

# DIRECTION Reportec 79

SOLUZIONI SERVIZI E TECNOLOGIE ICT

## ICT SECURITY

Intervista a Frank Mong, VP e General Manager di HP Security  
Il Report Check Point 2015 sulle minacce

## CLOUD

Dal Profiling online al Digital single market

## PRINTING

Il marketing dei Fratelli Carli  
lo stampa Ricoh

## DATA CENTER

Dimension Data partner a tutto tondo per la Digital transformation

#focus on

## SMART CITY: L'INTELLIGENZA INTORNO A NOI

Smart Building Solutions di Honeywell per il Vodafone Village  
Building automation nell'edilizia scolastica a Brescia  
Siemens controlla i consumi di EXPO 2015  
Una smartroad per il porto di Amburgo



Smau ti accompagna  
nello sviluppo e nella crescita del tuo business  
in qualità di partner di innovazione.



Nell'anno di **Expo 2015** Smau varca i confini nazionali per creare nuove occasioni di networking a livello internazionale supportando la crescita e lo sviluppo dell'ecosistema dell'innovazione Italiano. Attraverso il suo Roadshow Smau rappresenta il partner di riferimento a supporto della **"digital transformation" delle imprese e delle pubbliche amministrazioni** facilitando l'incontro diretto con 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 svolgono un ruolo fondamentale **per rilanciare l'economia italiana e l'innovazione made in Italy.**

## Le tappe 2015:

BERLINO  
12-13 marzo

PADOVA  
1-2 aprile

TORINO  
29-30 aprile

BOLOGNA  
4-5 giugno

FIRENZE  
8-9 luglio

MILANO  
21-22-23 ottobre

NAPOLI  
10-11 dicembre

<i>l'opinione</i>	Il software è importante, ma non è tutto	4
<b>FOCUS</b>	<b>SMART CITY: L'INTELLIGENZA INTORNO A NOI</b>	5
	Le Smart Building Solutions di Honeywell per il Vodafone Village	8
	Siemens tiene sotto controllo i consumi di Expo 2015	10
	Building automation nell'edilizia scolastica a Brescia	11
	Una smartROAD per il Porto di Amburgo	12
<i>l'opinione</i>	Il valore del dato	13
<i>ict security</i>	I device mobili sono l'anello debole nella sicurezza	14
	La sicurezza di HP parte dal software	16
	La Predictive Security nell'era della Digital Transformation	18
	Attacchi cyber crime più facili e meno costosi	20
	Hacker supercattivo: dai fumetti alla conquista di Internet	22
<i>cloud</i>	Cloud service: dal profiling online al Digital Single Market	24
<i>printing&amp;imaging</i>	Il marketing dei Fratelli Carli lo stampa Ricoh	26
<i>data center</i>	HP si rafforza nel software-defined data center	28
	Dimension Data: noi siamo il partner per la trasformazione digitale	30

l'indice

Direction Reportec - anno XIII - numero 79 mensile giugno 2015 Direttore responsabile: Riccardo Florio  
 In redazione: Giuseppe Saccardi, Gaetano Di Blasio, Paola Saccardi.  
 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.

**COGLI L'OPPORTUNITÀ  
 DI RICEVERE DIRECTION  
 COMODAMENTE NELLA TUA  
 CASELLA DI POSTA  
 SE SCEGLI DI RICEVERE LA  
 TUA RIVISTA VIA E-MAIL  
 SCRIVI SUBITO A  
 servizi@reportec.it**



**Mai più copie "rubate" dal collega, ma possibilità di  
 rapida condivisione dei nostri esclusivi contenuti.  
 Sfrutta il formato elettronico per una più veloce  
 consultazione e creati il tuo archivio personale.  
 Rispetta l'ambiente e aiutaci a usare meno carta**

## *Il software è importante, ma non è tutto*

*L'accento posto dalle aziende fornitrici di soluzioni ICT si è andato spostando sempre più dall'hardware al software e ai servizi. È da questi due settori che i manager si aspettano un incremento delle revenues e dei margini. E di fatto ciò ha un riscontro da parte del mercato.*

*È però vero che quando il novero dei fornitori di servizi finisce con il superare una soglia critica si assiste ad una parcellizzazione dei proventi e ciò può portare a non raggiungere gli obiettivi perseguiti e di conseguenza limitare il proprio aggiornamento tecnologico o l'attenzione dedicata alla componente fisica.*

*Non va perso di vista che software e servizi devono necessariamente viaggiare su una rete, girare su macchine fisiche, sia che si trovino nel cloud privato o ibrido, e la diffusione crescente dell'Internet of Things promette di introdurre nell'equazione un'altra variabile molto pesante per le infrastrutture in termini di caratteristiche fisiche quali capacità trasmissiva, resilienza e capillarità.*

*I nuovi servizi, soprattutto quelli a larga diffusione, richiedono infrastrutture di rete fissa o mobile capillari sul territorio e in grado di convogliare in tempi ridottissimi e in modo sicuro grandi volumi di dati.*

*Si consideri, per esempio, il settore delle utilities presenti in modo massiccio sul territorio, sia a livello provinciale sia regionale. Queste entità si sono o stanno attrezzando per fornire servizi al cittadino o alle aziende sul territorio di competenza. Servizi che vanno da Internet alla voce, dai dati alla videosorveglianza, al telecontrollo di impianti energetici. Per loro realizzare una rete efficiente è essenziale. Lo stesso Internet of Things implica la disponibilità sia di dispositivi periferici che monitorizzino un certo evento sia dell'infrastruttura di rete necessaria per convogliare al centro le informazioni raccolte e permetterne la conservazione ed elaborazione. Una cosa non vive senza l'altra. Anche in questo caso servono dispositivi periferici, IP o meno, dispositivi di aggregazione, dispositivi di switch per convogliare il traffico sulle dorsali, e così via.*

*In sostanza, serve una piattaforma hardware di rete di qualità che il crescere di esigenze di controllo automatico di infrastrutture distribuite sul territorio rende indispensabili per chi voglia erogare servizi. In questo la fibra ottica e la sua capillare diffusione è un valido aiuto, e il corretto abbinamento tra infrastruttura pubblica e una rinnovata rete privata pone le basi indispensabili per affrontare il cambiamento e trarre profitto dall'evoluzione in atto.*



di Giuseppe Saccardi

l'opinione

# SMART CITY: L'INTELLIGENZA INTORNO A NOI

**L**a crescita costante della popolazione mondiale e la sua concentrazione nei centri urbani, il crescente fabbisogno di sostentamento e di sfruttamento delle risorse idriche ed energetiche, spesso a discapito dell'ambiente, sono le ragioni che sempre più rendono urgente la necessità di trovare un modello sostenibile di vita per le future generazioni.

I centri urbani si stanno allargando e si sente parlare ormai frequentemente di trasformazione delle città tradizionali nelle cosiddette "smart city", ossia le città intelligenti del futuro, dove prevale un modello di vita sostenibile ed efficiente a favore di una migliore vivibilità.

Se finora nelle città è prevalsa una logica di funzionamento dei servizi divisa per settori verticali, i quali sono erogati indipendentemente, che siano i trasporti, la distribuzione di energia elettrica o della rete idrica, gli edifici e così via, in una smart city tutto questo deve far parte di un sistema interconnesso e integrato che consenta una maggiore ottimizzazione ed efficienza nell'erogazione dei servizi a cittadini, alle istituzioni pubbliche o private.

Il fine deve essere quello di creare un posto piacevole per vivere, lavorare e passare il tempo libero. Anche a livello sociale deve poter favorire l'inclusione e il sostegno di tutti e creare opportunità per coloro che ci vivono. E un altro fondamentale aspetto è quello della sostenibilità ambientale, per offrire a chi vive nei centri urbani una vita il più possibile sana e per lasciare in eredità alle future generazioni la stessa possibilità. Diventa quindi importante ridurre al minimo l'impatto che la vita dell'uomo ha sull'ambiente circostante, cercando di eliminare il più possibile gli effetti negativi che la vita urbana può causare.

### **Collaborare per costruire la città del futuro**

Per portare avanti il progetto di una smart city è necessaria una stretta partecipazione tra tutti gli attori che la coinvolgono, a partire dal cittadino, per passare alle istituzioni fino al settore privato, grazie ai quali è possibile mettere insieme più competenze possibili e trovare il giusto equilibrio di interessi che consentano di ottenere il benessere dei residenti e della comunità in senso più vasto. Gli stakeholder possono essere molteplici: leader politici e rappresentanti delle istituzioni; fornitori di servizi pubblici o privati quali l'acqua, l'energia elettrica, il gas, le comunicazioni e i trasporti, ma anche la raccolta dei rifiuti e così via; gli utilizzatori finali, ossia i cittadini e i rappresentan-

ti di business locali; gli investitori, banche private e tutti gli organismi finanziari in generale; infine i solution provider che possono essere tecnologici ma anche finanziari. Ciò che rimane fondamentale è trovare il consenso necessario tra queste figure perché soltanto mettendo insieme le diverse competenze si può costruire un progetto valido di smart city.

La collaborazione e la condivisione di informazioni sono quindi indispensabili per realizzare un progetto di smart city, senza di esse non è possibile offrire servizi e infrastrutture intelligenti al servizio della comunità.

### **La tecnologia a sostegno di una smart city**

Un aspetto fondamentale per realizzare una vera smart city è l'utilizzo della tecnologia, l'ICT, e soprattutto il raggiungimento di un livello di integrazione tale da migliorare l'efficienza del sistema, accrescerne i risultati economici, ridurre i costi e aprire le porte al business e ai servizi, migliorando la vita dei cittadini.

L'integrazione tecnologica, per essere realmente efficiente e portare valore, deve essere di tipo orizzontale, quindi deve interessare i differenti silos che finora sono rimasti separati e che compongono l'intero ecosistema urbano. L'interoperabilità, ossia l'interscambio e l'interazione di informazioni, è la chiave per realizzare un sistema che dall'alto governi i singoli sistemi e che funziona grazie all'integrazione delle tecnologie, sia in senso verticale sia orizzontale. Allo stesso tempo questo sistema richiede l'esistenza



di standard comuni che consentono alle tecnologie di diversi fornitori di interagire e agevolare il flusso e lo scambio di informazioni.

Ci sono alcune tecnologie che sono alla base di un smart city, senza le quali questa non può realizzarsi.

Innanzitutto è necessaria la predisposizione di una rete a banda larga che sia di supporto a tutta l'area urbana, e che deve comprendere infrastrutture dedicate che combinano connessioni via cavo, fibra ottica e wireless. Lo scopo ultimo è quello di fornire il libero accesso a una rete a banda larga a tutti i soggetti presenti in un'area urbana. In particolare lo sviluppo della fibra ottica rappresenta la soluzione ideale per offrire connessioni ad alta velocità e di conseguenza favorire lo sviluppo di servizi di connettività per i cittadini, le istituzioni e i privati. La rete diventa in pratica un servizio alla comunità. Grazie alla banda larga si possono poi abilitare una serie di applicazioni per la sicurezza, così come migliorare i servizi offerti dalla municipalità.

Grazie alla fibra ottica in particolare è possibile sfruttare l'installazione di sensori che in futuro saranno sem-



pre più utilizzati per fare rilevazioni in real time e per sviluppare soluzioni tecnologiche intelligenti. I sensori possono essere utilizzati, per esempio, per monitorare e gestire le necessità di mobilità dei cittadini, abilitando la creazione di un sistema di trasporti intelligente capace di rilevare il traffico e comunicare eventuali problemi di congestione da gestire. Oppure possono servire per effettuare rilevazioni ambientali così come per offrire servizi di monitoraggio all'interno degli smart building, gli edifici intelligenti in cui può essere utile rilevare il consumo di acqua, elettricità e gas, ma anche per la videosorveglianza. In particolare, quest'ultima, è fondamentale anche per attivare sistemi di sicurezza pubblica e di prevenzione. In futuro tra l'altro è auspicabile che ci sia una diminuzione dei costi dei sensori così come delle tecnologie RFID.

La disponibilità di una rete wireless è invece fondamentale in una smart city per supportare le connessioni dei molteplici mobile device presenti e l'utilizzo di applicazioni mobile, così come lo sviluppo dell'Internet of Things (IoT) che con-

sente di sfruttare la rete per connettere gli oggetti fisici che possono poi essere controllati da remoto.

Il flusso di informazioni che si possono raccogliere tramite questi sensori e da altre tecnologie a un livello più esteso consente, infine, di dar vita un sistema di intelligenza collettiva integrata della città che la rende davvero "smart". Un'intelligenza che deriva dall'utilizzo di sistemi e tecnologie ICT integrate e che rappresenta praticamente quello che si può definire il "sistema nervoso" alla base di una città moderna e intelligente. Le tecnologie più recenti, come il cloud computing, l'IoT, i Big Data, la Web Semantic avranno in più un ruolo importante per lo sviluppo delle smart city. Queste tecnologie possono assicurare economie di scala per le infrastrutture, la standardizzazione delle applicazioni, e soluzioni chiave per il software as a service, che possono far scendere notevolmente i costi di sviluppo e accelerare così lo sviluppo delle smart city in futuro.

### **Edifici sempre più Intelligenti**

Gli edifici sono parte integrante dell'ecosistema di una città ma soprattutto sono i luoghi dove le persone passano la maggior parte della propria vita, che sia l'abitazione privata, l'ufficio in cui lavorano o altri edifici, magari ricreativi, commerciali o di cura. Questo fa capire l'importanza che questi ambienti rivestono nella qualità della vita delle persone e a livello di impatto sull'ambiente urbano.

Grazie all'utilizzo delle moderne tecnologie gli edifici attuali possono essere progettati per offrire

molto di più di quello che finora è stato possibile e diventare più "green" e sostenibili.

Uno smart building (edificio intelligente) si può definire ecosostenibile quando mette in atto un utilizzo efficiente delle risorse, magari attraverso il riciclaggio di queste o l'utilizzo di energia pulita.

Un altro aspetto è quello della sicurezza che può essere garantita attraverso tecnologie di videosorveglianza e rilevamento e controllo degli accessi.

Dal punto di vista della qualità della vita all'interno, quindi di comfort, gli smart building possono offrire servizi di connettività, piuttosto che il controllo della temperatura e della qualità dell'aria, l'illuminazione automatizzata e così via. Soprattutto la capacità di questi edifici di regolare in modo automatico e integrato diversi aspetti che finora sono rimasti gestiti singolarmente è quello che maggiormente li differenzia dagli edifici tradizionali. Così come la possibilità di verificare attraverso il monitoraggio continuo di vari sensori lo stato di fornitura e disponibilità di tutti i servizi, come il riscaldamento o la disponibilità di acqua, per citarne alcuni.

In più, con lo sviluppo dell'Internet of Things (l'IoT) sarà sempre più possibile in futuro gestire da remoto anche gli elettrodomestici, connessi via WiFi, piuttosto che le telecamere adibite alla videosorveglianza, con la possibilità di interagire direttamente con essi tramite i dispositivi mobili o dal pc. \*

# LE SMART BUILDING SOLUTIONS DI HONEYWELL PER IL VODAFONE VILLAGE

*Una struttura avveniristica alla periferia di Milano, costata 300 milioni di euro, ottimizzata per ridurre i consumi energetici e migliorare l'esperienza lavorativa di 3mila persone*

**D**ue eccellenze tecnologiche si incontrano a Milano all'insegna dell'innovazione, della sostenibilità e dell'efficienza: le Honeywell Building Solutions per la realizzazione di edifici "smart" e la futuristica architettura del Vodafone Village.

Vodafone Village è la struttura avveniristica che ospita tutto il personale Vodafone che opera nell'area milanese, che supera le 3mila unità.

A curare gli aspetti tecnologici e di automazione Honeywell, un colosso mondiale che in Italia impiega 1400 persone, con tre siti produttivi e una struttura dedicata di Ricerca e Sviluppo.

«Honeywell Building Solutions realizza sistemi completi "chiavi in mano" per la gestione del ciclo di vita degli edifici intelligenti - ha spiegato Fabio Bruschi, District General Manager Italy di Honeywell

che comprendono gli aspetti di progettazione, ingegnerizzazione, installazione, assistenza e manutenzione, la componente di integrazione di sistemi e sottosistemi, i servizi per l'efficiamento energetico.

Honeywell dedica molte risorse alla componente software perché è sempre più questo il motore dell'innovazione, tanto che la metà dei nostri 22mila ingegneri sviluppa software. Tra le priorità che guidano il nostro sviluppo vi è quella di mettere a punto processi che riducano sempre più il consumo energetico e lo spreco di risorse».

## Un approccio all'avanguardia

In base a questo approccio Honeywell ha curato dall'inizio il progetto Vodafone Village, avviato nel 2006 con l'obiettivo di incrementare la produttività, l'efficienza e ridurre i costi sostituendo la precedente area uffici distribuita su 28 edifici, che costava moltissimo e risultava poco efficiente, con un'unica struttura.

La scelta del sito ha tenuto conto anche della posizione abitativa dei dipendenti in modo da ottimizzare gli aspetti logistici e ridurre tempi e costi di trasferimento, portando a identificare l'area ottimale nella zona Mecenate a Milano.

La realizzazione ha richiesto circa 3 anni e mezzo e ha coinvolto nel processo decisionale tutti i dipartimenti Vodafone, attraverso una serie di workshop indirizzati a recepire una serie di indicazioni direttamente dagli utilizzatori finali (overo i dipendenti) in relazione

al dimensionamento degli spazi, al layout delle postazioni, al loro aspetto, all'organizzazione delle adiacenze tra differenti divisioni di business, alle strutture accessorie e così via.

## I numeri del progetto

Vodafone Village prevede 3mila posti di lavoro e dispone di 1100 posteggi, caffetteria, teatro da 380 posti, 43 meeting room, giardino fotovoltaico sopraelevato da 800 m<sup>2</sup>, healthcare, bar e ristoranti, call center da 300 persone e perfino docce a disposizione per i dipendenti che vogliono approfittare delle pause lavorative per fare attività sportiva. L'area uffici si sviluppa su circa 30mila metri quadrati a cui corrispondono 27mila metri quadrati di finestrate per massimizzare l'efficienza energetica.

«L'obiettivo nella gestione degli spazi è che i dipendenti Vodafone possano lavorare al meglio possibile all'interno di ambienti ottimizzati - ha spiegato Gianbattista Pezzoni, Head of Properties and Facilities di Vodafone -. Si basa sul concetto di open space che permette modalità di lavoro più flessibili. Entro la fine del 2015 prevediamo di eliminare completamente le scrivanie assegnate, trasformandole in spazi comuni in base a una modello di lavoro basato sulla collaboration, anche da remoto, e la flessibilità, che porterà a predisporre 100 scrivanie per 120 dipendenti con una superficie media di 12 metri quadrati per postazione di lavoro».

**Fabio Bruschi,**  
District General  
Manager Italy  
di Honeywell



La struttura prevede un sistema di recupero delle acque piovane per l'irrigazione del verde, un generatore interno da 3,2 MW, dispone di un rivestimento esterno in cemento fotocatalitico (un brevetto di Italcementi per l'adsorbimento di inquinanti nell'aria) e ha richiesto la posa di 700 Km di cavi.

Sono stati implementati 70mila punti sensore. Grazie a questi sensori viene effettuata una regolazione automatica a ogni piano dei parametri di temperatura, umidità, luce, consumo energetico, viene ottimizzata la distribuzione delle auto nei parcheggi e gestita ogni risorsa all'insegna dell'efficientamento energetico. A livello di sicurezza, il Vodafone Village prevede 3500 punti anti-intrusione, 11mila punti antincendio, 1200 telecamere di sorveglianza e include al suo interno anche un Security Operation Center attivo 24 ore su 24, 7 giorni su 7 utilizzato sia per la gestione degli asset Vodafone sia per erogare servizi anticrimine informatico alla Polizia di Stato.

### Un ROI in otto anni

La struttura è stata realizzata modificando in modo molto consistente un edificio esistente che è stato ristrutturato con una spesa complessiva stimata in circa 300 milioni di euro. Rispetto a prima Vodafone ha ridotto del 50% le emissioni di CO2 e del 17% i consumi elettrici.

«Vodafone Village è un esempio applicativo di tutto quello che si

può realizzare di innovativo all'interno di un building di qualità - ha commentato Bruschi -. In questo edificio sono state implementate una serie di soluzioni all'avanguardia tecnologica che si traducono in una serie di vantaggi per tutti».

Honeywell ha fornito a Vodafone strumenti puntuali e certificati per misurare il risparmio economico (Post Investment Review) che prevedono il rientro dell'investimento in otto anni: un tempo molto contenuto considerato che la cifra in gioco è di 300 milioni.

«Per questo progetto abbiamo scelto Honeywell con cui collaboriamo da anni in modo proficuo - ha osservato Pezzoni - e di cui apprezziamo la competenza, la vastità dell'offerta e la capacità di fornire un servizio a tutto tondo, che ci hanno consentito di avere un unico interlocutore per un progetto così complesso».

### Honeywell Command & Control Suite

Il progetto è in costante evoluzione. Da oggi Vodafone, come gli altri clienti Honeywell, avranno inoltre la possibilità di disporre di alcuni strumenti in più.

«I sistemi dedicati al business, alla sicurezza e alla gestione di uno smart building generano costantemente grandi quantità di dati - ha osservato Dario Sala, Strategic Marketing Director Europe di Honeywell -. Trasformare i dati in informazioni operative e condividere tali informazioni con l'audience giusta e nel momento giusto rappresenta una vera sfida. Per questo Honeywell ha rilasciato Command and Control Suite».

Honeywell Command & Control Suite

è una soluzione che permette di rendere disponibili informazioni in modo semplice e di correlare le informazioni provenienti da diversi sistemi. Mette a disposizione: visualizzazione, comando e controllo dei sistemi di Building & Business attraverso tre componenti applicative realizzate sulla base della piattaforma Honeywell Enterprise Buildings Integrator (EBI):

- Command Wall: mette a disposizione un ambiente di lavoro integrato per la gestione dell'edificio che abilita un accesso rapido alle informazioni e una maggiore visibilità sul loro contesto.
- Incident workflow: facilita gli utenti nel processo decisionale e di risposta nelle situazioni critiche, integrando procedure, operazioni di emergenza e applicazioni aziendali.
- Enterprise dashboard: visualizza i KPI nei formati più avanzati e aiuta a prendere visione del consumo energetico e dell'efficienza. ✱



# SIEMENS TIENE SOTTO CONTROLLO I CONSUMI DI EXPO 2015

*Gli energy manager dei padiglioni possono controllare i consumi dallo smartphone in tempo reale tramite l'App per la gestione dell'energia sviluppata da Siemens per Enel*

L'avvento delle cosiddette smart grid riflette la convergenza di energia e informazione per aumentare l'efficienza energetica, abbassando contestualmente costi operativi ed emissioni.

In quest'ottica nasce Energy Management System (EMS) un software realizzato da Siemens in collaborazione con Enel Distribuzione alla base del funzionamento della smart grid di Expo, che consente di verificare, in tempo reale, lo stato di funzionamento di tutti i dispositivi della smart grid, effettuare operazioni di controllo e supportare i processi di manutenzione ordinaria e straordinaria, segnalando l'eventuale presenza di guasti e anomalie. Tutto ciò facendo leva su un'interfaccia Web e multilingue, basata su piattaforma cloud e accessibile con un semplice smartphone.

Il sistema di gestione dell'energia riceve anche i dati provenienti dalla piattaforma tecnologica che controlla l'infrastruttura di ricarica dei veicoli elettrici a disposizione per gli spostamenti di servizio all'interno dell'area di Expo 2015 o utilizzati dai visitatori per raggiungere la stessa.

EMS è una soluzione modulabile e personalizzabile basata su tecnologia cloud, che svolge funzioni di monitoraggio, supervisione, controllo e ottimizzazione dei flussi energetici di una smart grid, microgrid o smart city.

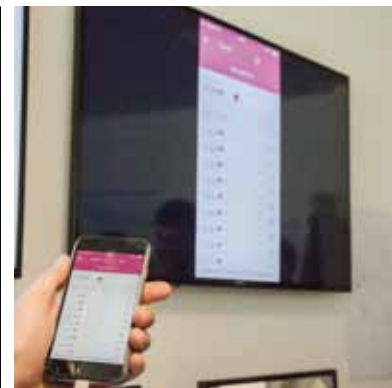
Tramite un'interfaccia utente semplice e intuitiva, mette a disposizione dell'energy manager uno strumento unico per il monitoraggio dei consumi e della produzione e per la supervisione e controllo a livello di Grid Operation di:

- SmartMeter e sistemi di Meter Data Management;

- SCADA (Supervisory Control And Data Acquisition) per la supervisione e controllo della rete di distribuzione elettrica;

- SCADA per la supervisione e controllo di consumi e generazione all'interno di Micro Grid.

Inoltre EMS integra, in linea con le esigenze delle



moderne Smart City, dispositivi e sistemi per la gestione degli impianti di automazione degli edifici, della mobilità elettrica e dell'illuminazione pubblica.

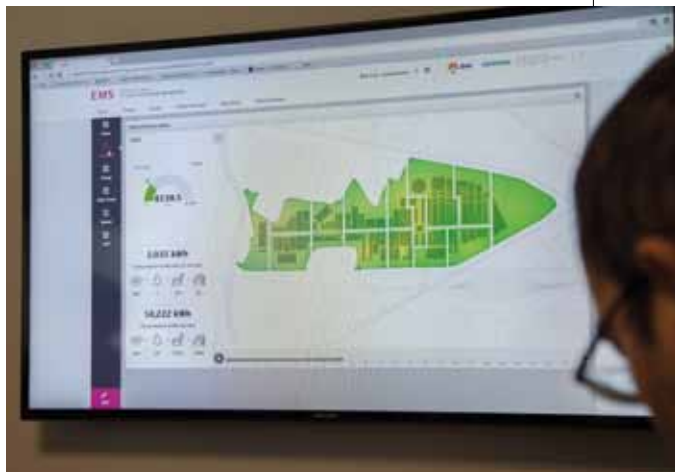
L'architettura della soluzione segue il paradigma dell'Internet of Things (IoT) e si avvale di un database non relazionale e di un sofisticato motore di policy per definire le politiche energetiche in modo semplice tramite interfaccia grafica.

Il sistema EMS è disponibile sia in modalità Software as a Service su abbonamento, sia in modalità On Premise su hardware dedicato presso il data center del cliente tramite licenza.

I servizi di EMS sono fruibili tramite un'applicazione Web HTML5, quindi disponibile su diversi dispositivi e sistemi operativi. L'applicazione, chiamata EMS Operation Center, è ottimizzata per dispositivi notebook/desktop.

È inoltre disponibile EMS Mobile, ovvero una App ottimizzata per smartphone e tablet (Android/iOS) che garantisce le medesime funzioni disponibili sul Web a seconda delle esigenze del cliente. Al fianco di una proposta Core, offre la possibilità di integrare ulteriori funzionalità di Energy Reporting, Active Demand e di Generation Forecast.

\*



# BUILDING AUTOMATION NELL'EDILIZIA SCOLASTICA A BRESCIA



*Un edificio scolastico pubblico all'insegna dell'automazione, del risparmio energetico e della sostenibilità ambientale realizzato da ABB*

La nuova sede del Liceo Artistico Olivieri di Brescia, realizzato dall'Assessorato Edilizia Scolastica della Provincia di Brescia si avvale di un sistema di building automation a standard internazionale KNX che prevede soluzioni inerenti la bioclimatica e le energie rinnovabili.

A implementare la soluzione è stata ABB, multinazionale nelle tecnologie per l'energia e l'automazione.

L'edificio dell'Istituto bresciano, in classe energetica B, si estende su quattro piani per un totale di oltre 5600 metri quadrati. La progettazione si è posta come obiettivo primario quello di sfruttare in modo ottimale le risorse naturali a disposizione, attraverso un impianto fotovoltaico da 20kW e un sistema di recupero dell'acqua piovana. La parte esterna è stata progettata secondo i canoni della bioedilizia, utilizzando materiali come il legno pressato e intonaci fotocatalitici per abbattere le polveri sottili. Per sfruttare al meglio l'illuminazione naturale e predisporre un'ottimale microcircolazione dell'aria tra gli ambienti sono stati collocati, ai due lati dell'edificio, due "pozzi" di luce e ventilazione. L'edificio è stato completamente cablato e dispone di una copertura Wi-Fi totale per l'e-learning.

Un esempio di come anche nell'edilizia scolastica sia possibile



introdurre elementi di progettazione all'insegna della sostenibilità e dell'efficienza energetica, in grado di ridurre i costi legati al riscaldamento e all'illuminazione, diminuire l'impatto ambientale e creare, nel contempo, un ambiente più confortevole e sicuro per la salute.

«Questo progetto rientra all'interno della più vasta tematica delle smart city - ha osservato Riccardo Izzi, Product Marketing Director, divisione Prodotti di Bassa Tensione di ABB Italia - riguardante una nuova visione urbanistica che fa leva sulla building automation applicata per migliorare l'efficienza energetica e accrescere sicurezza e comfort di edifici e immobili. In futuro, questa visione dovrà essere applicata sistematicamente anche alle città, per una migliore gestione dei servizi dedicati ai cittadini e un utilizzo ottimale delle risorse energetiche globali».

Le tecnologie di automazione implementate all'interno del sistema di building automation dell'Istituto consentono di regolare e controllare: l'illuminazione a seconda della presenza di persone e del livello di luce naturale; l'impianto di riscaldamento

attraverso termostati di regolazione presenti in tutte le aule; l'impianto antieffrazione; gli allarmi di evacuazione e le campanelle orarie.

È possibile inoltre monitorare l'ambiente esterno e interno, in modo da garantire le migliori condizioni possibili di comfort. I dati atmosferici raccolti da una centralina meteorologica vengono utilizzati per valutare l'apporto di luce naturale e, se necessario, attivare il comando automatico delle finestre a vasistas per una corretta circolazione dell'aria.

Alcuni sensori dislocati in diverse aule della scuola rilevano le condizioni di umidità, temperatura e concentrazione di anidride carbonica: i dati vengono elaborati e presentati in tempo reale, insieme ai consumi istantanei di energia, su un monitor collocato all'ingresso dell'istituto, sensibilizzando in questo modo l'utenza sui diversi aspetti di risparmio energetico ottenuti. \*

# UNA SMARTROAD PER IL PORTO DI AMBURGO

*È operativo il prototipo della soluzione SmartROAD sviluppata da Cisco per migliorare la gestione delle risorse, i flussi di traffico, il controllo delle condizioni delle infrastrutture e l'impatto ambientale*

L'Autorità Portuale di Amburgo (HPA) vuole trasformarsi in un porto intelligente. In questo percorso si inserisce l'adozione, per ora a livello prototipale, delle soluzioni smartROAD, sviluppate da Cisco e migliorate grazie alla collaborazione con una serie di partner: Philips (illuminazione intelligente), AGT International (software di analytics), T-System (la divisione servizi e consulenza IT di Deutsche Telecom), World Sensing (monitoraggio e sensori) e Kiwi (video analytics e anonimizzazione). Le soluzioni smartROAD si propongono di migliorare la gestione delle risorse, i flussi di traffico, il controllo delle condizioni delle infrastrutture e l'impatto ambientale intervenendo sulle seguenti quattro aree.

- **Traffic Management:** aiuta il responsabile della gestione della

viabilità del porto a monitorare il traffico stradale. Eventuali incidenti sono individuati automaticamente e il manager viene allertato, per coordinarsi con le altre autorità.

- **Sensori strutturali:** i sensori forniscono dati in tempo reale sulle condizioni di infrastrutture mobili quali il ponte di sollevamento Kattwyk Lifting Bridge, consentendo al dipartimento di manutenzione tecnica di pianificare in modo preciso e predittivo le operazioni di manutenzione e gli interventi di riparazione.
- **Sensori ambientali:** forniscono dati da usare per migliorare l'analisi della situazione ambientale nell'area portuale.
- **Illuminazione intelligente:** migliora la sicurezza di pedoni e ciclisti che transitano nel porto e, nel contempo, consente di ri-

sparmiare energia. Fa parte del prototipo anche la sperimentazione di una particolare modalità di illuminazione (Follow Me Lighting) impiegata su una delle strade per migliorarne specificamente l'utilizzo.

«Con smartROAD l'Autorità Portuale di Amburgo sta sperimentando per la prima volta un prototipo integrato di applicazione dell'Internet of Everything, operativo su una infrastruttura reale, che offre diverse e importanti opportunità di utilizzo sia per il porto sia per la città» ha osservato Sebastian Saxe, CIO e CDO di HPA.

Tutti i sensori e i sistemi presenti sono connessi da una infrastruttura di rete sicura. I dati vengono elaborati tramite una soluzione di analytics che mette a disposizione i risultati tramite un cruscotto integrato e centralizzato. Cisco ha anche realizzato una architettura di sicurezza complessiva che fornisce visibilità anche sui parametri legati agli aspetti di Safety & Security consentendo ai responsabili del porto di agire in tempo reale in caso di necessità.

Dal momento che per il monitoraggio del traffico sono utilizzate videocamere, è obbligatorio anonimizzare i dati. Per questa ragione Cisco ha implementato con la collaborazione di Kiwi un software che sfuma i volti delle persone e le targhe delle auto. Questo livello di informazione è eliminato direttamente a livello della videocamera e non entra nemmeno nella rete. \*





di Gaetano Di Blasio

## **Il valore del dato**

*Una gestione automatica dei dati basata su regole semplici consente di ottimizzare gli spazi storage e di ridurre il total cost of ownership dei dispositivi atti alla memorizzazione.*

*Le offerte in tal senso stanno maturando rapidamente e presto ci dimenticheremo completamente di tutte le problematiche legate alla classificazione dei dati, alla loro protezione e archiviazione.*

*Di fatto è pressoché impossibile valutare con precisione quanto valga un dato, fatta eccezione, forse, per i dati critici.*

*Questi ultimi, quantomeno, si arriva a identificarli, ma i dati memorizzati nel mondo sono dell'ordine degli Zettabyte, presto decine di Zettabyte. Di questi, circa due terzi sono prodotti dai consumatori, ma, riporta una recente infografica di Nexsan, sono le imprese a essere responsabili della conservazione, fruibilità e protezione per l'85% dei dati mondiali.*

*Il conservatore produce il dato e, di riflesso, questo assume un valore per il cloud provider o l'operatore telefonico che si sono impegnati a fornire determinati servizi. Se, però, si guarda oltre questi, che sono a tutti gli effetti big data, e li si osserva dal punto di vista degli insight che con gli analytics è possibile ricavarne, le logiche di valutazione cambiano completamente.*

*In attesa di regole condivise sulla privacy e partendo dal presupposto che almeno le analisi basate sui dati anonimizzati siano lecite, ci chiediamo: quanto vale un singolo dato in un campione statistico? Lasciando che i matematici formulino la giusta equazione, per le imprese la verità è semplice: tutti i dati hanno potenzialmente lo stesso valore. Anche perché il singolo dato potrebbe non essere importante oggi ma domani sì.*

*Le soluzioni di prossima generazione cancelleranno il problema, sempre grazie alla statistica, perché, in fondo, classificare il valore di un dato è molto più semplice di quanto fin qui ipotizzato: quello che si usa è importante, quello che non viene mai usato, non serve. Sembra troppo banale, ma bastano poche regole, per esempio, è evidente che questo non può valere per i file destinati alla conservazione elettronica sostitutiva. I sistemi di analisi già oggi disponibili consentono e consentiranno con sempre maggiore accuratezza e minor costo, di classificare i dati automaticamente, calcolando il valore del dato in base al suo utilizzo, che è poi ciò che serve per decidere se il dato va memorizzato su dispositivi a rapido accesso, più costosi, o su storage più lenti ed economici.*

# I DEVICE MOBILI SONO L'ANELLO DEBOLE NELLA SICUREZZA

**Il Report 2015 di Check Point sulle minacce rivela quali rischi corrono le imprese, attaccate, nel 2014, da 106 nuovi malware l'ora, 48 volte più che nel 2013**

di Gaetano Di Blasio

La pressione dei cybercriminali continua a crescere, tanto che per le imprese sembra una lotta senza speranza. Il problema, come sottolineano i responsabili di Check Point è che, nonostante episodi diffusi, come nel caso Cryptolocker, continua a mancare una cultura sulla sicurezza informatica in azienda.

Purtroppo, sviluppi tecnologici come la mobility e il cloud, adottati dalle imprese per aumentare la produttività, comportano nuovi rischi, ancora molto trascurati, facilitando il lavoro dei malintenzionati.

Presentando il Security Report 2015, Roberto Pozzi, Regional Director Southern Europe di Check Point Software Technologies, sottolinea quanto sia sempre più un'opera di sensibilizzazione presso i responsabili aziendali, affinché si cerchi di prevenire le falle che aiutano i cybercriminali nei propri intenti.

Rimarca Pozzi: «Solo armandosi di conoscenza e di solide soluzioni di sicurezza, le organizzazioni possono proteggersi contro minacce sempre più evolute. Rendendo la sicurezza un elemento fondamentale della strategia aziendale è possibile farne uno strumento di produttività, innovazione e maggiori prestazioni».

## I PRINCIPALI RISULTATI DEL RAPPORTO

Il dato che non meraviglia, ma cionondimeno preoccupa, riguarda i dispositivi mobili, con cui il proprietario/utilizzatore instaura un rapporto quasi di dipendenza, improntato sulla massima confidenza. Gli autori della ricerca calcolano che in un'organizzazio-

ne con più di duemila dispositivi mobili nella propria rete, vi è una probabilità del 50% che almeno sei di questi siano infettati o siano l'obiettivo di un attacco. È sempre più facile per un malintenzionato penetrare questi sistemi, perché senza troppa attenzione sono tanti gli utenti che cascano nelle trappole dei cybercriminali. I manager aziendali che sono stati intervistati si dichiarano sensibili alla questione: il 72% dei responsabili IT afferma che rendere sicure le informazioni contenute sui dispositivi mobili è la massima priorità nella strategia per la mobility. Mentre per il 67%, la seconda sfida riguarda il BYOD (Bring Your Own Device) o, più precisamente, la gestione dei dispositivi mobili che appartengono ai dipendenti.

David Gubiani, Technical Manager di Check Point Software Technologies Italia, durante la conferenza stampa, fornisce una dimostrazione di come possa essere semplice non solo "entrare" in uno smartphone, attraverso una mail o, per esempio, un post su un social, ma copiare i dati su esso contenuti o registrare una conversazione sia telefonica sia dell'ambiente in cui si trova il dispositivo.

È un esempio, ma i rischi sono veramente tanti, come mostra il report, basato sull'analisi approfondita di oltre 300mila ore di traffico monitorato in rete attraverso 16mila gateway e un milione di smartphone e grazie a una ricerca collaborativa. In particolare, sono 13mila i clienti (100 in Italia, la nazione con il più alto numero di partecipanti) che hanno consentito ai tecnici di Check Point di monitorare il traffico sui propri sistemi.

Il primo dato riguarda la crescita esponenziale del malware noto e sconosciuto: nel 2014 gli attacchi di malware sono cresciuti con una velocità allarmante. Il report rivela che 106 malware sconosciuti hanno colpito ogni ora le organizzazioni prese in esame: 48 volte in più rispetto ai 2,2 download all'ora rilevati nel 2013. Secondo gli autori del report, peraltro, preoccupa la crescita delle minacce 0 Day, a dimostrazione delle maggiori risorse dei Black Hat hacker (i cattivi), capaci di scoprire le vulnerabilità ben prima dei produttori di software.

Le sfide poste dal BYOD



Altro dato impressionante è il numero assoluto di nuovi malware: 142 milioni nel 2014 con una crescita del 71% rispetto al 2013. Però a colpire sono anche le minacce conosciute: per esempio, l'83% delle organizzazioni prese in esame è stata infettata da bot nel 2014.

### WEB SERVICE PERICOLOSI E DATA LOSS

Un altro rischio che corrono le imprese riguarda quella che viene spesso chiamata shadow IT, cioè i molti servizi Web che, in modalità cloud, vengono attivati dai dipendenti senza coinvolgere lo staff IT aziendale e spesso in modalità gratuita, quindi senza alcuna garanzia sulla sicurezza. Un problema spesso connesso con il BYOD, laddove il dispositivo usato per il privato contiene informazioni che magari vengono copiate nel cloud insieme alle foto delle vacanze.

A questi si aggiungono anche applicazioni più o meno discutibili, come Torrent e i vari Peer to Peer, o gli anonymizer. Secondo la ricerca, il 96% delle organizzazioni prese in esame ha utilizzato almeno una applicazione ad alto rischio nel corso del 2014, con una crescita del 10% rispetto all'anno precedente. Gli esperti hanno anche misurato un tasso pari a 12,7 eventi ad alto rischio l'ora: ciascuno di questi può essere un attacco che va a buon fine permettendo ai criminali informatici di accedere a una rete aziendale. La perdita di dati, peraltro, avviene spesso per errori o comportamenti scorretti del personale aziendale.

Più precisamente, la ricerca rivela che l'81% delle imprese coinvolte ha subito perdite di dati, il 41% in più rispetto al 2013.



**Roberto Pozzi,**  
*Regional Director Southern Europe di Check Point Software Technologies*  
**David Gubiani,**  
*Technical Manager di Check Point Software Technologies Italia*



### LE BUONE NOTIZIE

Lo scenario è certamente tragico, ma il rapporto completo mostra anche qualche risultato positivo, come l'impatto di tecnologie come la Threat Emulation di Check Point (catalogabile tra le soluzioni di sandboxing, semplificando un po'), che svolgono un'efficace azione di contenimento degli attacchi.

I responsabili locali della multinazionale israeliana sottolineano anche le elevate capacità della recente Threat Extraction, che va oltre la simulazione del codice sospetto, arrivando a riscrivere il codice stesso, "pulendolo" di tutte le componenti potenzialmente pericolose (per esempio un file di Word, di cui viene praticamente conservato solo il contenuto testuale). La tecnologia di Check Point, spiega Gubiani, consente di eliminare tutte le componenti attive e, in particolare, quelle che impattano sui controlli a livello di CPU, utilizzate per eludere le tecnologie di emulazione e sandboxing.

Concludendo, Pozzi e Gubiani rimarcano l'importanza dell'educazione alla sicurezza, che deve essere affrontata seriamente in azienda, definendo un vero e proprio regolamento aziendale, distribuito in tutta l'azienda e affisso in bacheca: non bastano raccomandazioni via mail. L'IT deve poi implementare sistemi che consentano di rafforzare il rispetto delle politiche aziendali e le policy di sicurezza attraverso automatismi e strumenti che delegano (per quanto possibile con le leggi italiane) la responsabilità all'utente finale:

per esempio avvisando che si sta inviando via mail un documento classificato e imponendo all'utilizzatore una scelta consapevole delle conseguenze. \*

# LA SICUREZZA DI HP PARTE DAL SOFTWARE

**Intervista a Frank Mong,  
Vice President and General  
Manager Security Solutions  
di HP Enterprise Security  
Products**

di Riccardo Florio

**A**ttaverso la divisione Enterprise Security Products, HP mette a disposizione delle aziende un set di soluzioni hardware e software adatto a rispondere alle esigenze di rilevamento delle minacce esterne e interne e a predisporre azioni di risposta che intervengono per proteggere dati, reti e applicazioni; il tutto affiancato da una "intelligence" di sicurezza globale e aggiornata in tempo reale.

Direction ha incontrato Frank Mong, Vice President and General Manager Security Solutions di HP Enterprise Security Products in occasione della sua visita in Italia durante l'evento HP Software Performance Tour, per sapere le direzioni di evoluzione dell'approccio HP alla sicurezza.

**Direction: Qual è un aspetto caratterizzante della vostra proposta di sicurezza?**

Frank Mong: Tre anni fa abbiamo messo a punto un'organizzazione denominata HP Security Research che si è posta alcuni obiettivi primari.

Il primo è di essere leader nell'individuare le vulnerabilità. HP promuove da otto anni il programma Zero Day Initiative indirizzato a

favorire la scoperta delle vulnerabilità su cui continuiamo a investire in modo importante. Oggi HP Research Security è la prima organizzazione del mercato per numero di minacce "zero day" individuate, che è almeno quattro volte superiore rispetto al nostro primo competitor: per esempio,

oggi più della metà di tutte le vulnerabilità legate alle soluzioni Microsoft è individuata da HP.

Si tratta di un aspetto molto importante poiché questo livello di intelligence ci consente di costruire le funzionalità di sicurezza che integriamo all'interno delle tecnologie HP. Non solo all'interno dei prodotti di sicurezza ma anche di stampanti, pc, sistemi storage e di rete. Utilizziamo queste informazioni per sviluppare virtual patch che consentono di individuare gli attacchi e chiudere le falle di sicurezza di ogni tipo e non solo quelle legate al malware.

Un altro obiettivo è di promuovere la ricerca sulla sicurezza del software e garantire le best practice per il suo sviluppo. Si tratta di un tema fondamentale perché oggi la maggior parte del software non viene creato da zero, ma realizzato assemblando componenti creati da diverse persone e questo lascia aperta la strada a innumerevoli vulnerabilità. Grazie alle soluzioni Fortify, HP consente di individuare le vulnerabilità insite all'interno di ogni tipo di codice e fornisce le indicazioni per sviluppare software più sicuro e affidabile.

**D: Quali sono gli aspetti di sicurezza su cui focalizzarsi per una protezione efficace?**

FM: Il presupposto delle nostre azioni è che bloccare rappresenta il punto di inizio, ma non esaurisce la protezione. Invece di focalizzarci sulle tecnologie di blocco il nostro approccio si concentra sulle falle di sicurezza, legate sia a minacce interne sia ad attacchi esterni.

Il malware è solo un tool per i cyber criminali, ma il tool più efficace è quello di riu-



**Frank Mong**  
di HP Enterprise Security  
Products

scire a sottrarre le credenziali di qualcuno, perché questo consente di superare tutte le barriere di protezione. L'unico modo per fronteggiare questo rischio è di analizzare i comportamenti per individuare eventuali anomalie.

È poi importante capire e conoscere intimamente le applicazioni e le possibili vulnerabilità e tenere sotto controllo i dati, soprattutto da parte delle grandi aziende che hanno l'esigenza di crescere in fretta perché questo spesso non consente loro di avere la piena consapevolezza e visibilità di tutti i rischi.

**D: Qual è l'impatto sulla sicurezza di fenomeni come il cloud e il BYOD?**

FM: Aspetti quali BYOD e cloud introducono nuove sfide per la sicurezza in termini di visibilità e controllo.

All'interno del proprio network un'azienda ha a disposizione molteplici tool per monitorare e controllare le attività. Ma quando si opera su un'infrastruttura esterna, per esempio di Amazon, questa visibilità scompare. Non si hanno informazioni su risorse e virtual machine e non sia ha controllo sul modo in cui vengono gestite le prestazioni e la scalabilità. Credo che assisteremo all'emergere di un nuovo mercato che è quello dei "cloud access security broker" che devono fornire innanzitutto visibilità su tutti questi aspetti.

**D: Qual'è il ruolo di HP in questo ambito ?**

FM: HP si propone come partner per garantire la sicurezza nell'accesso al cloud fornendo visibilità, protezione e governance tramite un approccio combinato e integrato

in cui le policy per l'accesso si combinano con tecnologie di network security, DLP, cifratura dei dati, Web Proxy e identity management. In tal modo possiamo fornire protezione per le risorse digitali on-premises, per quelle mobile off-premises, per l'utilizzo di servizi IaaS come Amazon Web Services e SaaS come salesforce.com e Office 365.

**D: Verso quali direzioni farete evolvere il vostro portfolio di soluzioni per la sicurezza?**

Crediamo che la prossima sfida da affrontare risieda nel cloud e ciò che faremo sempre più è di sfruttare le funzionalità di protezione contro gli attacchi e le minacce persistenti sviluppate per i nostri sistemi IPS così come la nostra tecnologia "zero day", per integrarle all'interno della HP Cloud Security Platform, centralizzando così le tecnologie di sicurezza e fornendone l'orchestrazione. È per noi fondamentale proteggere le applicazioni attraverso l'analisi del codice e l'inserimento al suo interno di "security intelligence". Basti ricordare che un baco in un sistema operativo per smartphone impatta simultaneamente centinaia di milioni di dispositivi nel mondo. Ci preoccupiamo anche di mettere le basi per sviluppare software sicuro per il futuro. Per esempio anche puntando sull'open standard Docker che rappresenta un approccio nuovo per allo sviluppare del codice, che punta su processi indipendenti e separati.

**D: Come è strutturata la vostra offerta?**

FM: Il nostro approccio nello sviluppo della tecnologia non è categorizzato in funzione

di soluzioni per proteggere hardware, software, network e così via, ma piuttosto in base alle differenti modalità di attacco e dell'approccio con cui il cyber crimine minaccia le aziende. Investiamo in tecnologia che, semplicemente, aiuti i buoni a difendersi dai cattivi. Ma la tecnologia, da sola, non risolve i problemi; servono le persone, che operino all'interno di processi controllati, con gli strumenti corretti. Su questo ci focalizziamo. Non aspiriamo a coprire tutti gli aspetti, ma puntiamo a essere i migliori in alcune aree specializzate: security research, security intelligence e tutto ciò che ruota attorno alla cifratura dei dati e alla loro categorizzazione e alla protezione delle applicazioni.

**D: Quali sono le ultime novità?**

Abbiamo acquisito sei mesi fa Voltage Security, un'azienda che ha sviluppato un formato unico e proprietario di cifratura chiamato HP Format Preserving Encryption. Questa tecnologia fornisce funzioni di cifratura senza alterare il formato originale dei dati e preservando l'integrità referenziale attraverso insiemi di dati distribuiti. Un tema importante in uno scenario di sicurezza dei Big Data poiché consente di garantire la protezione dei dati, anche all'interno di Hadoop, senza penalizzare le prestazioni nella fase di ricerca delle informazioni. Queste soluzioni saranno inserite all'interno di una nuova gamma di prodotti che saranno contraddistinti dal brand Voltage. \*

# LA PREDICTIVE SECURITY NELL'ERA DELLA DIGITAL TRANSFORMATION

**IDC fa il punto sull'evoluzione delle minacce e apre scenari verso nuovi approcci alla gestione del rischio**

di Riccardo Florio

In quella che IDC definisce l'era della terza piattaforma caratterizzata da milioni di App, miliardi di utenti e migliaia di miliardi di "things", sempre più pervasivamente connesse in Rete, la società di analisi evidenzia l'esigenza di un rinnovamento del modello di sicurezza.

I driver del cambiamento sono noti e hanno i nomi di big data, mobile, cloud, IoT, social business: ognuno, a suo modo, artefice contemporaneamente di nuove opportunità e di nuovi rischi.

Una delle ragioni primarie che devono indurre le aziende a mutare strategia nelle azioni indirizzate alla sicurezza aziendale è però la mutazione dello scenario di attacco.

Si è ormai concluso il processo evolutivo dell'attaccante, da singolo individuo in cerca di visibilità a membro di strutture ampie e organizzate, distribuite sul territorio, gestite con logiche manageriali, che non cercano solo di sferrare attacchi, ma che commercializzano prodotti pacchettizzati, disponibili a listino, coperti da supporto tecnico, assistenza post vendita e persino Service Level Agreement e servizi di Consulting. Un industria criminale che è riuscita

nell'impensabile risultato di surclassare per fatturato il mercato della droga.

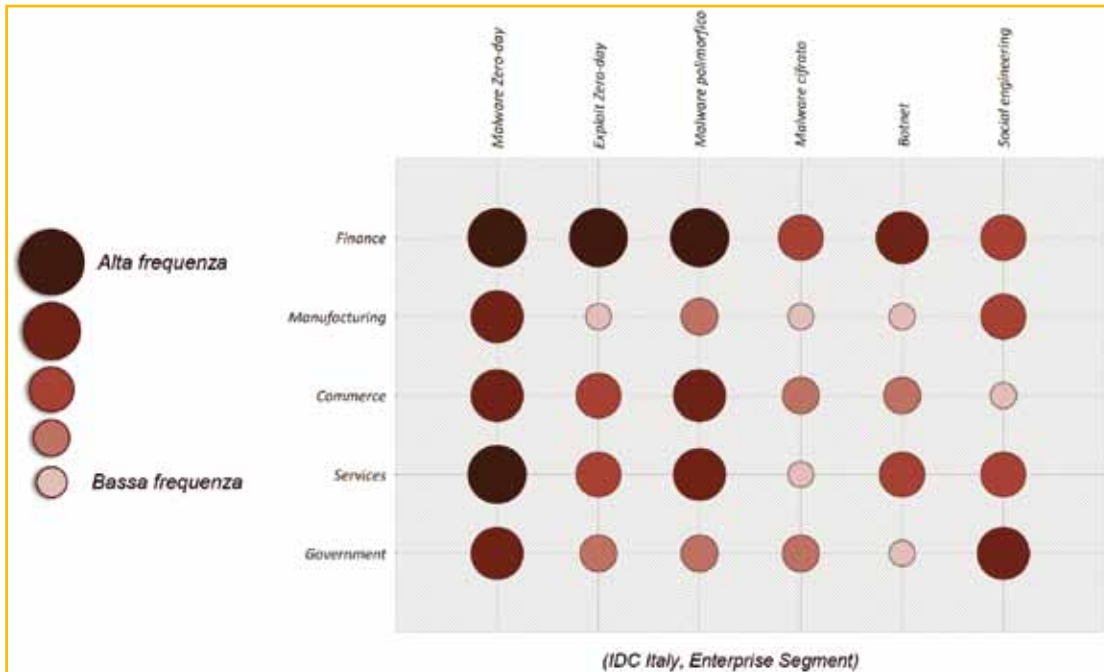
IDC evidenzia come, supportando con dati puntuali, al mutamento della natura degli attacchi faccia eco anche una crescita della loro frequenza. Tra i fenomeni in crescita vi è quello degli APT, gli attacchi mirati e persistenti che puntano a compromettere sistemi per restare per lungo tempo a operare indisturbati e inosservati. Non a caso IDC conferma come il tempo necessario per individuare le violazioni rappresenti un parametro che continua ad aumentare in modo preoccupante ampliando il rischio di esposizione, tanto che il tempo medio di individuazione si sta pericolosamente avvicinando a quello necessario per la compromissione dei sistemi.

L'indicazione che proviene da questi dati porta IDC a sostenere che la sicurezza vada approcciata non come un prodotto da affrontare meramente con strumenti tecnologici, ma piuttosto come una percezione ovvero un processo intersoggettivo in cui è necessario riuscire a definire il corretto "trade-off" tra tempo medio di risposta e budget investito in sicurezza.



(IDC Italy, 2015, n=110, Mid-large Enterprise)

*Frequenza degli attacchi alle aziende italiane di livello enterprise*



Le principali criticità di sicurezza IT

italiane continua invece a manifestare un'insufficiente attenzione al problema, spesso sorretta da superficiali convincimenti come quello di non rappresentare un target d'interesse o che sia facilmente possibile aggiustare le cose successivamente oppure ritenendo che sia sufficiente essere certificati o possedere un CISO per

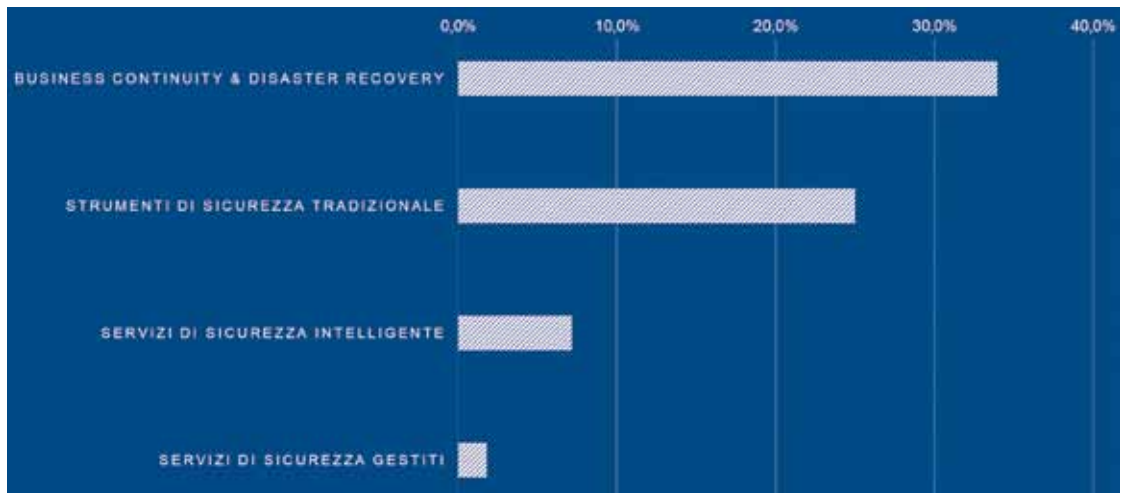
LE PREVISIONI

IDC evidenzia come, in tema di sicurezza, la priorità che in Europa guida l'agenda del business sia la protezione dei dati sensibili, seguita dall'esigenza di conformità a norme e regolamenti (IDC European Vertical Markets Survey, 2014, su 1588 rispondenti).

In Italia, all'interno del mercato mid-large Enterprise, IDC individua tra le principali criticità di sicurezza IT innanzitutto l'insufficienza del budget dedicato, ma anche la mancanza di conformità dei dipendenti alle policy e l'assenza di un'adeguata strategia della sicurezza. La principale priorità di investimento nel 2016 viene individuata dalla società di analisi nella business continuity & disaster recovery. Il segmento delle PMI

essere al sicuro.

La risposta suggerita da IDC risiede nel passaggio da un approccio reattivo a uno di tipo proattivo, integrando capacità algoritmica con intelligenza umana. Questo passaggio segnerà anche una crescita importante del mercato della sicurezza che, secondo IDC, raggiungerà nel 2020 un valore complessivo di 50 miliardi di dollari. \*



Le priorità di investimento in sicurezza nel 2016 in Italia

# ATTACCHI CYBER CRIME PIÙ FACILI E MENO COSTOSI

**Il Threat Report 2015 dei Websense Security Labs rivela nuove tecniche di elusione che riducono l'efficacia delle sandbox. Calano i prezzi del Malware as a Service**

di Gaetano Di Blasio

Il Threat Report 2015 dei Websense Security Labs si basa sui dati raccolti dal ThreatSeeker Intelligence Cloud, in grado di ricevere oltre cinque miliardi di input al giorno da 900 milioni di endpoint in tutto il mondo. Da quest'anno, però, sono state aggiunte altre fonti, frutto del lavoro di cooperazione tra diversi protagonisti della sicurezza, impegnati a contrastare le ingenti risorse di ricerca e sviluppo impiegate dalle organizzazioni cybercriminali.

L'interpretazione degli esperti dei Websense Security Labs, poi, si basa su interviste e indagini eseguite da ricercatori e ingegneri in Europa, Medio Oriente, Asia e Nord America.

Emiliano Massa, Director of Regional Sales Websense South EMEA (una region recentemente allargata comprendendo Francia e Israele), evidenzia una tendenza in particolare: effettuare attacchi diventa sempre più facile, grazie all'evoluzione dei servizi di cybercrimine.

In sostanza, si assiste alla crescita di un mercato, che risponde a tutte le logiche standard del business: aumenta la concorrenza e conseguentemente scendono i prezzi e vengono sviluppati nuovi servizi, più performanti e user friendly. Il risultato è un incremento di funzionalità all'avanguardia che agevolano i criminali nel loro intento. Per esempio catene di redirect, riutilizzo di codice e altre tecniche, che consentono tra l'altro a queste persone di rimanere anonime, rendendo l'attribuzione sempre più lunga e inaffidabile. Addirittura, afferma Massa, spesso non conviene neanche spendere tempo e risorse in attività forensi che non portano né a identificare l'origine dell'attacco né a comprendere come intervenire per evitare che si possa ripetere. Del resto, viene evidenziato nel rapporto, è diventato più difficile fare una corretta attribuzione di un attacco informatico, data la facilità

con cui gli attaccanti possono falsificare le informazioni, aggirare la registrazione e il monitoraggio o comunque rimanere anonimi. Spesso un'analisi delle stesse prove circostanziali può portare a conclusioni molto diverse.

Per questo in Websense hanno sviluppato, con il rilascio di Triton APX all'inizio dell'anno, le soluzioni DTP (Data Threat Prevention), che si basano sull'analisi delle anomalie osservate sulla rete, per esempio in termini di comportamenti non consueti per un utente o non congruenti al contesto. Come il caso di un utente che risulta loggato contemporaneamente da due IP diversi.

Il Threat Report 2015 dei Websense Security Labs spiega quali sono le tendenze comportamentali e tecniche del cybercrime e allo stesso tempo fornisce informazioni e suggerimenti utili per aiutare i professionisti della sicurezza a pianificare la loro strategia di difesa della rete.

Ecco altri tra gli aspetti principali emersi dallo studio. Innanzitutto, come accennato il cybercrime è più facile, anche per persone alle prime armi, accedendo più facilmente ed economicamente a exploit kit in affitto attraverso servizi Maas (Malware as a Service), così come all'acquisto o noleggio di porzioni o di un intero attacco informatico complesso e pluri strutturato. Infatti, si è affinata ulteriormente la capacità di abbinare tecniche nuove e tradizionali, dando origine a soluzioni maligne altamente evasive.

Sembra che gli autori degli attacchi si stiano concentrando più sulla qualità, piuttosto che sulla quantità come in passato. Peraltro, si parla di Digital darwinismo, facendo riferimento alla sopravvivenza delle minacce in grado di evolvere. Non solo: si assiste al riutilizzo di vecchie minacce, per esempio i macro virus.

Nello specifico, Luca Mairani, senior sales engineer di Websense, riporta di un recente attacco indirizzato in Italia, che partiva con mail plausibili con in allegato un file Word, il quale attivava una macro per scaricare malware, soprattutto Cryptolocker.

Se le minacce sono diminuite (i Websense Security Labs hanno osservato 3.9 milioni di minacce alla sicurezza nel 2014, il 5,1% in meno rispetto al 2013), sono però sempre più sofisticate, aumentando quelle utilizzate in attacchi con logiche multifase tipo APT. Qui, sottolinea Mairani, le criticità sono legate soprattutto a Java e altri sistemi,

come Acrobat Adobe o Microsoft Explorer, ma anche open source, che le aziende devono mantenere nella vecchia versione perché è la sola compatibile con le applicazioni legacy aziendali. Quindi non possono applicare le patch e rimangono esposti a vecchie e nuove vulnerabilità.



A rendere più sofisticati gli attacchi APT concorre anche il fatto che i cyber criminali hanno reinventato la metodologia di attacchi per ridurre la visibilità delle minacce. Lo hanno fatto seguendo in maniera sempre meno lineare la tradizionale catena di attacco. Gli attacchi sono più difficili da rilevare se alcuni stadi vengono saltati, ripetuti o applicati solo parzialmente, riducendo così la visibilità della minaccia stessa. Un'attività varia fortemente se svolta in una diversa fase della catena di attacco. Così come l'attività di spam si concentra sulle prime fasi della catena, altre fasi della catena subiscono diverse attività malevole.



(da sinistra)  
**Emiliano Massa,**  
*Director of regional sales  
 Websense South EMEA*  
**Luca Mairani,**  
*Senior sales engineer di  
 Websense*

Alcune fasi hanno visto un maggior numero di attività; altre ne hanno rilevate molto meno rispetto all'anno precedente.

Per concludere, va evidenziata ancora una volta la carenza di professionisti della sicurezza: ne mancano 2 milioni, secondo il rapporto e il problema, aggiunge Massa, è che la formazione di una figura altamente qualificata sulla cybersecurity richiede almeno 11 anni.

Ma il bisogno di aumentare l'IQ, cioè l'intelligenza sulla sicurezza non riguarda solo i professionisti, occorre continuare a insistere per educare i propri dipendenti e adottare strumenti automatici che impediscono ai dipendenti di commettere errori fatali o, peggio, atti dolosi intenzionali. Il rapporto continua a porre al primo posto le cosiddette minacce interne.

Due ultimi punti rilevati: la fragilità delle infrastrutture fragili, con un aumento delle minacce che si espandono nell'infrastruttura di rete stessa, per esempio vulnerabilità nascoste sono state rinvenute all'interno dei codici di base Bash, OpenSSL, SSLv3 e altri che sono stati in uso per decenni.

Infine, l'Internet of Things (IoT) che avrà un impatto notevole sull'esposizione agli attacchi informatici, poiché si stima che la crescita di dispositivi connessi raggiungerà una cifra tra i 20 e i 50 miliardi entro il 2020. ✨

# HACKER SUPERCATTIVO: DAI FUMETTI ALLA CONQUISTA DI INTERNET

**Attacchi DDoS, ricatti online e altre malignità realizzabili con tecniche in cloud. È più facile diventare un supercattivo di Internet che di un fumetto**

**R**oland Dobbins, Principal Engineer ASERT Team di Arbor Networks, ci porta nel mondo dei meccanismi narrativi dei fumetti americani e dell'ondata di film che ne vengono ricavati per illustrare come possa essere facile attuare attacchi, in particolare di tipo DDoS su Internet.

«Non esiste fumetto o graphic novel in cui vi sia alcunché di immutabile - spiega Dobbins -: buoni e cattivi non scompaiono mai veramente ma in un modo o nell'altro tornano sempre sulla scena o vengono riproposti in versioni profondamente o lievemente diverse all'interno di linee temporali alternative e così via. È decisamente più semplice diventare un supercattivo su Internet di quanto non lo sia mai stato nei fumetti».

Le regole per diventare supercattivi sono poche, precise e schematizzabili.

## AVERE UN MOTIVO

La prima "mossa" è quella di possedere o perlomeno inventarsi un motivo.

«Che sia per ideologia, per avidità, per dispute legate a giochi online o per puro e semplice nichilismo (per "divertirsi"), a tutti gli effetti esiste oggi su Internet un'infinità di malintenzionati effettivi o potenziali (ultima stima della popolazione collegata: 3 miliardi e in crescita) molti dei quali si sentono in dovere - per motivi reali o immaginari - di regolare una quantità di conti pressoché infinita. Indipendentemente dal segmento, dal focus, dal mercato, dai servizi o dall'utenza di un'organizzazione, là fuori c'è sicuramente qualcuno che sarà felice di poterne impedire la presenza su Internet - non importa chi o perché, è sufficiente sapere che personaggi del genere esistono e a quanto pare sono una caratteristica permanente della vita su Internet da sempre, fino anche a tornare indietro

alle sue radici legate alla Guerra Fredda, ad ARPANET e a iRC, apparentemente destinata a non abbandonarci mai».

## ARMARSI

Premessa l'esistenza dei cattivi, la seconda mossa è quella di procurarsi le armi ovvero sviluppare i mezzi necessari per perpetrare l'attacco oppure, come appare più semplice, acquisirli.

Anche tra i cattivi dei fumetti i veri innovatori sono relativamente rari. Nel mondo reale sono quelli che sviluppano nuove metodologie di attacco DDoS per poi venderle o utilizzarle in prima persona per raggiungere i propri obiettivi individuali.

«Dopodiché tali metodologie trovano inevitabilmente la strada per arrivare a un pubblico più vasto sotto forma di 'booter' o 'stresser' DDoS basati su cloud per consentire anche agli aspiranti Dr. Impossibile meno tecnicamente capaci di sfruttare tecniche DDoS altamente efficaci come quelle di saturazione dei link per riflessione/amplificazione oppure più sottili metodologie di attacco alle connessioni TCP - e tutto attraverso un'interfaccia Web grafica accessibile quando non addirittura esteticamente piacevole».

## IDENTIFICARE LE OPPORTUNITÀ

La terza fase riguarda l'identificazione delle opportunità. Anche metodologie di attacco DDoS elementari ben note riescono spesso ad avere la meglio su grandi organizzazioni ricche di risorse poiché, spiega Dobbins: «Sfortunatamente le best practice correnti del settore tese a massimizzare la disponibilità degli elementi di rete, dei server, degli stack applicativi, dei servizi e così via che sono state sviluppate e pubblicate finora e sono costantemente promosse e diffuse da molti operatori della community globale della sicurezza, tra cui Arbor ASERT, sono seguite più scrupolosamente nella loro violazione che non nella loro applicazione».

Questa condizione non fa che aprire la strada a ogni tipo di malintenzionato, compresi quelli che neanche si curano di effettuare particolari ricognizioni prima di lanciare attacchi DDoS mirati.

### DDOS FOR BITCOINS E IL CASO DD4BC

Tra i cattivi emergenti è interessante il caso di DD4BC, una banda di estorsori DDoS salita recentemente alla ribalta quando è passata dall'attaccare piccoli cambiavalute Bitcoin al colpire i casinò online e i siti di scommesse fino a mettere nel mirino istituti finanziari di alto profilo in numerosi angoli del mondo.

«I supercattivi di Internet più bravi, quelli dalle carriere criminali più longeve, sono coloro che sanno muoversi al meglio senza rischiare troppe attenzioni negative dalla combinazione dei vari enti responsabili della sicurezza e che sanno quando è il momento di scomparire discretamente dalla scena fino all'arrivo della successiva finestra di opportunità».

Quando si ha a che fare con supercattivi di Internet "dilettanti", piccoli successi iniziali a volte alimentano l'autostima portandoli a indirizzare i propri attacchi contro istituzioni di alto profilo.

«Nell'ultimo anno o giù di lì, un individuo o un'organizzazione che si fa chiamare DD4BC ('DDoS for Bitcoins') ha aumentato rapidamente sia la frequenza sia la portata dei propri tentativi di estorsione via DDoS spostando le proprie attenzioni dai cambiavalute specializzati in Bitcoin ai casinò online, alle società di scommesse e, ultimamente a importanti istituzioni finanziarie di Europa, Asia, Australia e Nuova Zelanda. Il modus operandi di DD4BC è in genere quello di lanciare un attacco DDoS a riflessione/amplificazione relativamente piccolo, sui 10gbps/15gbps, per poi inviare una email estorsiva con la richiesta di una cifra compresa tra 15 e 100 Bitcoin (in linea con quanto si ritiene che la vittima possa essere disposta a pagare) a un indirizzo di contatto ufficiale dell'azienda colpita. Queste richieste estorsive affermano tipicamen-



te che DD4BC è in grado di mettere in campo una capacità di attacco DDoS compresa tra 400gb/sec e 500gb/sec, lasciando quindi 48 ore di tempo per pagare minacciando in caso contrario di sferrare immensi attacchi DDoS contro la vittima che si rifiuti di cedere. Al momento non siamo a conoscenza di alcuna azienda o organizzazione che si sia piegata ai ricatti di DD4BC, quindi non sappiamo quanto possano essere lucrose le campagne DDoS estorsive condotte da questa persona o persone. Quel che abbiamo osservato è che, a oggi, DD4BC non sembra aver generato alcun attacco DDoS superiore a qualche decina di gb/sec, un volume purtroppo sufficiente a bloccare almeno inizialmente la disponibilità di molti obiettivi a causa della troppa diffusa assenza di preparativi adeguati da parte dei difensori. \*

# CLOUD SERVICE: DAL PROFILING ONLINE AL DIGITAL SINGLE MARKET

**Dalle linee guida del Garante Privacy italiano le sfumature che definiscono il confine tra gli strumenti di marketing da quelli della consapevole profilazione degli utenti ai servizi online**

*di Gloria Marcoccio e Alberto Manfredi*



Il 6 Maggio 2015 l'Autorità italiana Garante per la protezione dei dati ha pubblicato le Linee guida in materia di trattamento di dati personali per profilazione on line (Pubblicato lo stesso giorno sulla Gazzetta Ufficiale n. 103).

Le linee guida intendono chiarire ed indicare agli operatori stabiliti in Italia che offrono servizi della Società dell'Informazione (motori di ricerca, servizi cloud, servizi di pagamento on line, posta elettronica, social network, ..) apposite modalità per adempiere ai requisiti di legge privacy, essenzialmente Informativa e Consenso, nel contesto dei processi di profilazione on line (per finalità di marketing, per erogare uno specifico servizio, ..), sia nei riguardi degli utenti autenticati, cioè quelli che accedono ai servizi tramite un account, sia nei riguardi degli utenti che fanno uso dei servizi in assenza di autenticazione, come in caso di semplice navigazione on

line. Le modalità indicate dall'Autorità nelle sue linee guida comportano impatti anche di natura tecnica per la realizzazione e gestione dell'Informativa e del Consenso on line (in funzione anche degli elementi identificatori utilizzati quali le credenziali di accesso, i device fingerprinting,... e contesti di profilazione quali i servizi di posta elettronica, incrocio di dati e relativo utilizzo per più finalità,...)

Le linee guida non hanno di per se natura prescrittiva, ma come espressione della interpretazione di legge prodotta dalla Autorità competente hanno un chiaro valore per cui occorre tenerle presenti qualora i servizi erogati contemplino processi di profilazione on line di utenti, autenticati o meno.

La materia trattata è di ampio respiro e si presta certamente a diverse letture che, in funzione dei contesti tecnologici e soprattutto del business degli operatori interessati, possono far emergere nelle linee guida punti chiari ed altri decisamente meno. Tra questi hanno una particolare valenza, sia da un punto di vista normativo che implementativo, quegli aspetti che devono necessariamente trovare un coordinamento operativo con il Provvedimento sui cookie (questo, diversamente dalle linee guida, è di natura prescrittiva con relative specifiche sanzioni in caso di inadempienze) che entrerà in vigore nei primi giorni di Giugno 2015. Il riferimento è a quanto la linea guida indica in termini di misure relativamente all'Informativa, Consenso ed esercizio dei diritti degli interessati riguardo all'uso delle tecniche di device fingerprinting (riconoscimento di un device, in modo non necessariamente univoco, in base a suoi determinati parametri che sono direttamente accessibili in lettura via internet) che possono essere utilizzate sia ai fini della profilazione per azioni di marketing basate sull'analisi del comportamento

on line dell'utente, sia come supporto in processi di autenticazione&sicurezza on line (come ad esempio per alcuni servizi di mobile payment che sono legati anche all'identificazione del device).

Occorre poi ricordare che per alcuni tipi di profilazione<sup>1</sup> è necessario effettuare la Notifica all'Autorità Garante per i dati personali (sono previste sanzioni in caso di inadempienza): in una linea guida dedicata alla profilazione on line sarebbe quantomeno utile avere un riferimento che ricordi questo importante adempimento.

Deve poi sempre essere tenuto presente che le linee guida si rivolgono agli operatori della società dell'informazione che sono stabiliti in Italia: in conseguenza di ciò l'implementazione del complesso delle misure indicate nella linea guida da parte di tali aziende, potrebbe comportare uno squilibrio con possibili ricadute sul business rispetto al quadro di way of working valido per le aziende non stabilite in Italia, che comunque offrono servizi on line, notoriamente worldwide.

Questa linea guida fa poi amplissimo, spesso letterale, riferimento alle prescrizioni che il Garante ha emesso nei riguardi di Google l'anno scorso tramite apposito provvedimento nel quale sono stati previsti consistenti tempi di adeguamento dimensionati sulla complessità di quanto richiesto e la molteplicità dei sistemi Google interessati (per questi adempimenti Google sta seguendo un apposito protocollo di verifica concertato con l'Autorità).

Proprio in relazione alle tempistiche di adeguamento ed al notevole complesso di ambiti e misure considerate, pur essendo ben consapevoli che tali linee guida non hanno natura prescrittiva ma sono certo autorevole e competente interpretazione della normativa, sarebbe auspicabile, e sarebbe certo

una motivazione in più per procedere con implementazioni coerenti con essa, che l'Autorità valuti l'opportunità di pubblicare una Q&A di corredo e di indicare un grace period a favore di coloro che decideranno di allinearsi alla linea guida.

Un'ultima considerazione va rivolta alla recente pubblicazione della strategia sul mercato unico digitale europeo (Digital Single Market) da parte della presidenza della Comunità Europea ([http://ec.europa.eu/priorities/digital-single-market/index\\_en.htm](http://ec.europa.eu/priorities/digital-single-market/index_en.htm)) che nell'ambito dei 3 pilastri fondanti pone molta enfasi sul sostegno allo sviluppo del mercato e-commerce tra i 28 stati membri, armonizzando e semplificando norme e procedure, e sullo sviluppo del Cloud Computing e Big Data, con grande attenzione alla cyber security e privacy.

Pertanto un corretto e prosperoso sviluppo del mercato dei servizi online, di cui la profilazione è una delle tematiche importanti, è ormai un obiettivo europeo e non più soltanto nazionale. \*



<sup>1</sup> D.Lgs 196/03 art 37 comma 1 lettera d "Dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti"

# IL MARKETING DEI FRATELLI CARLI LO STAMPA RICOH

**La storica azienda di Imperia utilizza la soluzione per la stampa digitale Infoprint IP 5000 GP per realizzare campagne di direct mailing e precision marketing e migliorare il servizio alla clientela**

di Paola Saccardi

Forse non tutti sanno che la Fratelli Carli, storica azienda di Imperia che produce l'olio Carli, è nata nel 1911 quando la famiglia Carli, che già possedeva una tipografia, ebbe un abbondante raccolto dal proprio oliveto e decise di vendere porta a porta l'olio in eccesso.

Da quel lontano momento si è arrivati fino ad oggi, con la quarta generazione della famiglia Carli, che tuttora porta avanti l'attività dell'azienda e che continua a vendere alla rete di fedeli clienti (circa 1 milione) attraverso un modello distributivo peculiare, che prevede l'ordine (via telefono, posta o Web) e la consegna diretta.

Ma l'attività originaria della famiglia Carli, la tipografia, non è scomparsa, bensì ha continuato a fare da supporto al business dell'olio mantenendo «all'interno dello stabilimento un centro tipografico all'avanguardia che produce il materiale di marketing dell'azienda, come listini, brochure, cataloghi, flyer e depliant - spiega Marco Gardini, IT Operations Manager di Fratelli Carli -. Grazie a questo reparto abbiamo l'opportunità di controllare l'intero processo di stampa dall'ideazione alla divulgazione - continua il manager -, e di curare tutto il materiale destinato ai clienti. Una prerogativa che poche altre aziende al mondo possono vantare».

Tuttora l'azienda è stata classificata come Benefit Corporation, una delle poche presenti in Italia, ossia

un'azienda che oltre a perseguire obiettivi di profitto mira anche al rispetto della sostenibilità ambientale e alla creazione di una nuova cultura d'impresa a sostegno modello economico che tiene conto anche della dimensione sociale.

## UN PERCORSO FATTO D'INNOVAZIONE

La Fratelli Carli ha iniziato presto la sua strada verso la ricerca di tecnologie più avanzate a supporto delle proprie attività di business. Nel 1974 costituisce il primo centro di elaborazione dati (CED) IBM, dotandosi del primo mainframe e di stampanti ad impatto IBM-4245 per personalizzare i listini da inviare ai clienti per posta. Successivamente nel 2007 decide proseguire l'innovazione del CED acquistando due Infoprint IP4100 Simplex allo scopo di stampare bolle, fatture e listini. Ma ben presto nel 2011 l'azienda sente la necessità di avere un supporto stampa maggiore per le attività legate al marketing e in particolare per migliorare la comunicazione cartacea ai clienti, un aspetto su cui punta molto e che si appoggia anche sulla raccolta e l'analisi delle informazioni provenienti dalla vendita. È a questo punto che la Fratelli Carli decide di installare Ricoh Pro C900, la prima soluzione foglio singolo colore di Ricoh da 90 pagine al minuto, per produrre leaflet, brochure e flyer personalizzati, una scelta strategica per l'azienda che si rivolge direttamente alla propria clientela.

Nel 2012 acquista 3 Ricoh Pro C901 (90 ppm a colori per la stampa di produzione di qualità) sostituendo una delle due IP4100 Simplex per la produzione di bolle e fatture. Questi dispositivi per l'azienda rappresentano una svolta importante nel processo di stampa perché le consentono di unificare il flusso





produttivo che prima avveniva in due differenti fasi, quella della stampa del layout, attraverso l'appoggio presso altre tipografie e quella della stampa di dati variabili, gestita con la soluzione IP4100. Con la nuova soluzione la Fratelli Carli riesce, invece, a stampare direttamente su carta bianca, apportando vantaggi sotto molti aspetti, tra cui la semplificazione nel processo di acquisto della carta.

#### PIÙ POTERE AL MARKETING A COSTI CONTENUTI

L'ultima innovazione in casa Carli arriva proprio quest'anno a seguito dell'acquisto della soluzione che ha consentito realmente di mettere in atto una comunicazione one-to-one e strategie di precision marketing e direct mailing, con la possibilità di personalizzare l'offerta e di essere sempre più vicino alle esigenze dei propri clienti.

Dopo un'attenta fase di scouting e dopo aver valutato più opzioni provenienti da diversi fornitori la scelta dell'azienda ricade nuovamente sulle soluzioni di Ricoh, e in particolare sulla Infoprint IP 5000 GP AD1/AD2, un dispositivo inkjet fronte e retro a colori che è risultato ideale per soddisfare le esigenze di marketing e in grado di stampare volumi più consistenti.

In particolare la nuova macchina ha permesso di ottenere una maggiore flessibilità nelle tempistiche di stampa "tanto da consentirci di effettuare modifiche immediate in caso, per esempio, si trovino degli errori da correggere in



fretta, velocizzando di molto il processo che va dalla creazione alla stampa di idee e proposte che arrivano dal reparto marketing. In pratica abbiamo dato al marketing tutti gli strumenti necessari per fare quello che vogliono. In più abbiamo abbassato i costi di produzione e gestione, come, per esempio, quelli che riguardano le bobine della carta, che sono diminuite rispetto a prima, semplificando anche questo aspetto» spiega Gardini. Da notare che l'azienda stampa ogni giorno i Certificati di Garanzia, che contengono le analisi delle caratteristiche organolettiche dei prodotti realizzate dal laboratorio interno, per inserirle all'interno delle confezioni. Un processo che richiede una certa capacità e che grazie alla nuova soluzione è stato semplificato e velocizzato.

L'utilizzo di Infoprint IP 5000 GP ha rappresentato anche il passaggio per l'azienda a una tecnologia a getto di inchiostro e ciò ha portato dei vantaggi che riguardano la maggior semplicità di utilizzo e la minore necessità di manutenzione degli impianti. Mentre per contenere il costo dell'inchiostro è stato «sufficiente prestare attenzione alla scelta della carta più adatta alle diverse necessità per minimizzarne l'utilizzo» spiega il manager. La soluzione Infoprint IP 5000 GP offre tra l'altro una suite di gestione dell'inchiostro per l'ottimizzazione e il monitoraggio dell'utilizzo effettivo.

In conclusione, la Fratelli Carli, con il passaggio dalla tecnologia offset a quella digitale, e grazie alla capacità di analizzare e gestire i dati e la formattazione grafica mediante soluzioni software a corredo, è ora in grado di raggiungere ogni singolo cliente con messaggi mirati e personalizzati e aumentare la fidelizzazione. \*

# HP SI RAFFORZA NEL SOFTWARE-DEFINED DATA CENTER

**Il vendor spinge sull'innovazione dei modelli cloud e rafforza la sua strategia per un'infrastruttura convergente. Tra le ultime novità una nuova famiglia di sistemi storage all-flash HP 3Par**

di Riccardo Florio

**H**P punta su una sinergia sempre maggiore tra le proprie soluzioni server, storage e networking per affrontare il mercato all'insegna dell'innovazione e della flessibilità.

Per l'immediato futuro il vendor prepara novità e miglioramenti in ambito cloud, nel software-defined data center e nel suo modello di converged Infrastructure.

## IL FUTURO DELLO STORAGE È FLASH

Per accelerare il processo di trasformazione verso quello che viene definito come "all-flash data center", HP ha introdotto un nuovo drive SSD da 3,84 Terabyte di capacità: attualmente la massima capacità in un array all-flash Tier-1.

La tecnologia flash viene introdotta da HP nella nuova famiglia HP 3Par StoreServ 20000, scalabile fino a otto nodi, che si propone come soluzione ideale per il consolidamento di molteplici rack di storage di fascia alta. Due i modelli attualmente disponibili siglati 20800 e 20850.

Il sistema "all-flash" 3Par StoreServ 20850 è in grado di fornire oltre 3,2 milioni di IOPS con una latenza inferiore al millisecondo e oltre 75 Gbps di throughput per supportare applicazioni a elevate richieste prestazionali. Il sistema 3Par StoreServ 20800 è un sistema "converged flash" scalabile fino a 15 Petabyte di capacità utilizzabile. Entrambi i modelli si avvalgono del chip ASIC HP 3Par Thin Gen5 Express per una deduplicazione con accelerazione hardware.

L'elevata densità di capacità dei nuovi drive SSD da 3,84 Terabyte,

in combinazione con le tecnologie ASIC di compattezza dei dati presenti nei sistemi 3Par StoreServ, consentono a HP di sostenere di avere incrementato del 75% la capacità utilizzabile fornendo un costo per Gigabyte di storage all-flash utilizzabile pari a un dollaro e mezzo.

«HP sta costantemente facendo evolvere e crescere l'offerta 3Par - sostiene Yari Franzini, country manager HP Converged Infrastructure Italy -. HP 3Par StoreServ Storage offre l'accessibilità, la densità, la resilienza e la flessibilità multi-sistema necessari per metter la tecnologia flash a disposizione di ogni applicazione. Le prestazioni e i costi dei nuovi sistemi flash rappresentano la morte della virtualizzazione dello storage».

## MASSIMA SPINTA ALLA CONVERGENZA

HP ha annunciato l'espansione del suo portfolio Converged Systems per fornire maggiore flessibilità e scelta nei percorsi di trasformazione verso un'infrastruttura di tipo ibrido.

«Il software acquista una crescente importanza - continua Franzini - perché i nuovi modelli di riferimento sono di tipo software-defined. OneView rappresenta il punto di raccordo nella nostra vision per il software-defined data center: un ambito in cui HP può vantare un'offerta completa, basata sulla disponibilità interna di tutte le componenti: server, storage e networking».

Le novità includono HP OneView 2.0, la piattaforma per la gestione, il monitoraggio e il provisioning dell'infrastruttura, che unifica i



**Yari Franzini,**  
country manager HP Converged  
Infrastructure Italy

processi, le interfacce utente e le API attraverso server, sistemi storage e dispositivi di rete Virtual Connect di HP.

L'introduzione di nuovi template per il profilo del server rendono facile definire le impostazioni di configurazione di server, LAN e SAN da un unico punto centralizzato ed effettuare il provisioning in modo automatizzato. Inoltre, la disponibilità di nuovi profili di mobilità permette di migrare e recuperare i carichi di lavoro attraverso ogni tipo di piattaforma, configurazioni e generazioni di server. HP OneView 2.0 offre anche nuove funzionalità di automazione per le SAN per identificare e risolvere potenziali problemi prima che colpiscano il business. Con questa release HP ha anche introdotto importanti miglioramenti al processo di aggiornamento dei driver dei dispositivi e del firmware.

### TUTTA LA POTENZA DEL CLOUD

Per favorire la transizione verso un'infrastruttura ibrida HP sta rafforzando il portafoglio HP Helion, con il rilascio di HP CloudSystem Helion 9, nuova versione della soluzione di punta di enterprise cloud integrato, e con significativi miglioramenti a HP Helion Managed Cloud Services, la soluzione per gestire carichi di lavoro aziendali in un ambiente sicuro di cloud hosting. HP Helion CloudSystem 9.0 integra HP Helion OpenStack e la HP Helion Development Platform per fornire una piattaforma open source di livello aziendale nativa per il cloud per lo sviluppo di applicazioni e per le esigenze infrastrutturali.

HP Helion CloudSystem 9.0 mette a disposizione:

- supporto simultaneo per molteplici ambienti

cloud, tra cui Amazon Web Services (AWS), Microsoft Azure, HP Helion Public Cloud, la tecnologia OpenStack e VMware;

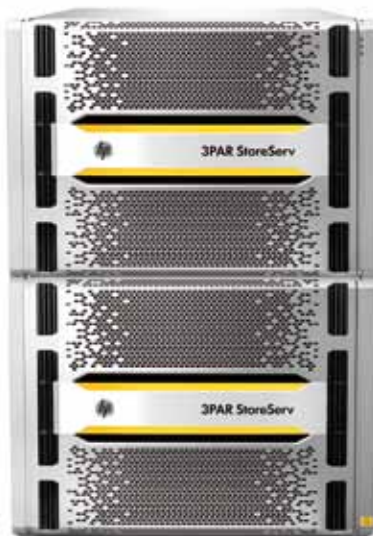
- l'ultima versione di HP Helion OpenStack;
- supporto per più hypervisor tra cui Microsoft Hyper-V, Red Hat KVM, VMware vSphere;
- supporto per cloud privati compatibili con AWS attraverso l'integrazione con HP Helion Eucalyptus;
- supporto per i dati non strutturati attraverso il progetto Swift OpenStack Object Storage;
- l'ultima versione di HP Cloud Service Automation, fornendo le funzionalità di gestione per controllare ambienti cloud ibridi.

HP Helion CloudSystem 9.0 è disponibile come software standalone o come infrastruttura blade-based o iper-convergente completamente integrata con HP ConvergedSystem. La disponibilità è prevista per la fine di quest'anno.

### LA PARTNERSHIP CON ARISTA

HP ha anche annunciato una nuova partnership con Arista Network a supporto della realizzazione di infrastrutture convergenti e open. La partnership mette a disposizione soluzioni aperte e flessibili per semplificare il provisioning e la manutenzione, tramite l'Extensible Operating System (EOS) di Arista e la sue piattaforme di rete programmabili, con l'integrazione al centro di HP OneView.

«La combinazione tra l'infrastruttura convergente di HP e le soluzioni di Arista Network rafforza la nostra posizione nell'ambito del data center e delle infrastrutture convergenti - ha commentato Franzini -. L'adozione di architetture di riferimento congiunte da parte di HP e Arista fornirà un percorso enormemente semplificato per i nostri clienti congiunti».



HP 3Par StoreServ 20000

## DIMENSION DATA: NOI SIAMO IL PARTNER PER LA TRASFORMAZIONE DIGITALE

**L'azienda prosegue su un percorso strategico che la vede proporsi non solo come system integrator, ma anche come partner strategico di sviluppo del business in un contesto di evoluzione digitale**

di Riccardo Florio

La definizione di "semplice" system integrator comincia a stare stretta a Dimension Data, che si propone sempre più come un referente per supportare le aziende a tutto tondo nel cambiamento verso un modello di impresa (o forse meglio dire di mondo) che diventa sempre più digitale.

Da questa nuova vocazione nasce un maggiore rafforzamento dell'offerta di servizi, un approccio consulenziale avvalorato da competenze sempre più trasversali, una serie di accordi con tutti i principali vendor per intervenire in modo competente all'interno di parchi tecnologici complessi e multivendor e una crescente versatilità nell'utilizzo di una piattaforma cloud globale messa in modo strategico al servizio di aziende e service provider.

«Per noi questa evoluzione rappresenta una sfida - spiega Paolo Panzanini, country manager di Dimension Data Italia - che non richiede solo competenze tecnologiche che sono nel nostro DNA da oltre un ventennio, ma anche capacità di gestione dei processi e di saper intervenire all'interno di parchi tecnologici multivendor fornendo le indicazioni per pianificare un'evoluzione corretta. Le aziende apprezzano questo approccio e ci stanno ad ascoltare perché vedono in noi una soluzione alle loro esigenze di business».

Un percorso che sfrutta il fatto di far parte del Gruppo giapponese NTT, mantenendo tuttavia una propria indipendenza con un proprio piano di sviluppo a medio e lungo termine e importanti previsioni di crescita.

Dei circa 85 miliardi di dollari fatturati da NTT nel 2015, Dimension Data

punta, infatti, a portarne in dote sette, che rappresentano quasi la metà di tutto il business fatto da NTT fuori dal Giappone.

Pur essendo una realtà distribuita su scala globale, all'interno di un modello di azienda uniformato in procedure e metodologie interne Dimension Data affronta il mercato proponendo soluzioni personalizzabili e costruite su misura per le esigenze del cliente, tenendo conto delle differenze tra i diversi Paesi in cui opera.

«Forniamo servizi operativi e progetti di trasformazione e aiutiamo i CIO sia a gestire la quotidianità sia a migliorare tramite l'innovazione - osserva Panzanini -. Non abbiamo tecnologie da posizionare, ma problemi da risolvere. La nostra mission primaria è quella di colmare i gap ed eliminare le inefficienze, anticipando e gestendo le richieste del business, per consentire alle aziende di sfruttare le opportunità che, troppo spesso, si perdono perché le risorse disponibili sono impegnate a mantenere l'operatività». In Italia Dimension Data interviene in molti ambiti, ma si concentra soprattutto nella gestione dei parchi tecnologici sia in contesti locali sia di tipo distribuiti, nella gestione delle risorse infrastrutturali del data center (server, storage e connettività) e nell'integrazione di soluzioni di comunicazione convergente.

Un peso sempre maggior nell'attività lo riveste il cloud a cui l'azienda ha dedicato una business unit specifica, per mettere a disposizione delle aziende e dei service provider servizi IaaS, SaaS, PaaS erogabili attraverso i propri 18 data center distribuiti su scala globale o sfruttando l'infrastruttura interna dei clienti.

L'azienda dispone anche di un'offerta IaaS proposta in modalità "white label" a cloud service provider che vogliono proporre servizi con il loro brand. Per coprire questo tipo di attività Dimension Data sta predisponendo un Canale di reseller e system integrator che gli consentirà di indirizzarsi anche a realtà troppo piccole per essere seguite direttamente. \*



**Paolo Panzanini**  
country manager di  
Dimension Data Italia

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

In oltre 250 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.

**edizione  
2015**



Sono disponibili anche  
**CLOUD COMPUTING E IT AS A SERVICE  
STORAGE**

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



# DE gustare

alla scoperta dei sapori d'Italia



NOTIZIE  
**ROAD TO DUBAI, LE ECCELLENZE ITALIANE SI PRESENTANO**

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

01 GIUGNO 2015

La Toscana di Biella

Agricoltura biodinamica

Asparago in cucina



4 ORE AGO  
NOTIZIE  
**OLIO, FIRMATO  
PROTOCOLLO PER  
VALORIZZARLO**



4 ORE AGO  
NOTIZIE  
**SARCHIO,  
SFOGLIETTE BIO PER  
TUTTI I GUSTI**

4 DEL AGO  
NOTIZIE  
**DIETA  
MEDITERRANEA  
PREMIO  
GRUPPO**



DE gustare  
alla scoperta dei sapori d'Italia

**Alla corte del RE**

**www.de-gustare.it**