

DIRECTION Reportec 89

SOLUZIONI SERVIZI E TECNOLOGIE ICT

FOCUS ON MOBILITY

Con le ultime novità da Fujitsu, Rad, Ericsson

INTERVIEW

Matt Brayley-Berger
HPE gestisce il ciclo
di vita delle applicazioni

Valerio Cencig
Il data office di
Intesa Sanpaolo

TECHNOLOGY

**IoT e M2M: un'evoluzione
che prosegue parallela**

TRENDS & MARKET

**Smart working: i dati IDC
parlano di progressi,
ma la strada è ancora lunga**

SECURITY
& BUSINESS

SPECIALE

La sicurezza della posta elettronica

PROTAGONISTI

Gastone Nencini, *country manager di Trend Micro*

La minaccia ransomware

I NUOVI PROTAGONISTI DELL'INNOVAZIONE AL SERVIZIO DI IMPRESE E PROFESSIONISTI

Al centro del nuovo progetto Smau sempre più occasioni di incontro e matching con un nuovo ecosistema di attori italiani a disposizione nel soddisfare le esigenze di innovazione di imprese, professionisti e pubbliche amministrazioni locali.



SMAU 2016 CONFERMA IL SUO RUOLO DI "MATCHING PLATFORM" PER L'INNOVAZIONE E L'AGGIORNAMENTO PROFESSIONALE

Smau è oggi la piattaforma indipendente e dinamica scelta ogni anno da oltre 50.000 imprenditori, manager di aziende e di pubbliche amministrazioni (dati Smau 2015) per crescere e aggiornarsi su temi quali **innovazione**, **tecnologia** e **digital**.

Grazie ai tanti progetti ed eventi, primo fra tutti il Roadshow, Smau è anche il partner che raccoglie gli operatori dell'ecosistema digitale e ICT, il meglio delle startup italiane, importanti Università e Business School, le Associazioni dell'Industria e del Commercio e tutte quelle realtà che stanno lavorando con passione ed energia per **rilanciare l'economia italiana** e l'**innovazione made in Italy**.

SMAU 2016 È:



BUSINESS MATCHING

Incontra il giusto partner e confrontati con potenziali fornitori per far decollare i tuoi progetti.



ORIENTAMENTO ALL'INNOVAZIONE

Scopri l'innovazione di startup, incubatori e centri di ricerca e innova con loro la tua impresa.



VALORIZZAZIONE DELLE ECCELLENZE

Conosci da vicino le imprese e le PA che hanno innovato e impara dai loro casi di successo.



FORMAZIONE E AGGIORNAMENTO

Aggiornati con i qualificati formatori e i numerosi workshop disponibili in ogni tappa.

LE TAPPE 2016

PADOVA
10-11 marzo

FIRENZE
7-8 aprile

BOLOGNA
26-27 maggio

BERLINO
16-17 giugno

TORINO
30 giugno-1 luglio

MILANO
25-26-27 ottobre

NAPOLI
15-16 dicembre

Direction Reportec
 anno XIV - numero 89
 mensile giugno 2016

Direttore responsabile: Riccardo Florio

In redazione: Giuseppe Saccardi,
 Gaetano Di Blasio, Paola Saccardi,
 Daniela Schicchi

Hanno collaborato: Gian Carlo
 Lanzetti, Edmondo Espa

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 Gian Galeazzo 2,
 20136 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

Mobility: rivoluzione che richiede molte scelte	4
Integrare la mobility nei processi per abilitare un lavoro "smart"	6
La tecnologie al servizio della protezione dei dispositivi mobili	9
Tre passi verso la mobility	12
Fujitsu: comunicare e lavorare sempre e ovunque	14
L'Internet of Things è mobile	18
Come evitare il calo di efficienza di una rete mobile	20

INTERVIEW

HPE ALM Octane per gestire il ciclo di vita dell'applicazione	23
Una struttura dedicata per diventare una data company	36

TECHNOLOGY

Machine to Machine: l'impianto idraulico dell'Internet of Things	26
Nuove opportunità per i sistemi di pagamento digitale	38
EMC la crescita arriva dal software	42

START UP

LinkedData center: una startup tra open data e semantic Web	30
--	-----------

TRENDS & MARKET

Italia: la rincorsa verso un modello di lavoro più flessibile	32
--	-----------

entrano in gioco, oltre che fattori ergonomici, anche aspetti connessi alla sicurezza, alla connettività a larga banda, alla gestione e al supporto delle applicazioni business.

Se, però, la scelta del dispositivo può essere semplice quando si parla di un device personale, quando si tratta di scegliere quello aziendale e di organizzare e gestire una flotta di dispositivi le cose possono cambiare e non essere più così semplici.

Gli aspetti a cui porre attenzione

Come osservato, nella mobility e nella scelta di come concretizzarla, la tipologia di dispositivi rappresenta solo una delle facce della medaglia. In pratica, entrano in gioco numerosi altri fattori. Tra questi la sicurezza e cioè la possibilità di implementare accessi sicuri e un'adeguata protezione dei dispositivi e la semplicità della loro gestione, soprattutto quando utilizzati in ambiti territoriali fortemente dispersi dove può essere difficile reperire in loco un adeguato supporto. A questo si aggiunge l'esigenza di aggiornare tempestivamente i software residenti dei dispositivi in modo che risultino allineati per quanto concerne applicazioni business o di sicurezza. Tutto questo, dando per scontata la dotazione di adeguate interfacce di comunicazione a larga banda.

Se un progetto aziendale di mobility interessa un numero ampio di dipendenti, distribuiti territorialmente e con necessità di interazione, a

quanto elencato va aggiunta una congrua capacità progettuale e l'identificazione preventiva di come gestire l'intera piattaforma di device mobili e delle applicazioni ivi residenti e la definizione di come intervenire periodicamente per mantenere l'insieme efficiente e atto a supportare senza degrado funzionale le applicazioni business.

Corollario a un progetto inerente la mobility, poiché in definitiva si tratta di dispositivi che verranno usati su reti pubbliche per trasferire, elaborare e scambiare dati e informazioni business, nonché per attività di comunicazione evoluta, ad esempio in videoconferenza, è l'opportunità di fare un'analisi preventiva di quali dati rendere accessibili e il carico di lavoro, dal punto di vista funzionale e di sicurezza, che implica una determinata applicazione.

In sostanza, nell'ambito progettuale una valutazione preventiva consiste nell'individuare quali dati vadano protetti e con che livelli di sicurezza sia opportuno dotarli, livello che dovrà corrispondere a determinate tipologie di utente e alla qualità di dati a cui ha accesso.

In sostanza, i dispositivi sono solo un elemento dell'equazione. Un altro indispensabile elemento è un robusto e flessibile sistema di gestione centralizzato che permetta di tenere sotto controllo i dispositivi e l'uso che ne viene fatto, garantendone la sicurezza e l'allineamento con le applicazioni business. *

Integrare la mobility nei processi per abilitare un lavoro "smart"

La mobilità apre a nuovi modelli di lavoro che superano i limiti legati alla collocazione fisica di dispositivi, applicazioni e persone

Il modo di lavorare sta cambiando. Un cambiamento all'insegna di flessibilità, razionalizzazione e ottimizzazione nelle relazioni interne ed esterne, guidato dalla tecnologia. Per indicare questa evoluzione viene usata la terminologia smart working, un termine che, per una volta, non è dettato solo dall'IT ma anche dall'amministrazione pubblica che ha recepito i cambiamenti in atto con l'approvazione da parte del Consiglio dei Ministri di un Disegno di legge specifico dedicato a questo tema.

Lo smart working è un tema articolato e complesso che non va identificato con la mobilità. Tuttavia, lo smart worker è solitamente anche un mobile worker e le due cose coincidono. Da un punto di vista tecnologico, la disponibilità di un dispositivo personale, di soluzioni di comunicazione e collaborazione avanzate così come quella di una connessione di rete mobile è da considerare scontata;

peraltro l'evoluzione degli standard di trasmissione (3G, 4G) degli ultimi anni ha anche garantito la larghezza di banda adatta a gestire contenuti di ogni tipo e dimensione inclusi quelli multimediali. Ciò che, invece, non è scontato è l'inserimento in modo strutturato dei paradigmi di mobilità e di lavoro in mobilità all'interno dei processi lavorativi. Questo passaggio, infatti, richiede il coinvolgimento di molteplici e diversificate figure aziendali, oltre che flessibilità.

L'IT deve farsi carico di predisporre efficaci sistemi di gestione dei dispositivi mobili aziendali per renderli sicuri, facilmente configurabili, coerenti con le esigenze delle diverse categorie di lavoratori e integrati nei workflow aziendali.

Il management deve far rientrare il concetto di mobilità e di lavoratore mobile all'interno di una visione strategica e di una pianificazione operativa che esaltino e portino, così, valore

aggiunto al business aziendale. Il dipendente, da parte sua, deve attraversare un passaggio culturale e formativo, che lo porti a utilizzare gli strumenti mobili in modo efficace e congruo e che lo veda consapevole e responsabile rispetto ai possibili rischi per la sua azienda.



In assenza del realizzarsi contestuale di queste condizioni l'inserimento della mobilità cessa di essere un componente di smart working, per restare confinata in un utilizzo soggettivo che può, al più, migliorare il lavoro di alcuni ma, più spesso, tende a portare con se non pochi danni collaterali.

Viceversa, quando il tema della mobilità viene inserito in modo strutturato e pervasivo all'interno dei processi aziendali diventa abilitante per nuove opportunità altrimenti non accessibili.

Solo per citarne alcune: un recupero di tempi morti che si traduce in un incremento del tempo lavorato; una maggiore soddisfazione del dipendente che riesce a coniugare meglio la vita privata e quella professionale; la riduzione dei costi di trasferimento e trasporto; un incremento di produttività che deriva da poter avere a disposizione in ogni momento gli strumenti più idonei a svolgere l'attività lavorativa; una presenza più radicata e pervasiva presso i clienti che contribuisce al rafforzamento della relazione con l'azienda.

In sintesi, il dipendente lavora meglio, di più ed è più soddisfatto e l'azienda ottiene maggiori performance di business e aumenta la fidelizzazione dei clienti: si verifica la classica situazione "win-win". ❁



IDC MOBIZ MOBILITY FORUM 2016

Dalla Mobile Enterprise all'Enterprise of Everything

22 Giugno | Milano, Centro Svizzero

Scenario

Lavorare fuori sede e in movimento è diventato uno dei volani di crescita per le aziende di ogni dimensione. Una **"mobile-first enterprise"** può oggi infatti aspettarsi tangibili miglioramenti nel modo in cui interagisce con i dipendenti, i clienti e i partner, con benefici visibili nella produttività interna, nella customer satisfaction, nei processi di business. Tuttavia, **IDC coglie ancora alcune criticità**, soprattutto lato IT, che ostacolano il pieno sviluppo della mobility: mancanza di competenze interne, incertezze circa la sicurezza, investimenti, scarsa conoscenza di ROI e TCO. Due fenomeni aiuteranno le aziende a **superare questa impasse**: uno demografico, ovvero il ricambio generazionale della forza lavoro IT; l'altro tecnologico, l'**Internet of Things**. Sensori e dispositivi intelligenti connessi creeranno reti di persone e oggetti che rivoluzioneranno tutti i settori industriali e il nostro modo di vivere. La "mobile enterprise" di oggi diventerà la **"enterprise of everything"** di domani.

Key Words

Enterprise Mobility Management (EMM), Mobile Device Management (MDM), Mobile Application Management (MAM), Mobile Enterprise Application Platform (MEAP), BYOD/CYOD, Mobile security, Cloud, IoT, M2M, Wearables, Smart working, #GenMobile

Premium
Sponsor



The power to do more



PER INFORMAZIONI

Nicoletta Puglisi, Senior Conference Manager, IDC Italia
npuglisi@idc.com - 02 28457317

http://www.idcitalia.com/ita_mobiz16

 #IDCMobiz16



La tecnologie al servizio della protezione dei dispositivi mobili

Si amplia la diffusione di tecniche biometriche e di funzionalità software sempre più avanzate



La sicurezza costituisce uno degli elementi più critici di un dispositivo mobile e nella sua scelta. Il fattore critico deriva dalla sua stessa flessibilità. Tramite un dispositivo mobile l'utilizzatore può accedere dall'esterno del perimetro aziendale alle risorse interne e ciò apre la strada, non solo potenziale, alla possibilità di esportare volutamente o meno dati sensibili. In generale, suggerisco agli esperti del settore, un dispositivo mobile dovrebbe disporre di robusti criteri di sicurezza, anche superiori a quelli di un desktop. Quest'ultimo, infatti, si trova all'interno di un perimetro aziendale fortemente protetto mentre un dispositivo mobile non ha questo beneficio ed è più facilmente attaccabile o asportabile. La diffusione dello smart working e di modalità di lavoro nell'ambito di smart city appositamente attrezzate (parchi, vie commerciali, biblioteche, ambienti comunali, eccetera), incrementa ulteriormente i rischi. La sicurezza rappresenta quindi una delle più grandi sfide, anche se non sempre è percepita nella sua completa estensione. Tra i metodi sempre più diffusi per

identificare in modo univoco l'utilizzatore di un dispositivo mobile ci sono e tecniche biometriche. Peraltro, è una diffusione che deriva, anche, dal crescere dell'importanza di aspetti legali, derivanti anche da normative nazionali e comunitarie, che ne spingono sempre più l'adozione.

Il metodo alla base della sicurezza biometrica consiste nel verificare caratteristiche del tutto personali quali le impronte digitali, i lineamenti del volto, l'immagine della retina, l'iride, il timbro vocale, la calligrafia, la struttura venosa delle dita, la geometria della mano per autenticare un individuo tramite comparazione.

La comparazione può essere condotta in due modi, che implicano tipicamente diversi utilizzi del sistema biometrico: la verifica o l'identificazione. Il processo implica due fasi. La prima consiste nella registrazione del tratto biometrico, che viene catturato, estrapolato e convertito in un codice binario in grado di generare un modello biometrico che sarà memorizzato in modo persistente e invariabile, nel tempo, all'interno di un database. Questo modello costituirà la base per una comparazione basata su metodi statistici e metriche tipici del sistema biometrico prescelto. Per rendere più veloce il sistema o per applicazioni particolari, il modello originale può essere memorizzato anche

direttamente su una smart card, ovviamente con tecniche cosiddette di tampering, che ne impediscono la dannosa manomissione.

La seconda fase è quella di "matching". Quando l'utente richiede l'accesso tramite il proprio dispositivo mobile è chiamato a sottomettere il tratto caratteristico precedentemente registrato all'apposito lettore biometrico, in modo che venga rilevato e comparato con il modello presente nel database.

Nelle applicazioni di verifica biometrica l'immagine acquisita viene sovrapposta al modello per verificare l'identità dichiarata della persona (è il caso utilizzato per le tecniche di autenticazione). Il metodo della verifica, impiegato in un sistema di autenticazione, può essere poi abbinato ad altri elementi di identificazione, come user ID, password, token, smart card e così via, per incrementare ulteriormente il livello complessivo di sicurezza dell'intero sistema

Le principali e più sicure tecniche di sicurezza basate sul riconoscimento biometrico, eventualmente abbinabili, sono:

- Impronte digitali: il trattamento biometrico delle impronte digitali è quello più diffuso e utilizzato da maggior tempo. Il modello biometrico viene solitamente realizzato su una rappresentazione sintetica numerica dell'impronta di partenza. L'univocità del modello all'interno di un database biometrico non è però garantita in assoluto e, soprattutto





in grandi archivi dattiloscopici, a più di una impronta può corrispondere un medesimo modello.

- Rilevamento della retina: prevede l'uso di un fascio di luce a infrarosso a bassa intensità che illumina la parte posteriore dell'occhio. Si tratta di

un sistema attualmente utilizzato in ambiti che richiedono un livello di sicurezza particolarmente elevato poiché non sono, a oggi, noti meccanismi efficaci per replicare la struttura vascolare della retina.

- Struttura venosa: è basato sulle caratteristiche della rete venosa delle dita e della mano di un individuo, caratteristiche che si sviluppano addirittura antecedentemente alla nascita. L'acquisizione di questi tratti biometrici avviene tramite sensori che rilevano la forma e la disposizione delle vene delle dita, del dorso o del palmo della mano utilizzando una sorgente luminosa a lunghezza d'onda prossima all'infrarosso. Ha il vantaggio di essere percepito come poco invasivo poiché non richiede il contatto del corpo con la superficie del sensore e fornisce un'accuratezza elevata, in genere superiore a quelli basati sulle impronte digitali.

A queste tecniche si aggiunge anche quella della topografia della mano, una tecnica basata sulla rilevazione delle proprietà geometriche dell'arto acquisite in modalità bidimensionale o tridimensionale mediante un apposito sistema di scansione che rileva caratteristiche quali la forma, la larghezza e lunghezza delle dita, la posizione e la forma delle nocche o del palmo della mano.

Va, però, considerato che quelli acquisiti sono tratti distintivi e non caratterizzanti in modo unico un individuo e che possono essere soggetti ad alterazione nel tempo. ❁

Tre passi verso la mobility

L'introduzione, in azienda, di nuovi paradigmi di lavoro in mobilità è preferibile avvenga per gradi

Come per tutti i progetti, gli esperti suggeriscono di affrontare il tema della mobility in azienda organizzandolo per passi successivi. È indubbiamente un approccio che permette di correggere eventuali errori e di affrontare il passo successivo una volta consolidati i precedenti e liberate tutte le risorse che vi sono state dedicate.

Il primo passo coinvolge il back-end e fa riferimento alla strategia aziendale. In sostanza, si riferisce a come il back-end IT deve essere organizzato e di che strumenti deve disporre al fine di fornire ai dipendenti gli strumenti adeguati alle esigenze di business del singolo utilizzatore di un dispositivo mobile. Cosa che può coinvolgere aspetti ergonomici e funzionali. Ad esempio, se un particolare utilizzatore svolge un compito che richiede il frequente trasferimento di volumi consistenti di dati o fa parte di un gruppo di lavoro distribuito che ha la necessità di lavorare sul medesimo progetto, deve essere fornita l'applicazione adatta e un dispositivo con caratteristiche ed equipaggiamento

adeguato. È in questa fase che, oltre alla selezione delle applicazioni e dei dati da rendere accessibili, si può procedere al raggruppamento degli utilizzatori in classi di servizio, in modo da poter facilitare l'aggiornamento delle prerogative e delle applicazioni a cui hanno diritto di accedere.

Il passo successivo può essere indirizzato alla scelta dei dispositivi con cui equipaggiare i dipendenti. Si tratta, in sostanza, di scegliere i mezzi fisici che il dipendente dovrà usare nello svolgimento del suo compito quotidiano, per accedere a file, dati, dialogare con colleghi o clienti e questo in funzione delle condizioni ambientali e di sicurezza in cui i suoi compiti verranno svolti.

Oltre alle esigenze del singolo, ad esempio il lavoro in un ambiente ostile o in magazzini o cantieri, la scelta migliore, richiede una ragionevole conoscenza dell'offerta del mercato, delle caratteristiche dell'offerta, dei prezzi e così via, in modo da poter valutare i benefici e gli impatti in termini





di operatività e di sicurezza a seconda della scelta effettuata. Quello che gli esperti del settore suggeriscono, è di porre particolare attenzione, stante la continua crescita degli attacchi informatici, alla presenza di robuste procedure di sicurezza per evitare pericolose intrusioni. Questo aspetto, debitamente considerato, coinvolge le caratteristiche e le dotazioni fisiche di un dispositivo. Se non ha la possibilità, ad esempio, di leggere smart card o non dispone del lettore di impronte digitali, per non parlare di soluzioni ancor più sofisticate come la lettura dell'iride o della configurazione

venosa di una mano, il livello di sicurezza potenziale sarà basso. Naturalmente la sicurezza, oltre a dispositivi fisici di verifica legati ai parametri biometrici, può essere rafforzata con ulteriori scelte applicative. Per esempio, stabilendo a livello di policy che, con un dispositivo cellulare su cui è difficile siano presenti criteri di sicurezza fisica avanzati, l'unico accesso consentito sia quello alla posta elettronica, mentre con un tablet, dotato di hardware di sicurezza più potente, sia possibile poter accedere all'intera gamma di applicazioni aziendali.

Il terzo passo coinvolge gli utilizzatori e può rappresentare quello finale nel deployment di una infrastruttura mobile. Coinvolge la formazione del dipendente sulla sicurezza, sul tipo di nuove minacce e sui rischi di un utilizzo

non corretto del dispositivo che gli è stato assegnato. Va però evitato il rischio di far sorgere all'utente, il desiderio di bypassare i criteri e le procedure aziendali, per evitare di dover rafforzare ulteriormente la gestione centralizzata.

Se per trasferire un file di grosse dimensioni un utente non ha a disposizione l'applicazione adatta, infatti, potrebbe essere tentato di ricorrere a cartelle condivise nel cloud o a usare una chiave USB o altre applicazioni e dispositivi che sono, oramai, presenti nativamente nei dispositivi e nel software di base. *

Fujitsu: comunicare e lavorare sempre e ovunque

La richiesta di soluzioni di mobility in azienda, anche grazie alla disponibilità delle risorse offerte dalle soluzioni in cloud, è in costante crescita, supportata dalla necessità di aumentare la produttività e la velocità delle risposte.

Gli elementi critici in questi progetti sono legati principalmente alla sicurezza: da un lato, infatti, è necessario bilanciare il beneficio che l'azienda ottiene grazie all'utilizzo di questi dispositivi da parte dei suoi dipendenti, con i costi e la semplicità d'uso degli stessi; dall'altro si tratta di dare agli utenti le corrette informazioni e le misure da adottare in caso di perdita

dei dati (riferito come Data Loss Prevention) o di smarrimento del dispositivo.

Ciò significa non solo il dover prevedere e attivare meccanismi automatici di avviso in caso di imprevisto rilevato sui dispositivi mobili utilizzati, ma anche, e prima ancora, definire

Piattaforme come Windows 10 Pro, sicurezza biometrica, servizi di management, connettività 4G/LTE e GPS integrato caratterizzano i dispositivi mobili di ultima generazione di Fujitsu

le autorizzazioni di accesso al dato. Oltre a ciò, dal momento che i dispositivi mobili sono la porta di accesso all'azienda, fondamentale è saper informare i propri dipendenti sul loro corretto utilizzo, perché si tratta di device che ai fini pratici si configurano sempre di più come veri e propri uffici mobili.

Fabrizio Falcetti, business program manager di Fujitsu Italia



Soluzioni per un mercato professionale

In questo scenario complesso le soluzioni di Fujitsu sono rivolte a un mercato professionale. Da questa decisione strategica deriva la scelta di Fujitsu di utilizzare piattaforme standard come Windows 10 Pro per i tablet e implementare su molte unità anche sistemi che rendano più semplice l'utilizzo degli stessi e l'adozione di sistemi di sicurezza.

Esaminiamo, per esempio, uno degli ultimi nati in casa Fujitsu, lo Stylistic R726. È un dispositivo mobile che integra un lettore SmartCard RFID di ultima generazione per l'autorizzazione all'accesso oppure può utilizzare un lettore di impronte venose PalmSecure. Grazie alla tastiera magnetica si trasforma in un vero e proprio notebook. Se si prende, poi,

in considerazione il modello Stylistic V535, si dispone, invece, di un vero e proprio tablet completamente rugged che può essere utilizzato in situazioni e ambienti che possono risultare, anche, particolarmente critici.

«La possibilità di utilizzare device che adottino sistemi operativi standard e professionali offre molti vantaggi», osserva Fabrizio Falcetti, business program manager di Fujitsu Italia, che aggiunge: «permette una più immediata integrazione nella infrastruttura IT aziendale, consente una più veloce implementazione, un minor impatto sull'utente che si trova ad usare lo stesso sistema operativo a dispetto di diversi strumenti e la semplicità da parte dell'IT di implementare un numero minore di regole di sicurezza».

A questo si affiancano i Servizi MDM (Mobile Device Management) End User Services erogati da Fujitsu per supportare le aziende nella gestione del parco Tablet e Smartphone.

Stylistic Q736: il tablet 2 in 1

Questa impostazione delle soluzioni di Fujitsu per la mobility è particolarmente evidente nell'ultimo dispositivo che si è aggiunto alla sua linea di tablet, lo Stylistic Q736, che è stato presentato in occasione dell'ultimo Mobile World Congress.



Fujitsu Stylistic Q736



Si tratta di un tablet 2 in 1 con livelli di sicurezza che Falcetti non esita a definire senza precedenti. E questo con ottimi motivi. Include, infatti, diverse tecnologie di sicurezza, tra cui PalmSecure, un esclusivo sistema di scansione biometrica delle vene del palmo della mano sviluppato da Fujitsu, che risulta ancora più accurato, veloce, facile e igienico rispetto ad altri scanner di autenticazione disponibili sul mercato.

Il nuovo tablet con schermo da 13,3", che si può trasformare istantaneamente in un classico notebook tramite la connessione di una tastiera opzionale, fornisce una elevata sicurezza attraverso l'identificazione biometrica o la tecnologia SmartCard, e prevede anche la possibilità di dotarlo di un supporto per una SmartCard contactless, sfruttando la tecnologia NFC (Near Field Communication).

Inoltre, lo Stylistic Q736 equipaggia anche drive criptati e TPM Intel, che consente l'archiviazione sicura di password e chiavi d'accesso, proteggendo ulteriormente il dispositivo contro l'accesso non autorizzato a dati sensibili.

Fujitsu è anche storicamente impegnata nello sviluppare e produrre unità caratterizzate

da elevati standard di sicurezza e affidabilità, e nel mantenere per le sue soluzioni un eccellente equilibrio tra design e performance.

Il nuovo Fujitsu Stylistic Q736 si presta ottimamente a un suo utilizzo in mercati verticali dove è ugualmente importante usufruire di uno strumento pratico e flessibile, ma anche e soprattutto garantire la sicurezza del dato. A questo si aggiunge un accesso protetto al tablet stesso, ad esempio per le cartelle dei pazienti in ambito sanitario, o i dettagli dei conti bancari nei servizi finanziari.

«Il nuovo Stylistic Q736 - osserva Falcetti - assicura che gli utenti, una volta autenticati, possano accedere ai dati aziendali da ogni luogo e in qualsiasi momento. Il tablet è dotato per questo di connessione ai server aziendali attraverso la rete 4G/LTE e di un GPS integrato».



Fujitsu Stylistic R726



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.

L'Internet of Things

è mobile

La previsione del Mobility Report diffuso da Ericsson rivela che l'IoT (Internet of Things) entro il 2018 rappresenterà la grande categoria di dispositivi wireless connessi. Il video la killer application tra i giovani

Ericsson ha rilasciato l'edizione 2016 del proprio Mobility Report che raccoglie le previsioni sulle reti mobile e il loro utilizzo da parte delle diverse categorie di utenti. Il primo dato che emerge riguarda l'IoT, che si appresta al "sorpasso". Questi dispositivi cresceranno fino a diventare, entro il 2018, la prima per unità di device connessi tramite Sim, scavalcando i telefoni cellulari e continuerà a crescere su una base annua del +23% fino al 2021, quando su 28 miliardi di dispositivi connessi, quasi 16 saranno dispositivi IoT. Un incremento che si registrerà soprattutto in Europa Occidentale, dove è attesa una crescita del 400% entro il 2021.

«L'IoT sta accelerando dal momento che i costi dei dispositivi si abbassano ed emergono nuove applicazioni. A partire dal 2020», afferma Rima Qureshi, senior vice president e Chief Strategy Officer di Ericsson, aggiunge:

«L'implementazione commerciale delle reti 5G fornirà ulteriori funzionalità necessarie per l'IoT, come lo slicing di rete e la capacità di connettere esponenzialmente più dispositivi rispetto a oggi». Già oggi si è raggiunta la quota di 5 miliardi di persone connesse in mobilità, ma il numero totale di abbonamenti alle reti mobili è di 7,4 miliardi, dato che alcune persone hanno più dispositivi connessi e quindi Sim.

Significativa anche è la crescita dell'LTE: entro fine anno, secondo Ericsson, le reti commerciali LTE supporteranno picchi di velocità dati in downlink fino a 1 Gbps (per esempio in Giappone, Stati Uniti, Corea del Sud e Cina), anche grazie ai 150 milioni di nuove sottoscrizioni al 4G/LTE registrate nel primo trimestre 2016, che portano il totale a 1,2 miliardi.

Si prevede diventerà lo standard di rete dominante dal 2019. Per quanto riguarda il traffico dati, nel 2021 i flussi

generati da video costituiranno circa il 70% del totale, trainati ancora da Youtube. Il traffico dati generato da Netflix si attesterà tra il 10 e il 20% del traffico video da mobile totale. Sono i giovani protagonisti di questi cambiamenti: secondo il report il consumo di traffico dati per guardare video su

smartphone è cresciuto del 127% in soli 15 mesi (2014-15). Nell'arco di quattro anni (2011-15) il tempo speso dai giovani guardando la TV/video su uno schermo televisivo è calato del 50% e di contro il tempo speso guardando TV/video su uno smartphone è aumentato dell'85%. ❁

Mobile subscription essentials	2014	2015	2021 forecast	CAGR 2015-2021	Unit
Worldwide mobile subscriptions	7,100	7,300	9,000	5%	million
> Smartphone subscriptions	2,600	3,200	6,300	10%	million
> Mobile PC, tablet and mobile router* subscriptions	250	250	300	5%	million
> Mobile broadband subscriptions	2,900	3,500	7,700	15%	million
> Mobile subscriptions, GSM/EDGE-only	4,000	3,600	1,200	-15%	million
> Mobile subscriptions, WCDMA/HSPA	1,900	2,100	3,100	5%	million
> Mobile subscriptions, LTE	500	1,100	4,300	25%	million
> Mobile subscriptions, 5G			150		million

Traffic essentials**	2014	2015	2021 forecast	CAGR 2015-2021	Unit
> Monthly data traffic per smartphone	1.0	1.4	8.9	35%	GB/month
> Monthly data traffic per mobile PC	3.9	5.8	20	25%	GB/month
> Monthly data traffic per tablet	1.8	2.6	10	25%	GB/month
Total monthly mobile data traffic	3.2	5.3	52	45%	EB/month
Total monthly fixed data traffic	50	60	150	20%	EB/month

Mobile traffic growth forecast	Multiplier 2015-2021	CAGR 2015-2021
All mobile data	10	45%
> Smartphones	12	50%
> Mobile PC	2	15%
> Tablets	6	35%

Monthly data traffic per smartphone	2015	2021	Unit
> Western Europe	1.9	18	GB/month
> Central and Eastern Europe	1.4	11	GB/month
> Middle East and Africa	1.0	6.0	GB/month
> Asia Pacific	1.0	6.5	GB/month
> North America	3.7	22	GB/month
> Latin America	1.2	7.0	GB/month

Come evitare il calo di efficienza di una rete mobile

Garantire la sincronizzazione delle “base station” è un affare complicato e costoso. RAD illustra come è possibile farlo e che tecnologie ha sviluppato

Supportare servizi e applicazioni di nuova generazione nelle reti mobili richiede un'accurata sincronizzazione dei clock di tutte le stazioni base.

La sincronizzazione può avvenire tramite un Master centrale, per esempio con lo standard IEEE 1588 (riferito come Precision Time Protocol o PTP), un protocollo utilizzato per sincronizzare i clock in reti; in alternativa può essere originata a livello locale dalla stessa stazione base. In entrambi i casi, come primo riferimento, viene utilizzato il GNSS ovvero il sistema satellitare globale di navigazione, in inglese Global Navigation Satellite System, da cui deriva l'acronimo.

Il motivo sta nel fatto che il GNSS distribuisce lo stesso riferimento temporale in ogni punto della superficie terrestre e, di fatto, agisce come “Primary Reference Time Clock” e cioè come clock principale a cui riferirsi per la sincronizzazione di dispositivi.

In condizioni ottimali permette di sincronizzarsi con un'accuratezza di 50 miliardesimi di secondo !

Pur accurato e presente ovunque sulla terra si tratta pur sempre di un segnale elettrico a bassa potenza



e, di conseguenza, soggetto a interferenze. Tecnicamente si parla di jamming, che può derivare da un evento naturale come nel caso di un temporale con forti e prolungate scariche elettriche, essere dovuto ad altre trasmissioni radio o anche a disturbi voluti.

È quest'ultimo il rischio reale per i dispositivi di rete perché, per disturbare e rendere inintelligibile il segnale ai fini della sincronizzazione, mette in guardia l'azienda specializzata RAD, bastano apparecchi che possono essere acquistati per pochi euro e con questi mettere in crisi l'operatività di una stazione base di una rete mobile. La cosa si aggrava in ambiti urbani dove vi è un'alta concentrazione di veicoli. Alcuni automobilisti potrebbero aver installato a bordo sistemi di

disturbo radio per impedire ai sistemi di registrazione del percorso o della velocità di funzionare, ma con l'effetto collaterale di disturbare anche le stazioni base.

Evitare il jamming? Un affare complicato

Due sono le modalità per limitare i danni che possono verificarsi.

La prima consiste nell'adottare tecniche di ricezione del segnale che mitigano l'impatto del jamming.

Il secondo è più complicato, perché richiede di intervenire sul progetto della rete. In pratica, una stazione base soggetta a jamming necessita di disporre di una frequenza di riferimento precisa sino a che il jamming passa e si riceve di nuovo il segnale GNSS. La cosa non è per niente facile. Se un orologio da polso ha un'impresione di qualche secondo ogni due mesi per una imperfezione del suo oscillatore al quarzo nessuno si lamenta. Anzi, lo si considera estremamente preciso. In una rete mobile l'accuratezza deve, invece, essere di sei ordini di grandezza superiore ovvero milioni di volte. Serve quindi un riferimento estremamente preciso e disponibile in ogni stazione base, possibilmente a costi contenuti.

Dove è possibile recuperare un segnale di sincronismo di questo tipo e renderlo disponibile a tutte le stazioni base di una rete mobile?

Un candidato naturale, osserva RAD, è la Synchronous Ethernet (SE) ovvero l'insieme di standard ITU-T per



distribuire le frequenze sul livello fisico di Ethernet.

Il problema è che, mentre lo standard è supportato a livello del “core” di una rete, solo una parte delle reti mobili esistenti supporta SE sino a livello di stazione base.

Una soluzione a questo problema è fornita tramite il Distributed Grandmaster (GM).

L'approccio si basa su un piccolo Precision Time Protocol Grandmaster situato localmente a quello che viene riferito come un cloud di stazioni base. Il fatto che il GM sia posizionato a non più di due o tre “hop” dalle applicazioni finali permette di assicurare un elevato livello di accuratezza del sincronismo.

Da RAD la soluzione che combina tecniche hardware e software

Per migliorare la sincronizzazione e ridurre il jamming, RAD, rappresentata in Italia da CIE Telematica suo partner storico e con una consolidata esperienza nella realizzazione di reti di accesso fisse e mobili, ha reso disponibile e brevettata la

soluzione MiCLK, una soluzione PTP GM che comprende tutte le tecniche illustrate per garantire il sincronismo del clock.

Il dispositivo equipaggia svariate tecniche di mitigazione del jamming, compreso il filtraggio del rumore fuori banda e tecniche di filtraggio digitale adattativo. Per queste ultime, il tutto si basa su software che rimuove le interferenze in modo da massimizzare il rapporto segnale/rumore qualsiasi scenario si dovesse verificare. Per fornire la potenza di calcolo necessario, incluso nell'apparato c'è un processore ARM dedicato. L'effetto combinato del software e della potenza di calcolo, evidenzia RAD, permette di ridurre la potenza del segnale di jamming di sino a 30 dB se confrontato con dispositivi GNSS convenzionali disponibili “off-the-shelf”.

Non ultimo, evidenzia RAD, MiCLK equipaggia anche svariati schemi di backup per garantire il clock, incluso la ricezione della frequenza di riferimento sia tramite Sync-Ethernet che PTP (noto anche come Assisted Partial Timing Support o APTS). ✱



SPECIALE

LA SICUREZZA DELLA POSTA ELETTRONICA

Attacchi mirati con tecniche di spear phishing dimostrano le vulnerabilità rappresentate dalla posta elettronica e generate spesso da comportamenti erronei o avventati

pag.6-15



CYBER ATTACK

FORCEPOINT

La febbre di Star Wars ha colpito anche gli esperti informatici di Forcepoint, che hanno battezzato una nuova botnet "Jaku" (o Jakku), come il desolato pianeta di frontiera della famosa saga fantascientifica, centro di traffici illeciti.

pag.5

PROTAGONISTI

GASTONE NENCINI, TREND MICRO: LA MINACCIA RANSOMWARE

È una tipologia di malware in rapida diffusione, soprattutto per l'elevato ritorno economico che offre al cyber crimine. La prevenzione resta la prima linea di difesa da affiancare a soluzioni di sicurezza specifiche come quelle proposte da Trend Micro.



pag. 18-19

IN QUESTO NUMERO:

CYBER ATTACK

pag.3

- Che la forza sia con noi contro gli attacchi informatici

pag.4

- La protezione tradizionale non basta più

SPECIALE

pag.6

- La sicurezza della posta elettronica

pag.9

- HPE Secure Mail: protezione end-to-end per posta e allegati

pag.12

- Check Point: protezione Zero-Day per le e-mail cloud-based

pag.14

- Barracuda, maggiore protezione contro gli attacchi e-mail mirati

SOLUZIONI

pag.16

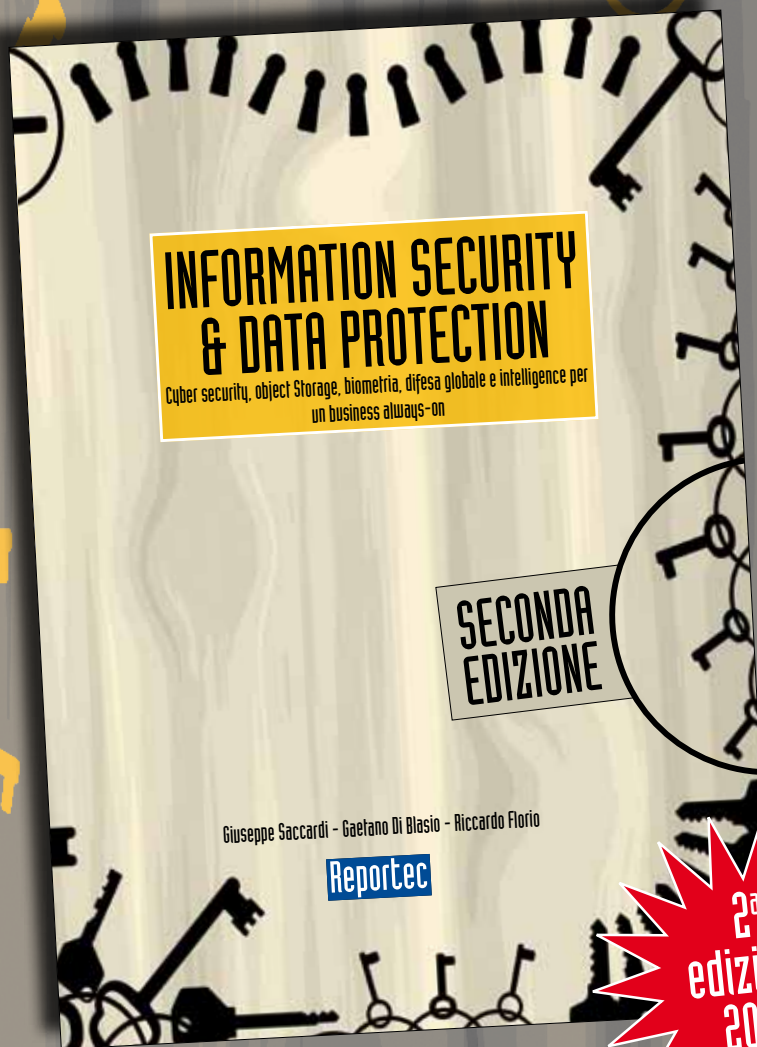
- Servizio F-Secure: rileva gli attacchi entro 30 minuti

PROTAGONISTI

pag.18

- Gastone Nencini, Trend Micro: la minaccia ransomware

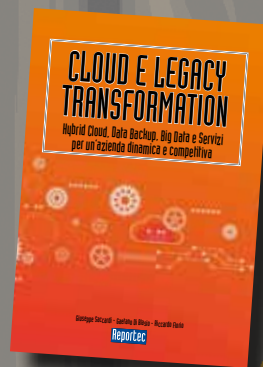
È disponibile il nuovo libro **SICUREZZA E PROTEZIONE DEI DATI**



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.



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

CHE LA FORZA SIA CON NOI CONTRO GLI ATTACCHI INFORMATICI

Dalla botnet Jaku assalto all'Asia. Minacce interne e nuovi ransomware nel Threat Report di Forcepoint

di Gaetano Di Blasio



La "febbre di Star Wars ha colpito anche gli esperti informatici di Forcepoint, che hanno battezzato una nuova botnet "Jaku" (o Jakku), come il desolato pianeta di frontiera della famosa saga fantascientifica, centro di traffici illeciti. È una delle rivelazioni del Forcepoint Global Threat Report 2016.

Jaku è stata scoperta a seguito di un'indagine durata 6 mesi dalla squadra Forcepoint Special Investigations, che ha identificato l'Asia come bersaglio della rete.

Il report mette in evidenza alcune delle più recenti minacce in evoluzione, con dati raccolti da oltre tre miliardi di data point al giorno in 155 paesi in tutto il mondo. Oltre a Jaku, tra i principali risultati si trova:

- il rilevamento di una nuova ondata di ransomware opportunistici;
- l'incremento delle violazioni ai causate da insider sia malevoli sia "accidentali";
- il gap tra i controlli per la sicurezza dei cloud provider e quelli delle aziende loro clienti;
- la convergenza continua di vettori di attacco via e-mail e via Web in pratica il 90% dei messaggi indesiderati contengono una o più URL malevole e inoltre milioni di macro dannose sono inviate.

Secondo il rapporto, nel 2015, le campagne di contenuti dannosi via email sono aumentate del 250% rispetto al 2014, guidate in gran parte da malware e ransomware. Gli obiettivi di questi ultimi, in particolare, si stanno affinando e vengono identificati come target paesi, economie e settori in cui c'è maggiore probabilità che possa essere pagato un alto riscatto. Sono, peraltro, gli Stati Uniti a ospitare il maggior numero di siti Web di phishing rispetto a tutti gli altri paesi messi insieme.

Eppure, spiega Luca Livrieri, responsabile prevenzione per Italia e Spagna di Forcepoint, la minaccia maggiore continua a essere rappresentata dagli insider. I dipendenti stessi delle aziende che, spesso commettono stupidi errori di comportamento cliccando su link pericolosi senza criterio. Preoccupano, anche, tecniche di evasione avanzate, che stanno guadagnando popolarità e sono la combinazione di più metodi di evasione, come per esempio la frammentazione IP e la segmentazione TCP, per creare nuovi modi che consentono di aggirare i controlli di accesso mediante mascheramento del traffico e strategie di watering holes. (infezione di server affidabili comunemente utilizzati dalla vittima).

LA PROTEZIONE TRADIZIONALE NON BASTA PIÙ

FireEye propone una piattaforma per la protezione, in tempo reale, dalle minacce avanzate. L'intervista a Marco Riboli, senior vice president Southern Europe.

di Riccardo Florio



I cambiamenti finanziari, geopolitici ed economici hanno fatto del 2015 un anno molto impegnativo per l'Europa, il Medio Oriente e l'Africa (EMEA), che si riflette anche nelle minacce e negli attacchi informatici. Dal report M-Trends 2016, realizzato da Mandiant, azienda posseduta da FireEye, emerge uno scenario sempre più complesso fatto di attacchi altamente specializzati in grado spesso di aggirare le difese tradizionali basate sulle firme digitali (come firewall, IPS, antivirus, gateway), in cui cresce il numero di breccie nella sicurezza che diventano di dominio pubblico mentre diventano sempre più diversificate le origini e le motivazioni degli attacchi, a livello globale.

FireEye è approdata in Italia da qualche anno forte di oltre 4700 clienti in 67 Paesi, tra cui oltre 730 delle aziende Forbes Global 2000 e per fronteggiare le nuove generazioni di cyber attacchi ha progettato e realizzato una piattaforma di sicurezza basata su una macchina virtuale che fornisce protezione in tempo reale dalle minacce per aziende e pubbliche amministrazioni di tutto il mondo.

Marco Riboli, senior vice president Southern Europe

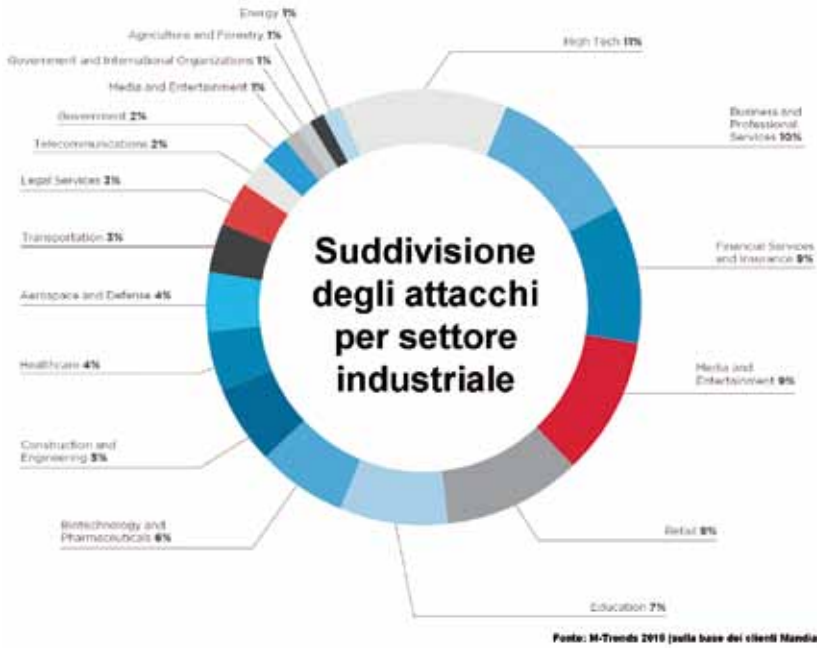
di FireEye delinea il quadro delle nuove minacce e i punti di forza di FireEye.

Direction: FireEye ha realizzato il report M-Trends 2016 che analizza lo scenario dei cyber attacchi. In base alle vostre ricerche quali sono i principali elementi di cambiamento in atto nello scenario della sicurezza aziendale?

Marco Riboli: Nei cyber attacchi analizzati abbiamo registrato un'impennata di casi dove l'attaccante è riuscito a compromettere sistemi critici per il business, bloccando o mettendo in seria difficoltà le operazioni aziendali. Infatti, sono diversi i casi nei quali l'attaccante è riuscito a colpire nel cuore l'azienda, riuscendo ad esempio a mettere offline i sistemi di broadcasting o a cifrare tutti i dati delle cartelle cliniche dei pazienti.

D: Quali sono le principali minacce, da dove arrivano, quali metodi utilizzano?

MR: Le minacce sono sempre più legate alla motivazione degli attaccanti: Il cyber-crime continua a creare nuove strategie per massimizzare i ritorni



finanziari delle loro campagne e il ransomware è diventato il loro principale strumento. Il cyber-espionage continua a puntare a vantaggi competitivi a discapito delle aziende o delle nazioni colpite, mentre gli hacktivist o i cyber-terroristi sono spinti da motivazioni politiche. Anche le App infette stanno diventando un veicolo di attacco sempre più frequente. Dato che ogni gruppo ha obiettivi e motivazioni diverse, è sempre più importante riuscire subito a dare un'attribuzione chiara all'attacco in corso per permettere la corretta gestione dell'incidente ed evitare conseguenze più gravi.

D: Cosa serve alle aziende per difendersi in modo efficace ed eventualmente come deve essere ripensata l'infrastruttura di sicurezza?

MR: Oggi, più che mai, le compromissioni informatiche sono inevitabili e richiedono di ripensare alla sicurezza aziendale in termini totalmente diversi rispetto al passato, spostando l'attenzione sulla mitigazione o eliminazione delle conseguenze per il business di un incidente informatico. La domanda da porsi è: sono preparato a rispondere a un attacco?

D: L'Italia rispetto ad altri Paesi ha delle specificità che richiedono un approccio particolare ?

MR: Una volta connessi a Internet non esiste più un reale limite geografico o regionale in quanto si diventa parte di una rete globale dove gli attaccanti sono sempre in agguato. Un sistema debole connesso a Internet diventa subito terreno fertile per un attaccante. Pertanto, se si è sottovalutato per molto tempo il reale rischio informatico, oggi la sfida per l'Italia potrebbe proprio essere il rimettersi in pari velocemente con una protezione adeguata.

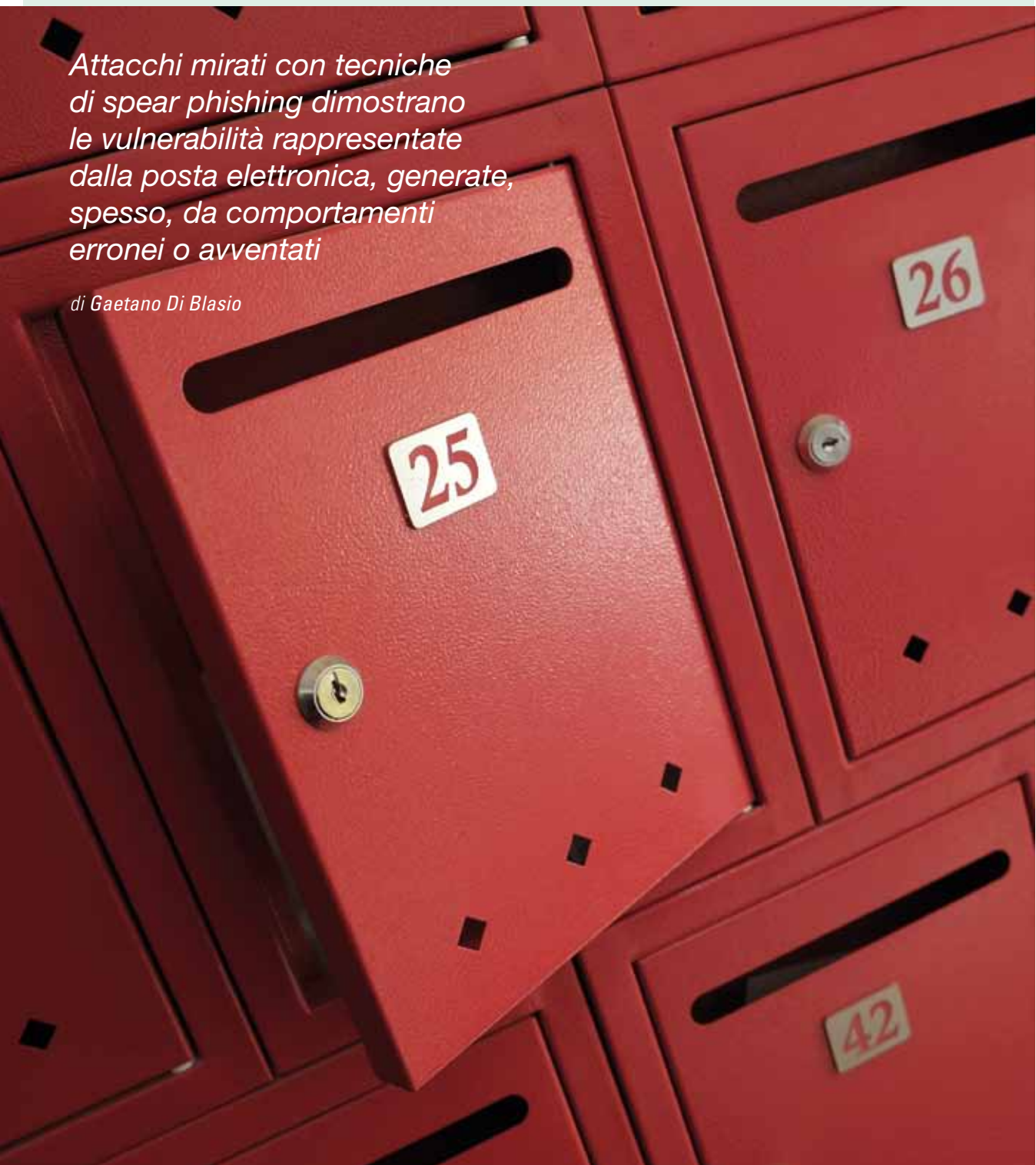
D: In che modo FireEye si propone di rispondere a queste nuove sfide ?

MR: Con tre elementi strettamente collegati tra loro: tecnologia capace di identificare attacchi sconosciuti; esperti che ogni giorno lavorano nell'analisi e risoluzione dei più importanti attacchi informatici; intelligence raccolte tramite l'infiltrazione di "spie" nei gruppi degli attaccanti.

LA SICUREZZA DELLA POSTA ELETTRONICA

Attacchi mirati con tecniche di spear phishing dimostrano le vulnerabilità rappresentate dalla posta elettronica, generate, spesso, da comportamenti erronei o avventati

di Gaetano Di Blasio



L'Instant messaging sta crescendo anche in ambito business, trainato dal massiccio utilizzo cui gli utenti sono avvezzi nel loro privato. Nonostante il successo di queste nuove forme di comunicazione, la posta elettronica è attualmente un elemento critico nei processi aziendali, sia essa parte integrante strutturata di quest'ultima o un elemento d'uso comune che ha sostituito strumenti tradizionali, come le vecchie circolari.

Ormai è normale utilizzare l'email per una fattura, anzi, la PA, con la PEC e la fattura elettronica ha definitivamente rotto un tabù, che, prima o poi sarà una regola per ogni impresa e procedura.

Ma la criticità risiede anche in utilizzi meno raccomandabili: è, per esempio, una consuetudine comune è quella di utilizzare la casella di posta elettronica come repository non solo delle corrispondenze importanti con colleghi, collaboratori, clienti e fornitori, ma anche di file e documenti che possono essere così recuperabili in qualsiasi momento, anche attraverso un dispositivo mobile. Inoltre, lo sviluppo della Unified Communication e Collaboration non fa altro che confermarne l'utilità. Questo, però, insieme allo sviluppo della mobility fornisce continui grattacapi ai responsabili dei sistemi informativi e della sicurezza in particolare.

La protezione dei dati sta diventando sempre più importante e oramai una priorità per i dipartimenti IT in alcuni settori economici come sanità e finanza, in particolare per quanto riguarda i dati privati dei clienti o assistiti. Non si tratta solo di regolamenti

cui adeguarsi, perché piuttosto che le sanzioni per una mancata uniformità, i rischi maggiori in caso d'incidente sono i danni derivanti dalla perdita di fiducia da parte della clientela. Chi manterrebbe il conto in una banca dopo che questa non è riuscita a impedire che il vostro conto corrente venisse prosciugato?

L'email è una delle principali forme di comunicazione verso l'esterno, cioè oltre il firewall. Se non adeguatamente protetta, si trasforma, anche, nella principale via per immettere nel sistema aziendale del malware o, più in generale, dei kit software preposti a sferrare attacchi all'infrastruttura. Ma non basta entrare, bisogna anche uscire con i dati copiati ed è sempre l'email a rappresentare una delle vie d'uscita più vulnerabili e, come tale, utilizzata per portare le informazioni all'esterno dell'azienda.

La posta come mezzo per il malware e via per la fuoriuscita delle informazioni

Se guardiamo solo l'ultimo decennio, possiamo osservare come la posta elettronica sia stata utilizzata per realizzare varie tipologie di truffe o attacchi informatici. Vanno ricordati, per esempio, i "worm", cioè un particolare tipo di codice malware il cui scopo era di penetrare nel computer della vittima lasciando traccia del suo passaggio con un virus, praticamente impedendone l'uso. Per entrare utilizzava un messaggio email contenente un allegato infetto e, per diffondersi si "autoinviava" a tutti i contatti della vittima stessa. Il più famoso è "I Love

You", il cui scopo era compiere il "giro del mondo" nel più breve tempo possibile.

Ancora oggi evoluzioni di I Love You o semplicemente pezzi di codice che lo componevano sono utilizzate in alcune fasi degli attacchi mirati o di quelli persistenti (Advanced Persistent Threats).

Per il dipartimento che si occupa della sicurezza informatica la sfida consiste nel riuscire a implementare un sistema per la protezione della posta elettronica che sia facile da integrare nel sistema informativo e non penalizzi i processi di business per i quali l'email è, ormai, vitale, ma al tempo stesso che sia conforme alle leggi nazionali e internazionali e ai regolamenti industriali.

Una soluzione che appare "definitiva" è la crittografia che renderebbe illeggibile i dati e le informazioni contenute nelle mail, soprattutto se a essere cifrati fossero tanto i messaggi quanto i file allegati. Ma non è così semplice. Gli approcci tradizionali non riescono a garantire la sicurezza che ci si aspetta quando il messaggio è codificato. I sistemi legacy, come S/MIME e PGP PKI, sono complessi, spesso troppo per l'IT aziendale. Inoltre non sono compatibili con piattaforme molto diffuse, quali Gmail, Yahoo e Android. Dall'altro lato, chiavi simmetriche utilizzate da sistemi proprietari, potrebbero generare un falso senso di sicurezza, perché, al costo di una complessa gestione delle chiavi, che dovranno essere memorizzate in un database a sua volta sicuro, potrebbero portare a un grave danno in dati "persi",

allorquando una chiave venisse compromessa. Anche implementare sistemi di posta proprietari personalizzati rischia di aggiungere complessità, senza aumentare affidabilità e sicurezza.

Per ridurre il rischio, la risposta non può essere rinunciare alla posta elettronica, né restringerne l'utilizzo. Eppure, anche a causa di queste problematiche molte imprese continuano a basare molti processi critici su una documentazione cartacea, che non solo rallenta il go to market e le decisioni interne, ma impone costi di gestione elevati e ostacola l'efficientamento.

In realtà c'è un rischio anche maggiore, considerando l'attuale tendenza alla digitalizzazione di molti processi. Oggi il consumatore medio è abituato a gestire la propria vita personale e familiare con strumenti quali i dispositivi mobili, dove la posta elettronica è ancora molto impiegata, ma sempre più soppiantata da altre forme di comunicazione. Per un'impresa rimanere ancorata al cartaceo può significare "l'estinzione". Si pensi a quanti portali offrono servizi come la prenotazione di visite specialistiche, viaggi, soggiorni oppure preventivi per assicurazioni e prestiti bancari, senza dimenticare l'e-commerce e immaginando quanti servizi ancora da inventare sorgeranno a breve. Si potrà restare scettici sulla dematerializzazione nella Pubblica Amministrazione, ma non si può restare fuori dalla corsa alla digitalizzazione. Neanche se le proprie attività sono "limitate" a rapporti con altre imprese.

HPE SECURE MAIL: PROTEZIONE END-TO-END PER POSTA E ALLEGATI

Una soluzione di crittografia che affronta gli aspetti della protezione della posta elettronica non dimenticando di affrontare temi quali la sicurezza in ambito mobile e cloud.

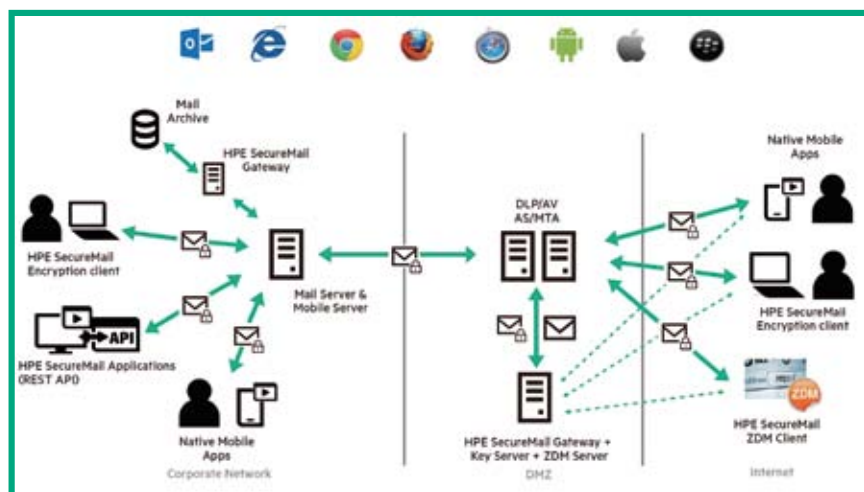
di Gaetano Di Blasio

HPE Security, la divisione dedicata alla sicurezza informatica all'interno della neo costituita HP Enterprise, dopo la riorganizzazione del colosso statunitense, ha sviluppato un'interessante soluzione modulare denominata HP SecureMail per la protezione tramite crittografia della posta elettronica. Una delle caratteristiche più importanti di HPE SecureMail è l'unicità della soluzione. In pratica la stessa sia per i computer desktop sia per i dispositivi sia per gli ambienti cloud. La decifratura può essere fatta dal pc, via Web o dal device mobile, tanto da un utente interno quanto da quello esterno e comprende scansione e filtraggio della posta in ingresso e in uscita. La soluzione può essere installata sia on premise sia su cloud pubblici o privati, come

pure in ambienti ibridi, come nel caso di un servizio come Office 365 di Microsoft. In particolare, sono supportati sistemi quali Outlook, Exchange, Blackberry Enterprise Server (BES) e altri sistemi di mobile device management (MDM). Questo è possibile anche perché HPE SecureMail mantiene una completa separazione tra la crittografia e il metodo di autenticazione, lasciando libertà di scelta per quest'ultimo, compresi Active Directory, LDAP o sistemi proprietari con propri portali.

Altresì rilevante è la centralità del dato nella

Schema di funzionamento di HPE SecureMail



protezione sia del messaggio sia degli attachment, che sono memorizzati su storage interni e non di terze parti. In altre parole tutto viene cifrato e protetto, in modo che quandanche la posta venisse intercettata, il contenuto criptato non sarebbe di alcun valore.

Fondamentale è il sistema per la gestione delle chiavi per le prestazioni e la qualità del servizio. Basato sullo standard sviluppato da HPE, l'HPE Identify-Based Encryption (IBE), il sistema di cifratura non richiede che sia memorizzata o gestita alcuna chiave di cifratura.

È un aspetto cruciale, perché impedisce al malintenzionato di acquisire tali chiavi e riduce drasticamente gli oneri di un amministratore.

Inoltre, questo permette che i messaggi possano essere inviati a qualsiasi destinatario senza che questi debba preventivamente effettuare alcun tipo di configurazione. È anche grazie a ciò che la soluzione presenta un'elevata scalabilità. Le grandi imprese possono, dunque, contare su ampi margini, ma non solo. La soluzione è anche integrabile nelle infrastrutture per la sicurezza della posta già in essere in azienda, quali i sistemi anti-virus, anti-spam o di content filtering, nonché quelli preposti all'archiviazione dei messaggi.

A proposito di quest'ultima operazione, va segnalato che HPE SecureMail fornisce più opzioni per un'archiviazione delle mail basata su policy con un controllo supervisionato. I messaggi vengono memorizzati come normali mail, ma, grazie alle

HPE SecureMail Mobile Edition

HPE SecureMail Mobile Edition consente di leggere e inviare email codificate; funziona su dispositivi iOS, Android e BlackBerry, che è possibile controllare attraverso policy di utilizzo e sicurezza.

La soluzione, in questo modo estende la protezione centrata sui dati di HPE Security e rende conforme alle normative per la privacy e la security la gestione dei messaggi email e loro allegati, residenti o in transito sui dispositivi. Tutto questo, spiegano in HPE, senza modificare l'utilizzabilità del dispositivo da parte dell'utente finale. Più precisamente, è stata progettata una user experience nativa che integra la sicurezza con le capacità delle app e permette di applicare le policy di sicurezza in maniera non invasiva.

La soluzione estende la compliance ai dispositivi mobile, con una protezione end-to-end di messaggi email e attachment, mitigando il rischio di violazioni alla confidenzialità dei dati.

L'utilizzo di una tecnologia completamente "push", elimina il rischio di falle nelle procedure di sicurezza, mentre un sistema di Mobile Device Management (MDM) completa e migliora la sicurezza e la compliance, senza entrare in conflitto con le policy.

capacità di indicizzazione, ricerca, visualizzazione, e identificazione dei dati interni alle mail stesse, HPE SecureMail semplifica le richieste durante eventuali audit, contenziosi e indagini.

Sempre grazie alle caratteristiche di HPE IBE, non occorrono le descrizioni aggiuntive delle chiavi, tipicamente richieste dai sistemi PKI e Open PGP.

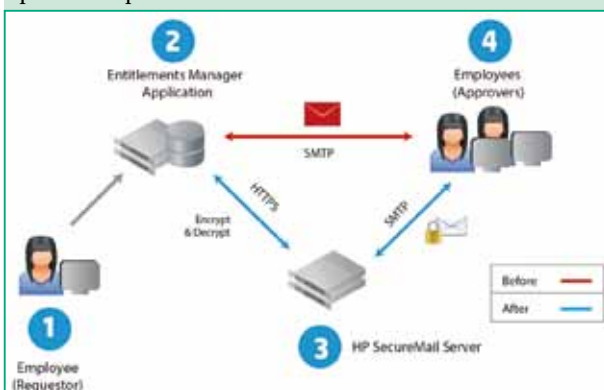
HPE SecureMail Application Edition

La protezione centralizzata dei dati fornita di HPE SecureMail può essere estesa ai dati strutturati e destrutturati presenti nei messaggi e gli attachment che vengono inviati, ricevuti e gestiti direttamente da applicazioni di business, portali o siti Web destinati a raccogliere o contenere informazioni riservate.

Questa estensione è attuata grazie ad HPE SecureMail Application Edition, che abilita una maggiore penetrazione in azienda dei processi di business automatizzati, proteggendo i dati che vengono gestiti direttamente dalle applicazioni, rendendo sicura la posta elettronica end to end interna e proveniente dal cloud.

HPE SecureMail Application Edition protegge i dati contenuti nel messaggio non appena questo viene spedito dall'applicazione, prima che passi dal backbone di posta, e per tutto il percorso fino alla destinazione. Un'architettura che assicura la compatibilità con tutte le normative su ricordate.

La soluzione è compatibile con qualunque client, sia esso desktop, mobile o Web, e con tutti gli attuali browser disponibili per pc o dispositivo mobile.



Un flusso di lavoro con un processo di approvazione basato su email che utilizza HPE SecureMail Application Edition

HPE SecureMail Cloud

Cifrare messaggi di posta dal computer in ufficio o da uno smartphone, distribuendoli attraverso portali, drive USB o altri sistemi di storage diventa facile con HPE SecureMail Cloud, che non richiede sforzi aggiuntivi da parte del destinatario.

Tutto questo è possibile grazie a una soluzione cloud erogata in modalità Software as a Service (SaaS) che consente di proteggere email, file e documenti senza investire in infrastrutture on premise.

Con la tecnologia di HPE SecureMail, che è accessibile via cloud, i mittenti devono semplicemente "premere" il bottone invio sicuro sul sistema di posta, da pc o device mobile, mentre il destinatario non vede modificata la propria experience e non deve far altro che aprire il messaggio.

I documenti crittografati sono, a quel punto, sicuri e distribuibili senza timore tramite portali, chiavette USB e vari storage di rete, senza bisogno di capire la crittografia. Un modulo software che è disponibile per il download permette l'accesso da un pc Windows per la crittografia dei documenti di Office.

La soluzione è utilizzabile anche via smartphone, senza bisogno di definire un nuovo account di posta né di definire un'apposita cartella di posta per i messaggi crittografati.

HPE SecureMail Cloud è disponibile in una versione Standard e in una Enterprise che dispone di alcune caratteristiche esclusive che consentono di aggiungere le funzionalità previste nella versione per l'on premise.

CHECK POINT: PROTEZIONE ZERO-DAY PER LE E-MAIL CLOUD-BASED

Il nuovo SandBlast Cloud protegge le e-mail dei clienti Microsoft Office 365 da malware conosciuti e sconosciuti

di Giuseppe Saccardi



Nathan Shuchami, head of advanced threat prevention di Check Point

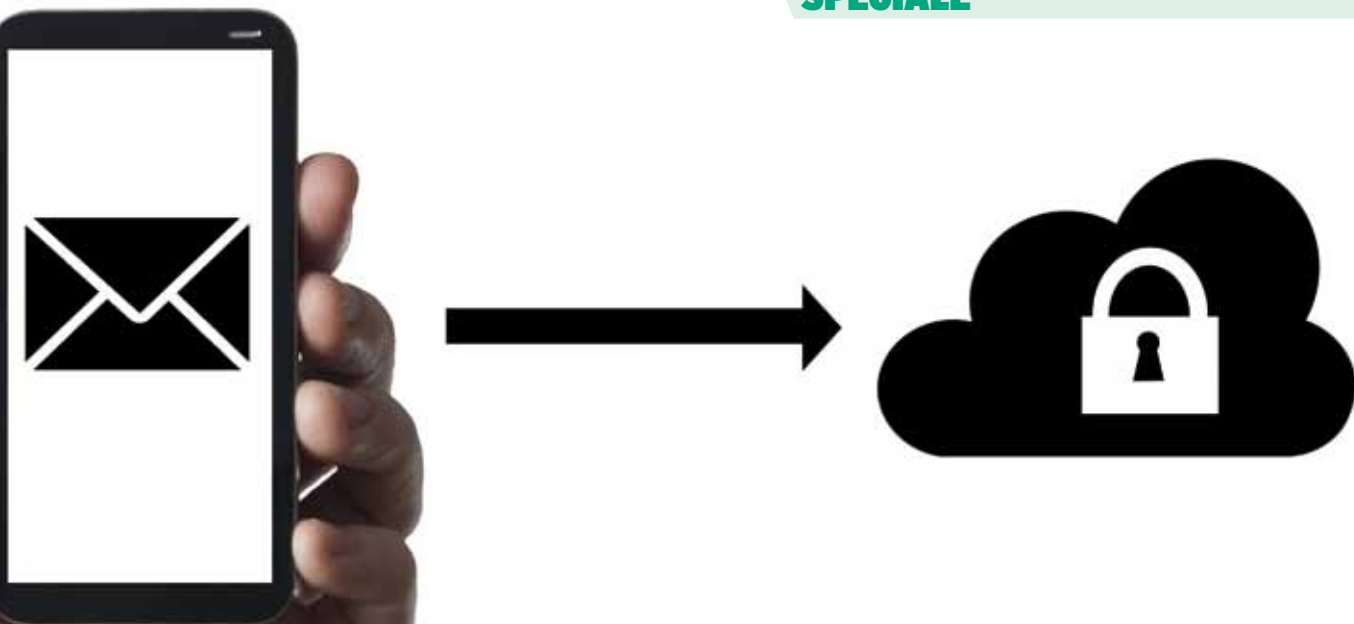
Continua la rincorsa tra attaccanti e difensori. Dal momento che le aziende stanno rapidamente migrando le proprie e-mail verso le infrastrutture cloud e gli hacker si sono attrezzati, Check Point Software Technologies ha studiato la contromossa. La società ha annunciato la disponibilità di SandBlast Cloud, una soluzione ideata per difendere le aziende dalle principali e più attuali minacce dei cyber criminali, che sfruttano le e-mail come ingresso principale per i propri attacchi.

SandBlast Cloud, l'ultimo arrivato della linea di mercato di soluzioni SandBlast, è stato progettato al fine di salvaguardare la sicurezza delle aziende con un'e-mail Microsoft Office 365 dalle minacce sofisticate quali ransomware e APT.

L'obiettivo di base è di consentire alle organizzazioni di migrare verso le infrastrutture cloud in tutta sicurezza. SandBlast Cloud è dotato del rilevamento a livello della CPU di Check Point e delle funzionalità di Threat extraction che prevengono, in modo proattivo, gli attacchi prima che colpiscano gli utenti.

Se, da un lato, l'e-mail ha permesso di trasmettere in modo più efficace che mai comunicazioni e informazioni, dall'altro, riconosce la società, rappresenta anche un vettore privilegiato per trasmettere malware, anche di tipo ransomware. In proposito, secondo il Data breach investigations report 2016 di Verizon, gli allegati delle e-mail sono il mezzo più comune per recapitare contenuti malevoli e i dati mostrano, inoltre, che gli utenti hanno aperto e cliccato sul 12% circa degli allegati infetti ricevuti. Considerando il fatto che l'intervallo trascorso tra la ricezione del contenuto e il primo click è stato solo di 3 minuti e 45 secondi è evidente che prevenire che questi file malevoli vengano recapitati agli utenti è essenziale al fine di evitare il propagarsi delle infezioni.

«I metodi degli hacker sono in continua evoluzione e



le aziende rischiano sempre più di cadere vittime di attacchi via e-mail personalizzati, quindi devono armarsi di misure di sicurezza proattive e sofisticate, per mantenersi un passo avanti alle minacce più evolute. SandBlast Cloud offre uno dei livelli di protezione più elevati sul mercato ai clienti con un'e-mail Office 365, attraverso una soluzione cloud pura, che fornisce contenuti sicuri velocemente, con una visibilità completa, e gestibili attraverso il relativo portale cloud-based», ha dichiarato Nathan Shuchami, head of advanced threat prevention di Check Point.

Nella lotta infinita, che ogni giorno viene portata avanti, per difendersi dalle email infette che possono causare violazioni dei dati, perdite finanziarie e diminuzione della produttività, le aziende devono, in sostanza, poter contare su una evoluta soluzione di sicurezza cloud per le proprie email, in grado non solo di prevenire gli attacchi dei malware esistenti, ma anche riuscire a individuare, in modo proattivo e quindi bloccare, le eventuali minacce non ancora conosciute, appena vengono individuate.

SandBlast Cloud fornisce in tal senso agli utenti di Office 365 una difesa stratificata, per essere al sicuro contro le minacce conosciute e sconosciute. Questo compito è assolto dalla protezione antivirus e dalla URL reputation, che protegge gli utenti dalle minacce conosciute, mentre le funzionalità avanzate, tra cui Threat extraction e Threat emulation, evitano che malware sconosciuti e minacce zero-day siano recapitate all'utente finale.

Tra le principali caratteristiche che possiamo riconoscere a SandBlast Cloud vi sono:

- Integrazione con Microsoft Office 365, gestita come una soluzione cloud.
- Alto tasso di rilevamento malware attraverso mediante tecnologia brevettata di analisi a livello della CPU.
- La trasmissione di versioni sicure e ricostruite dei formati di documento più diffusi, nel giro di secondi, e l'accesso completo al file originale, nell'arco di minuti, una volta che è stata ultimata l'analisi completa.

Come prodotto SandBlast Cloud sarà disponibile, sul mercato, a partire dall'estate 2016.

BARRACUDA, MAGGIORE PROTEZIONE CONTRO GLI ATTACCHI E-MAIL MIRATI

Disponibili nuove funzionalità per la protezione contro le minacce avanzate per le soluzioni in cloud Essentials for Office 365 ed Email Security Service

di Ricardo Florio

Barracuda Networks ha reso disponibili nuove funzionalità anti-phishing e di difesa contro gli attacchi mirati per le proprie soluzioni cloud per la sicurezza email Barracuda Essentials for Office 365 e Barracuda Email Security Service.

Barracuda Essentials for Office 365 è una soluzione per la protezione di e-mail, dati e infrastruttura cloud che mette a disposizione funzioni di sicurezza multi-layer, di archiviazione e di backup che favoriscono un uso più rapido, sicuro ed efficiente di Microsoft Office 365.

Barracuda Email Security Service è una soluzione SaaS pensata per bloccare le minacce provenienti dalle e-mail prima che queste possano avere accesso alla rete aziendale. È un servizio che si propone come possibile alternativa alle soluzioni basate su software e hardware per garantire sicurezza delle e-mail sfruttando i vantaggi di flessibilità e scalabilità del cloud. Barracuda Email Security Service



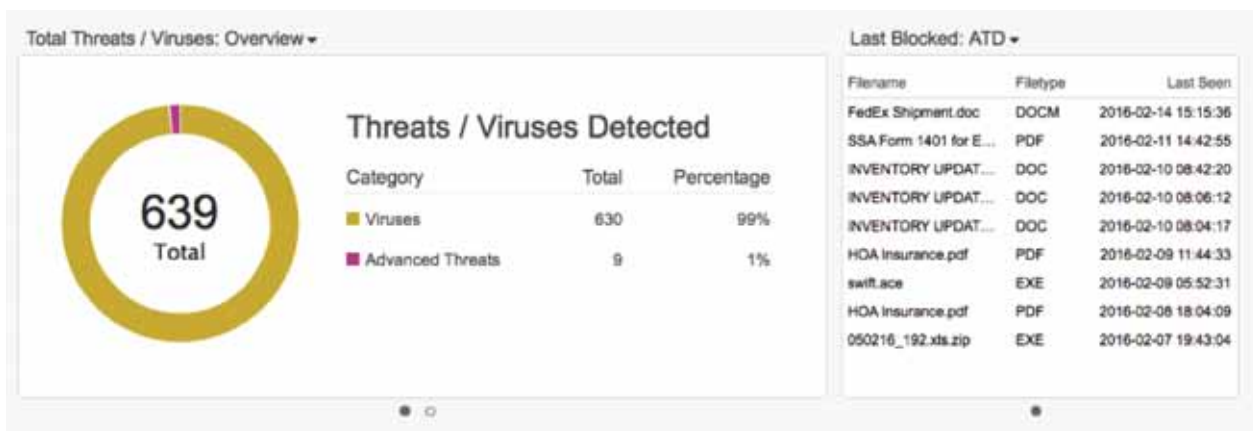
gestisce il traffico delle e-mail in entrata e in uscita per fornire protezione contro le perdite di dati e possibili attacchi e permette di crittografare i messaggi e di eseguire lo "spool" delle e-mail qualora i server di posta non siano disponibili.

Le nuove funzionalità: Advanced threat protection e Link protection

Le nuove funzionalità introdotte da Barracuda sono indirizzate ad aziende di ogni dimensione, in ambienti sia cloud sia on premise, per la protezione contro attacchi mirati diffusi tramite allegati di posta elettronica, per inibire l'accesso a URL pericolosi e contrastare le pratiche di phishing. Sfruttano un patrimonio di conoscenze aggregate, raccolte anche grazie a 150mila clienti distribuiti in tutto il mondo, per trasformarle in informazioni utili a fornire funzionalità avanzate di protezione.

La componente di Advanced Threat Protection coniuga tecnologie comportamentali, euristiche e di sandboxing per proteggere gli utenti dal malware, dagli attacchi mirati e "zero day" diffusi tramite gli allegati e-mail. Il framework di analisi di Barracuda

I risultati del blocco delle minacce di un'istanza di Email Security Service utilizzando la funzione Advanced threat protection



unisce la conoscenza delle minacce veicolate da molteplici vettori, quali e-mail, reti, applicazioni, Web, mobile e utenti.

La funzione di Link Protection di Barracuda è pensata per proteggere gli utenti che cliccano su link dannosi o fraudolenti aprendo questi link all'interno di una sandbox protetta. Si tratta di una tecnologia particolarmente utile per gli utenti remoti che accedono alle e-mail da dispositivi mobili e che potrebbero accidentalmente cliccare su URL compromessi. Link Protection identifica le anomalie negli URL, blocca l'accesso e avvisa l'utente della possibile minaccia. «Gli attacchi mirati stanno diventando un fenomeno comune - ha osservato BJ Jenkins, presidente e CEO di Barracuda -. Il phishing è il punto di lancio più diffuso per gli attacchi multilayer: è chiaro che il possesso di una tecnologia anti-phishing e la formazione degli utenti sono passaggi critici nella protezione dell'azienda. Barracuda si trova nella posizione ideale per individuare e aggregare le minacce attraverso tutti i vettori, il che ci permette di avere una visione olistica dello scenario delle minacce. Siamo in grado di utilizzare queste conoscenze e

aggiornare le nostre soluzioni di sicurezza in tempo reale, offrendo alle aziende clienti di ogni dimensione una protezione completa contro questi attacchi mirati a un costo vantaggioso, un beneficio in genere riservato a quelle organizzazioni che dispongono di budget e risorse molto elevati».

Barracuda ha previsto una nuova versione di Essentials for Office 365 denominata Email Security Edition che include, in un unico bundle, le funzioni di sicurezza e-mail Link protection e Advanced threat protection e che sarà disponibile a partire da 1,80 Euro al mese per utente. I clienti Barracuda Email Security Service possono usufruire della funzionalità anti-phishing Link protection senza costi aggiuntivi mentre la componente Advanced threat protection può essere aggiunta all'abbonamento esistente con un costo aggiuntivo a partire da 1,40 Euro al mese per utente.

SERVIZIO F-SECURE: RILEVA GLI ATTACCHI ENTRO 30 MINUTI

F-Secure Rapid Detection Service combina sensori, intelligence e monitoraggio h24 effettuato da un team di esperti allo scopo di combattere gli attacchi informatici

di Giuseppe Saccardi

Se non stai rilevando incidenti alla tua sicurezza, probabilmente è perché ti stai perdendo qualcosa. Questo è il messaggio che F-Secure ha lanciato in occasione della presentazione di un suo nuovo servizio di rilevazione delle intrusioni e di risposta agli incidenti per scoprire le minacce presenti sulla rete aziendale.

Il servizio gestito Rapid Detection, ha evidenziato l'azienda, si è proposto di combinare il meglio dell'uomo con l'intelligenza delle macchine per informare le aziende in soli 30 minuti dalla rilevazione di una minaccia.

Il fatto è che, in media, le violazioni di dati possono durare settimane, mesi o persino anni prima di essere rilevate. Secondo Gartner, la più grande area di bisogni insoddisfatti è, quindi, rappresentata da un'efficace rilevazione di attacchi mirati e di violazioni. Le organizzazioni, in pratica, non riescono a effettuare diagnosi precoci di una violazione e, secondo l'analista, ben il 92% di violazioni restano nascoste all'organizzazione che è stata colpita. Molte aziende si basano solamente sulla difesa



Pekka Usva, vice president of Advanced Threat Protection in F-Secure

perimetrale per proteggersi che è, sì importante, ma solo come parte di una strategia di sicurezza informatica globale.

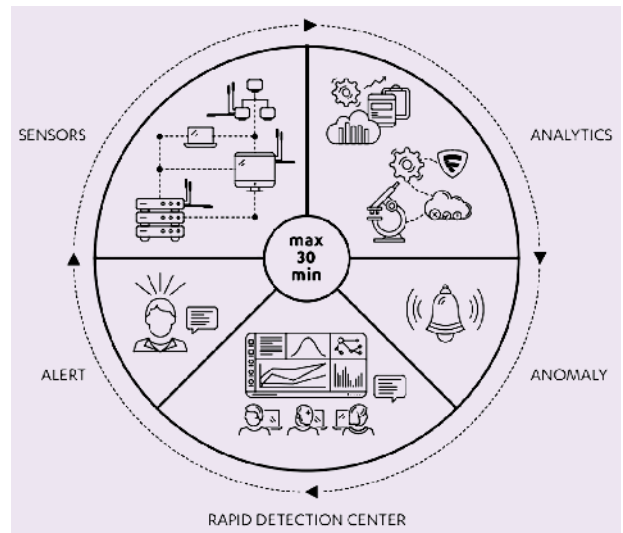
Con attori di minacce avanzate che colpiscono le organizzazioni con attacchi altamente mirati, un tentativo di attacco finirà, inevitabilmente, col superare i controlli di sicurezza e penetrare nella rete. La capacità nel riuscire a rilevare velocemente le intrusioni e a rispondere in modo immediato è, pertanto, fondamentale, ma non è semplice da mettere in atto.

«Le aziende si stanno rendendo conto che da sole fanno realmente fatica a rilevare intrusioni e a rispondere agli incidenti ha osservato Pekka Usva, VP of Advanced Threat Protection in F-Secure -. Creare al proprio interno un sistema appropriato di questo tipo è estremamente difficile e costoso e richiede anni per poterlo fare. Ecco perché ha senso affidarsi a un servizio gestito, che fornisca un immediato e tangibile ritorno sull'investimento».

Il meglio dell'uomo e della macchina

Il servizio Rapid Detection di F-Secure si basa,

L'architettura del servizio di rilevamento rapido degli attacchi



come abbiamo accennato, sulla forza dell'intelligenza umana unita a quella della macchina in modo da fornire un servizio all-in-one di rilevazione delle intrusioni e di risposta pronto a entrare in azione immediatamente.

Il servizio consiste di tre componenti principali: sensori di rete e degli endpoint che raccolgono dati sugli eventi e le attività; l'analisi comportamentale e l'intelligence delle minacce di F-Secure che analizzano i dati e identificano le anomalie; il Rapid Detection Center presidiato da un team di esperti di sicurezza informatica 24 ore al giorno, sette giorni su sette, in grado di identificare e gestire gli incidenti di sicurezza.

Quando viene rilevata una violazione un esperto contatta il cliente entro 30 minuti con una risposta per l'incidente e per fornire servizi opzionali di investigazione on-site se necessario.

«La componente umana è un fattore decisivo - ha commentato Erka Koivunen, cyber security advisor di F-Secure -. Gli attaccanti del resto sono umani, quindi per scoprirli non ci si può basare solo sulle

macchine. Il fattore umano elimina anche i falsi positivi, che rappresentano, senza ombra di dubbio, un ampio spreco di risorse».

Nel momento in cui una violazione viene rilevata, il servizio Rapid Detection è in grado di fornire, anche, delle informazioni che possono suggerire azioni per la fase di risposta. Il team preposto alla sicurezza del cliente riceverà informazioni su come la violazione è avvenuta, su come isolarla e otterrà consigli su come porre rimedio.

Con una rilevazione veloce, una diagnosi accurata e i consigli di un esperto su come rimediare alla situazione, le aziende possono limitare i danni e tornare al loro business prima possibile. F-Secure può, in aggiunta, fornire altri servizi on-site opzionali per la gestione degli incidenti e le investigazioni di tipo forense.

Rapid Detection, precisa F-Secure, è un servizio che si integra con i diversi ecosistemi esistenti e fornisce un ulteriore livello di sicurezza per rafforzare la strategia di sicurezza informatica dell'azienda.

LA MINACCIA RANSOMWARE



Gastone Nencini,
country
manager di
Trend Micro
Italia



È uno dei malware più insidiosi e in rapida crescita. Sfrutta spesso la posta elettronica per installare un programma che inibisce l'utilizzo di sistemi e file facendo leva sulla scarsa consapevolezza dei rischi da parte dei dipendenti

È decisamente un astro nascente nel panorama del cyber crime. Si tratta del ransomware, un tipo di malware che impedisce o limita l'accesso degli utenti al loro sistema, bloccandone lo schermo oppure impedendo l'accesso ai file. Le più moderne famiglie di ransomware, collettivamente classificate come cripto-ransomware, sono invece in grado di cifrare determinati tipi di file presenti sui sistemi infetti, rendendoli inaccessibili.

Alle vittime malcapitate viene offerta la possibilità di riprendere il controllo di sistemi e file dietro pagamento di una somma in denaro. Il nome di questo malware deriva proprio dalla parola inglese ransom, che significa riscatto.

Pagare o non pagare ?

Le vittime sono spesso tentate di risolvere subito il problema cedendo al ricatto. Tuttavia, l'esperienza dimostra che non vi è alcuna garanzia che pagando il riscatto si riesca a ottenere la chiave di decrittografia o lo strumento di sblocco necessario per riottenere l'accesso ai sistemi infetti o ai file presi in ostaggio: i documenti e file spesso sono persi. D'altronde non è saggio pensare a impostare un rapporto di fiducia con qualcuno che vi sta ricattando.

I prezzi del riscatto possono variare in base alla variante di ransomware o anche ai tassi di cambio in corso delle valute digitali. Infatti, grazie all'anonimato offerto dalle valute digitali, chi sfrutta i ransomware spesso richiede il pagamento del riscatto in Bitcoin. Esistono tuttavia molteplici varianti e alcune ransomware prevedono anche opzioni alternative di pagamento come carte regalo iTunes e Amazon.

Il comportamento dei ransomware

È possibile incorrere in questa minaccia attraverso una varietà di mezzi. Un ransomware può essere scaricato sul sistema quando un ignaro utente si trova a visitare siti Web compromessi. Oppure può essere diffuso come "payload" che viene rilasciato da "exploit" su sistemi vulnerabili oppure scaricato da parte di altri malware. Molti ransomware sono noti per essere distribuiti come allegati di e-mail spam.

Una volta eseguito nel sistema, un ransomware può bloccare lo schermo del computer o, nel caso di cripto-ransomware, crittografare file predeterminati. Nel primo scenario, viene visualizzata un'immagine a tutto schermo che impedisce alle vittime di usare il loro sistema. L'immagine solitamente notifica l'infezione in atto e mostra le istruzioni su come gli utenti possono

pagare per il riscatto. Il secondo tipo di ransomware impedisce l'accesso a file potenzialmente critici o importanti, come documenti e fogli di calcolo.

Per esempio, i laboratori Trend Micro sono stati i primi a intercettare un'ondata di attacchi crypto-ransomware che ha flagellato l'Europa nel corso delle festività natalizie, facendo leva sulle attitudini all'online shopping e inviando migliaia di mail in cui si cercava di persuadere le vittime ad aprire allegati o cliccare link correlati a spedizioni di pacchetti o altre merci acquistate. Il link conduceva a un sito controllato dai cyber criminali, dove all'utente veniva chiesto di inserire un codice "captcha"; questo innescava il download di un file che crittografava tutti i documenti del computer.

Come proteggersi

La migliore protezione contro i ransomware è impedire che possano raggiungere il sistema. Per non farsi sorprendere da attacchi di questo genere è, dunque, meglio adottare sin da subito misure preventive mantenendo costantemente nel tempo pratiche efficienti di protezione e seguendo alcune semplici regole.

La diffusione della sicurezza all'interno dell'azienda e la consapevolezza rappresenta sempre e comunque una pratica da perseguire poiché i dipendenti sono molto spesso l'anello debole della catena di protezione.

La posta elettronica è uno dei principali veicoli per i ransomware e, di conseguenza, imparare a diffidare di allegati provenienti da mittenti poco affidabili, contenenti un eseguibile, un file compresso o altrimenti sospetto deve far nascere il sospetto e farci essere più attenti. È importante che gli utenti adottino comportamenti responsabili e verifichino attentamente le e-mail ricevute prima di aprire allegati o cliccare su link che potrebbero sembrare sospetti. Una delle caratteristiche tipiche del phishing o delle tecniche di social engineering, che

alimentano la diffusione di ransomware, è l'urgenza sempre associata alla comunicazione, in modo da spingere l'utente a ridurre la cautela per la percezione di dover agire in fretta. Anche questo è un segnale da valutare per riconoscere e-mail o attività sospette.

È necessario installare le ultime versioni e applicare configurazioni delle soluzioni di sicurezza conformi alle best practice come quelle fornite da Trend Micro, per impostare una sicurezza multi-livello.

Va predisposta l'impostazione di policy mail per bloccare le potenziali minacce contenute negli allegati, così come installare soluzioni anti-spam o di email scanning. È importante anche che le soluzioni di sicurezza siano mantenute aggiornate e che vengano applicati i più recenti aggiornamenti critici e patch per il sistema operativo e per gli altri software chiave (per esempio il browser). Infatti, così come i produttori di sicurezza sono costantemente al lavoro per aggiornare i propri strumenti, anche gli scrittori di ransomware costantemente modificano i loro metodi e tattiche, per cercare di rendere inefficaci gli strumenti di protezione.

Da ultimo, ma non meno importante, è bene conservare sempre una copia in backup non in linea o in cloud dei propri dati critici e più importanti.

Trend Micro, grazie alla sua infrastruttura Smart Protection Network, mette a disposizione un'infrastruttura per la protezione automatizzata degli ambienti fisici, mobili, virtuali e cloud che sfrutta una tecnologia di assegnazione del livello di reputazione di URL, e-mail, file e App per abilitare una difesa efficace e in tempo reale contro ogni tipo di minaccia, incluse quelle cosiddette "zero day".

A questa tecnologia Trend Micro abbina una gamma di soluzioni di sicurezza che abitano una protezione multi-livello e persino un tool gratuito (Ransomware File Decryptor) per provare a decifrare i file cifrati da certe famiglie di ransomware.

#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

HPE ALM Octane per gestire il ciclo di vita dell'applicazione

Hewlett Packard Enterprise ha rilasciato HPE ALM Octane, un software per Application Lifecycle Management (ALM) studiato per aiutare le aziende ad accelerare i processi DevOps. Questa nuova soluzione fa leva su "toolset" di sviluppo largamente utilizzati come Jenkins e GIT per supportare i team che seguono le metodologie Lean, Agile and DevOps.



Matt Brayley-Berger, worldwide senior product marketing manager for HPE Software illustra le caratteristiche e i punti di forza della nuova soluzione.

Direction: Qual è la principale leva di business che ha portato al lancio di Octane?

Matt Brayley-Berger, worldwide senior product marketing manager HPE Software presenta la nuova soluzione pensata per garantire sicurezza ed efficienza delle applicazioni

Matt Brayley-Berger: I processi di delivery delle applicazioni basati sulle metodologie Lean, Agile and DevOps permettono di trasformare il processo di sviluppo e il modo di lavorare dei team di sviluppatori. Consentono di rilasciare le applicazioni più rapidamente, ma gli strumenti software che i team di sviluppo utilizzano oggi per gestire il rilascio del software devono essere cambiati per supportare questi processi. Stiamo riscontrando una

forte domanda per nuove generazioni di tool software per il ciclo di vita delle applicazioni e la gestione della qualità che siano ottimizzati per le metodologie Lean, Agile and DevOps ma anche in grado di supportare processi maturi e legacy quali Waterfall e il delivery iterativo. HPE ALM Octane è stato sviluppato per rispondere a queste specifiche sfide.

D: Dove inizia e dove finisce l'Application Lifecycle Management e perché è tanto importante?

MBB: L'Application Lifecycle Management (ALM) ha a che

fare con l'evoluzione degli asset nel corso della creazione di software pensati per risolvere un problema di business. Questi asset possono includere contenuti legati alla pianificazione e al portfolio, requisiti, test, le modalità di realizzazione dell'applicazione e del suo rilascio, la gestione dei difetti riscontrati durante l'intero ciclo di vita. Una piattaforma ALM per essere efficace deve comprendere i collegamenti tra tutti i diversi aspetti del ciclo di vita e questo è un aspetto centrale di HPE ALM Octane. Comprendere le relazioni tra i diversi asset, permette ai team di stabilire le priorità di lavoro, di definire l'impatto del cambiamento e di prendere decisioni più efficaci.

D: In che modo HPE combina la qualità del software con uno sviluppo rapido e sicuro?

MBB: Parte tutto dalla comprensione e dalla gestione del processo di rilascio. Il software viene pensato, definito e realizzato con l'obiettivo di fornire uno strumento a supporto di un obiettivo di business ed essere messo in produzione a disposizione dell'utente finale. Con il rilascio di ALM Octane, HPE

fornisce la capacità di gestire le fasi del rilascio, di tenere sotto controllo i diversi aspetti in cui è richiesta la valutazione della qualità (in modo manuale o automatizzato), di supportare il team nel capire rapidamente l'impatto sul business quando qualcosa non raggiunge il livello di qualità previsto.

D: Quali sono i punti di forza di HPE ALM Octane e come risponde alle esigenze dell'azienda?

MBB: HPE ALM Octane fornisce benefici all'utente finale in relazione a tre aspetti. Il primo è la velocità. HPE ALM Octane aggiunge valore a strumenti di sviluppo e collaborativi open source ampiamente utilizzati dai team di sviluppo che adottano procedure di sviluppo Agile. Per esempio strumenti GIT (gestione e controllo di versione), Jenkins (integrazione del software) e sistemi di Continuous integration (sviluppo collaborativo); HPE ALM Octane espande il loro valore gestendo e collegando tra loro le fasi di pianificazione, test, analisi dei difetti e delle versioni, priorità di backlog, cambiamenti e scrittura di codice. Il secondo aspetto è la qualità.



HPE ALM Octane implementa un processo continuo di controllo della qualità nel rilascio del software DevOps. È stato progettato per processi rapidi di sviluppo e per team che sfruttano Continuous Integration for DevOps per le fasi di test. L'esecuzione dei test è collegata in modo intrinseco ai processi di Continuous Integration e i risultati sono disponibili automaticamente, mentre le funzioni di gestione dei difetti e di tracking sono disponibili tramite un'interfaccia utente estremamente intuitiva. Inoltre HPE ALM supporta ChatOps tramite l'integrazione con Slack per



abilitare una risoluzione più rapida dei problemi.

Il terzo aspetto è la scalabilità. Le aziende stanno adottando architetture cloud ibride scalabili e orientate ai servizi. Le soluzioni ALM future sono pensate per supportare questa trasformazione. HPE ALM Octane è progettato intrinsecamente per il cloud ibrido, per operare in modalità SaaS gestito da HPE oppure su HPE Hellion.

D: In che modo il cloud si inserisce all'interno di Octane?

MBB: Mano a mano che più aziende di sviluppo applicativo si indirizzano verso il

cloud pubblico come mezzo per rilasciare applicazioni su larga scala, diventa una scelta naturale rivolgersi verso ambienti di sviluppo e test che sfruttano la medesima infrastruttura cloud pubblica. Per questo motivo, i fornitori di servizi cloud pubblici come Amazon hanno iniziato a creare soluzioni PaaS per accelerare lo sviluppo e il test nel cloud. L'approccio al cloud aiuta a collegare i processi di costruzione/test/rilascio delle applicazioni destinate al public cloud di Amazon. Non intende rimpiazzare lo sviluppatore e gli strumenti di test utilizzati nei processi

continui di rilascio e neppure a voler gestire il rilascio di molte applicazioni, servizi o applicazioni composite destinati all'infrastruttura ibrida. Il team HPE ALM Octane sta lavorando con quello di Amazon per costruire soluzioni congiunte. HPE ALM Octane è una soluzione cloud-based che sarà resa disponibile in seguito anche in modalità on-premise.

D: Come si inseriscono gli strumenti di analytics?

MBB: Dato che la piattaforma HPE ALM Octane cattura e gestisce una grande quantità di dati rilevanti di progetto, ci sono diversi modi differenti in cui è possibile sfruttare queste informazioni. HPE sta lavorando su un'iniziativa di ALM di tipo predittivo in cui stiamo applicando metodologie di analytics mutate da quelle sui big data alla grande quantità di dati creati durante il ciclo di vita del rilascio del software. Attualmente abbiamo a disposizione due algoritmi previsionali che possono essere utilizzati insieme a HPE ALM oppure HPE ALM Octane. Questi due sono focalizzati sugli aspetti predittivi legati ai difetti e su quelli correlati alle fasi di test e produzione. ❁

Machine to Machine: l'impianto idraulico dell'Internet of Things

L'evento M2M Forum 2016 evidenzia un settore di grande dinamismo, in cui molti degli ostacoli tecnologici sono stati superati, ma resta ancora molto da fare per la definizione di standard



E abbastanza frequente, quando le tecnologie sono relativamente giovani e non si è degli addetti ai lavori, che si sia indotti in confusione da sigle che richiamano funzionalità in parte sovrapponibili e che richiedono, un approfondimento per poter essere comprese. E' il caso, per esempio di IoT

(Internet of Things) e di M2M (Machine to Machine) acronimi sempre più presenti sul mercato IT. Può capitare, frequentando gruppi di discussione dedicati all'IT, di incappare in una definizione, non del tutto ortodossa per i puristi del settore, ma rivelatrice della relazione che lega i due termini.

L'importanza di batterie a lunga durata

Altro driver importante e, nel passato, vero freno allo sviluppo del settore, è stato quello della durata delle batterie alloggiare nei moduli M2M. Ora credibilmente superato dallo standard wireless Weightless sostenuto da ARM e Cable & Wireless Worldwide che consente longevità superiori ai dieci anni.

Per capire quanto sia fondamentale quest'aspetto si pensi al confronto tra la durata della batteria di un normale smartphone, rispetto alla necessità di mantenere operativi tutti i giorni dell'anno macchinari e controller disposti in tutto parti del mondo senza l'intervento umano.



L'impianto idraulico di un mondo "smart"

Tubi, rubinetti, sensori, interruttori, miscelatori, spie, rilevatori. A tutto questo, metaforicamente, si potrebbe ricondurre la relazione tra IoT e M2M, sigle,

rispettivamente, di Internet of Things e Machine to Machine, recenti oggetti del M2M Forum 2016.

Parlare di IoT significa essere all'interno di una sorta di ecosistema idraulico (pubblico, locale o privato)

costruito su tubi "intelligenti" che sono in grado di ricevere e scambiare grandi quantità di dati da un numero potenzialmente illimitato di moduli M2M intelligenti e bidirezionali. Questi moduli sono resi univoci da un Location Tag e, pur "parlando" diversi protocolli di comunicazione, sono in grado di inviare i dati via middleware (ponte tra la struttura IT e le reti di comunicazione) come informazioni elaborabili da parte delle rispettive "business platform".

Un settore in espansione

Gli operatori convenuti al M2M Forum danno evidenza di un comparto che sta enormemente accelerando lo sviluppo di nuove soluzioni applicabili nei molti settori dell'industria e dei servizi per puntare, di conseguenza, a un'offerta allargata di soluzioni M2M/

L'evoluzione delle embedded SIM

Allo stato attuale, buona parte delle soluzioni M2M sono state realizzate inserendo nei dispositivi delle normali SIM telefoniche, appositamente modificate per auto, variazioni del modem router, interruzioni di corrente, revisioni delle policy di accesso alla rete, indirizzi IP in conflitto, NAT e proxy server.

Secondo M2MLab dell'operatore telefonico NoiTel e U-Blox la strada è già, in buona parte, tracciata e va nella direzione di poter integrare le funzionalità SIM all'interno dei chip di controllo dei dispositivi. Il motivo di questo passaggio è fondamentalmente relativo alla sicurezza: i dispositivi sono spesso remoti o isolati e l'eSIM saldata all'interno del modulo M2M offre migliori garanzie di difesa dagli attacchi di pirateria e dai tentativi di clonazione.

Questo ritardo è stato accumulato a causa delle difficoltà nello stabilire, di comune accordo con le centinaia di operatori mobile, uno standard mondiale sulle Application Layer e Platform Layer dei circuiti eUICC (embedded Universal Integrated Circuit Card), il circuito integrato contenuto nelle SIM telefoniche. Per comprendere meglio le ragioni di tutto questo, basta ricordare che SIM è l'acronimo di Subscriber Identity Module e, com'è facile intuire, è la parte fondamentale per identificare l'utente e indirizzare i servizi di fatturazione. Senza entrare in eccessivi dettagli tecnici, questi due Layer gestiscono da un lato dispositivo il Provisioning Profile che integra identità, sicurezza, operatività, policy rule del singolo modulo; dall'altro, il livello della piattaforma gestisce le funzioni di ogni eUICC in termini di "rule enforcement", "disabling & enabling operation" e sicurezza.

Questo per il mondo business, poiché per il mercato mobile di tipo "commercial", questo processo, sarà suddiviso in due fasi: quella preliminare che vedrà una SIM ancora rimovibile, ma completa delle funzioni di riconfigurazione automatica e una seconda dove sarà a tutti gli effetti incorporata nei dispositivi. Lo standard, sviluppato dall'insieme degli associati della Global System Mobile Communication Association (GSMA), sembra ormai maturo per essere acquisito dall'intero mercato mondiale degli OEM e degli sviluppatori.



IoT pronte e adattabili secondo le diverse combinazioni di area geografica, tipologia di struttura coinvolta, disponibilità e capillarità di canali di comunicazione mobile.

Il tutto migliorando, assieme alle associazioni che ne stanno perfezionando gli standard, i livelli di prestazioni, affidabilità e scalabilità degli elementi essenziali dell'ecosistema M2M.

Ci sono stati tuttavia dei fattori decisivi, risolti solo recentemente, senza i quali quest'accelerazione d'offerta non sarebbe stata possibile.

Gli aspetti abilitanti per il M2M

Uno degli aspetti discriminanti è il livello di copertura e stabilità delle comunicazioni wireless messe in campo rispetto alle specificità del territorio e degli ostacoli strutturali, tenendo conto che il solo

Wi-Fi soffre, troppo spesso, di prestazioni e livelli di sicurezza insufficienti rispetto alle esigenze aziendali e che la disponibilità di connessioni wireless dedicate caratterizzate da un segnale stabile e capacità di mitigazione delle interferenze, può comportare, in molti casi, costi troppo elevati.

Per ovviare a quest'aspetto sono state perfezionate diverse tecnologie di trasmissione radio a bassa frequenza e dal costo molto inferiore finalizzate, soprattutto, ai progetti che necessitano coperture "very long range" e "very deep range", mentre per aree più ristrette di tipo outdoor, come campus universitari, complessi alberghieri o fieristici e medie aziende, sono nate diverse proposte di Wi-Fi Carrier come quelli di Ruckus che ottimizzano i costi e garantiscono qualità e banda per uso professionale.

I campi di applicazione sono infiniti e, se da un lato è stato l'automotive il settore che per primo ha colto le opportunità di offrire nuove esperienze di guida e si è ritagliato nuovi spazi di business (anche grazie al fatto che costi e latenze della comunicazione satellitare non

rappresentavano l'ostacolo principale), dall'altro si osservano già innumerevoli casi di progetti altrettanto ambiziosi in grado di affrontare esigenze complesse mantenendo semplicità d'implementazione e costi accessibili anche per modelli di business non sempre ad alto valore aggiunto.

Alcuni esempi

Si pensi, per esempio, al caso di un'enorme "farm" americana con estensione di migliaia di ettari e alla necessità di avere sotto controllo lo stato delle colture, per calibrarne l'irrigazione in funzione del tipo di semina, di terreno e di situazione climatica, di programmarne il raccolto laddove sia necessario e di monitorare gli spostamenti delle mandrie al pascolo. Progetto relativamente semplice da realizzare nelle immense pianure americane, ma molto più complesso in un comprensorio agricolo montano dove dislivelli, punti ciechi e cambi climatici più repentini possono introdurre elementi di complessità nella struttura del networking.

Oppure si pensi a una completa integrazione tra mo-

vimento treni, servizi d'informazione in tempo reale e controllo degli afflussi all'interno di una linea metropolitana su più livelli, laddove la copertura di tipo wide area debba necessariamente integrarsi con quella di tipo deep area per poter avere la piena copertura, sia nell'ampiezza delle rete orizzontale sia nella profondità verticale dei vari livelli.

Benché reti, protocolli di comunicazione e soluzioni possano essere i più diversi e a volte intercambiabili, sarà fondamentale saper scegliere oculatamente in base al modello economico, coniugando costi di implementazione e gestione, la velocità delle trasmissioni e il tipo di latenza accettabile, la necessità di chiusura o apertura verso altre reti e, non ultimo, la soluzione software di controllo e gestione che consenta la migliore leggibilità, gestione e analisi delle informazioni da parte dei vari livelli dell'organizzazione.

Su questi esempi le soluzioni radio proprietarie LO.RA della francese Kerlink e quelle di SIGFOX suggeriscono, per le loro potenzialità, numerosi spunti, peraltro, molto interessanti. ✨

LinkedData center: una startup tra open data e semantic Web

I dati linkati con un mercato da 325 miliardi di euro in Ue e 8 miliardi in Italia

Si ispira a quanto sta avvenendo in Gran Bretagna, Enrico Fagnoni, coder con 25 anni di esperienza nello sviluppo di soluzioni tecnologiche e di processi di software engineering e fondatore di LinkedData Center. Inghilterra dove negli ultimi mesi sono sorte più di 400 startup che propongono servizi e applicazioni commerciali che sfruttano l'enorme miniera di dati disponibile sul Web. Repository cresciuti con l'evoluzione della rete. Prima i link ai documenti, poi quelli collegati alle persone, rappresentati dal successo planetario dei social network. Oggi è arrivato il turno dei dati a essere linkati tra di loro. Una promessa irresistibile. Infatti già si

dice che chi sarà in grado di sfruttare la potenza di questa massa sterminata di dati sarà il prossimo vincitore del Web. È un mercato dall'enorme potenziale. L'UE fissa a 325 miliardi di euro nei prossimi cinque anni l'asticella del mercato europeo e a oltre otto miliardi quello italiano. Un segmento che creerà nuovi posti di lavoro generando risparmi presso le Pubbliche Amministrazioni pari a circa 1,7 miliardi di euro. Un'opportunità che Fagnoni, da oltre dieci anni impegnato in progetti connessi all'architettura del Semantic Web, non intende lasciarsi sfuggire: «Ci sono voluti sei di anni di ricerca. Anni intensi, di duro lavoro. Ma dallo scorso aprile

scorso siamo pronti». Tecnicamente LinkedData Center è una startup innovativa, ma come precisa Fagnoni, al quale il termine non piace molto, l'enfasi più che sulla ricerca di finanziatori è sul mercato e sull'acquisizione di nuovi clienti. «Ci rivolgiamo alle aziende di qualsiasi dimensione e agli sviluppatori per fornire loro le infrastrutture necessarie per creare valore con i linked open data. Data marketing, social network analysis, knowledge base creation and analysis, fraud detection, asset ma-





Enrico Fagnoni fondatore di LinkedData Center

agement sono alcune delle aree in cui la tecnologia che proponiamo può essere sfruttata con profitto» afferma l'esperto coder.

Una tecnologia quella proposta dall'azienda lariana innovativa, ma al tempo stesso già matura. In grado di sfruttare a vantaggio della clientela le opportunità offerte dal crescente numero di dataset reperibili come open data, utilizzabili dunque anche per fini commerciali. Dati che, solo per fare un esempio, una startup può sfruttare per testare la propria idea di business; oppure per metterla meglio a fuoco. «Forse non tutti i dati di cui abbiamo bisogno sono immediatamente disponibili. Ma gli spazi sono immensi. Si tratta di esplo-

rare con metodo e curiosità quello che già abbiamo a disposizione», dichiara Fagnoni, convinto che Tim Berners-Lee, uno degli inventori del World Wide Web, avesse pienamente ragione quando predisse che la condivisione di dati, di qualunque natura in rete, avrebbe generato, in modi spesso imprevedibili, il loro riutilizzo creativo.

L'azienda ha già al proprio attivo collaborazioni importanti. «Telecom ci segue da tempo. Ma stiamo lavorando per ampliare la no-

stra platea di partner», ci dice Fagnoni che, nel frattempo, ha deciso di insediare i laboratori dell'azienda a Esino Lario, in provincia di Lecco. Questo anche in vista del prossimo evento mondiale che a giugno vedrà coinvolta la comunità di sviluppatori facente capo a Wikipedia e aggiunge

ancora Fagnoni: «Puntiamo molto sulla visibilità dell'evento e sulla possibilità per noi di esserne al centro. Arriveranno da tutto il mondo oltre un migliaio di programmatori e noi vogliamo esserci. Per fare conoscere la nostra azienda e allo stesso tempo sfruttare al meglio la visibilità di un evento che questa piccola comunità si è aggiudicata scalzando la concorrenza di realtà importanti come Bogotà e Atlantic City. Centri di riferimento che potevano contare su mezzi ben più consistenti di quelli a disposizione di Esino». Più o meno lo stesso spirito che anima l'avventura di LinkedData Center. ❖

Italia: la rincorsa verso un modello di lavoro più flessibile

I risultati di uno studio IDC Cornerstone mostrano che, mentre le aziende italiane hanno lavorato bene nell'adozione delle nuove tecnologie, come ad esempio i dispositivi touch, ancora molta strada deve essere fatta per progredire oltre le barriere organizzative e culturali che si oppongono al lavoro flessibile

In Italia il 20% delle imprese non fa ancora uso dell'orario flessibile e il 27% non consente di lavorare





da casa. In Europa le cose vanno meglio. Le indicazioni sono contenute in uno studio, "Future People: Le postazioni di lavoro nell'era della trasformazione digitale", promosso da Cornerstone OnDemand e condotto da

Idc su un campione di 1352 professionisti HR e business manager in 16 paesi europei, che ha analizzato le tendenze e gli sviluppi del lavoro flessibile, della leadership, della gestione delle performance e dello stato delle

HR nelle organizzazioni con oltre 500 addetti. Si tratta di uno degli studi più ampi mai condotto in Europa, su un campione specifico di responsabili delle risorse umane.

Le ragioni di questa ricerca? La trasformazione digitale sta cambiando il modo in cui le organizzazioni operano e la forza lavoro produce valore in Europa. Questi cambiamenti pongono enormi sfide per la gestione delle risorse umane, poiché i dipendenti richiedono spazi di lavoro flessibili e tecnologie di collaborazione all'altezza delle soluzioni consumer, mentre i processi delle risorse umane diventano sempre più digitali e self-service. Di conseguenza, le risorse umane e le line of business devono concordare su quali siano le nuove funzioni da attribuire alla funzione del personale. Da questa ricerca si apprende, anche, che la trasformazione digitale è attualmente una priorità per il 57,4% delle aziende europee: con questo termine si vuole qui soprattutto intendere la riorganizzazione della funzione IT secondo un approccio più allineato con le istanze di business.

Più attenzione al lavoro flessibile

Alcuni aspetti specifici del lavoro flessibile sono collegati a tecnologie abilitanti e la libertà di lavorare da remoto ha un impatto importante sul senso di appartenenza dei lavoratori e sulla loro disponibilità a raccomandare l'impresa a terzi. Ciò significa che i sistemi e le tecnologie per il lavoro flessibile dovrebbero essere una priorità dei Ceo e non dovrebbero essere trattati come un comune progetto IT di carattere marginale.

Per esempio, in merito all'accettabilità del lavoro da casa/da remoto, è stata riscontrata una sostanziale differenza tra nord e sud, dove i paesi del nord Europa mostrano la maggiore accettazione, mentre quelli del centro-sud quella inferiore. Ciò dipende da differenze culturali e manageriali, oltre che da un diverso grado di maturità nell'adozione di determinate tecnologie. Per progredire nelle politiche del lavoro flessibile, le multinazionali europee devono pianificare paese per paese. Lo studio ha, anche, rilevato che le organizzazioni che adottano un approccio collaborativo,

una forte mobilità interna dei dipendenti e un sistema di apprendimento aperto e collaborativo registrano un maggiore tasso di crescita. Dallo studio emerge, altresì, il desiderio che le risorse umane coprano nuove aree, come le statistiche relative alle performance dei dipendenti, l'educazione alla leadership e la semplificazione delle procedure burocratiche.

La situazione in Italia

Guardando nel dettaglio i risultati dell'Italia, ci pare importante evidenziare che la

percentuale di rispondenti orgogliosi del loro posto di lavoro e disponibili a raccomandarlo è circa il 59%. Sono 12 punti percentuali sotto la media europea del 71% e il più basso risultato misurato su dieci paesi. Considerato che i manager e le risorse umane sono i portatori e i sostenitori fondamentali dei valori aziendali, il fatto che soltanto il 59% sia disposto a raccomandare la propria azienda è un dato in qualche modo allarmante, secondo questo studio.

Anche altri studi sul tema "employee engagement" vedono l'Italia posizionata

piuttosto in basso rispetto agli altri paesi europei. Una possibile spiegazione è la competizione limitata per la selezione del talento in un mercato del lavoro abbastanza rigido, tradizionale e regolamentato. Un'altra ragione importante è che le organizzazioni italiane intercettate dallo studio attribuiscono, come detto all'inizio, una valutazione relativamente bassa al lavoro flessibile, che rappresenta un fattore importante per il benessere dei dipendenti. I risultati mostrano che mentre le aziende italiane hanno lavorato bene nell'adozione



L'impegno di Cornerstone

«Era inevitabile che anche le risorse umane evolvessero da un focus basato su processi e automazione a uno che privilegi l'engagement e l'impatto sul business - osserva Franco Gementi, regional sales manager Italia di Cornerstone. Ci vuole agilità prima di tutto. Ossia essere molto più veloci di prima e puntare con decisione sulla centralità delle persone, anche per effetto della crescente importanza acquisita dalla mobilità interna.

Tutto questo per avere delle HR più vicine al business e per creare le condizioni per la misurazione degli impatti».

A questo riguardo, aggiunge, Cornerstone propone una suite, Unified Talent Management strutturata su sette moduli, per la gestione delle competenze aziendali che tiene conto di tutte queste indicazioni e di quelle espresse dai clienti. Si tratta, in sostanza, di un approccio pragmatico ma moderno di gestione di relazioni, performance, formazione e anche analytics. Ai responsabili delle risorse umane, nell'era della digital transformation, Gementi propone una serie di raccomandazioni su cosa concretamente fare per cogliere meglio i vantaggi della innovazione tecnologica: estendere la mobilità dei dipendenti, costruire una cultura di partecipazione, sviluppare partnership con le aree di business, connettere la forza lavoro, migliorare la collaborazione, favorire l'innovazione e l'engagement offrendo flessibilità e opportunità di sviluppo.

Cornerstone è una azienda di Santa Monica (California) leader nelle soluzioni cloud di talent management. Le sue soluzioni sono usate oggi da quasi 25 milioni di utenti in circa 2600 organizzazioni di 191 Paesi, tra cui l'Italia dove è presente dal 2011. Un cliente europeo è Bnp Paribas che nel 2008, a seguito della sua espansione e quindi dell'ampliamento di organico, ha implementato applicazioni di Cornerstone stimolata dai vantaggi offerti da modello SaaS e dalla possibilità di rispondere alla sfide a carattere globale e locale attraverso varie funzionalità e un portafoglio di attività formative configurabili in base a assi funzionali e tematici.

Da ultimo: oltre alla suite prima citata, l'offerta dell'azienda comprende anche le seguenti soluzioni: Extended Enterprise, per offrire formazione e networking alla rete di clienti e partner; Mobile, per migliorare il coinvolgimento delle risorse umane su tutti dispositivi; e Analytics per permettere di prendere decisioni ragionate grazie alla visione in tempo reale della forza lavoro.

delle nuove tecnologie, come ad esempio i dispositivi touch, ancora molta strada deve essere fatta per progredire oltre le barriere organizzative e culturali che si oppongono al lavoro flessibile. Questo riguarda in modo particolare la formazione IT, gli open-space e la mobilità interna. Per quanto riguarda la collaborazione, lo studio rileva che i manager di linea in Italia sono più negativi rispetto ai colleghi europei. Tuttavia, la ricerca evidenzia alcuni segnali di cambiamento in corso. Le più importanti opportunità di crescita per le risorse umane in Italia sono indicate nell'analisi delle performance dei dipendenti (43%), nella disponibilità di migliori strumenti di self-service (34%), nella modellizzazione dei percorsi di crescita (34%).



Una struttura dedicata per diventare una data company

Intesa Sanpaolo è il gruppo bancario nato dalla fusione di Banca Intesa e Sanpaolo IMI, che offre servizi a oltre 11 milioni di clienti avvalendosi di una rete di oltre 4100 sportelli presenti su tutto il territorio nazionale.

L'istituto ha una presenza selettiva in Europa centro-orientale e nel Medio Oriente e Nord Africa, grazie a circa 1200 sportelli e 8,2 milioni di clienti delle banche controllate operanti nel "commercial banking" in 12 Paesi e vanta, inoltre, una rete internazionale specializzata nel supporto alla clientela corporate, che presidia 28 Paesi.

Valerio Cencig, responsabile direzione data office di Intesa Sanpaolo, illustra le ragioni che hanno portato

Valerio Cencig, responsabile direzione data office di Intesa Sanpaolo spiega l'importanza di creare un ufficio dedicato ai dati, che diventeranno, il futuro, una delle principali voci di bilancio



una realtà con queste caratteristiche a dotarsi di una struttura espressamente dedicata ai dati.

Direction:
come nasce la decisione di

dotarsi di una struttura dedicata ai dati?

Valerio Cencig: La predisposizione di un data office è nata nel 2015 a seguito di una consapevolezza forte e decisa da parte della banca in relazione all'importanza dei dati rispetto alle esigenze di compliance, di

supporto al business e della creazione di una piattaforma digitale per accompagnare il processo di trasformazione della banca in una "data company".

D: In quale contesto organizzativo e gerarchico è inserita?

VC: Il Data office riporta al Chief Financial Officer, testimoniando la valenza "business oriented" che si è voluto dare a tale ruolo.

D: Per quali utenze? Ossia come vengono impiegati i dati una volta raffinati?

VC: L'unico vero limite all'utilizzo dei dati, ovviamente nel rispetto dei vincoli dei consensi privacy, è l'immaginazione: non ci sono distretti della banca che non possono beneficiare di un utilizzo intelligente e innovativo dei dati.

D: Quali sono i rapporti con il CIO, il marketing e la componente finanziaria ?

VC: Il CIO è il partner di eccellenza; tutte le altre figure (CIO compreso) sono tendenzialmente utenti dei dati e, come tali, centri di competenza in grado di muovere intelligenze finalizzate a migliorare il loro modo di "fare banca".

D: Che competenze hanno le persone che operano nel Data office ?

VC: Le competenze sono multidisciplinari, perché il data office deve tornare a riunire competenze che, negli ultimi anni, si sono evolute in modo separato, privilegiando la specializzazione, ma anche l'isolamento, rispetto a una visione olistica e interconnessa dei fenomeni.

D: Quali sono le tecnologie che usate al

vostro interno ?

VC: La scelta della tecnologia è un fattore critico di successo ma, allo stesso tempo, tuttora, non esistono modelli consolidati di riferimento. Occorrerà, quindi, sperimentare e accettare di sbagliare, pronti a correggere la rotta. In questa fase è meglio adottare tecnologie ibride (innovative e tradizionali) per conferire maggiore resilienza alle architetture. Allo stesso tempo occorre aprire un osservatorio continuo sul mercato delle tecnologie, per cogliere le opportunità.

D: Come sono i rapporti con i vendor di tecnologie ?

VC: I vendor di tecnologie devono sempre più diventare dei partner che aiutano il committente a realizzare il miglior punto di incontro tra le tecnologie del mercato e le esigenze specifiche del cliente.

D: Quali sono le sfide per un data office in un business aziendale sempre più digitale?

VC: La sfida più grande è sviluppare una "vision" coerente sui dati e condividerla con la banca, facendo ricorso alle migliori capacità

relazionali e, soprattutto, dedicando tanto tempo ai processi di formazione e di change management. Come dice Gartner l'ostacolo maggiore al cambiamento è la resistenza al cambiamento.

D: Quale è a suo modo di vedere la "chimica" che sostiene questa nuova funzione all'interno e agli occhi dei clienti?

VC: Spiegare e dimostrare che usare bene i dati significa migliorare la capacità di servire al meglio i bisogni del cliente interno e di mercato. I dati diventeranno nel futuro la principale voce di bilancio; ed è già così per le "data company".

D: Cosa auspica bisognerebbe fare per dare a un'organizzazione un connotato veramente data-driven?

VC: Innanzitutto separare i dati, che sempre più devono diventare una risorsa condivisa, dai processi: passare dal concetto di possesso a quello di accesso in un'ottica di Data as a Service. Inoltre è necessario comprendere che, a occhi capaci, i dati dischiudono un "insight" profondo su come migliorare prodotti e servizi. ✨

Nuove opportunità per i sistemi di pagamento digitale

La forte digitalizzazione in atto, sia in ambito aziendale, sia personale è un cambiamento di costumi e abitudini che ha un forte impatto non solo nel sociale, ma anche nelle relazioni tra fornitori di servizi finanziari e fruitori dei medesimi.

Quello che chiede il mercato e quello a cui le entità finanziarie dovranno far fronte è abbastanza chiaro ed emerge da analisi di mercato recenti. È un'evoluzione che ha interessato anche l'Unione Europea, che ha emesso una direttiva in proposito. Secondo uno studio condotto proprio sul territorio europeo da Finextra Research per conto di CA Technologies, le istituzioni europee, appartenenti al settore dei servizi finanziari, percepirebbero la nuova direttiva sui pagamenti elettronici (Payment Services Directive 2 - PSD2) come opportunità di crescita del business e non solo come un obbligo di legge.

La ricerca "Preparing for PSD2: exploring the business and technology implications of the new payment services directive" ha evidenziato che i fornitori di servizi di pagamento, tra cui le

La digitalizzazione e la direttiva europea PSD 2 sui servizi di pagamento, aprono nuove prospettive per i servizi finanziari



banche tradizionali, imprese Fintech, operatori di telecomunicazioni ed soggetti terzi prestatori (detti TPP - Third Party Providers), vedrebbero la direttiva PSD 2 come un volano per sviluppare prodotti e servizi finanziari innovativi, offrire una customer experience agevole e di incrementare il fatturato.

Cosa si propone la direttiva PSD 2

La direttiva PSD 2 si propone di rendere più sicure le

transazioni, tutelare i consumatori, agevolare i pagamenti elettronici e stimolare la riduzione delle tariffe.

La nuova direttiva è stata pubblicata nel gennaio di quest'anno sulla Gazzetta ufficiale dell'Unione Europea e dovrà essere attuata entro l'inizio del 2018. Con essa, le banche, vengono sollecitate a concedere ai TPP un accesso sicuro ai conti dei clienti sulla base della disponibilità di informazioni relative ai conti di

pagamento, contribuendo a realizzare un mercato europeo dei pagamenti più efficiente e a creare un adeguato "level playing field", ovvero condizioni di parità per i diversi prestatori di servizi di pagamento.

Il parere degli interessati

Le organizzazioni finanziarie europee sono piuttosto concordi nel considerare la direttiva come una opportunità. Alessandro Bocca, head of acquiring (Online & Retail) presso il Gruppo Banca Sella, vede nella PSD 2 un'occasione favorevole su cui la banca può far leva per arricchire la propria offerta di pagamenti: «Il più delle volte il sistema bancario non è riuscito a tenere il passo con le esigenze di pagamento degli esercenti». Aggiunge Bocca: «In Italia siamo stati noi i primi gateway a integrare i pagamenti Sofort. Non ci limitiamo alle carte; se un cliente vuole usare un PSP Sofort anziché pagare dal portale della propria banca, noi gliene forniamo i mezzi.

Cerchiamo di metterci al loro servizio; se ciò significa accogliere anche prestatori di servizi quali Sofort,



ben vengano. Il mercato dei pagamenti sta cambiando, quindi, la banca, deve cambiare per restare competitiva».

Anche CheBanca! intravede nella direttiva PSD2 l'opportunità di acquisire nuovi clienti, come spiega Roberto Ferrari, direttore generale: «Crediamo nel concetto di open access e open banking, perciò riteniamo che questa sia una buona occasione per proporci come account information service provider o come payment initiation service provider.

In realtà operiamo in questo modo già da qualche tempo. Poco più di un anno fa abbiamo lanciato un nuovo portafoglio digitale chiamato WoW (Wallet of Wallets), che si muove in questa direzione. È un servizio aperto a qualsiasi carta di credito e prepagata, non solo alle nostre».

La direttiva offre alle banche prospettive di guadagno. Jurgen Vroegh, global head della divisione Payments di ING, riconosce l'importanza della PSD2 per gli istituti di credito affermando: «La PSD2 è una tappa cruciale sulla via verso un mercato aperto dei servizi finanziari. Un'occasione per ripensare

i propri modelli di business e trasformarli in un servizio migliore alla clientela, facendo rete con i nuovi operatori, adottando nuove tecnologie e imparando dai concorrenti più agili».

Secondo un esponente della banca olandese Abn Amro, stanno nascendo moltissime opportunità, come, per esempio, la realizzazione di una piattaforma bancaria aperta e sicura. In Italia, anche presso Iccrea Holding, hanno confermato che la PSD2 è una priorità.

L'impatto della PSD2

Pur essendo ancora parzialmente in discussione, la rapidità dei cambiamenti introdotti dalla PSD2 è notevole. Secondo i responsabili di Iccrea Holding, la PSD2 modificherà in maniera so-

stanziale, e "presto", il mercato europeo dei pagamenti, poiché saranno i nuovi attori non bancari a trasformare completamente il contesto. Per Ferrari di CheBanca!, invece, il potenziale ingresso dei GAFA (Google, Amazon, Facebook e Apple) nell'arena finanziaria sulla scia tracciata dalla direttiva PSD2, costituisce una delle principali sfide per gli attuali player. «Sono sicuro che dovranno decidere entro il 2018 se convenga loro proporsi come TPP (ndr "terzi prestatori"), account information service provider o payment initiation service provider», spiega Ferrari, che conclude: «Questo potrebbe aprire la strada a una tipologia di concorrenza più forte e potente di quanto le banche non abbiano dovuto



fronteggiare finora.

Un conto è sfidare gli istituti di pagamento, un altro competere con società quali Google o Amazon».

Un'altra community interessata è quella delle Fintech. Con l'entrata in vigore della PSD2, queste imprese aiuteranno le banche a innovare e creare nuove fonti di gettito, migliorando l'offerta alla clientela.

Le telco e i retailer potranno offrire piattaforme proprie di pagamento, ridurre le commissioni sulle operazioni, consolidare i rapporti con i clienti e proporsi come prestatori di identità.

L'IT sicuro, leva del cambiamento

Stando allo studio, diversi soggetti bancari e prestatori terzi, i cosiddetti TTP,

avrebbero già iniziato il percorso per conformarsi alla direttiva. L'IT giocherà un ruolo centrale e importante come portatore e attuatore di questo cambiamento a livello aziendale. La PSD2 costringerà le banche a facilitare l'accesso ai conti dei clienti e a offrire informazioni sui conti bancari, previo consenso dei correntisti, alle app di terze parti.

Molti dei soggetti interpellati caldeggiano, per esempio, l'impiego di API (Application Programming Interface) per concedere ai terzi l'accesso alle informazioni sui conti. Non sorprende che le nuove banche, prive di vincoli storici e munite di API, possano finire con il padroneggiare la sfida rappresentata dalle API aperte.

«Accogliamo con favore il

passaggio alla PSD2.

Già da qualche anno lavoriamo sull'open banking e sulle API aperte, in linea con la nostra filosofia di banca», dichiara Sophie Guibaud, Vice President European Expansion di Fidor, challenger bank tedesca.

Quello che sarà necessario sarà la cosiddetta "strong authentication", un'autenticazione a due fattori, per appurare l'identità del fruitore di un servizio di pagamento. Quello che si preannuncia è un momento di transizione per il settore che offrirà a operatori del canale e system integrator possibilità di business.

Si tratta, infatti, non solo di sviluppare o dotarsi di apparati a norma, ma di realizzare vere e proprie infrastrutture altamente digitalizzate e sicure, che possano permettere un'interazione con il cliente e con le App totalmente protetta e garantita.

Cosa che, di certo, richiede uno skill adeguato e investimenti in risorse finanziarie e umane strategici e ben studiati, ma che può portare a risultati economici molto positivi per gli operatori che decidessero di investire in tecnologie e soprattutto in know how. ❖



EMC la crescita arriva dal software

Fatturato 2015 in crescita del 12% sul 2014, grazie al contributo dei partner di canale e all'affermazione delle soluzioni di automazione dello storage e ripristino dati

Segno positivo per il Fiscal Year 2015 di Emc, che ha chiuso l'anno registrando un +12% sul fatturato del 2014. Un salto confermato nel primo quarter 2016, in crescita del 7% in euro sullo stesso periodo dell'anno scorso.

«A sostenere questi risultati è stata soprattutto l'attenzione che rivolgiamo a partner e clienti - commenta Marco Fanizzi, amministratore delegato di Emc Italia. Oggi il 70% del nostro business è realizzato grazie al contributo di questo braccio commerciale».

Grande la soddisfazione dell'ad per i risultati della filiale italiana, che detiene il 28,5% del market share storage locale (fonte Idc), con un picco del 33,5% nel



Marco Fanizzi, CEO di EMC Italia

quarto trimestre 2015. Alla realizzazione del suo fatturato contribuiscono soprattutto i prodotti, che oggi pesano per il 70%, mentre i servizi calano al 30% con una flessione che gioca a beneficio dei partner.

«Da parte nostra preferiamo concentrarci sugli aspetti consulenziali, restando all'edge dei servizi - puntualizza Fanizzi. Quelli più tradizionali sono affidati ai partner che hanno la possibilità di estendere il proprio perimetro di business offrendo valore».

All'interno di quel 70% di fatturato realizzato con i prodotti, cresce il contributo del software, oggi a quota 42%. A comporre il dato sono soprattutto le

soluzioni dedicate alla gestione e all'automazione dello storage dei data center (Vipr), accanto a quelle di backup e di ripristino dei dati (Avamar).

«Osservato per industry, il fatturato 2015 mette in evidenza l'effervescenza di settori come il Finance, il Manufacturing, la Sanità e la PA locale - continua l'amministratore delegato, puntualizzando come la maggior parte degli investimenti di oggi si concentri, ancora oggi, sulle piattaforme tradizionali. Sulle nuove piattaforme si registrano alcune fughe in avanti, ma siamo ancora nell'ordine dei PoC, con progetti che spostano in cloud i workload meno critici e sfruttano le nuove piattaforme per guadagnare in agilità» conclude Fanizzi. ❁



DE gustare

alla scoperta dei sapori d'Italia

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

3 ORE AGO

SAVATURE NOTIZIE

**LUGANA E AMICI ALLA
PROVA DEL TEMPO**

READ MORE

7 ORE AGO

NOTIZIE

**FAUNA SELVATICA,
UN SERIO PROBLEMA
PER L'AGRICOLTURA**

READ MORE

4 ORE AGO

EVENTI

**FESTA ARTUSIANA
SOTTO IL SEGNO
DELLA CUCINA
SOSTENIBILE**

READ MORE

01 GIUGNO 2015

La Toscana di Biella

Agricoltura biodinamica

Asparago in cucina

21 GIUGNO AGO

NOTIZIE

**COCKTAIL LOW
ALCOHOL. DUOMO 21
LANCIA IL NUOVO
TREND**

READ MORE

21 GIUGNO AGO

NOTIZIE

**TEATRO DEL G
PER SCOPRIRE
MEGLIO DI M**

READ MORE

2 GIUGNO AGO

NEWS NOTIZIE

**SAN MIGUEL, IL GIRO
DEL MONDO IN UNA
BOTTIGLIA**

READ MORE

4 GIUGNO AGO

NOTIZIE

**VINO E AR
INSIEME P**

READ MORE

DE gustare
alla scoperta dei sapori d'Italia



Alla corte del RE

www.de-gustare.it

The World is Your Workplace

FUJITSU

shaping tomorrow with you



Fujitsu LIFEBOOK S936 Massima sicurezza con sensore palmvein integrato

Il nuovo dispositivo leggero e touch Fujitsu LIFEBOOK S936 è il compagno ideale per chi viaggia spesso. Il vano modular bay garantisce tutta la flessibilità necessaria durante gli spostamenti, mentre protegge i dati dentro e fuori l'ufficio.

- Processore Intel® Core™ i7 vPro™
- Windows 10 Pro
- Massima sicurezza con il sensore palmvein opzionale
- Notebook sottile, 33,8 cm (13,3 pollici) con display WQHD e opzione touch, con un peso di soli 1,37 kg
- Modular bay per drive ottico o seconda batteria



Schermate simulate, soggette a modifica. App Windows Store vendute separatamente. La disponibilità di app e l'esperienza possono variare in base al mercato.

workplace.it.fujitsu.com

© Copyright 2015 Fujitsu Technology Solutions. Fujitsu, il logo Fujitsu e i marchi Fujitsu sono marchi di fabbrica o marchi registrati di Fujitsu Limited in Giappone e in altri paesi. Altri nomi di società, prodotti e servizi possono essere marchi di fabbrica o marchi registrati dei rispettivi proprietari e il loro uso da parte di terzi per scopi propri può violare i diritti di detti proprietari. I dati tecnici sono soggetti a modifica e la consegna è soggetta a disponibilità. Si esclude qualsiasi responsabilità sulla completezza, l'attualità o la correttezza di dati e illustrazioni.

Viene presentato il prodotto pre-rilascio, soggetto a modifica.

Le app vengono vendute separatamente. Offerta di aggiornamento a Windows 10 valida per dispositivi Windows 7 e Windows 8.1 qualificati (compresi i dispositivi già in possesso) per un anno dalla disponibilità dell'aggiornamento a Windows 10.

Per maggiori informazioni visita la pagina windows.com/windows10upgrade.



Windows 10 Pro