clienti, come spiega Ugo Mastracchio, sales engineer manager di Zebra Technologies: «Si tratta di una vera e propria piattaforma di enterprise touch computing che consente al personale aziendale di avere funzionalità aggiuntive vantaggiose, come, per esempio, in ambito retail quelle che servono a ingaggiare la clientela e offrirle prodotti e servizi mirati, non soltanto a servirla». In pratica degli strumenti che consentono di affiancare allo svolgimento di attività operative anche una strategia di business più mirata al coinvolgimento del cliente stesso.

I dispositivi professionali della serie TC5, realizzati per soddisfare le esigenze specifiche di settori quali la logistica, la grande distribuzione e il retail, si aprono al mondo Android, ma con la necessaria sicurezza



Inoltre Zebra Technologies si avvale anche delle collaborazioni dei propri application partner per lo sviluppo di soluzioni che soddisfano esigenze specifiche in settori verticali, oltre a mettere a disposizione servizi di supporto e manutenzione che i

partner possono offrire direttamente ai clienti.

Le caratteristiche della serie TC5

I due dispositivi palmari TC51 e TC56 sono equipaggiati con sistema operativo Android 6.0 Marshmallow, ma a questo aggiungono il supporto di Zebra Mobility DNA, una suite in grado di offrire la sicurezza delle applicazioni, strumenti per lo sviluppo e applicazioni mobile per gli utenti finali. Un componente di questa suite è Mx (Mobility Extension)



che viene preinstallato sui dispositivi e consente di proteggere il dispositivo, impedendo agli utenti del dispositivo di installare o aprire app non autorizzate. In più Zebra si impegna per i primi 6 anni dall'acquisto del dispositivo a fornire le patch

per le vulnerability segnalate da Google.

I device sono dotati della necessaria robustezza per resistere a cadute accidentali, anche in acqua, o per essere utilizzati in aree polverose, come magazzini o altri luoghi ostili.

Un altro aspetto interessante è la maggiore velocità di performance della serie TC5 che Zebra riferisce sia cinque volte superiore grazie al processore ex-core a 65 bit da 1,8 GHZ che consente di utilizzare diverse applicazioni business, anche con

intensivo uso di grafica. Allo stesso tempo anche il consumo energetico della batteria è stato reso più efficiente e il processore utilizza il 15% in meno di potenza.

I nuovi device sono dotati di un ampio schermo

di 12,7 cm e zone touch personalizzabili Active Edge e offrono un'elevata qualità di scansione per catturare velocemente i codici a barre 1D e 2D anche se sporchi o danneggiati, mentre un'altra funzionalità utile nel settore è la cattura dei documenti

tramite SimulScan, un componente di Mobility DNA che consente di acquisire simultaneamente diverse informazioni, codici a barre, campi di testo, immagini, firme, che vengono direttamente inviate dal device per velocizzare le procedure di ordini e fatturazione, per esempio. La fotocamera con cui sono equipaggiati i nuovi palmari è di 13 MP.

La batteria PowerPrecision+ ha una durata di 14 ore, assicura Zebra, per garantire continuità agli operatori e con la possibilità di sostituirla facilmente e attraverso una modalità (Warm Swap) che mantiene la connettività perché non richiede di riavviare il dispositivo.

Performante è anche la connessione wireless con il TC51 dotato di Wi-fi e funzionalità di roaming mentre il TC56 dispone anche di 4G LTE per un utilizzo sul campo in aree esterne.

Le configurazioni dei device sono basate su Android Open Source e offrono una modalità standard che include Google Mobile Services e Android for Work, mentre quella professionali vengono forniti senza per consentire una maggiore riservatezza delle informazioni. ❁

Pure Storage e Cisco: infrastruttura scalabile

Ben Savage, EMEA head of channels & alliances di Pure Storage



FlashStack è la soluzione che combina storage all flash e componenti di elaborazione ad alte prestazioni

Si rafforza la partnership tra Cisco e Pure Storage, dando vita a una nuova soluzione infrastrutturale in cui convergono le soluzioni storage Flash Array di Pure Storage con i componenti di elaborazione e di rete forniti da Cisco. La soluzione si chiama FlashStack ed è stata progettata, configurata, implementata e supportata congiuntamente da Cisco e da Pure Storage, nonché testata e validata da entrambi i vendor. La nuova infrastruttura convergente è disponibile in due versioni. La prima, denominata FlashStack Mini, combina storage Pure Storage FlashArray //m10, server Cisco Unified Computing System (UCS) Mini, hardware di interconnessione Cisco e

software di virtualizzazione VMware o Microsoft. Si tratta di una soluzione che può scalare fino a 25 Terabyte di capacità di memorizzazione, 8 nodi di elaborazione e adatta a centinaia di utenti. Questa versione si indirizza alle aziende del segmento medio e agli ambienti con uffici distribuiti, soprattutto per applicazioni di desktop virtuale, consolidamento dei carichi di lavoro e per deployment isolati di applicazioni Microsoft e Oracle. Alle aziende di fascia enterprise e ai service provider si rivolge la soluzione propriamente denominata FlashStack, che può integrare i FlashArray di Pure Storage siglati //m20, //m50 e //m70, gli switch Cisco Nexus, i blade server

Cisco della Serie UCS. Questo modello può scalare fino a 500 Terabyte di capacità e 32 nodi di elaborazione ed è adatto agli ambienti con migliaia di utenti per applicazioni "Tier 1", carichi di lavoro per analytics e attività di consolidamento del data center.

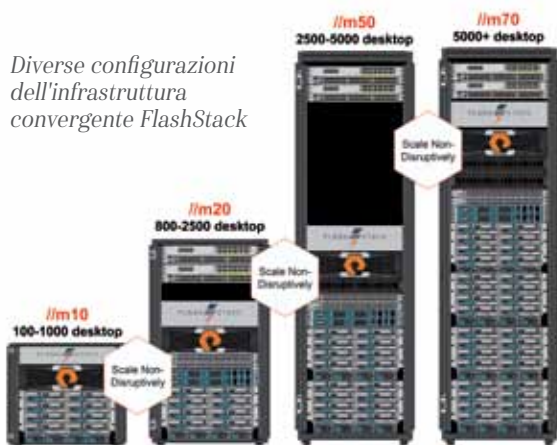
I benefici di questa soluzione vengono riassunti da Ben Savage, EMEA head of channels & alliances: «FlashStack è un'infrastruttura convergente caratterizzata da componenti "best of breed", design flessibile e una scalabilità da singola applicazione ad ambienti cloud "all flash".

Offre maggiore semplicità grazie alla sua natura di sistema convergente, pretestato e prevalidato; garantisce più

flessibilità e scalabilità grazie all'approccio modulare, al supporto flessibile e a un modello di pagamento a consumo; abilita un incremento di efficienza attraverso le elevate prestazioni fornite dalla tecnologia all flash e all'integrazione del software; infine reduce il Total Cost of Ownership (TCO) grazie a un'accelerazione nel deployment, una riduzione dei consumi energetici e delle esigenze di raffreddamento». La partnership tra Cisco e Pure storage è in atto ormai da un anno e mezzo e, finora, ha portato a circa 900

clienti congiunti. È tra questi che i vendor intendono individuare i primi destinatari delle soluzioni FlashStack. Le soluzioni Pure Storage si basano su un modello di vendita di tipo indiretto a due livelli e sono distribuite da Arrow, Systematica e Computer Gross. Sulla nuova soluzione è in corso un programma di "enablement" per individuare pochi e selezionati partner di Canale che do-

vranno veicolare FlashStack individuati tra le aziende con una forte presenza negli specifici settori verticali di interesse della soluzione che si rivolge in modo particolare ai mercati finanziario, manifatturiero e PA. ✱



Diverse configurazioni dell'infrastruttura convergente FlashStack

DEgustare

alla scoperta dei sapori d'Italia

giornalisti, enologi, chef, nutrizionisti, esperti alimentari vi promettono un'esperienza nuova



www.de-gustare.it

Le aziende rinnovano le reti per supportare la digitalizzazione

Le nuove strategie di digitalizzazione, l'adozione della mobility e della collaboration sono tra le ragioni che spingono le aziende a rinnovare le proprie reti informatiche.

Un report di Dimension Data mostra il livello di evoluzione in corso

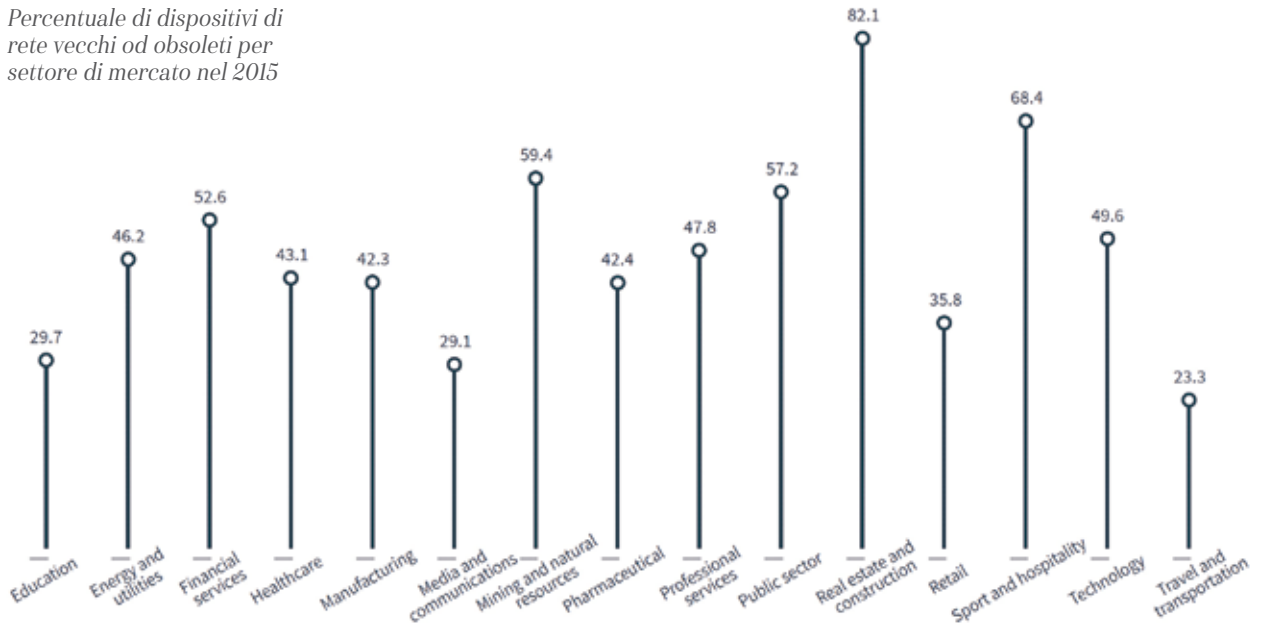
Le aziende si stanno rendendo conto dell'importanza di rinnovare le proprie reti informatiche. È quello che emerge da una ricerca condotta da Dimension Data, società specializzata nell'offerta e gestione di soluzioni e servizi ICT, che ha pubblicato il Network Barometer Report 2016, un'analisi dello stato delle reti che nasce dal monitoraggio dei propri clienti. Il report contiene i dati raccolti da 300mila incidenti di servizio registrati sulle reti dei clienti e prende in esame 320 Technology Lifecycle Management Assessments inerenti 97mila dispositivi di rete presenti nelle aziende di qualsiasi

dimensione, appartenenti a differenti settori di mercato e che operano in 28 paesi. Quest'anno il Report ha messo in evidenza un'inversione di tendenza che rompe con il processo di invecchiamento delle reti iniziato nel 2010, mostrando, invece, una battuta di arresto nella progressiva obsolescenza di queste. L'esigenza di rinnovare le reti aziendali e il loro ciclo di vita è invece un nuovo trend che emerge dall'analisi di Dimension Data e sembra andare di pari passo con la diffusione di strategie che prevedono ambienti di lavoro in mobilità, così come l'utilizzo dell'Internet of Things e del software-defined

networking. In questo senso il rinnovamento delle reti diventa parte di una strategia più ampia che si colloca all'interno di una visione architeturale.

Allo stesso tempo nonostante il refresh delle reti sia in crescita, c'è da tenere presente che la questione della sicurezza rimane comunque un aspetto importante in quanto il rinnovamento non rende immuni dai pericoli ma, al contrario, pare che le attività di patching, utili proprio per coprire eventuali problematiche, siano piuttosto trascurate. In realtà sembra che il numero di aziende con almeno una vulnerabilità nella sicurezza sia

Percentuale di dispositivi di rete vecchi od obsoleti per settore di mercato nel 2015



il più alto negli ultimi anni. Andre Van Schalkwyk, senior practice manager Network Consulting, di Dimension Data ha precisato comunque che: «L'invecchiamento delle reti non è necessariamente un aspetto negativo: le aziende devono comprenderne le implicazioni. Si apre la strada

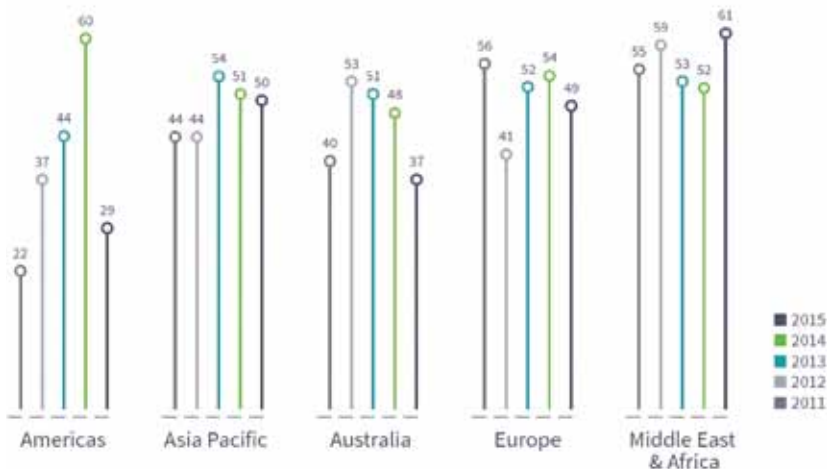
a un concetto di supporto differente con un conseguente incremento graduale dei costi di supporto». La scelta se rinnovare o meno le reti dipende dalla volontà dell'azienda di sostenerne i relativi costi, non è una strada obbligata, tuttavia bisogna tenere presente che l'invecchiamento

delle reti potrebbe non consentire di supportare iniziative quali il software-defined networking e l'automazione o di gestire i volumi di traffico necessari per la collaboration o il cloud.

Evoluzione dell'obsolescenza dei dispositivi di rete per i principali settori di mercato.



Percentuale di dispositivi di rete vecchi e obsoleti per area geografica e anno.



I risultati del Report

Quello che il Report mostra dall'analisi dei dati in possesso di Dimension Data è che per la prima volta in cinque anni, le reti sono sempre più giovani. In particolare, il 58% dei dispositivi risultano attualmente nuovi, con un incremento dell'11% rispetto allo scorso anno.

In pratica le aziende stanno rinnovando le proprie apparecchiature prima del loro ciclo di vita. Le strategie di digitalizzazione sembrano essere in cima ai pensieri delle aziende, compresa la mobilità del lavoro e la collaborazione, l'Internet of Things, e l'automazione.

L'automazione della rete è proprio uno dei requisiti fondamentali per porre le basi dello sviluppo di una strategia digitale. Le organizzazioni che si muovono in

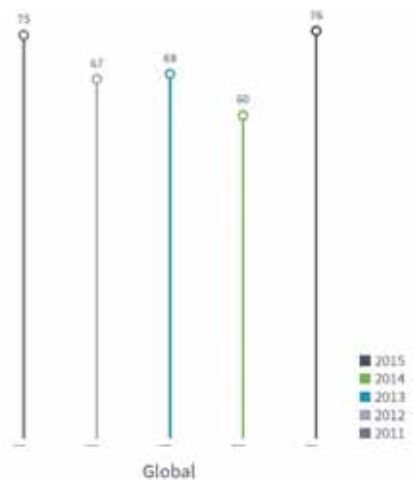
questo senso hanno la necessità di aggiornare le reti con apparecchiature in grado di supportare l'automazione utilizzando approcci software-defined.

Nel dettaglio, a seconda delle aree geografiche, risulta che in Europa, Asia Pacifica e Australia l'età delle reti aziendali si è ridotta in linea con la media globale, mentre nelle Americhe, il numero di dispositivi vecchi e obsoleti è diminuito molto più velocemente, dal 60% riportato nel Report del 2015 al 29% registrato nel Report del 2016. Il Report suggerisce che questo fenomeno può essere dovuto alla distribuzione della spesa accumulata a seguito dei quattro anni di vincolo finanziario. Secondo Van Schalkwyk infatti sembrerebbe che i clienti delle Americhe stiano eseguendo

il refresh delle reti con infrastrutture programmabili di nuova generazione. In Asia Pacifica e Australia il rinnovamento delle attrezzature rientra nel ridisegno delle reti per data center. In Medio Oriente e Africa, invece, l'età delle reti è in crescita, molto probabilmente come conseguenza dell'incertezza economica, in particolare in Sud Africa.

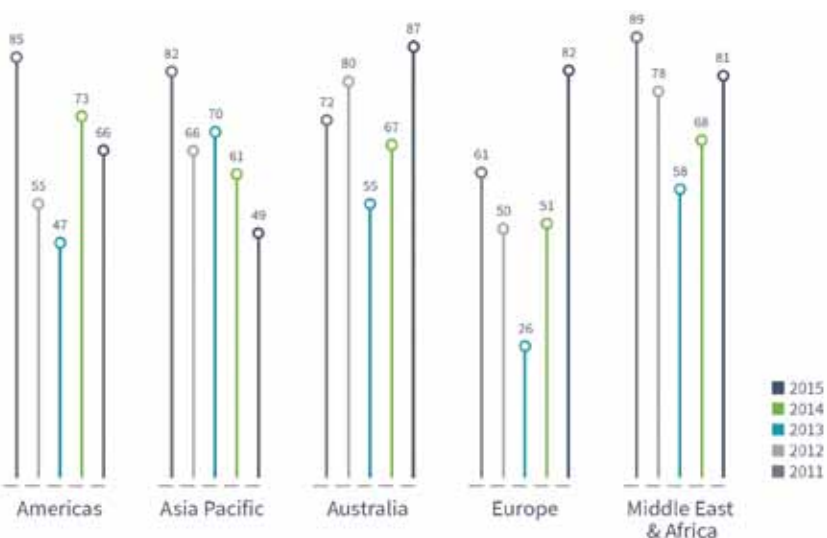
C'è poi l'aspetto della sicurezza delle reti che dipende sia dall'aggiornamento sia dall'utilizzo delle patch che contribuiscono a coprire eventuali falle e apportare miglioramenti. I nuovi dispositivi presentano certamente una minore esposizione ai rischi ma non sono automaticamente al sicuro,

Percentuale di dispositivi di rete per cui il produttore ha pubblicato almeno una notifica in cui segnalava la presenza di una vulnerabilità di sicurezza sul proprio prodotto



l'utilizzo delle patch è sempre consigliato. Secondo il report, dei 97mila dispositivi di rete rinvenuti da Dimension Data, il numero di quelli che presenta almeno una vulnerabilità nota nella sicurezza è aumentato dal 60% del Report 2015 al 76% riportato del 2016, il più alto dato degli ultimi cinque anni. Inoltre se si analizzano gli ultimi tre anni si può notare un trend di crescita in Europa, che passa da una percentuale del 26% del 2014 al 51% del 2015 fino ad arrivare all'82% registrato nel Report del 2016. Sempre negli ultimi tre anni, le vulnerabilità di rete sono aumentate anche nelle organizzazioni in Medio Oriente e Africa. In Australia, l'87% dei dispositivi di rete presenta almeno una vulnerabilità conosciuta, mentre in Asia Pacifica e nelle Americhe, le reti sono lievemente meno vulnerabili, rispettivamente 49% e 66%, rispetto al 61% e al 73% dell'edizione precedente. Sempre dal Report emerge che sulle reti monitorate la risposta agli incidenti è del 69% più veloce mentre i tempi di ripristino del 32% più veloci. Il 37% di questi incidenti è causato da errori di configurazione o umani che

Percentuale di dispositivi di rete con almeno una vulnerabilità per area geografica e anno.

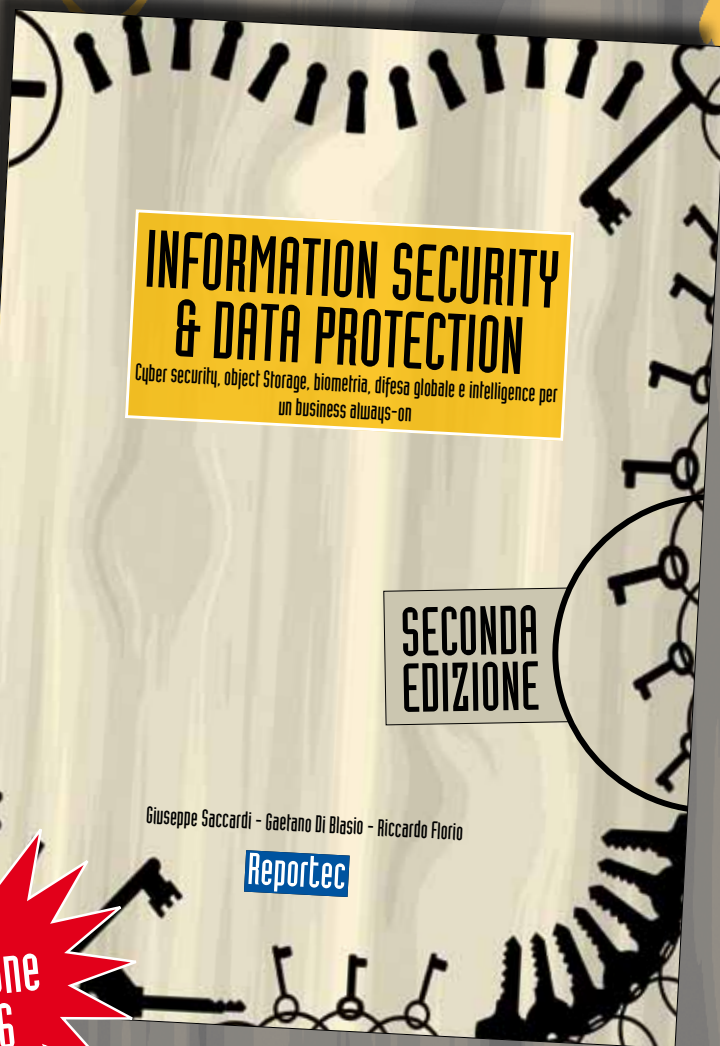


possono essere evitati grazie al monitoraggio, alla gestione delle configurazioni e a un'automazione adeguati, suggerisce Dimension Data. Anche l'adozione di dispositivi che supportano l'IPv6 sta crescendo, secondo il Report dal 21% dello scorso anno al 41% di quest'anno, in virtù dell'incremento di dispositivi attuali sulle reti. Ciò consente alle organizzazioni dotate delle nuove reti di supportare le strategie di digitalizzazione, abilitando la connettività per l'Internet of Things, per i big data e gli analytics. L'adozione del software-defined networking, invece, pare non essere così immediata. Se da una parte l'interesse verso questo approccio alla rete è presente nel mercato, dall'altra si trova

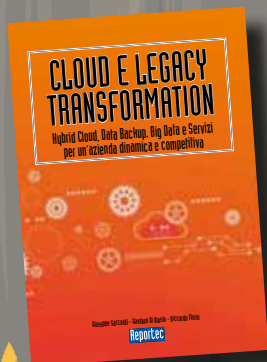
ancora nella fase iniziale di adozione e oggi poche reti aziendali sono capaci di supportare questo paradigma di rete flessibile. Nel 2015 meno dello 0,4% dei dispositivi potevano supportare WAN software-defined e solamente l'1,3% degli switch dei data center erano SDN-ready, secondo il Report. Un altro trend in corso all'interno delle organizzazioni è l'adozione di standard wireless più recenti. La percentuale di access point che supportano il protocollo 802.11n e oltre è passata dal 26,5% nel Report del 2015 al 33,4% di quest'anno. Ciò è dovuto al fatto che le aziende necessitano di questi access point per gestire una capacità di trasmissione più elevata richiesta dalle strategie di mobilità e di collaborazione. ✨

È disponibile il nuovo libro **SICUREZZA E PROTEZIONE DEI DATI**

In oltre 200 pagine il punto sulla situazione della cybersecurity e sulle dinamiche aziendali nella protezione del dato e della continuità del business. Una tematica sempre più vitale per le imprese, le quali devono mettere in conto che saranno attaccate. Ormai esistono sistemi automatici e pressioni da parte dei cybercriminali, tali per cui nessuno può sentirsi al sicuro: chi non è ancora stato attaccato lo sarà e, se non subirà danni gravi, sarà solo perché chi l'ha assalito cercava qualcos'altro.



2^a
edizione
2016



È disponibili anche
CLOUD E LEGACY TRANSFORMATION

Il libro è acquistabile al prezzo di 48 euro (più IVA 22%) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444

Teorema fa crescere l'innovazione

Diciotto anni fa nasceva Teorema, con molte idee e pochi mezzi, in linea con la tradizione delle migliori aziende tecnologiche americane. Da allora, l'azienda triestina ha continuato a crescere grazie a una costante dedizione verso l'innovazione tecnologica e alla ricerca (con un solido legame con il MIUR), unita alla passione e all'impegno delle persone.

Gli ultimi sei mesi stanno segnando un balzo in avanti dell'azienda caratterizzato da una spinta verso l'ampliamento dell'organico, l'innovazione tecnologica e una più capillare diffusione sul territorio, accompagnata da investimenti importanti. La nuova sede di Milano, che si aggiunge a Padova e a quella "storica" di Trieste collocata all'interno del Science Park, risponde all'esigenza non solo di ospitare un organico in ampliamento, ma anche di fornire un contesto più idoneo e coerente con le



attività di innovazione che stanno ridefinendo il carattere dell'azienda decretandone la crescita.

Tra le iniziative ricordiamo il lancio, lo scorso marzo, di Tilt (Teorema Innovation Lab Trieste), un incubatore per promuovere e favorire lo sviluppo di soluzioni innovative orientate alla tecnologia ICT, in cui gli sforzi di aziende private confluiscono con quelli di realtà pubbliche del mondo tecnologico come AREA Science Park di Trieste e l'Università di Trieste.

Un bando per l'innovazione

Teorema attraverso TILT ha anche avviato un bando indirizzato sia a persone fisiche sia a startup per vagliare i progetti digitali più innovativi indirizzati alla realizzazione di soluzioni IT per il mondo B2B all'interno di

L'azienda triestina continua a promuovere nuove iniziative orientate ai più recenti sviluppi tecnologici: dall'IoT, ai big data all'analytics

ambiti quali realtà virtuale e aumentata, IoT, big data e business intelligence, machine learning, servizi cognitivi, building automation, digital marketing e il mondo delle App. Il bando selezionerà progetti imprenditoriali originali e non ancora consolidati sul mercato, con l'obiettivo sia di favorire la crescita di startup innovative sia di individuare quelle di cui diventare soci per affiancarne e sostenerne lo sviluppo. Ai vincitori saranno messe a disposizione

risorse economiche, gestionali, formative e amministrative a cui si aggiungerà il network commerciale di TILT e parte del patrimonio intellettuale di Teorema.

«In questi mesi - ha commentato Michele Balbi, presidente di Teorema - abbiamo incontrato persone di grande talento con idee davvero originali. Ma succede anche che la mancanza di esperienza commerciale e gestionale o l'incapacità di strutturarsi e darsi dei processi penalizzino l'impresa e determinino il fallimento dell'iniziativa. Con TILT e con questi bandi vogliamo supportare concretamente i futuri imprenditori inserendoli in un ecosistema dove possono trovare team con visione ed esperienza, strumenti e risorse per sviluppare e crescere, anche su mercati internazionali».

Arriva il TeoLab

Mentre Tilt comincia ad avviarsi per la sua strada, Teorema mette già in campo un altro progetto denominato Teo Lab.

Michele Balbi, presidente e fondatore di Teorema ci spiega: «Teo Lab è, nel contempo, spazio, gruppo di lavoro, modello di sviluppo

e acceleratore tecnologico in cui un team dedicato di persone analizza le nuove tecnologie e i dispositivi per realizzare le condizioni per portare l'innovazione in modo rapido fino al cliente finale. Siamo orgogliosi di poter mettere a disposizione delle persone interessate la



Michele Balbi, presidente e fondatore di Teorema

nostra area Ricerca e Sviluppo attraverso i Teo Lab nei quali è possibile conoscere ma, soprattutto, provare le tecnologie più innovative e all'avanguardia attualmente disponibili».

Le soluzioni Teorema per il B2B

Proprio tra le soluzioni rese già disponibili da Teorema,

per favorire il processo di innovazione e digital transformation all'interno delle aziende ricordiamo Teorema Collaboration Portal, un'intranet aziendale basata sulla piattaforma Microsoft Office 365 e pensata appositamente per le aziende italiane. In questa intranet confluiscono diversi elementi importanti: dagli strumenti di gestione documentale, knowledge management, business intelligence, workflow fino alle tecnologie necessarie a distribuire contenuti multimediali e creare un vero e proprio canale TV a livello corporate.

Un'altra soluzione pacchettizzata di Teorema è Read Point: si tratta di un sistema per la gestione documentale che consente di creare e gestire un archivio condiviso, di definire un workflow di verifica e approvazione di ogni documento e di pubblicare regole di servizio o note operative in modo che possano essere lette sul portale aziendale.

Michele Balbi ha preannunciato, inoltre, che gli obiettivi di fatturato, di 8 milioni di euro per il 2016, saranno ampiamente rispettati e che per il 2017 la crescita attesa sarà a due cifre. ❁

#VUOILMIONUMERO?

**VUOI
IL MIO
NUMERO?**

dejavu.it



95051730109

“LA TUA FIRMA È LA NOSTRA FORZA.”
IVAN, GIOVANE PAPÀ CON UNA FORMA GRAVE DI SCLEROSI MULTIPLA.

PRENDI NOTA, DAI IL TUO 5X1000 A FISM.

Scegli di donare il 5x1000 alla Fondazione Italiana Sclerosi Multipla, firmando nel riquadro “finanziamento della ricerca scientifica e della università” e inserendo il codice fiscale 95051730109.

CODICE FISCALE FISM: 95051730109 | NUMERO VERDE: 800.094.464 | www.sostienici.aism.it

**SCLE
ROSI
MULT
IPLA**
ONLUS
fondazione
italiana

un mondo
libero dalla SM

ABBONATI TI REGALIAMO LA SICUREZZA E IL CLOUD



DIRECTION

la rivista per i professionisti dell'ICT



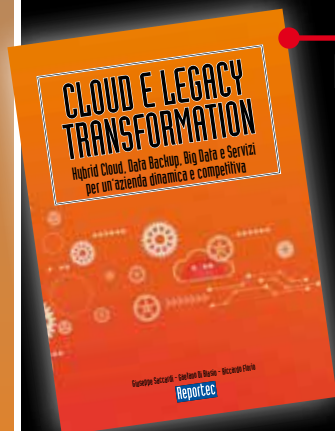
PARTNERS

la rivista per il Canale ICT a valore

**ABBONATI SUBITO A DIRECTION O PARTNERS
A SOLI 61 EURO**

**RICEVERAI I 10 NUMERI DEL 2017 E,
IN OMAGGIO,
2 LIBRI**

**DEDICATI ALLA SICUREZZA IT
E AL CLOUD,
DEL VALORE DI 100 EURO**



vai su

www.reportec.it/abbonamenti
e compila il modulo di abbonamento