

DIRECTION Reportec **67**

SOLUZIONI SERVIZI E TECNOLOGIE ICT

IPSWITCH PORTA ALLE
PMI IL **MONITORAGGIO**
DI RETE ENTERPRISE

L'**EUROPA** ACCELERA
SULLA **FATTURAZIONE**
ELETTRONICA

REPORT **ICT SECURITY**

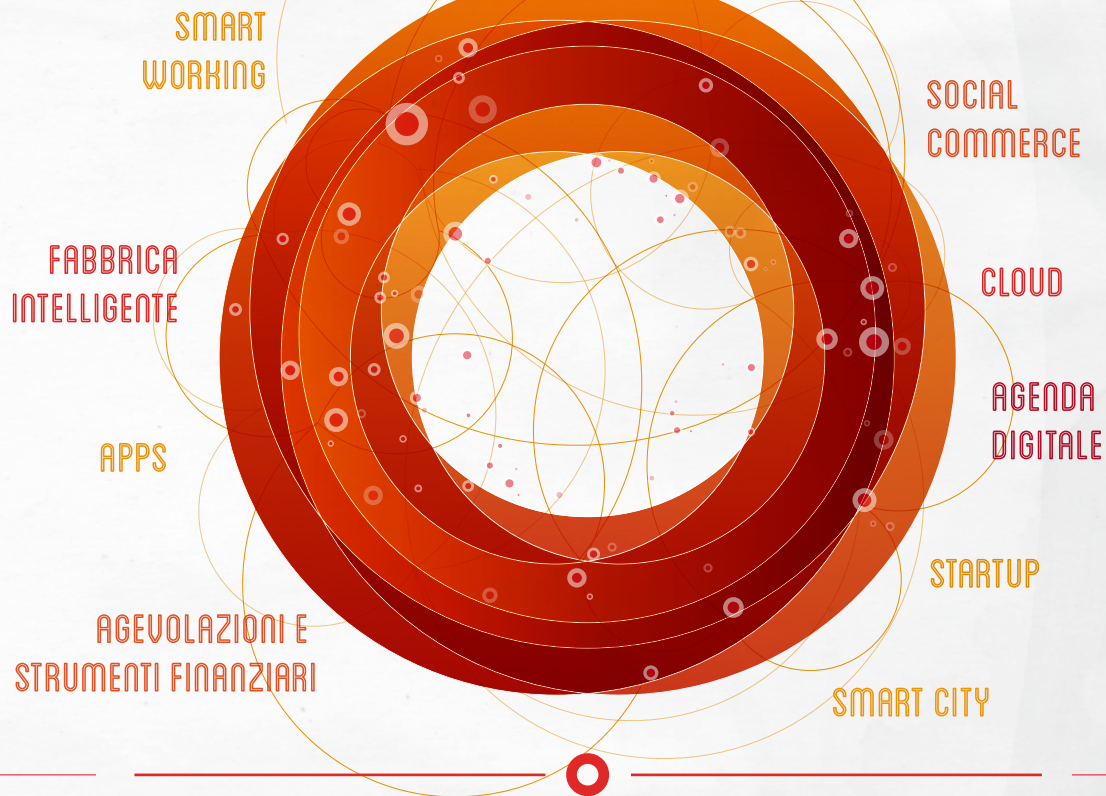
Crescono i rischi generati dallo sviluppo di cloud, mobilità e social network, che alimentano la proliferazione di Big Data sulla sicurezza sempre più difficili da analizzare. Un trend che spinge verso l'adozione di tecnologie specializzate, integrate tra loro e capaci di rispondere alla minacce in tempo reale

Con approfondimenti dedicati a:

HP ESP • TREND MICRO • IBM • FORTINET
WEBSense • SYMANTEC • DELL SONICWALL

SMAU

ACCELERATORE DI INNOVAZIONE PER LE IMPRESE ★



LE **STARTUP** POSSONO ESSERE UN ACCELERATORE DI SVILUPPO PER LA MIA IMPRESA? TABLET, APP, CLOUD COMPUTING, NUOVI GESTIONALI INTEGRATI E BUSINESS INTELLIGENCE, NE PARLANO TUTTI MA COME POSSO SFRUTTARLI PER IL MIO BUSINESS? QUALI SONO LE AGEVOLAZIONI E GLI STRUMENTI FINANZIARI A DISPOSIZIONE DELLA MIA IMPRESA?

SMAU ROMA
19-20 MARZO 2014

SMAU PADOVA
16-17 APRILE 2014

SMAU TORINO
14-15 MAGGIO 2014

SMAU BOLOGNA
4-5 GIUGNO 2014

SMAU FIRENZE
2-3 LUGLIO 2014

SMAU MILANO
22-23-24 OTTOBRE 2014



Nel 2013 oltre 85.000 imprenditori e manager hanno sfruttato Smau per innovare la propria impresa.

SMAU: I PROTAGONISTI MONDIALI DELL'INNOVAZIONE; IL TALENTO UNICO DEGLI OPERATORI ITALIANI; LE MIGLIORI SCHOOL OF MANAGEMENT. INSIEME A DISPOSIZIONE DELLA TUA IMPRESA.

IN COLLABORAZIONE CON

Gartner



SDA Bocconi

smau

www.smau.it



contact@smau.it



+39.02.283131



CONTATTI

ICT security

4

Modelli di business e minacce in evoluzione	5
I nuovi rischi della mobilità	6
L'evoluzione della Network security	8
Una nuova generazione di firewall	10
Lo spear phishing per arpionare target mirati	12
SCADA: un rischio trascurato	13
Le Advanced Persistent Threat	14
Spostare la protezione nel cloud	16
La sicurezza delle applicazioni	18
La security intelligence di IBM	19
La sicurezza multilivello di HP ESP	20
HP Fortify per lo sviluppo di codice sicuro	21
HP ArcSight: la piattaforma per la protezione dei dati	22
HP TippingPoint Next Generation Firewall e IPS	24
La protezione estesa di Fortinet	26
La sicurezza unificata di Websense	27
La Content Security di Trend Micro per rispondere alle nuove minacce	28
Soluzioni per la protezione in ambienti virtualizzati e cloud	30
Le nuove sfide: attacchi mirati, mobilità, SCADA	32
La roadmap di Symantec per sconfiggere le minacce avanzate	34
I firewall Dell Sonicwall per le esigenze enterprise	35

communication

Servizi VoIP in ambito business sempre più utilizzati anche grazie al cloud	36
Video trasferite in Pirelli, basta viaggi	36

networking

Ipswitch porta alle PMI il monitoraggio di rete enterprise	37
--	----

l'opinione

L'allineamento catartico tra IT e business	38
--	----

server&storage

Data Center più disponibile con il sistema di refrigerazione di Emerson	39
Con Fujitsu vShape ed ETERNUS fai più con meno	39

software

Con F5 e VMware più sicuri i desktop virtuali	40
Software AG migliora la gestione mobile	40

docu.management

L'Europa accelera sulla fatturazione elettronica	41
--	----

cloud

Microsoft Cloud Platform: nuovi servizi da Dimension Data	42
Da IBM un marketplace per il cloud d'impresa	42

Direction Reportec - anno XII - numero 67 mensile aprile 2014 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**

ICT SECURITY

Il tema della sicurezza diventa sempre più critico all'interno delle aziende sotto la spinta di minacce più sofisticate, cybercriminali più organizzati e di una diffusione delle informazioni che, tra cloud, social network e mobilità, è diventato difficilissimo tenere sotto controllo.

La protezione si sposta quindi verso i temi dell'integrazione tra differenti tecnologie specializzate, interventi in tempo reale e policy aziendali inserite in modo strategico all'interno dei processi di business



Modelli di business e minacce in evoluzione

La trasformazione in atto sia a livello tecnologico sia di modelli di business porta a rivedere approcci e strategie per far fronte a un cyber crime che diventa sempre più efficiente e organizzato

È in atto una “business transformation” che sta ridefinendo completamente i processi aziendali, aumentando la produttività, cambiando le relazioni di lavoro e sviluppando attività completamente nuove.

Gli strumenti di social business o social collaboration ne sono un esempio. Un altro riguarda tutto il mondo delle “App” mobile, che, oltre ad aprire a servizi prima impensabili, sta portando alla nascita di aziende nuove dedicate a nuovi business. Ancora, il video ad alta definizione sta cambiando il modo di relazionarsi, riducendo gli spostamenti o permettendo servizi come lo sportello bancario pseudo-virtuale, in cui l’operatore è in remoto, o la telemedicina, con un esperto che “serve” presidi medici multipli.

In conseguenza di ciò il tema della sicurezza aziendale si arricchisce ogni giorno di nuove sfaccettature, approcci e metodologie.

Il malware è quanto mai in aumento in termini numerici e alcune stime valutano in 12mila all’ora il numero delle nuove minacce, mentre le vulnerabilità per Android hanno già da tempo superato quota 1 milione.

L’escalation delle minacce non è però solo quantitativa ma anche qualitativa e la nuova generazione di attacchi che non è altro che il riflesso di un’evoluzione nelle logiche e metodiche del mondo degli hacker, che sono diventati profes-

sionisti del crimine, che operano in modo organizzato e strutturato, con logiche e modalità identiche a quelle del business legale, vendendo servizi illeciti a listino, coperti persino da garanzie contrattuali sul livello di servizio fornito.

Non solo i dati ma anche le altre risorse aziendali rappresentano un target per il cyber crimine poiché, per esempio, i server compromessi possono essere utilizzati come base per inviare altro malware o lanciare attacchi del tipo Distributed Denial of Service (DDoS).

Rispondere al cambiamento del cyber crime

I cyber criminali non puntano solo a sottrarre i dati dell’azienda, ma attaccano anche la sua interfaccia di comunicazione verso l’esterno ovvero il sito Web, al fine di danneggiarne l’immagine o ridurne l’operatività, magari per l’azione di un concorrente che si è rivolto a un’organizzazione di cyber crime. Il numero complessivo delle pagine Web infette continua così a crescere a un ritmo di migliaia al giorno

e l’Italia si posiziona ai primi posti nella lista dei Paesi che ospitano il maggior numero di siti Web infetti. Tutto ciò evidenzia alcuni requi-

siti che dovrebbero caratterizzare una piattaforma di sicurezza ICT a supporto di una strategia efficace di protezione in ambito manifatturiero. Il primo punto è che, innanzitutto, è necessario **affrontare in maniera unificata i rischi** associati a tutti i processi aziendali e predisporre un modello di protezione integrato in cui tutti gli strumenti di controllo possano essere gestiti e osservati da un punto unico. L’integrazione, però, da sola non basta, perché gli attacchi operano contemporaneamente su più fronti e con più vettori, con tecniche sofisticate che gli consentono di occultarsi molto bene e di superare controlli di primo livello. Diventa allora importante predisporre un **meccanismo di analisi** che sia in grado di comprendere quello che sta accadendo e di correlare le informazioni di sicurezza per riuscire a individuare eventuali anomalie che rappresentano i prodromi per l’identificazione di azioni nocive e che possono emergere solo da una visione dello scenario complessivo. Si tratta di un compito che diventa sempre più difficile perché quelli della sicurezza sono veri e propri Big Data. Si stima che in media i sistemi di un’azienda

enterprise producano 10-15

Terabyte di dati di sicurezza a settimana: una quantità di informazioni enorme che gli analisti prevedono raddoppierà entro un anno. *

Si deve affrontare in modo unificato il rischio associato a tutti i processi aziendali e predisporre un modello di protezione integrato

I nuovi rischi della mobilità

Il panorama tecnologico è in continua evoluzione. L'esplosione della mobilità ha drasticamente cambiato il modo di condurre gli affari delle organizzazioni e le modalità di lavoro delle persone. Questo cambiamento ha anche costretto le aziende a far fronte a una serie di nuove vulnerabilità che crescono in numero e in pericolosità e sono sempre più frequentemente in grado di attribuire al cyber criminale il controllo totale sull'obiettivo del suo attacco

Negli ultimi anni diversi fattori hanno contribuito a cambiare il punto di vista sulla sicurezza e a sfatare l'idea che rappresenti un costo a perdere, intravedendo in essa, sempre più spesso, opportunità se non addirittura un motore per il business.

Uno dei fattori più rilevanti in tal senso è l'insieme di opportunità derivanti dall'utilizzo di strumenti wireless e dall'accesso alle risorse IT aziendali da remoto e in mobilità. L'utilizzo sempre più diffuso della posta elettronica mobile, in particolare, ha spinto molte aziende ad attivare una serie aggiuntiva di servizi usufruibili via cellulare o smartphone, a partire, ancora una volta, da società di telecomunicazioni e banche. È evidente che attività del genere presentano un prerequisito imprescindibile di sicurezza, per garantire la riservatezza delle transazioni, di qualunque natura esse siano.

I temi della "mobile security"

La mobilità fornisce un contributo essenziale al processo di "business transformation" che ridefinisce completamente i processi aziendali, aumentando la produttività, cambiando le relazioni di lavoro e sviluppando attività completamente nuove.

Le tematiche di sicurezza legate alla mobilità sono riconducibili a molteplici aspetti.

Un primo tema riguarda l'utilizzo di dispositivi di tipo personale in cui sono archiviate informazioni che caratterizzano in modo orizzontale la vita di un individuo includendo sia la sfera personale sia quella professionale.

Peraltro i dispositivi mobili non sempre sono progettati per fornire il livello di affidabilità e resistenza necessario per un utilizzo aziendale.

Un secondo aspetto coinvolge l'aspetto applicativo e i rischi per i sistemi operativi mobili e le App.

Per avere un'idea della portata del rischio si pensi che il numero di App potenzialmente nocive per Android è stato stimato abbia raggiunto l'impressionante numero di un milione. Si tratta di un fenomeno che ricorda quello che ha caratterizzato altri sistemi operativi di grandissima diffusione, come Windows, con la differenza che lo sviluppo tecnologico sta rendendo tutto più rapido portando il numero di minacce a crescere in numero e in pericolosità.

La consumerizzazione

Un più recente fenomeno è quello della cosiddetta "consumerization", tradotta in "consumerizzazione". In sintesi, si tratta dell'ingresso in azienda di tecnologie nate per il mondo consumer e, pertanto, non progettate con i requisiti tipici di

affidabilità e sicurezza delle soluzioni di classe enterprise.

Ma le problematiche connesse a tale fenomeno vanno ben oltre gli aspetti prettamente tecnologici e, riguardando direttamente aspetti sociali, riguardano molto da vicino l'organizzazione del lavoro e i processi di business.

Tutto è cominciato con il "boom" del social software o delle applicazioni di social networking accessibili via Web. Sono sempre di più gli studi che testimoniano come, perlomeno in taluni ambiti funzionali (come il marketing) o settori industriali (anche, ma non solo, quelli dedicati al mercato consumer), l'utilizzo oculato di Facebook, Twitter, YouTube o altri strumenti analoghi, può essere utile per il business aziendale, non solo in termini di immagine. In ogni caso, esiste una spinta costante all'utilizzo di tali strumenti da parte dei dipendenti che già hanno account personali su tali siti. Ma navigando nei blog e nei siti di social networking gli utenti si espongono a diversi pericoli.

Sul Web, però, gli strumenti utili non si limitano al social software: le migliaia di applicazioni disponibili per smartphone e tablet sono diventate uno strumento irrinunciabile per milioni di persone che le usano per organizzare le proprie attività nel tempo libero, più che per divertimento.

Per tali individui, diventa naturale usare tali "App" anche nel lavoro e farlo attraverso il loro dispositivo personale, cui sono abituati e che si sono scelti.

Verso il BYOD

Un terzo fondamentale aspetto riguarda le modalità di utilizzo dei dispositivi mobili che trova descrizione nella sigla **BYOD (Bring Your Own Device)**, che rappresenta una conseguenza del fenomeno più ampio della consumerizzazione, portando con sé i rischi legati a un uso promiscuo, personale e aziendale, di dispositivi informatici.

Il BYOD descrive un meccanismo in base al quale le aziende concedono ai dipendenti di usare per lavoro i loro dispositivi personali, non solo quelli mobili. Ciò genera elevati rischi per la sicurezza dei dati, nonché la perdita di controllo sugli strumenti di lavoro da parte dell'azienda. D'altro canto, genera effetti benefici altrettanto potenti, per esempio, in termini di soddisfazione del dipendente e di produttività.

Più in generale, l'estensione in rete dell'azienda, il successo di Internet, intranet ed extranet hanno favorito lo sviluppo di soluzioni e strumenti informatici, sia hardware sia software, che rispondono a esigenze di protezione differenti dal passato. Un mondo quindi completamente nuovo che coglie impreparate molte aziende, ma per il quale ci si può e si deve organizzare, anche perché le minacce hanno cambiato forma e obiettivi: il mondo virtuale della Rete sta diventando sempre più simile a quello reale, solo un po' più "cattivo", perché più distaccato.

Una soluzione parziale al problema è stata fornita dai principali produttori di software con soluzioni o appliance per la **protezione degli endpoint**, che si preoccupano di verificare che un dispositivo mobile che si vuole connettere alla rete aziendale soddisfi i requisiti di sicurezza e conformità necessari: per esempio che abbia installato l'ultima patch del sistema operativo o che non abbia disattivato funzioni di protezione.

Queste soluzioni forniscono una protezione efficace per evitare di portare all'interno della rete aziendale malware contratti all'esterno,

ma non c'è tecnologia che tenga per proteggersi dalla superficialità e dalla noncuranza manifestata troppo spesso dagli utenti.

La possibilità di lasciare incustodito il proprio dispositivo mobile o di connettersi a una rete domestica che non dispone dei sistemi di protezione di quella aziendale, lascia aperta la possibilità di smarrire o di diffondere informazioni aziendali importanti e riservate, incluse password di accesso alla rete aziendale, dati sensibili o business critical.

Quella di **privilegiare l'utilizzo di uno strumento unico** è, peraltro, un'abitudine diffusa all'interno del mondo dei business manager che facilmente si trovano a ospitare sul proprio dispositivo mobile personale dati fondamentali per l'azienda: per esempio password di accesso alla rete che, di fatto, lasciando una porta aperta all'intero network aziendale.

Non è poi insolito l'uso di software o di servizi online (per esempio Dropbox) pensati per un uso domestico, per trattare o archiviare dati critici con modalità che sfuggono al controllo dell'IT, spesso con insufficiente consapevolezza dei rischi.

Tutto ciò apre innumerevoli falle nella sicurezza aziendale che vanno affrontate attraverso un approccio strategico che definisce modalità e regole per l'uso dei dispositivi mobili e preveda altresì opportune tecnologie di gestione e controllo per verificarne il rispetto. *



L'evoluzione della Network security

Cambia il modo di concepire la sicurezza della rete, mentre si consuma il passaggio da una visione centrata sugli aspetti tecnici del network verso quelli di tipo applicativo

Nello scenario attuale in cui l'accesso avviene in mobilità, le risorse sono nel cloud e i dipendenti utilizzano una vasta gamma di configurazioni di login da remoto, la rete è sempre più esposta a rischi. L'adozione di difese di tipo tradizionale, sebbene essenziali, in assenza di un'adeguata contestualizzazione globale e della presenza di un'intelligence automatizzata dedicata alla sicurezza, non è più in grado di fornire una protezione efficace contro le nuove tipologie di attacco.

Il primo passo per contrastare queste minacce è la consapevolezza che qualsiasi connessione che "chieda" alla rete aziendale di entrare, potrebbe trasportare traffico nocivo. Di conseguenza qualunque utente, applicazione e sistema dovesse chiedere accesso alla rete, è necessario controllare chi sia e cosa vuole fare.

Peraltro, va ormai definitivamente abbandonato il concetto di perimetro. Se in precedenza, anche se la connessione poteva avvenire praticamente in qualsiasi punto, una transazione o un'operazione da compiere era sempre riconducibile a una macchina, con il cloud anche questo punto fermo è saltato.

Una protezione efficace richiede l'adozione di una serie di funzionalità integrate e interoperabili, ognuna ottimizzata per fronteggiare specifiche minacce, capaci di for-

nire informazioni puntuali e organizzabili secondo viste idonee a comprendere la situazione e a prendere le decisioni che meglio sposino le policy di sicurezza con i rischi e le esigenze di business dell'impresa.

La parola chiave in merito ai rischi di intrusione è dunque una sola: prevenzione.

Una revisione nell'approccio strategico

La convergenza dei servizi di rete sul protocollo IP acuisce ulterior-

mente il problema: si pensi alla realizzazione di infrastrutture critiche che si appoggiano o sono comunque collegate alla rete aziendale e da qui a Internet.

Predisporre misure efficaci di sicurezza significa affrontare anche una revisione della rete che però non è, come molti pensano, necessariamente di natura tecnologica, ma prevalentemente di carattere strategico.

Ovviamente il problema di come impostare una strategia per l'infrastruttura di rete aziendale si abbina anche al modo di predisporre l'inserimento di nuovi dispositivi partendo dalla situazione preesi-

Dal video streaming alle botnet

Un altro pericolo arriva dal video streaming. Attraverso la fruizione di video on-line, per esempio dal sito di YouTube, è possibile che un inconsapevole utente scarichi sul suo computer trojan horse, ovvero programmi che potrebbero contenere codice dannoso in grado di sottrarre dati confidenziali.

Un altro elemento di rischio può essere posto dai siti Web che utilizzano la cifratura SSL (Secure Socket Layer). Infatti, molti sistemi di sicurezza non esaminano il "tunnel SSL" all'interno del quale vengono trasportati in modalità punto-a-punto i dati criptati, rendendo il traffico SSL un possibile vettore da sfruttare per predisporre azioni indirizzate alla sottrazione dei dati. L'utilizzo del protocollo SSL in Web server predisposti da malintenzionati può anche diventare un veicolo con cui trasportare trojan e bot al di là della protezione del firewall e farli penetrare nella rete aziendale protetta. Una volta installati i bot sono in grado di costruire reti di collegamento tra computer che sfruttano analoghe sessioni SSL per far fuoriuscire informazioni dall'azienda o per introdurre virus informatici e trojan.

Da ultimo, ma non certo per importanza, va citato il fenomeno dei botnet che realizzano reti di computer "controllati" da un cyber criminale, che li può utilizzare per inviare un attacco o uno spam su grande scala, senza che l'utente del computer si accorga di niente. Il fenomeno è in espansione e si prevede che in futuro le botnet, e chi le governa, assumeranno il ruolo di centrali distribuite di comando e controllo. In realtà, già oggi esistono botnet disponibili a noleggio, come altri servizi di hacking a pagamento.

stente e determinando il minor impatto possibile. Da questa esigenza specifica, ma basilare nel contesto di un'operatività aziendale che non può subire interruzioni, non possono quindi prescindere i fornitori di piattaforme, che si trovano a dover predisporre modelli architetturali in grado di adattarsi da subito alle nuove esigenze e ai requisiti di business, integrando l'esistente, elevando le prestazioni e mantenendosi aperti per un'evoluzione scalabile.



Sicurezza per una rete sempre più guidata dalle applicazioni

Un altro tema da sottolineare nell'evoluzione della network security riguarda il legame tra i requisiti applicativi e le caratteristiche dell'infrastruttura di rete nonché il progressivo orientamento verso un modello orientato ai servizi e al cloud.

Il passaggio da una visione centrata sulla parte "tecnica" di una rete a quella "applicativa" ha profonde implicazioni a livello di sicurezza, anche perché coinvolge nel processo decisionale e di cambiamento un insieme di figure manageriali e aree di responsabilità aziendale più orientate al business e che, per molto tempo, sono state sostanzialmente non interessate a quanto era

ritenuto di esclusiva competenza del reparto IT.

La sicurezza del futuro non potrà, quindi, essere un elemento aggiuntivo del sistema informativo o dell'infrastruttura aziendale ma, invece, un componente pervasivo e integrato di entrambi, come pure di tutti gli elementi tecnologici, anche non IT, presenti in azienda.

Un primo elemento che emerge è che sicurezza e rete sono due cose che è sempre più opportuno siano **pensate e sviluppate in modo parallelo**. Una tale sinergia appare poi tanto più necessaria quanto più la rete agisce come integratore e come base per applicazioni convergenti e per l'erogazione di servizi.

Si tratta del punto di arrivo di

un processo di convergenza tra security e networking che parte da lontano: quando gli switch hanno cominciato a fare i router e questi ultimi hanno iniziato a controllare gli accessi tramite le ACL (Access Control List).

Un ulteriore elemento in grado di caratterizzare il modello architetturale e condizionare l'efficacia di protezione della rete è la capacità di **implementare un livello di intelligenza** e di distribuirlo in base agli specifici requisiti di business.

Si tratta di un requisito ormai irrinunciabile, in uno scenario caratterizzato dalla dispersione delle informazioni nel cloud e da modelli di business innovativi che richiedono di operare in tempo reale su scala globale.

Questo ha favorito l'affermazione di appliance dedicate, pronte a integrare una serie di funzionalità di sicurezza in costante ampliamento ed evoluzione.

Nell'ultimo periodo soprattutto due ambiti sono emersi come i più critici nell'ambito della network security: gli attacchi DDoS (Distributed Denial of Service) e la lotta alle intrusioni, che ha portato allo sviluppo di Firewall e IPS (Intrusion prevention system) di "prossima generazione. *

Una nuova generazione di firewall

Scompare l'idea di un perimetro esterno e si affacciano firewall di nuova generazione in grado di esercitare il controllo a livello delle applicazioni e di fornire maggiore efficacia nella Intrusion Prevention

Uno dei primi problemi che le aziende si sono poste con l'apertura verso il Web è stato il controllo degli accessi alla rete aziendale, per il quale sono stati sviluppati opportuni protocolli di autenticazione. È stato però subito evidente che dalla Rete potevano arrivare sul sistema e sul Web aziendale dei malintenzionati. Inizialmente, si temeva più che creassero danni per gioco, mentre oggi si sa che vogliono colpire in maniera mirata.

Sono nati i firewall, che si preoccupavano di "chiudere" alcune porte della rete, permettendo il passaggio solo di "traffico giusto". Ma ben presto, il traffico "cattivo" ha imparato a mascherarsi e i firewall a farsi più furbi e a intensificare i controlli.

L'escalation tra tecniche d'intrusione e sistemi per rilevarle e bloccarle è storia. La rincorsa prosegue, ma il modo di fronteggiarsi tra aspiranti intrusori e aziende ha cambiato ritmo e, da entrambe le parti, si adottano sistemi più automatizzati e sofisticati.

I Next Generation Firewall rappresentano uno degli ultimi step di questo percorso evolutivo.

I Next Generation Firewall

La prima definizione di Next Generation Firewall si deve a Gartner che nel suo "Magic Quadrant for Enterprise Network Firewalls" del 2009 ha individuato come requisiti caratterizzanti per questo tipo di solu-

zioni l'integrazione delle seguenti funzioni:

- analisi approfondita dei pacchetti (Deep Packet Inspection),
- Intrusion Detection,
- capacità di riconoscere le applicazioni,
- capacità di controllo granulare.

Inoltre i Next Generation Firewall differiscono da quelli tradizionali nella loro efficacia quando operano anche come sistemi di Intrusion Prevention (IPS).

Le ragioni per indirizzarsi verso un firewall di nuova generazione sono molteplici, ma possiamo evidenziare le principali.

La prima riguarda la possibilità di controllo a livello di applicazione poiché oramai la stragrande maggioranza delle violazioni sfruttano le vulnerabilità collocate all'interno di applicazioni.

Si tratta, in realtà, di una conseguenza dell'evoluzione e dell'innovazione di approccio degli attacchi che si stanno spostando dalle reti, per sfruttare le falle anche dei sistemi operativi e delle applicazioni. Di conseguenza, dato che gli hacker sono sempre più ingegnosi nello scoprire nuovi percorsi dati, è fondamentale rendere sicuro l'intero flusso. Un controllo a livello di applicazione è quindi di fondamentale importanza perché permette alle organizzazioni di impostare policy specifiche per un utente, per ogni applicazione che utilizza.

Una seconda motivazione riguarda la

diffusione della mobilità e la crescita fenomenale di App a cui sono associate moltissime vulnerabilità, tanto che i campioni unici di minacce indirizzati al sistema Android hanno già superato abbondantemente l'impressionante numero di un milione.

Un ulteriore driver riguarda la constatazione che le nuove minacce come le APT (Advanced Persistent Threat) stanno aumentando di numero, mentre gli obiettivi si estendono progressivamente dalle aziende più grandi per includere, potenzialmente, qualsiasi tipo di organizzazione. L'importanza delle tecnologie firewall evolute diventa evidente se si considera che la prima fase di un attacco APT è di penetrare le difese di rete in modo inosservato.

In definitiva, in un contesto di reti senza perimetro, minacce persistenti e utenti remoti, i Next Generation Firewall rappresentano soluzioni in grado di contribuire a elevare il livello di protezione



della rete senza impattare su processi e infrastruttura.

L'importanza della sandbox

Questa classe di dispositivi prevede solitamente anche sofisticate funzionalità di Intrusion Prevention e anche se l'aspetto caratteristico più enfatizzato di queste soluzioni è l'attenzione a livello applicativo, un altro elemento che emerge come soluzione largamente utilizzata è l'impiego di un meccanismo di "sandboxing".

La scatola di sabbia fa pensare alla lettiera del gatto, ma negli Usa è il quadrato in cui giocano i bambini più piccoli al parco, tipicamente "smontando" con la loro grazia i giocattoli, senza rischiare di farsi male. Si tratta di "smontare" il codice sospetto, che viene instradato in una zona sicura e isolata, dove viene tenuto sotto controllo: alle volte se ne simula il funzionamento, altre volte lo si lascia semplice-

mente decantare. Insomma, si cerca di capire cosa fa. Se risulterà di natura maligna si prenderanno le contromisure.

Aspetto fondamentale dei sistemi di sandboxing è **classificare il malware** che viene riconosciuto come tale, in modo da poterlo facilmente identificare una seconda volta.

La logica, inoltre, è creare una "signature" o qualcosa che permetta co-

munque ad altri sistemi di riconoscere "l'impronta" di questo malware. Tale signature viene propagata su tutti i sistemi del produttore attraverso servizi di aggiornamento su scala globale, un po', banalizzando, come avviene da tempo per gli antivirus. Ogni vendor ha il proprio sistema e, purtroppo, quando c'è, la condivisione delle informazioni, in questi casi, è comunque a posteriori. *

Attacchi DDoS: un rischio ad ampio spettro

Gli attacchi di Distributed Denial of Service (DDoS), che consistono nel "bombardare" un servizio Web con grandi volumi di traffico fino a metterlo in tilt, si sono costantemente moltiplicati negli ultimi dieci anni, allargando gli ambiti di impiego fino a diventare oggi una delle principali minacce alla sicurezza informatica.

Si stanno intensificando, per esempio, gli attacchi mirati di sabotaggio aziendale che sfruttano questa tecnica nell'ambito del gaming online e del commercio elettronico.

Per le telco e i service provider quello dei DDoS sta diventando un problema serio, ma in realtà a subire le conseguenze è l'industria dei servizi online nel suo complesso. Ormai persino le piccole aziende agricole riescono a vendere i propri prodotti DOP o IGP in tutto il mondo attraverso Internet e c'è chi si sente sicuro, magari perché ritiene di non avere concorrenti o di essere troppo ben voluto per diventare un bersaglio. Il problema, però, sono i danni collaterali degli attacchi destinati a data center di provider, che si ripercuotono a catena su una pluralità di servizi.

Dallo spionaggio industriale a quello dei servizi segreti, il passo è purtroppo breve e la Cyber War è una preoccupazione che agita molti governi.

Il primo caso di Cyber War che viene citato è l'attacco che nel 2007 ha isolato da Internet l'ex Repubblica sovietica d'Estonia proprio con attacchi DDoS. La Russia, principale indiziato nega. In nome della Cyber Defense si investe, ricordando la Guerra Fredda, nella corsa agli "armamenti", in termini di CyberWarefare, cioè nel dotarsi di competenze, risorse umane e "armi" informatiche, compresi gli strumenti DDoS.

In futuro le possibilità di attacco terroristico o di sabotaggio aumenteranno vertiginosamente con l'esplosione dell'Internet of Thing. L'Internet delle Cose, infatti, è un fenomeno crescente che prevede il progressivo collegamento di un numero sempre maggiore di dispositivi in Rete. Macchine di ogni tipo, dagli impianti industriali a sensori vari sono e saranno sempre più in grado di comunicare tra loro ed essendo connessi a Internet potranno essere sfruttati per penetrare in network aziendali (è già successo che un sistema per il monitoraggio dei frigoriferi di un supermercato fosse usato per arrivare ai POS e rubare numeri di carte di credito).



Lo spear phishing per arpionare target mirati

Uno degli strumenti più efficaci per estorcere importanti informazioni è il phishing mirato, che rappresenta il primo grimaldello con cui scardinare le difese di aziende e organizzazioni e che sfrutta al meglio le informazioni liberamente accessibili sui social network

La posta elettronica resta uno dei veicoli d'infezione preferiti o, quantomeno, uno degli strumenti utilizzati per le sofisticate tecniche di phishing o "spear phishing", quello, cioè, mirato. Lo spam tradizionale è infatti in calo, stando ad alcuni rilevamenti, ma sta crescendo quello collegato ai social network. Al contrario, sempre più efficaci si dimostrano gli attacchi mirati che partono con una e-mail di phishing appunto.

Quest'ultima tecnica si è evoluta, per cui bloccare tali e-mail è molto più difficile che in passato, in quanto non si tratta di messaggi rivolti alla massa, quindi standardizzati e facilmente riconoscibili. Lo spear phishing si basa su dati appositamente raccolti per colpire uno specifico target. Si tratta di e-mail personalizzate, che non sono state osservate da altri sistemi precedentemente e che non sembrano "estrane" all'azienda.

Gli attacchi di phishing, in passato, erano tutti basati sulla stessa procedura: l'e-mail inviata a centinaia di migliaia di indirizzi contava sulla legge dei grandi numeri. Statisticamente una piccola percentuale di destinatari reagiva finendo nella trappola dei cybercriminali e infettando il pc.

L'efficacia del sistema si basa sulla statistica e sull'ingenuità degli utilizzatori. Anche se

di poco, però, la cultura di questi ultimi sulla sicurezza è andata aumentando negli anni e, parallelamente, è calata l'efficacia del phishing tradizionale. Ovviamente la maggior parte del merito va al miglioramento dei sistemi anti-spam e anti-phishing, che adesso includono tecnologie come: la "reputation" del mittente, che classifica gli indirizzi di spedizione per bloccare quelli che notoriamente riversano spam; l'analisi lessicale sul contenuto delle e-mail per individuare frasi e combinazioni di parole o schemi usati di solito per lo spam; l'integrazione con gli antivirus, che identificano i codici maligni noti abbinati alla posta elettronica.

Un modello di attacco sempre più mirato

Il modello degli attacchi di phishing si è evoluto negli ultimi anni e, soprattutto, si è fatto ancora più mirato: indirizzandosi a piccole comunità, come possono essere i dipendenti o, più in dettaglio, i quadri di una specifica impresa. Si è anche semplificato, perché non contiene direttamente il malware,

ma un link a un sito Web, non di rado legittimo, dove però è stato annidato il kit maligno. Inoltre, i server utilizzati non risentono di una cattiva reputazione, perché inviano pochi messaggi che non sono riconosciuti come spam.

Chiaramente questo presuppone qualche sforzo in più, per esempio per compromettere un sito legittimo senza che i

Lo spear phishing attacca in modo mirato le figure professionali dirigenziali per conseguire un livello di accesso più ampio alle risorse aziendali

suoi gestori se ne accorgano, anche solo per il tempo necessario a portare a termine l'attacco.

Rispetto allo spam, il phishing ha tassi di redemption più elevati, se poi è mirato l'efficacia è alta. Tali sforzi andranno ripagati, quindi il bottino sarà ricco: per esempio un numero elevato di dati, come i numeri di carte di credito o proprietà intellettuali (per esempio brevetti).

Anche l'analisi lessicale fallisce e lascia passare il phishing sofisticato, perché i contenuti, essendo mirati, sono compatibili con il contesto e non riconosciuti come spam. Gli antivirus non trovano malware da analizzare e bloccare.

Occorrono soluzioni più sofisticate, che eventualmente siano in grado di seguire il link verso il codice maligno, riconoscerlo come tale e bloccare il download di dati compromessi. Meglio se possono operare in tempo reale. *

SCADA: un rischio trascurato

I sistemi SCADA, sebbene sovrintendano al controllo di infrastrutture di importanza primaria, non sempre dispongono di pratiche di sicurezza rigorose e sono sempre più spesso presi di mira dai criminali con l'intenzione di causare disagi ai fini di ricatto, terrorismo o estorsione

Gli Industrial Control Systems (ICS) sono dispositivi, sistemi, reti e controlli utilizzati per operare e/o automatizzare i processi industriali, presenti in quasi ogni settore, dalla produzione di veicoli al trasporto, dall'energia al trattamento delle acque.

Gli ICS comunicano con i sistemi e le reti SCADA (Supervisory Control And Data Acquisition) che forniscono agli operatori i dati per le attività di supervisione e la capacità di controllo per la gestione dei processi.

La sicurezza di sistemi ICS/SCADA resta un tema importante perché sono comunemente utilizzati per il funzionamento di industrie di grande rilevanza e per il monitoraggio e controllo della maggiore parte dei servizi essenziali ai cittadini, come la fornitura di acqua, elettricità, gas e anche i mezzi di trasporto.

In ambito industriale i sistemi ICS/SCADA sono utilizzati da tempo e, mano a mano che l'automazione continua a evolversi e diventa più importante a livello mondiale, la loro

diffusione e importanza cresce.

Una crescita a cui, purtroppo, fa eco una mancanza di protezione ben documentata e ampiamente conosciuta. È noto, per esempio, che attraverso Internet si possono effettuare ricerche che restituiscono facilmente l'accesso ai pannelli di controllo di sistemi SCADA, l'identificazione delle macchine e delle loro funzioni. Altri siti vengono sempre più spesso utilizzati per la diffusione di informazioni legate ai dispositivi ICS/SCADA come, per esempio, i loro indirizzi IP.

Tutto ciò ha favorito e continua a favorire le azioni del cyber crimine che, negli ultimi anni, ha segnato importanti punti a proprio favore con minacce quali Stuxnet considerato uno dei codici malware più sofisticati che sia mai stato scritto.

Sistemi con requisiti specifici di protezione

Va rimarcato che i sistemi ICS/SCADA, sebbene simili nelle funzioni ai sistemi di ICT Security, differiscono notevolmente da questi ultimi

nel modo di interpretare l'esigenza di sicurezza. La prima priorità dei sistemi IT di sicurezza è tipicamente la protezione dei dati mentre nei dispositivi ICS/SCADA si tende a privilegiare l'affidabilità e l'accessibilità dei dati per non compromettere la produttività.

Ogni sistema SCADA presenta poi **caratteristiche specifiche** in termini di requisiti di disponibilità, architettura, obiettivi e requisiti prestazionali e questo richiede che vengano trattati in modo unico.

Solitamente i sistemi SCADA non prevedono di default la presenza di soluzioni anti malware. Questo è legato sia alla loro natura intrinsecamente legacy sia perché si tratta di macchine deputate al controllo di altri strumenti per cui una qualsiasi forma di ritardo nel calcolo computazionale introdotta da un sistema di controllo potrebbe causare inconvenienti. Per questa ragione solitamente il controllo dei sistemi SCADA viene effettuato a livello di singola macchina in modalità batch e, in molti casi, non è neppure possibile effettuare controlli in rete. Un altro problema di cui le aziende solitamente non si preoccupano è che le macchine SCADA sono **gestite e mantenute da terze parti**. Pertanto, se non si ha la possibilità di esercitare un'azione di controllo sui processi di queste terze parti o se non si mette a loro disposizione un sistema per effettuare un controllo in linea della macchina, il rischio di introdurre malware su uno di questi dispositivi diventa elevato. *



Le Advanced Persistent Threat

Aumenta il numero degli attacchi mirati, che adottano una combinazione di tecniche sofisticate e una strategia basata su più fasi.

Il target di questi attacchi è prevalentemente quello delle organizzazioni Enterprise, delle utility, delle aziende del settore energetico o delle grandi imprese industriali, ma la loro diffusione si sta estendendo a ogni livello

Tutti i rapporti divulgati dalle principali società impegnate nella sicurezza concordano su un dato: aumentano il numero degli attacchi "mirati", cioè condotti con un preciso fine, e di quelli "silenti", cioè orientati a un obiettivo evitando di "far rumore". Sono quelli che vengono raccolti nella categoria cosiddetta Advanced Persistent Threat (APT).

Gli aggettivi "advanced" e "persistent" indicano le caratteristiche principali di questi attacchi: l'uso di tecniche sofisticate, la combinazione delle stesse in una strategia basata su più fasi e la tenacia con cui questa viene applicata con continuità fino all'ottenimento dell'obiettivo e oltre. Oltre, perché in casi come lo spionaggio, il malware è progettato per annidarsi e continuare a spiare indisturbato anche per anni.

Il target di questi attacchi è prevalentemente quello delle organizzazioni Enterprise, delle utility, delle aziende del settore energetico o delle grandi imprese industriali. Si tratta di processi di attacco che fanno un uso massiccio del social engineering favorito dalla disponibilità di informazioni presenti sui siti di social network.

Un Advanced Persistent Threat è un processo di attacco che segue regole precise e determinate e che è stato studiato e definito tanto da poter essere ricondotto a diverse fasi specifiche.

Le fasi preliminari e di preparazione di un attacco APT

1 - Ricognizione - Come detto, gli APT sono perlopiù attacchi mirati, che, come nella migliore strategia di guerra, sono preceduti da una fase di studio del "nemico". In questo caso, il cybercriminale cerca dati sul bersaglio da colpire, partendo, tipicamente, dal sito Web e facendo sfoggio di capacità deduttive. Per esempio, un'offerta di lavoro in cui si ricerca personale specializzato in un determinato applicativo software permette di comprendere quali sistemi vengano utilizzati in un'azienda, identificando potenzialmente delle vulnerabilità. In generale, si vuole trovare dati personali tra i profili online, gli indirizzi e-mail, gli organigrammi aziendali, gli hobby e interessi sui Social Network.

Più informazioni si ottengono, maggiori sono le probabilità di affinare le successive fasi di attacco.

2 - Adescamento - Questa fase è diventata più facile di quanto si possa immaginare con la diffusione dei sistemi mobile. La cultura sulla sicurezza informatica è scarsa ed è facile incuriosire, soprattutto se si conoscono (vedi fasi uno) i punti deboli della persona cui si spedisce un messaggio mirato. Inoltre, quando questi messaggi arrivano sullo smartphone, dove complice la "visibilità ridotta" e soprattutto l'abitudine a cliccare prima e pensare dopo, è alta la possibilità che il malcapitato caschi nella trappola. Quasi certamente non se ne accorgerà, perché il cybercriminale si guarderà bene dal creare disturbo, magari gli manderà un secondo messaggio di scuse perché il primo aveva avuto un comportamento strano, tranquillizzando gli eventuali dubbiosi. I filtri antispam possono fermare attacchi di massa, ma nel caso di quelli mirati i messaggi puntano su comunicazioni normalmente attese dall'utente, che spesso questi filtri considerano attendibili. Gli attacchi mirati usano anche messaggi apparentemente inviati dal proprio capo e quindi la sicurezza aziendale, teoricamente, andrebbe estesa anche alla pagina Facebook dei dipendenti. Per l' momento, le informazioni sulle minacce raccolte dai sistemi di sicurezza dovrebbero correlare Web ed e-mail, anche considerando che il 92% dello spam via e-mail contiene un URL.

3 - Dirottamento - L'esca della fase due molto spesso reindirizza verso un sito Web dove è annidato un

I processi di attacco mirati fanno uso massiccio del social engineering sfruttando anche le informazioni disponibili sui social network



exploit kit. Anche in questo caso, c'è molta differenza tra gli attacchi APT di massa e quelli mirati. I primi cercano di adescare il maggior numero di persone, ma per questo non possono essere troppo sofisticati nel messaggio e nel tipo di trappola. Per quelli mirati, ci si può anche prendere la briga di attaccare un sito insospettabile per installarvi sopra il kit di malware.

4- Exploit - La fase centrale è fondamentale per l'attacco vero e proprio, cioè della penetrazione all'interno delle difese avversarie. Gli exploit sono sempre più sofisticati: per esempio i Blackhole utilizzano sistemi di cifratura difficili da identificare con soluzioni antivirus. Decisamente più efficaci possono essere i gateway di ultima generazione, come i Next Generation Firewall, ma non tutti arrivano a comprendere il reale funzionamento del malware, che, talvolta, rimane "inattivo" a lungo dopo l'installazione sulla rete del bersaglio.

I sistemi che filtrano il traffico sulla base di signature, potevano essere efficaci in passato quando i kit erano numericamente di meno e basati su relativamente poche va-

rianti, ma ormai sono inadeguati. Gli exploit kit, adesso colpiscono con un malware di tipo dropper (che si deposita direttamente nel sistema informatico attaccato), solo quando rileva una porta aperta sicuramente vulnerabile. In caso contrario devia l'utente verso una pagina Web normale e rimane nascosto, aspettando la prossima occasione.

Parte l'attacco vero e proprio

5 - Installazione - Siamo a quello che viene considerato l'attacco vero e proprio in cui il nemico avanza pronto a sfondare le barriere esterne. Non a caso, dunque, è qui che si concentrano i cosiddetti sistemi di protezione perimetrale, analizzando ogni file che penetra nella rete per rilevare eventuale malware. Come accennato, però, non è facile come prima rilevare i codici maligni di nuova generazione attraverso signature e pattern, perché questi utilizzano pacchetti dinamici.

6 - Comando e Controllo (C&C) - Una volta compiuta l'installazione del primo malware, il sistema informativo è presto in balia del cyber criminale che predispone un canale per la comunicazione tra l'host com-

promesso e il server C&C. Il malware contatta "casa" e attiva il download di strumenti e di altro codice maligno per inviare informazioni. Evidentemente, in questa fase occorre un sistema che analizzi il traffico in uscita, ma sono ancora poco diffusi. Ne occorrono di abbastanza sofisticati, infatti, perché attraverso strumenti semplici, come un DNS dinamico i cybercriminali evitano il rilevamento delle operazioni di chiamata a casa verso indirizzi statici. Tuttavia è possibile inibire l'uscita di dati verso sistemi che non siano noti e quindi inibire l'uso di DNS che rimandano a server di "command and control". Del resto chi vuole nascondere la propria ubicazione geografica è in genere sospetto.

7 - Azione - La fase finale è quella in cui l'attacco va tipicamente a buon fine se non si è riusciti a intervenire prima. Certamente, anche qui ci sono ancora margini per bloccare il furto dei dati obiettivo dei cyber criminali, ma occorre disporre di sistemi in grado, per esempio, d'identificare una password che sta uscendo dalla rete aziendale oppure di rilevare traffico criptato verso l'esterno con chiavi di cifratura illecite o estranee al proprio sistema di crittografia.

Appare dunque evidente che la predisposizione di una protezione efficace da un attacco mirato deve tenere conto delle vulnerabilità associate a ognuna di queste fasi, con contromisure in grado di operare in modo sinergico. *

Spostare la protezione nel cloud

Le opportunità offerte da un modello di sicurezza as-a-service richiedono, per essere sfruttate, di effettuare le opportune verifiche sulle caratteristiche di tutte le variegate componenti del servizio, dalle caratteristiche dell'infrastruttura, alle normative di competenza, alla cancellazione dei dati in tempi e modi certi

L'esigenza di una crescente sicurezza nell'accesso alle informazioni è fortemente aumentata con la diffusione di Internet e dello sviluppo di modelli di interazione tra aziende che hanno portato al concetto di azienda estesa.

I problemi di sicurezza si sono ulteriormente enfatizzati con la diffusione dell'utilizzo di risorse IT sotto forma di servizio o, come si dice oramai usualmente, nel cloud. L'attenzione alla sicurezza fruita sotto forma di servizio deriva, da una parte dalla complessità del tema dal punto di vista tecnologico e della gestione e, dall'altra, dalla complessità legislativa, che rende difficile per chi non abbia alle spalle un team dedicato alla sicurezza, districarsi tra leggi, norme e responsabilità.

Diversi sono, infatti, gli aspetti che vanno affrontati per sfruttare il potenziale miglioramento nei processi di business, nella flessibilità e nell'efficienza dell'IT, fornito dal passaggio a un ambiente Cloud.

Tra questi, per esempio, la possibilità di realizzare in azienda servizi e controlli scalabili e di tipo pervasivo, il poter realizzare una solida sicurezza non solo di tipo perimetrale ma distribuita a tutti i livelli di business, avere la garanzia della disponibilità dei servizi a livello applicativo e infrastrutturale. Si tratta di punti non semplici da garantire sia per

la vastità delle risorse coinvolte sia per la rapidità del cambiamento e che, congiuntamente, implicano il dover affrontare aspetti complessi. Quello che però è caratteristico di tutti i servizi di sicurezza fruibili tramite Cloud è che le applicazioni rese disponibili dai provider sono state pensate per essere fruite tramite Web e comprendono classi di funzioni e applicazioni che devono poter fornire:

- un aggiornamento continuo e quasi in tempo reale delle regole di sicurezza per contrastare minacce note e di nuovo tipo;
- una capacità di controllo ampia che si estenda fino al livello applicativo;
- capacità di gestione e reportistica;
- continuità operativa e disponibilità dei dati.

Si tratta di servizi che in ambito Cloud, a seconda della complessità specificità settoriale, possono essere fruiti su base contrattuale o richiesti su base on-demand. In genere la tariffazione prevede sia un contributo sulla base del numero di utenti coinvolti che in base alle risorse (storage, server, client virtuali) fruite e in questo non si discostano da quanto avviene per gli altri servizi PaaS o SaaS. In ogni caso la fruizione di Security-as-a-Service può prevedere sia il demandare in toto gli aspetti inerenti la sicurezza al provider su Cloud che farlo in modo parziale o limitato nel tempo.

La riservatezza dei dati e i problemi normativi

Strettamente connesso alla sicurezza in generale vi è quello della sicurezza dei dati nel cloud e quello delle diverse normative delle varie nazioni in cui questi dati possono venirsi a trovare memorizzati fisicamente. Il problema deriva dal fatto che queste normative sono anche molto differenti tra loro e quello che è permesso in una nazione non lo è, in generale, in un'altra e non sempre è chiaro cosa può avvenire dei dati personali o di quelli di pertinenza di una azienda.

Non a caso, anche il **Garante della Privacy** ha sentito l'esigenza di evidenziare alcuni aspetti da considerare per un utilizzo consapevole del cloud, che si possono riassumere in questi punti:

- verifica dell'affidabilità e competenze del fornitore;
- attenta selezione dei dati gestiti in modalità cloud;
- controllo dell'effettiva allocazione fisica dei dati;
- utilizzo di servizi che favoriscono la portabilità dei dati e la loro disponibilità in caso di necessità;
- esigere dal fornitore opportune garanzie in merito alla sicurezza dei dati e delle tecniche di trasmissione oltre alla gestione di situazioni critiche che possono comprometterne la corretta conservazione;
- stabilire in fase contrattuale il Service Level Agreement a cui riferirsi, le penali previste e i tempi di conservazione dei dati dopo la scadenza del contratto.

La scelta del cloud service provider

Per quanto riguarda la scelta del fornitore è anche importante effettuare delle verifiche sulle certificazioni che possiede, oltre che sui servizi offerti e sulla qualità della sua infrastruttura, sull'idoneità della piattaforma tecnologica, sulle competenze del personale e sulle misure di sicurezza che garantisce in caso si verificano situazioni di criticità. Se il **fornitore non fa parte dell'Unione Europea** è meglio verificare che sia possibile effettuare il trasferimento dei dati personali verso il Paese in questione (consentito nei casi previsti dal D.lg. 196/2003) e che ci sia una legislazione che garantisca un adeguato livello di protezione della Privacy. Altrimenti è opportuno sottoscrivere dei modelli di contratto che siano stati approvati dalla Commissione Europea e dal Garante della Privacy. Se, invece, il fornitore svolge un ruolo da intermediario appoggiandosi a un terzo soggetto, è opportuno non perdere di vista l'allocazione fisica dei server.

L'azienda deve sapere con certezza sotto quale giurisdizione risiedono i dati per conoscere la legge applicabile nel caso di controversie tra l'utente e il fornitore del servizio o in cui l'autorità giudiziaria debba eseguire ordini di perquisizioni, sequestro e così via.

Infine è sempre opportuno accertarsi a priori dei tempi che intercorrono dalla scadenza del contratto alla cancellazione definitiva dei dati da parte del fornitore che li ha avuti

in gestione, il quale deve garantire di non conservare i dati oltre i termini stabiliti per contratto. Sempre nell'ottica di un passaggio ad altro fornitore è utile privilegiare i servizi che garantiscono la portabilità dei dati, quindi basati su formati e standard aperti, che facilitino la transizione da un sistema cloud a un altro, anche se gestiti da fornitori diversi.

Nella scelta del fornitore di servizi di sicurezza per l'ambito cloud Enterprise perlomeno tre aspetti andrebbero accuratamente considerati:

- La **disponibilità di policy**, procedure e standard da adottare e cioè la possibilità di acquistare oltre ai servizi software anche le capacità umane necessarie per disporre del necessario supporto nello sviluppare i servizi necessari sulla base della specificità

aziendale, a partire da una approfondita valutazione delle policy esistenti e della loro efficacia.

- L'esistenza di un **framework di riferimento** che permetta di traslare le policy e le procedure in servizi reali applicabili alle attività di business, fornire informazioni parziali e globali inerenti il livello di sicurezza esistente, nonché fornire una visione sul grado di efficacia delle specifiche policy e procedure attivate.
- Adeguati servizi di **Security Services Management** che permettano di fondere in un unico insieme le attività di business e di sicurezza. Ciò può essere ottenuto mediante funzioni di sicurezza e la possibilità di sviluppare un modello di Governance e di valutazione dei risultati dello specifico ambiente business. *



La sicurezza delle applicazioni

Nonostante alle componenti applicative siano imputabili il maggior numero di vulnerabilità, la loro sicurezza resta ancora per certi versi trascurata. Serve un approccio di protezione che ne segua l'intero ciclo di vita, dalla fase di sviluppo, al rilascio in produzione, al costante aggiornamento

La diffusione di nuove tecnologie cloud e mobili ha notevolmente incrementato la richiesta di sviluppo di nuovi software contribuendo ad accelerare ulteriormente l'esigenza di fornire in tempi rapidissimi una risposta alle richieste espresse dai clienti. Tutto ciò sta mettendo alla prova la capacità di molte organizzazioni di effettuare test di sicurezza approfondita prima della distribuzione dell'applicazione.

Gli attacchi provenienti dal Web, il malware, il Denial of Service sono tutti ambiti in cui è sacrosanto preoccuparsi ma non sono gli unici. Infatti, nonostante tutti gli analisti concordino sul fatto che la maggior parte degli attacchi avviene attraverso lo strato software perché è qui che si trovano le maggiori vulnerabilità, la sicurezza applicativa continua a essere uno dei componenti più trascurati nelle strategie di protezione.

Non solo quelle sviluppate in casa, ma anche le applicazioni commerciali sono troppo spesso erroneamente considerate sicure a priori. Purtroppo, a volte per superficialità a volte per oggettiva difficoltà, i produttori di software non hanno la possibilità o il tempo di eseguire

tutte le prove e i test necessari, in un contesto globale in cui i dettami del time-to-market la fanno da padroni e dove non sempre le aziende hanno a disposizione le risorse o le competenze per effettuare esaustive attività di test.

La sicurezza delle applicazioni richiede innanzitutto di preoccuparsi della loro affidabilità intrinseca prima del rilascio.

Certamente prevedere un controllo efficace a monte di ogni rilascio è il sistema in prospettiva che riduce al minimo i rischi per l'utilizzatore e i costi per lo sviluppatore.

Nonostante la maggior parte degli attacchi avvenga attraverso lo strato software, la sicurezza applicativa continua a essere trascurata

Gli strumenti software per svolgere questi compiti esistono ma richiedono competenza (e quindi costi) e un corretto inserimento all'interno del processo di gestione. A essere più penalizzate sono solitamente le software house più piccole oppure in casa le proprie applicazioni con un approccio talvolta eccessivamente superficiale.

Inoltre, troppo spesso quando si commissiona all'esterno lo sviluppo applicativo, si tende a valutare solo l'aspetto funzionale della soluzione, senza un controllo sugli

standard di sicurezza adottati. Lo stesso può accadere per le applicazioni usufruite in modalità as-a-service di cui si sa poco nulla in relazione agli standard di sicurezza.

Il risultato è di inserire all'interno del proprio sistema informativo delle componenti il cui livello di sicurezza è inferiore a quello previsto dalle policy aziendali, abbassando di conseguenza il livello di sicurezza dell'interno ambiente IT.

Il problema delle patch

Un ulteriore elemento caratteristico della sicurezza applicativa è quello legato alle patch, che dovrebbero garantire la protezione nel tempo di un'applicazione rispetto a minacce che, al tempo del suo rilascio, non erano magari neppure concepibili oppure che sono state rese possibili dall'evoluzione tecnologica degli strumenti a disposizione degli hacker, ma che troppo spesso correggono anche difetti di programmazione che avrebbero potuto essere eliminati alla fonte.

Purtroppo il numero di patch è diventato talmente elevato che la sua gestione è diventata essa stessa una vulnerabilità.

L'avviso della disponibilità di una patch è, infatti, utile per proteggere l'azienda se questa viene applicata in tempo reale ma, nello stesso tempo, contribuisce a diffondere la conoscenza sull'esistenza della vulnerabilità stessa e sui modi per sfruttarla. *

La security intelligence di IBM

Un approccio strategico che punta a consentire alle organizzazioni di prendere decisioni più accurate, permettendo di elaborare più informazioni, in modo più efficiente, nell'intera infrastruttura IT

L'impegno di IBM per la sicurezza è attuato attraverso due divisioni indipendenti: IBM Security Systems e IBM Security Services. La prima focalizzata sullo sviluppo e vendita di prodotti e soluzioni, la seconda concentrata sull'offerta di servizi, gestiti e non, anche in cloud e non necessariamente vincolati all'utilizzo di prodotti IBM, ma aperti anche alla gestione di soluzioni di terze parti.

Un doppio binario che concretizza un approccio alla sicurezza a 360 gradi, ben sintetizzato dall'**IBM Security Framework**, che evidenzia la protezione di dati, applicazioni, persone e infrastrutture. Un approccio che attinge valore dalla combinazione di sforzi in ricerca e sviluppo, a partire da quello realizzato dal team X-Force, e nel delivery ai clienti, attraverso i dieci security operation center e le modalità cloud.

Un approccio, infine, che comprende soluzioni studiate per la sicurezza negli ambiti tecnologici più innovativi, quali i Big Data, il cloud e la mobility, abilitando nuovi e vantaggiosi processi e modelli di business.

Per poter realizzare questo modello di sicurezza IBM, oltre a un'integrazione con le soluzioni di system management, prevede l'applicazione di soluzioni analitiche che consentono una più efficace correlazione tra gli eventi della sicurezza e una più accurata prevenzione, grazie all'analisi predittiva. È anche su questo che si basa il concetto di security

intelligence, che consente alle organizzazioni di usare tool integrati su un framework comune e di sfruttare un insieme di dati unificati per affrontare i problemi sull'intero spettro della sicurezza. Uno dei più importanti "casi d'uso" nei quali la security intelligence si dimostra di particolare valore è il consolidamento dei silos di dati, dove si comprende come, anche grazie agli analytics, sia possibile combattere le minacce in maniera più integrata ed efficace. Componente centrale del modello di sicurezza intelligente di IBM è la **QRadar Security Intelligence Platform** (derivante dall'acquisizione di Q1 Labs), che fornisce una serie integrata di soluzioni, progettate per aiutare le imprese a implementare una security intelligence totale, basata su un sistema operativo unificato e gestita attraverso una

singola console. Supportato da un sistema di SIEM, QRadar integra una serie di applicazioni per la sicurezza e il monitoraggio della rete in una soluzione unificata, che consente di implementare risorse per la sicurezza e l'attività operativa di rete sulla base di un'analisi di un insieme completo di fonti di dati.

IBM è anche impegnata nella **Cloud Security** da tre punti di vista.

IBM Security Systems mette a disposizione soluzioni per la protezione delle infrastrutture e delle applicazioni a chi fornisce servizi cloud e alle imprese che realizzano cloud privati. Il secondo aspetto riguarda le soluzioni stesse di IBM Security Systems, che sono a disposizione di Managed Service Provider interessati a offrire in cloud servizi di sicurezza. Infine, il terzo punto di vista è quello della divisione IBM

Security Service, che, attraverso i propri dieci SOC (Security Operation Center) nel mondo, fornisce servizi gestiti di sicurezza in cloud.

IBM Security ha anche sviluppato soluzioni di classe enterprise che indirizzano gli aspetti dei rischi legati al mobile. Questo comprende rendere sicuri i dispositivi, proteggere l'accesso alle risorse aziendali e abilitare la realizzazione e l'utilizzo di applicazioni mobili sicure. *



IBM Information Security Framework

La sicurezza multilivello di HP ESP

Per rispondere alle nuove esigenze di protezione HP ha messo a punto una strategia per la gestione del rischio che prevede interventi sia sul versante della protezione richiesta dalle aziende, sia per garantire agli utenti un accesso sicuro alle corrette risorse aziendali, ponendo le basi per un approccio unificato alla sicurezza

Attraverso la divisione Enterprise Security Products, HP fornisce soluzioni di sicurezza e di compliance per le imprese, promuovendo l'adozione di una metodologia end-to-end come modo migliore per una difesa efficace.

La piattaforma HP di Security Intelligence e Risk Management mette a disposizione i sistemi di nuova generazione HP TippingPoint firewall (NGFW) e per la prevenzione delle intrusioni (NGIPS), le soluzioni software per la protezione dei dati ArcSight, la famiglia Fortify per la sicurezza dello sviluppo applicativo e Atalla per garantire transazioni sicure, in un contesto di integrazione che coinvolge servizi, applicazioni e prodotti.

Questa gamma di soluzioni segue un processo evolutivo che prevede sia la trasformazione e il miglioramento continuo di ciascuna tecnologia verticale, sia un'integrazione sempre più spinta delle diverse funzionalità al fine di sfruttare al massimo la sinergia di strumenti che affrontano su piani diversi il tema della protezione, migliorando la gestione e incrementando il livello di intelligenza necessario a fronteggiare le nuove minacce che operano in modo sempre più stratificato.

Le soluzioni di sicurezza di HP sono rese disponibili in diverse modalità, per favorire le differenti esigenze aziendali, per esempio prevedendo suite integrate e servizi erogati via cloud in modalità on-demand.

Alle soluzioni tecnologiche HP affianca una rete di servizi tra le più estese al mondo e il valore aggiunto offerto dalla possibilità di avvalersi di prestigiosi laboratori di ricerca specializzati.

Questi includono HP Security Research, la struttura che conduce ricerche e fornisce servizi di intelligence per l'intero portafoglio di soluzioni HP ESP, e HP DV Labs, il team di ricerca per la scoperta del-

le vulnerabilità nel settore della sicurezza, che trasferisce tutte le sue scoperte ai produttori di software interessati per favorirli nella creazione di patch e che provvede a creare i filtri di protezione utilizzati sui sistemi HP TippingPoint Next Generation Firewall/IPS.

I DV Labs forniscono anche il servizio HP Reputation Digital Vaccine (RepDV) basato sull'analisi incrociata di milioni di data stream raccolti giornalmente dalla rete mondiale di sensori TippingPoint Lighthouse Network, che permette di effettuare operazioni di blocco dell'accesso o di monitoraggio in base al valore di un indicatore di reputazione o di rischio e alla localizzazione geografica.

DV Labs gestisce anche il programma pubblico di ricerca Zero-Day Initiative (ZDI), che premia i ricercatori di tutto il mondo in modo che individuino nuove vulnerabilità.*



Le soluzioni che compongono la piattaforma di Security Intelligence e Risk Management di HP Enterprise Security Products

HP Fortify per lo sviluppo di codice sicuro

HP Fortify è la piattaforma HP Hadatta a effettuare test di sicurezza del codice di tipo statico, dinamico e in tempo reale.

HP Fortify predispone un approccio proattivo di Software Security Assurance per affrontare in modo sistematico il rischio di vulnerabilità nel software sulla base del principio che è più efficace e conveniente proteggere le applicazioni mentre sono in fase di sviluppo che farlo dopo che sono state rilasciate.

HP Fortify Software Security Center è una suite di soluzioni altamente integrate pensata per automatizzare e gestire la sicurezza applicativa e prevenire le vulnerabilità di sicurezza all'interno delle applicazioni.

HP Fortify Software Security Center consente di testare la sicurezza delle applicazioni e di identificare le vulnerabilità sia in modalità on-premises sia on-demand.

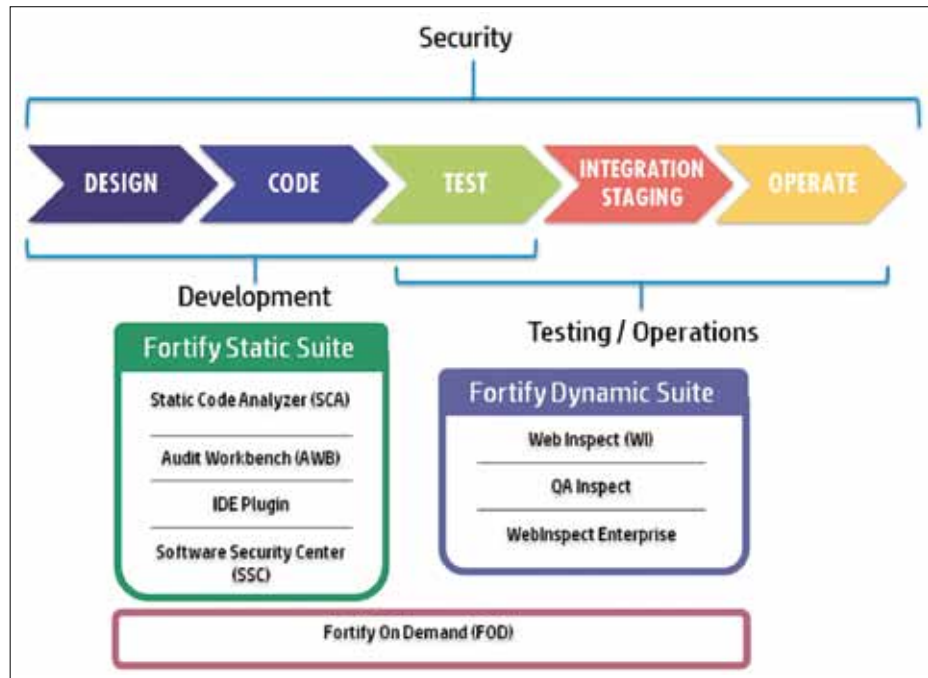
Questa suite svolge due attività fondamentali a supporto della gestione di sicurezza del software.

La prima è di mettere a disposizione funzioni di test di sicurezza per identificare

le vulnerabilità lungo il ciclo di vita

di un'applicazione, sia sviluppata internamente sia esternamente, attraverso tecnologie di test statico, dinamico e di analisi ibrida (statico-dinamica)

HP Fortify è una gamma di strumenti pensati per favorire uno sviluppo sicuro e per predisporre ambienti di test adatti a verificare la sicurezza del software



Gli ambiti d'intervento dei componenti della famiglia HP Fortify

in tempo reale.

La seconda attività riguarda l'analisi del ciclo di vita del processo di sviluppo attraverso funzioni di automazione di gestione, tracciamento, correzione e governance del rischio associato al software enterprise.

Analisi statica e dinamica

HP Fortify Static Code Analyzer (SCA) è la tecnologia sviluppata da HP per valutare il livello di sicurezza del software e rendere sicuro il codice legacy mentre questo viene sviluppato.

Questa tecnica analizza ogni percorso che l'esecuzione e i dati possono seguire per

identificare ed eliminare le vulnerabilità di sicurezza nel codice sorgente.

La soluzione proposta da HP utilizza diversi algoritmi e una base di conoscenza estesa di regole di codifica sicure per analizzare il codice sorgente di un'applicazione alla ricerca di vulnerabilità che potrebbero essere sfruttate in applicazioni distribuite. Fortify SCA ha la capacità di rilevare più di 500 tipi di vulnerabilità in 21 linguaggi di sviluppo e più di 700mila componenti a livello di API.

HP WebInspect è uno strumento automatizzato e configurabile che effettua test dinamici sulla sicurezza delle applicazioni Web e test di penetrazione. Imita le tecniche di hacking e gli attacchi, consentendo di analizzare a fondo le applicazioni e i servizi Web per individuare possibili vulnerabilità di sicurezza. *

HP Fortify on Demand: la sicurezza applicativa come servizio cloud on-demand

HP Fortify on Demand (FoD) è il servizio di tipo Software-as-a-Service di analisi del codice che consente alle aziende di testare la sicurezza del software in modo rapido e accurato, senza richiedere l'acquisto di hardware o l'installazione di software.

HP FoD è disponibile per **assessment sia statici sia dinamici** e con diverse opzioni all'interno di ciascuna di queste categorie. Fortify on Demand non richiede l'acquisto di alcun hardware né l'installazione di alcun software: è sufficiente caricare il codice e scegliere il tipo di test che si desidera effettuare per ottenere un report dettagliato. È possibile acquistare singole valutazioni o un abbonamento di un anno per valutazioni illimitate di una particolare applicazione. È possibile caricare i file e avviare una valutazione statica del codice oppure, se è stata acquistata una valutazione dinamica, è possibile verificare la URL. Questo servizio supporta Web, mobile e applicazioni thick-client sia sviluppati internamente sia da organizzazioni di terze parti.

HP Fortify on Demand estende i test anche alle **applicazioni mobili** prendendo in considerazione i tre livelli che costituiscono lo stack tecnologico: client, rete e server. Il servizio permette di comprendere dove vengono richiesti i dati sensibili, come si spostano attraverso l'applicazione, come sono utilizzati e così via.

HP FoD fornisce anche un servizio per effettuare i test delle applicazioni Web in produzione senza causare interruzioni dell'attività.

HP ArcSight: la piattaforma per la protezione dei dati

HP ha raggruppato all'interno della famiglia ArcSight le soluzioni software indirizzate a proteggere i dati attraverso il monitoraggio, l'analisi e la correlazione di eventi di sicurezza provenienti da differenti tipologie di sorgenti.

HP ArcSight è una piattaforma integrata di **Security Intelligence e Risk Management** in grado di abbinare le funzionalità di un sistema di gestione delle informazioni e degli eventi di sicurezza (SIEM) con un approccio preventivo basato su un modello di analisi intelligente delle minacce, effettuato su scala globale attraverso una serie di servizi predisposti da HP.

Questa piattaforma fornisce visibilità sulle attività che interessano l'intera infrastruttura enterprise correlando log, ruoli dell'utente e flussi di rete per individuare eventi legati alla sicurezza in base ai quali definire priorità e predisporre risposte efficaci e preventive a minacce di vario tipo.

HP ArcSight Enterprise Security Manager (ESM)

HP ArcSight ESM rappresenta l'elemento centrale e abilitante di questa famiglia di soluzioni. Si tratta di una **soluzione SIEM** per la raccolta, l'analisi e la correlazione delle informazioni di sicurezza e degli eventi di rischio, la protezione delle applicazioni e la difesa della rete e per il Governance, Risk management and Compliance (GRC).

HP ArcSight ESM è in grado di effettuare analisi capaci di correlare:

- minacce esterne come malware e attacchi di hacker;
- minacce interne come le violazioni di dati e le frodi;
- rischi derivanti da flussi applicativi,
- modifiche della configurazione;
- problemi di conformità che scaturiscono dal mancato superamento dei controlli.

HP ArcSight ESM automatizza le operazioni di ricerca e analisi su Big Data di informazioni, la produzione di report per la compliance e raccoglie dati di business intelligence. Il fulcro tecnologico di questa soluzione è costituito dalla quinta generazione (con prestazioni fino

HP ArcSight Command Center



a 30 volte superiori rispetto alla versione precedente) del motore di correlazione **Correlation Optimized Retention and Retrieval Engine (CORR-Engine)** che permette di scattare nel livello di risposta, in funzione della minaccia che ci si trova a dover affrontare.

L'integrazione con il file system di **Hadoop (HDFS - Hadoop Distributed File System)** consente di sfruttare il CORR-Engine per effettuare funzioni avanzate di analytics in tempo reale oppure di inviare ad alta velocità ad Hadoop i log normalizzati dal CORR-Engine per una lettura da HDFS (per esempio per operazioni di batch analytics).

HP ArcSight utilizza anche il motore **HP Reputation Security Monitor** che permette di analizzare in tempo reale gli indirizzi IP e i DNS potenzialmente dannosi, al fine di contrastare gli attacchi che sfruttano le vulnerabilità delle applicazioni Web.

L'interfaccia **HP ArcSight Command Center** riunisce funzionalità amministrative e di reportistica Web-based con funzioni di configurazione, distribuzione, analisi dei log e gestione delle modifiche, attraverso un'impostazione basata su cruscotti altamente personalizzabili. Anche le applicazioni di terze parti possono essere integrate direttamente all'interno del front end Web di HP ArcSight ESM.

HP ArcSight Application View

HP ArcSight Application View consente di controllare automaticamente le applicazioni per fornire

HP Reputation Security Monitor (RepSM)

Si tratta di uno strumento di Threat Intelligence basato su un livello di reputazione che viene definito sulla base di dati provenienti dalla comunità di sicurezza globale e di rilevazioni effettuate da HP.

RepSM fornisce un ulteriore livello di intelligenza al SIEM per operazioni di correlazione in tempo reale, abilitando una reazione attiva in risposta alle attività dannose e stabilendo il livello di priorità con cui fronteggiare attività sospette.

In tal modo fornisce un utile sistema per identificare le APT, che risultano spesso non individuate dai controlli di sicurezza basati su signature e, più in generale, abilita operazioni di sicurezza in risposta ad attacchi sconosciuti con azioni manuali o automatiche.

L'utilizzo di RepSM abbinato ad ArcSight Application View permette di avere visibilità sul comportamento di un malintenzionato all'interno di un'applicazione e di controllare, per esempio, se effettua connessioni esterne e se queste sono verso un sito o un IP da considerare pericolosi.

un'analisi intelligente sulle minacce, combinando i log degli eventi di sicurezza generati dalle diverse applicazioni, incluse quelle legacy o personalizzate che, in molti casi, non sono state progettate per fornire capacità di registrazione dei log.

HP ArcSight Application View fornisce funzionalità di registrazione dei log senza la necessità di alcuna personalizzazione e mette i dati raccolti a disposizione di HP ArcSight ESM, integrandoli nei suoi dashboard e report.

Questa soluzione fornisce una capacità di monitoraggio delle applicazioni (**Java, .NET e Cold Fusion**) sensibile al contesto e può essere utilizzata per contribuire a colmare le lacune di sicurezza legate alle modalità di accesso degli utenti o a un utilizzo improprio delle applicazioni: per esempio, distingue tra l'accesso di un utente autorizzato a un'applicazione durante il normale orario di lavoro e il suo accesso ripetuto di sabato a mezzanotte.

Rappresenta anche una soluzione complementare al software HP ArcSight

Identity View focalizzato sul monitoraggio dell'identità degli utenti e pensato per proteggere le aziende enterprise da possibili minacce interne a cui, di fatto, può mettere a disposizione ulteriori dati legati alla sicurezza.

Inoltre, consente di correlare le informazioni sugli eventi legati alle applicazioni con quelle associate ai sistemi IDS/IPS: per esempio gli attacchi intercettati dai sistemi IDS/IPS possono essere correlati a uno specifico login alla applicazione, per conseguire una migliore visibilità su ciò che l'attaccante sta cercando di ottenere.

HP ArcSight Threat Response Manager

HP ArcSight Threat Response Manager (TRM) che mette a disposizione funzionalità cloud-ready per accelerare il rilevamento delle minacce e le azioni di risposta alle APT.

Rilasciato come un add-on cloud-ready per la piattaforma HP ArcSight di Security Information and Event Management (SIEM), ArcSight TRM è una soluzione end-to-end di sicurezza di rete e monitoraggio che ac-

celera il rilevamento delle minacce e automatizza l'intero processo di risposta.

Questa soluzione consente di gestire ed elaborare ad alta velocità le informazioni di sicurezza, analizzare i dati (strutturati e non strutturati), monitorare gli eventi e predisporre azioni automatiche una volta che una minaccia è stata rilevata. In caso di rilevamento, prima che il personale di sicurezza provveda a disattivare manualmente l'account, ArcSight TRM interviene per interrompere immediatamente l'accesso. *

HP ArcSight Risk Insight

HP ArcSight Risk Insight è una delle soluzioni software aggiunte più recentemente da HP al suo portafoglio d'offerta.

Abilita, tramite ArcSight ESM, funzioni di analisi del rischio e di impatto sul business, fornendo:

- una mappa del rischio dei servizi di business;
- una mappatura degli asset che estende il modello di ArcSight ESM;
- una serie di indicatori di rischio capaci di aggregare molteplici fonti;
- funzioni per l'analisi di conformità dei processi di business.



Mappa degli asset in HP ArcSight Risk Insight

HP TippingPoint Next Generation Firewall e IPS

I dispositivi della gamma HP TippingPoint di nuova generazione forniscono il livello di visibilità necessario a riconoscere quali applicazioni stanno girando sulla rete aziendale e chi sta accedendo a tali applicazioni per poi consentire di predisporre le policy richieste per bloccare e controllare le applicazioni non richieste. Questo livello di visibilità e controllo consente alle organizzazioni di restringere l'accesso generale di certi dipendenti alle applicazioni di trasferimento dei file nel cloud, qualora sussista il rischio che la proprietà intellettuale possa essere memorizzata in contrasto alle policy aziendali.

Per fronteggiare i rischi legati alla mobilità i Next Generation Firewall e Intrusion Prevention System (IPS) di HP abilitano il blocco automatico del codice nascosto o dannoso che può introdursi in rete, ricorrendo a capacità di blocco delle vie d'uscita in modo da evitare la fuoriuscita di dati sensibili verso destinazioni "command-and-control". Per rispondere ai rischi introdotti dal BYOD gli utenti delle soluzioni HP TippingPoint han-

no a disposizione controlli sulle

policy delle applicazioni a livello granulare, che consentono anche di gestire l'interazione con le più diffuse piattaforme social e consumer come Facebook, Google e Twitter.

Tra i punti distintivi di queste soluzioni vi è anche la semplicità d'uso che le rende adatte anche alle organizzazioni prive di personale specializzato. L'installazione e il rilascio in produzione può avvenire, secondo HP, in meno di un'ora e mettendo a disposizione una singola interfaccia di gestione in grado di condividere la configurazione delle policy per la sicurezza di rete.

L'affidabilità è un altro aspetto su cui HP intende rimarcare il valore dei propri dispositivi mentre, per quanto riguarda l'efficacia della propria tecnologia di protezione nel bloccare possibili minacce, HP mette sul piatto l'attività del team di ricerca DVlabs che ha pubblicato a oggi oltre 7.400 filtri e che è costantemente impegnato in operazioni per arrestare gli exploit e bloccare gli attacchi.

Tutti i modelli NGFW dispongono di una porta di rete RJ-45 10/100/1000 per la gestione out-of-band oppure possono essere gestiti in modalità in-band tramite porte di rete.

In un contesto di reti senza perimetro, minacce persistenti e utenti remoti, gli NGFW/NGIPS rappresentano soluzioni versatili per esercitare una protezione che non impatta su processi e infrastruttura

Inoltre è presente una porta seriale RJ-45 per la console.

L'appliance HP TippingPoint SMS mette a disposizione un sistema di management centralizzato per la condivisione di configurazioni e policy di sicurezza della rete attraverso i firewall e i sistemi IPS di nuova generazione.

Le soluzioni HP TippingPoint NGIPS individuano le nuove vulnerabilità presenti sulla rete e intervengono applicando delle "patch" virtuali che fermano sul nascere la diffu-

HP TippingPoint NGFW S1050F

È la soluzione entry level adatta per le implementazioni di rete delle filiali.

Si tratta di un dispositivo da rack di dimensioni 1U che supporta un throughput fino a 500 Mbps in modalità solo firewall, che lo rende adatto a supportare fino a 250mila connessioni simultanee e fino a 10mila nuove connessioni per secondo; se utilizzato in modalità Firewall+IPS+Application control il throughput massimo suggerito è di 250 Mbps.

I valori di latenza tipici di questo dispositivo nella modalità d'utilizzo Firewall+IPS sono inferiori a 600 microsecondi. Il throughput a disposizione per la realizzazione di VPN IPsec è di 250 Mbps con la possibilità di creare fino a 1250 tunnel VPN.

Il firewall S1050F dispone di 8 GB di storage integrato su memoria Flash CFast rimovibile. La connettività di rete prevede otto porte RJ-45 10/100/1000 più 1 porta 10/100/1000 per l'alta disponibilità.



HP TippingPoint Next-Generation Firewall S1050F

sione di traffico dannoso. Di fatto, i sistemi IPS di HP ottimizzano le prestazioni del traffico legittimo effettuando una continua pulizia della rete e assegnando la massima

HP TippingPoint NGFW S3010F/S3020F

I Next Generation Firewall S3010F/S3020F sono apparati di dimensioni 2U indicati per le implementazioni di rete di campus e filiali, essendo adatti per un numero di connessioni simultanee rispettivamente di 500mila e 1 milione.

La capacità storage in dotazione è di 8 GB, mediante memoria Flash CFast rimovibile.

La connettività di rete prevede 8 porte 10/100/1000 e 8 porte 1 Gbps SFP rame/fibra a cui si aggiunge 1 porta 10/100/1000 per l'alta disponibilità.

Il tempo di latenza tipico in modalità Firewall+IPS è inferiore a 120 microsecondi e possono essere stabilite fino a 500mila (S3010F) o un milione (S3020F) di sessioni contemporanee.

Il modello 3010F mette a disposizione un throughput di 500 Mbps in modalità Firewall+IPS+Application control che sale a 1 Gbps quando utilizzato in modalità di solo Firewall. Una banda di 500 Mbps a disposizione per le VPN IPsec. Il modello S3020F raddoppia il throughput arrivando a 2 Gbps in modalità solo Firewall e 1 Gbps quando opera come Firewall+IPS+Application control.



HP TippingPoint Next-Generation Firewall S3010F/S3020F

HP TippingPoint NGFW S8005F/S8010F

Al top della gamma si collocano i due modelli S8005F e S8010F di dimensioni 2U adatti per 10 e 20 milioni di connessioni simultanee.

Si tratta di apparati indicati per le implementazioni di rete dei data center che dispongono di 32 GB di storage integrato su memoria Flash CFast rimovibile.

La connettività di rete prevede 8 porte 10/100/1000, 8 porte 1 Gbps SFP rame/fibra, 4 porte 10 Gbps SFP rame/fibra e 2 porte 10/100/1000 per l'alta disponibilità.

Il tempo di latenza tipico in modalità Firewall+IPS è inferiore a 120 microsecondi e possono essere stabilite fino a 50mila nuove connessioni al secondo.

A livello di prestazioni il modello S8005F mette a disposizione un throughput di 5 Gbps in modalità solo Firewall o di 2,5 Gbps in modalità Firewall+IPS+Application control e 1,5 Gbps per le VPN IPsec; questi numeri raddoppiano sul modello S8010F.



HP TippingPoint Next-Generation Firewall S8005F/S8010F

priorità alle applicazioni mission critical.

Queste soluzioni dispongono anche di funzioni di elevata disponibilità e ridondanza e sono caratterizzate da una latenza tipica di pochi microsecondi, per proteggere dispositivi di rete, software di virtualizzazione, sistemi operativi e applicazioni da attacchi senza impattare sulle prestazioni. *

La protezione estesa di Fortinet

Le innovazioni software del produttore combattono le minacce avanzate e accelerano le prestazioni, per una sicurezza integrata che abilita il cloud

Con la release 5.2 del sistema "operativo" per la sicurezza FortiOS, Fortinet migliora le prestazioni e aggiunge funzionalità per combattere le APT (Advanced Persistent Threat). In particolare, viene abilitato l'Advanced Threat Protection Framework, che non è un prodotto, come ci spiega Antonio Madoglio, System Engineer Manager di Fortinet: «Si tratta di una soluzione, che parte dal controllo degli accessi e comprende la prevenzione delle minacce e il loro rilevamento, la risposta agli incidenti e il monitoraggio continuo in un ciclo virtuoso».

Tale soluzione risponde all'evoluzione delle minacce APT, che prevedono diverse fasi di attacco con utilizzo di tecniche miste.

È dunque necessaria una protezione multilivello, che parta dal controllo degli accessi, attuato con le funzionalità di firewalling, l'autenticazione a due fattori e il vulnerability management.

Segue poi la prevenzione delle minacce, realizzata con le capacità di Web filtering, IPS, application control, deep flow antimalware e antibot. Con la funzionalità e i servizi di sandboxing in cloud, client reputation e botnet reporting, invece, vengono aumentate le possibilità di rileva-

mento delle minacce. Oltre le barriere, il framework prevede una fase di incident response, attuata con i FortiGuard Service, la messa in quarantena dei dispositivi e il servizio di FortiGuard Update.

Conclude il ciclo il monitoraggio continuo realizzato con le soluzioni di reportistica, la ricerca dei laboratori FortiGuard e le soluzioni SIEM (Security Information Event Management), di log management e intelligence service dei partner di Fortinet.

Fondamentale è la funzione della sandbox. Quest'ultima permette di verificare che un codice sospetto non nasconda del malware. Per questo viene effettuata una simulazione del suo funzionamento in un'area isolata e protetta. Con la 5.2 vengono aggiunte tecniche antievasive e aumentate le capacità di protezione attraverso la condivisione delle informazioni su scala globale.

Un'altra novità importante introdotta nella nuova versione del software riguarda la capacità di analizzare ad alta velocità il traffico crittografato: «Abbiamo moltiplica-

to per 5 le prestazioni nell'analisi del protocollo SSL. Se questo tipo di analisi diventasse un collo di bottiglia finirebbe con l'essere disattivata», spiega Joe Sarno, Regional Vice President EMEA EAST di Fortinet, che sottolinea: «I rischi sono elevati, perché con l'uso del cloud il traffico criptato è aumentato del 50%».

A questo annuncio si aggiunge quello, pure importante, del nuovo Fortigate 1500D che aumenta particolarmente le prestazioni, beneficiando delle caratteristiche fornite dalla nuova generazione, la sesta, dei network processor Fortinet, abilitando così la network security platform che integra anche funzionalità di networking.

Secondo i dati forniti dal produttore, FortiGate-1500D raggiunge un throughput del firewalling di 80 Gbps, mentre per intrusion prevention e controllo applicativo arriva a 11 Gbps, con una latenza fino a 3 microsecondi.

L'accelerazione garantita dai processori dedicati si può apprezzare, come sottolinea Madoglio, anche nella parità di prestazioni nelle analisi con Ipv4 e Ipv6, anche quest'ultimo, infatti, viene elaborato via hardware.

Da segnalare la connettività ad alta velocità fornita da 8 porte 10 GigaEthernet (SFP+) e 32 porte GigaEthernet comprese nel formato rack 2U, adatta a soddisfare le nuove esigenze di rete. *

Il Framework per l'Advanced Threat Protection di Fortinet



La sicurezza unificata di Websense

La popolarità degli strumenti di collaborazione basati su Web, gli applicativi Internet sempre più complessi, i social network e la presenza di applicazioni software-as-a-service hanno contribuito all'aumento delle minacce miste, sempre più mirate, avanzate e persistenti, rappresentando un'enorme sfida per le aziende a causa dell'aumento delle possibilità di perdita di dati e dei rischi per la sicurezza. Per far fronte alle minacce e agevolare l'utilizzo delle potenzialità delle nuove tecnologie in un contesto di costanti tagli al bilancio, le organizzazioni devono cambiare il modo in cui proteggono i contenuti che creano, utilizzano e comunicano, per offrire una migliore protezione al minore costo di gestione.

Websense si propone di aiutare le aziende a risolvere queste sfide legate alla sicurezza, a prevenire gli attacchi e favorire la collaborazione, la comunicazione e la condivisione delle informazioni.

Per realizzare questi obiettivi ha sviluppato la soluzione **Websense Triton**, per la protezione unificata di Web, posta elettronica e prevenzione dalla perdita dei dati.

Triton interviene su tre fronti:

- **Analisi unificata dei contenuti** che comprende l'analisi delle minacce in tempo reale eseguita da Websense Advanced Classification Engine (ACE). ACE è inoltre supportato da Websense ThreatSeeker Network, una rete globale che analizza le minacce potenziali alla

Una protezione basata sull'architettura Triton permette di fronteggiare minacce note e sconosciute, coprendo tutte le fasi degli attacchi APT (Advanced Persistent Threat)

sicurezza attraverso l'uso di tecniche di analisi avanzate in tempo reale, basate sulla reputazione e sul comportamento. Questa rete invia ad ACE i nuovi dati raccolti sulla sicurezza per classificare in modo dinamico il contenuto in ingresso e in uscita.

- **Gestione unificata** per ottenere la visibilità di tutti gli eventi relativi alla sicurezza di Web, e-mail e dati e impostare policy granulari per i dati riservati. La console Websense Triton consente di gestire CPU, memoria, servizi di software, messaggi hardware e altri processi attraverso un'interfaccia grafica intuitiva.
- **Piattaforma unificata** che riunisce le prestazioni di un'installazione locale con la flessibilità di un software Cloud, consentendo di applicare le stesse policy, a prescindere dalla configurazione del deployment: appliance, cloud o ibrida.

L'architettura unificata Websense Triton fornisce una protezione continua contro potenziali minacce facendo affidamento sulle tecnologie: **Websense ThreatSeeker Intelligence Cloud**, che comprende classificazioni di sicurezza assegnate prima di autorizzare il passaggio di una richiesta; **Websense ACE**, con

difese online in tempo reale e controlli DLP implementati durante una procedura di richiesta; **Websense ThreatScope**, per il sandboxing con analisi del malware che può essere utilizzato dopo una richiesta per rilevare eventuali minacce e comunicazioni sconosciute.

Grazie all'architettura unificata e all'integrazione delle soluzioni, Websense è in grado di controbattere tutte le fasi di un attacco APT (Advanced Persistent Threat): ricognizione, adescamento, dirottamento, exploit, installazione, call back. Inoltre, Websense dispone della soluzione di monitoraggio **Triton RiskVision**, che unisce la Data Loss Prevention a una tecnologia di sandboxing multi-layer, per fornire funzionalità di identificazione delle minacce più avanzate e andando oltre la semplice identificazione del malware attraverso analisi euristiche e di comportamento.

Scalabile attraverso le piattaforme e le infrastrutture di rete esistenti, Triton RiskVision unisce in un'unica appliance difese APT (Advanced Persistent Threat) in tempo reale, intelligence globale di sicurezza, file sandboxing e rilevazione data loss/data theft, secondo quanto sostenuto dai responsabili di Websense. *

Le fasi di un attacco APT



La Content Security di Trend Micro per rispondere alle nuove minacce

L'azienda giapponese risponde alle nuove sfide con un'ampia gamma di prodotti per proteggere i dati ovunque questi risiedano, in ambienti fisici, virtuali, mobili o cloud

Trend Micro si è posta, in anticipo sui tempi, molte questioni legate alle nuove sfide tecnologiche e dei nuovi modelli di archiviazione, accesso e distribuzione delle informazioni per arrivare a proporre un modello di sicurezza basato su un framework unificato per la gestione e la protezione di dati, infrastrutture, applicazioni e dispositivi mobili. L'offerta di sicurezza integra prodotti, servizi e soluzioni per la sicurezza dei contenuti, affrontando due sfide critiche legate alle tempistiche.

La prima è di minimizzare il tempo necessario per **proteggere l'azienda** da minacce nuove e sconosciute, accelerando il periodo necessario per identificare le minacce, sviluppare una protezione e per renderla operativa. La seconda sfida riguarda la necessità di ridurre il tempo per **gestire la sicurezza** adottando una soluzione che sia in grado di minimizzare la complessità oltre che di fornire una protezione efficace.

Per far fronte a entrambi questi requisiti Trend Micro coniuga una protezione immediata capace di "chiudere" le finestre delle vulnerabilità, con una sicurezza integrata che riduce la complessità e minimizza il tempo necessario per acquisire, rilasciare e gestire la sicurezza dei contenuti. Il modello

Trend Micro integra la protezione dei dati estesa attraverso l'intera organizzazione con la sicurezza dalle minacce e dagli attacchi mirati che sfrutta a livello locale le analisi e le correlazioni effettuate su scala globale mediante un'intelligenza distribuita.

Il risultato è una protezione in grado di affrontare il tema della riservatezza e della protezione dei dati in ambienti fisici, virtuali e in-the-cloud. A completare questo quadro per una sicurezza data centrica Trend Micro pone una piattaforma di gestione unificata e basata su policy che coordina in modo sinergico le diverse attività di analisi intelligente. Una caratteristica distintiva dell'approccio di Trend Micro è anche la capacità delle soluzioni di sicurezza di essere consapevoli del contesto per capire chi accede a quali dati, come (tramite e-mail, Instant Messaging, USB e così via), quando (consapevolezza temporale) e dove (consapevolezza geografica).

Il vendor promuove anche una dife-

sa di tipo personalizzato basata su un modello ciclico organizzato in quattro fasi:

- **Rilevamento:** il primo step prevede di identificare gli attacchi con tecniche avanzate di rilevazione sulla rete e la protezione dei punti chiave come il gateway e-mail.
- **Analisi:** vengono quindi valutate le minacce utilizzando analisi "sandbox" specifiche per ogni azienda e l'accesso integrato a un meccanismo di intelligenza globale (Smart Protection Network).
- **Adattamento:** per bloccare ulteriori attacchi con black list e firme personalizzate che vengono rilasciate verso la rete, i gateway e gli endpoint.
- **Risposta:** utilizzando profili di attacco e analisi intelligente degli eventi che avvengono su tutta la rete, per consentire un contenimento e attività di bonifica

La Smart Protection Network

Alla base del suo approccio verso la sicurezza Trend Micro pone la Smart Protection Network, un'infrastruttura per la protezione automatizzata degli ambienti fisici, mobili, virtuali e cloud progettata per tutelare gli utenti dalle minacce a fronte di un impatto ridotto su reti e sistemi. Abbinando tecnologie "in-the-cloud" a client leggeri, diventa possibile accedere alle più recenti misure di protezione ovunque e in qualsiasi modo ci si connetta: da casa, dalla rete aziendale o anche in viaggio.



Smart Protection Network

**Smart Protection Network
 analizza oltre 100mila eventi
 al secondo e blocca più di 30
 milioni di attacchi Web al
 giorno**

Trend Micro Smart Protection Network sfrutta un approccio di difesa intelligente basato sulle conoscenze collettive ottenute dell'ampio e globale bacino dei clienti Trend Micro, mettendo in relazione i dati provenienti da oltre 70 miliardi di query giornaliera.

Smart Protection Network prevede l'assegnazione di reputazione a livello di URL in base a fattori quali l'età del sito Web, le modifiche cronologiche all'ubicazione del sito e le indicazioni di attività sospette scoperte tramite l'analisi del comportamento delle minacce informatiche.

La tecnologia Trend Micro verifica anche la **reputazione** di ciascun file ospitato su un sito Web o allegato a un messaggio e-mail prima di consentire l'accesso all'utente e impedisce di scaricare le App dannose. La tecnologia di reputazione delle App mobili può anche essere integrata dai fornitori di servizi e dagli sviluppatori delle applicazioni per fornire App di migliore qualità e un maggiore livello di protezione agli App store. La Smart Protection Network è integrata nei prodotti e nei servizi Trend Micro fra cui le proposte mobile, endpoint, server, network, messaging, gateway e SaaS destinate sia a un pubblico consumer sia business. Per rispondere alle nuove tipologie di minacce Trend Micro ha anche sviluppato funzioni analitiche in grado di intervenire su Big Data per identificare una gamma più ampia di nuove minacce.

A tale riguardo il vendor ha predisposto anche i **Threat Intelli-**

gence Services, che rispondono alle esigenze di grandi realtà enterprise, pubbliche amministrazioni e partner. Si tratta di un'offerta di servizi che permette di utilizzare l'intelligence della Trend Micro Smart Protection Network per costruire o ottimizzare le infrastrutture di sicurezza, in un'ottica di contrasto alle sottrazioni di dati e altre possibili minacce.

Correlare gli eventi per definire la reputazione di file, URL e App

La capacità di Trend Micro di stabilire il livello di reputazione è basata sull'interazione tra due attività. La prima è la raccolta degli eventi di sicurezza che avviene in tempo reale a livello globale; la seconda è la correlazione di questi eventi, che costituisce uno degli elementi in cui Trend Micro rivendica la propria eccellenza tecnologica e che consente di intervenire in modo accurato e selettivo, garantendo un elevato livello di protezione senza penalizzare in modo inutile l'utente.

La tecnologia di correlazione con l'analisi del comportamento mette in relazione tra loro diversi gruppi di attività per determinare se queste siano o meno dannose. Infatti, un'attività singola prodotta da una minaccia Web potrebbe apparire innocua, ma quando più attività vengono rilevate insieme, è più facile identificare la presenza di una minaccia reale.

Aggiornando continuamente il pro-

prio database delle minacce in base a questo tipo di analisi, Trend Micro abilita una **reazione automatica**

che interviene in tempo reale per proteggere dalle minacce e-mail e Web.

Attraverso cicli integrati di feedback si realizza una comunicazione continua tra i prodotti Trend Micro, le tecnologie e i centri di ricerca delle minacce attivi 24 ore su 24 e 7 giorni su 7. Ogni nuova minaccia identificata tramite una verifica di routine della reputazione di un singolo cliente aggiorna automaticamente tutti i database delle minacce di Trend Micro e blocca ogni successiva interazione del cliente e di tutti i clienti Trend Micro con una specifica minaccia.

Poiché le informazioni raccolte sulle minacce sono basate sulla reputazione dell'origine della comunicazione e non sul contenuto della specifica comunicazione, la riservatezza delle informazioni personali o aziendali resta tutelata.

La Smart Protection Network mette anche a disposizione **white list in-the-cloud** che sfruttano uno dei database più grandi al mondo, per un'identificazione rapida e accurata degli eventi sicuri al fine di minimizzare i falsi positivi. Le soluzioni Trend Micro per la protezione degli endpoint interrogano le white list ogni volta che viene individuato un file sospetto per verificare se sia o meno sicuro. *

Soluzioni per la protezione in ambienti virtualizzati e cloud

Le soluzioni software di Trend Micro rispondono alle nuove esigenze di sicurezza che caratterizzano il progressivo percorso verso la virtualizzazione, che solitamente inizia con il consolidamento server, prosegue con la virtualizzazione estesa per server e desktop, per approdare infine al cloud. Trend Micro punta a favorire il conseguimento di tali obiettivi tramite soluzioni in grado di fornire protezione integrata per differenti tipologie di minacce.

Trend Micro Deep Security per gli ambienti virtualizzati

Trend Micro Deep Security include un ventaglio di differenti tecnologie di sicurezza e anti-malware specializzate e si avvale di funzioni anti-malware di tipo agentless. Sviluppata in stretta collaborazione con VMware, Deep Security è adatta a proteggere i sistemi virtualizzati e supporta VMware vSphere 5.0 e VMware vShield Endpoint 2.0 garantendo compatibilità retroattiva con gli ambienti vSphere 4.1 e supportando anche ambienti a modalità mista. Deep Security si integra con VMware e le sue API vShield Endpoint e VMsafe, fornendo protezione per le Virtual Machine sia agentless sia basata su agent.

Il fatto che Trend Micro Deep Security sia specificamente progettato per gli ambienti virtuali, con una stretta integrazione con le API dell'hypervisor di VMware, un'architettura di sicurezza di tipo agentless e la certificazione EAL4 con-

sente di massimizzare la densità di macchine virtuali all'interno di un sistema fisico senza pregiudicare la sicurezza, favorendo la riduzione dei costi e migliorando il ROI. L'architettura della piattaforma prevede i seguenti componenti:

- **Deep Security Virtual Appliance**, che applica in modo trasparente i criteri di protezione sulle macchine virtuali VMware;
- **Deep Security Agent**, un componente software installato su server fisico o su macchine virtuali non VMware, garantisce il rispetto dei criteri di protezione del data center.
- **Deep Security Manager** per la gestione centralizzata, con possibilità di creare profili di sicurezza e di applicarli ai server, di monitorare gli avvisi e le azioni preventive eseguite in risposta alle minacce, di distribuire gli aggiornamenti della protezione ai server e di generare rapporti su tutto il data center, sia esso fisico che virtuale, qualsiasi sia la piattaforma di virtualizzazione scelta.

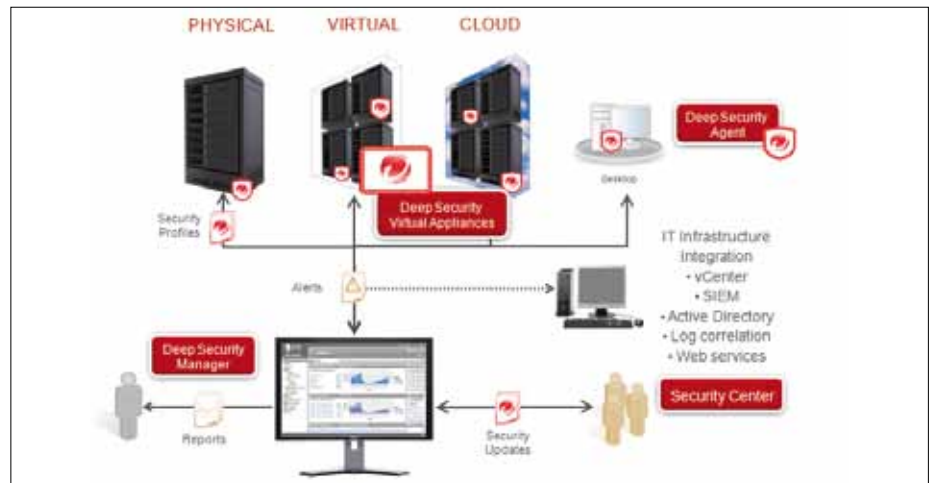
La protezione offerta da Deep Security

si estende all'ambiente cloud sino a comprendere i Cloud Client in modo da estendere il perimetro della protezione e correlando in real time il grado di reputation di siti web, dei file scambiati e delle entità sorgenti delle e-mail. L'architettura risponde anche a precisi aspetti normativi e di conformità e, in particolare, soddisfa quanto previsto, tra gli altri, da standard quali il PCI DSS 2.0, HIPAA, NIST e SAS 70.

Il livello di sicurezza fornito da Deep Security prevede molteplici funzionalità di protezione.

- **Intrusion Detection e Prevention (IDS/IPS)**. Fornisce un'analisi approfondita dei pacchetti per rilevare e bloccare possibili attacchi, analizzando il traffico alla ricerca di anomalie a livello di protocollo, di indicazioni su exploit e di violazioni delle policy di sicurezza.
- **Virtual Patching**. Consente di individuare le vulnerabilità a livello host e suggerisce le regole da applicare per proteggere ap-

Trend Micro Deep Security



- plicazioni e sistemi.
- **Firewall.** Un sistema “stateful” di classe enterprise, che abilita la segmentazione della rete e le operazioni di audit richieste dallo standard PCI.
 - **Protezione delle applicazioni Web.** Protegge le applicazioni Web da attacchi sofisticati come “SQL injection” e “cross-site scripting”.
 - **Protezione antivirus.** Fornisce una protezione malware “agentless” attraverso un’appliance virtuale VMware.
 - **Integrity Monitoring.** Rileva e segnala modifiche potenzialmente nocive e inconsuete relative ai file critici del sistema operativo e delle applicazioni.
 - **Controllo applicativo.** Prevede una serie di regole per fornire visibilità e controllo sulle applicazioni che accedono alla rete.
 - **Analisi del registro e dei log.** Analizza il log del sistema operativo e delle applicazioni per individuare importanti eventi di sicurezza, generare avvisi e fornire informazioni ai sistemi SIEM.
 - **Virtualization Compliance.** Abilita l’isolamento delle virtual machine e funzionalità di “hardening” che proteggono e isolano le applicazioni per l’elaborazione dei pagamenti da altre macchine virtuali presenti sullo stesso hardware. La maggior parte delle funzioni sono disponibili come appliance VMware sia con agent sia in modalità agentless.

Queste caratteristiche, oltre a intervenire per la protezione dei server business-critical e degli endpoint,

Deep Security as a Service

In linea con il paradigma cloud, Trend Micro ha reso disponibile Deep Security anche in modalità as-a-service. L’obiettivo è di proteggere le istanze degli utilizzatori attivate sui server. È un servizio compatibile con i tool di cloud deployment più utilizzati (Chef, Puppet, Rightscale, OpsWorks e così via) che fornisce una istant-on security riconoscendo automaticamente le nuove istanze quando vengono lanciate e che permette di personalizzare specifiche policy in modo che vengano applicate immediatamente e automaticamente ai server dell’ambiente cloud. Quest’offerta di servizi mette a disposizione un ampio portfolio di funzioni di sicurezza che includono: Intrusion detection and prevention, Firewall, Anti-malware, Web reputation e Integrity monitoring. Il servizio mediante la console di controllo centrale, permette di attivare le diverse funzioni in modo da aggiungere in modo elastico la sicurezza ad una specifica istanza di un server virtuale. Amazon ha certificato Deep Security come scanner pre-autorizzato per le Web App su Amazon Web Services, eliminando la necessità di passaggi manuali per l’abilitazione di uno scanner di vulnerabilità e aumentando la sicurezza attraverso l’abilità di scansionare continuamente le applicazioni distribuite e i Web server alla ricerca di vulnerabilità, malware e link pericolosi.

consentono a Deep Security di favorire la conformità allo standard PCI DSS tramite una soluzione unica, gestita centralmente, che risponde a 7 regole PCI e oltre 20 sotto controlli.

Trend Micro SecureCloud

Trend Micro fornisce sicurezza “dal cloud” con l’infrastruttura Trend Micro Smart Protection Network e sicurezza “per il cloud” con server e tecnologie crittografiche.

Per la protezione multilivello per i dati che risiedono all’interno dei cloud pubblici o privati Trend Micro ha sviluppato SecureCloud, una soluzione che protegge i dati di livello enterprise all’interno degli ambienti cloud mediante l’uso di crittografia e di tecniche di key management basate su policy. Questa tecnologia permette di tutelare i dati del cloud e di favorire la flessibilità necessaria per rivol-

gersi a cloud provider differenti, senza essere vincolati al sistema crittografico di un unico vendor. SecureCloud consente di esercitare il controllo sulle modalità e sui punti di accesso alle informazioni per mezzo di funzioni che permettono di autenticare l’identità e l’integrità dei server che richiedono di accedere a volumi storage sicuri. Questa soluzione abilita anche il **rilascio automatico delle chiavi di cifratura**. Gli utenti possono gestire le loro chiavi crittografiche per ambienti Amazon EC2, Eucalyptus e VMware vCloud direttamente tramite il servizio hosted Trend Micro SecureCloud o da un key server SecureCloud installato all’interno dei loro data center fisici. Trend Micro SecureCloud è disponibile mediante abbonamento mensile o annuale, oppure tramite licenze software tradizionali. *

Le nuove sfide: attacchi mirati, mobilità, SCADA

L'ultima frontiera in termini di minacce è rappresentata dagli attacchi mirati la cui notorietà cresce di pari passo con il livello di danno che sono in grado di arrecare, ulteriormente aggravato dall'alto livello di efficacia che solitamente riescono a conseguire, favorito dalla difficoltà incontrata dalle soluzioni di protezione tradizionale nel contrastarle. Si tratta, infatti, di processi di attacco che sfruttano molteplici tecniche e che sono in grado di operare in modo inosservato anche per lunghissimo tempo.

Trend Micro Deep Discovery per rilevare gli attacchi mirati

Deep Discovery è il fulcro della soluzione di difesa personalizzata Trend Micro contro gli attacchi mirati e consente di rilevare e analizzare le minacce e anche di adattare i meccanismi di protezione per reagire agli attacchi.

Deep Discovery prevede il monitoraggio a livello di rete con tecnologia sandbox personalizzata e in tempo reale, per rilevare precocemente eventuali attacchi. L'approccio di Deep Discovery punta a individuare contenuti, comunicazioni e com-

portamenti dannosi su tutte le fasi della sequenza di attacco. La soluzione è costituita da due componenti.

- **Deep Discovery Inspector** che effettua l'ispezione del traffico di rete, il rilevamento delle minacce e l'analisi e la segnalazione in tempo reale.
- **Deep Discovery Advisor**, opzionale, che abilita un'analisi personalizzata aperta e scalabile della sandbox, la visibilità sugli eventi di sicurezza a livello di rete e le esportazioni di aggiornamento della sicurezza.

Trend Micro Smart Protection Platform

Smart Protection Platform è la soluzione di sicurezza pensata per proteggere le aziende dalle minacce ma, soprattutto, per rilevare e rispondere agli attacchi mirati.

Smart Protection Platform offre una protezione multilivello per reti, endpoint e server ed è costituita da tre componenti.

Deep Discovery è in grado di individuare contenuti, comunicazioni e comportamenti dannosi attraverso tutte le fasi in sequenza che caratterizzano un attacco mirato

Il primo è Trend Micro Smart Sensor, una soluzione software che effettua il monitoraggio degli endpoint analizzando i livelli di processo e le attività di comunicazione delle reti del sistema. Grazie a Smart Sensor è possibile

effettuare un'analisi sull'intera catena di eventi implicati in un attacco mirato e comprendere il comportamento dei malware, incluso il metodo di delivery, l'esecuzione e le implicazioni a livello di comunicazioni e sistema. Il secondo componente è Deep Discovery Email Inspector per la protezione dalle e-mail di spear phishing, che rappresentano oggi il tipico punto di partenza per gli attacchi mirati. Deep Discovery Email Inspector utilizza motori avanzati di protezione e un sistema di sandbox per identificare allegati nocivi, analizzare le minacce e impostare policy automatiche per la quarantena o il blocco delle e-mail.



Trend Micro OfficeScan per la sicurezza degli ambienti VDI

OfficeScan è la soluzione per la sicurezza indirizzata alle medie e grandi organizzazioni e pensata per rispondere alle sfide specifiche degli endpoint implementati all'interno di ambienti VDI.

OfficeScan si integra con Citrix XenDesktop e VMware View permette di massimizzare il numero di desktop virtualizzati per host, contribuendo a migliorare il ROI legato agli ambienti VDI, senza incidere sugli standard di sicurezza.

È in grado di identificare gli endpoint virtualizzati e di ottimizzare l'efficienza della protezione risorse attraverso la serializzazione delle operazioni di scansione e degli aggiornamenti di sicurezza, evitando pertanto i tipici problemi di rallentamento che coincidono con gli update degli antivirus o il riavvio delle macchine.

Il terzo tassello che compone Trend Micro Smart Protection Platform è l'ultimo aggiornamento (3.6) della soluzione Deep Discovery Inspector che estende la capacità di analisi di sandbox e migliora l'integrazione SIEM.

La soluzione Trend Micro Mobile Security a supporto del BYOD

A supporto delle esigenze di protezione alimentate dal BYOD Trend Micro mette a disposizione Trend Micro Mobile Security, una soluzione di sicurezza rivolta alle aziende enterprise e di media dimensione per la protezione di un'ampia gamma di dispositivi mobili quali iPhone, iPad, sistemi in ambiente Android, Blackberry OS e Apple iOS.

Questa soluzione integra gestione dei dispositivi e delle applicazioni dei dispositivi mobili e protezione multilivello dei dati (dalla crittografia, alla DLP, alla cancellazione da remoto) attraverso una singola console di gestione centralizzata. Consente al business di avere visibilità e controllo ma, nel contempo, lascia la libertà ai dipendenti di condividere i dati in modo sicuro attraverso ambienti fisici, virtuali e cloud.

Trend Micro Mobile Security verifica quali App possono essere installate, consente il blocco per i dispositivi mobili e offre la possibilità di definire policy che consentano di autorizzare o negare la connessione a Microsoft Exchange in base al livello di compliance del dispositivo.

Gli amministratori hanno visibilità su numero, tipologia e configurazione dei sistemi mobili e possono applicare policy di sicurezza comuni su differenti dispositivi, differenziate in base alla posizione geografica del dispositivo. Tra le funzionalità offerte vi è la possibilità di disabilitare la fotocamera del dispositivo mobile, la connessione Bluetooth e il lettore di schede SD. Trend Micro Mobile Security prevede l'integrazione con la console Trend Micro Control Manager che ne abilita l'interazione con molte soluzioni Trend Micro, consentendo anche di centralizzare le policy di sicurezza. per la gestione degli endpoint. Mobile Security è comunque dotata anche di una console di management indipendente.

La soluzione prevede anche l'integrazione con Mobile App Reputation

Services, il servizio che fa parte dell'infrastruttura di sicurezza Smart Protection Network di Trend Micro, grazie al quale è possibile individuare le App sospette, in modo da attivare operazioni di correlazione con gli inventari delle applicazioni degli utenti raccolte da Mobile Security per predisporre azioni di sicurezza preventive.

Soluzioni per la protezione dei sistemi SCADA

Gli strumenti e le tecnologie di Trend Micro possono essere utilizzati anche per proteggere in modo efficace gli ambienti SCADA aggirando l'ostacolo della difficoltà di effettuare controlli diretti, puntando sull'analisi di anomalie nel traffico di rete che caratterizzano i sistemi correlati alla macchina SCADA.

Trend Micro mette anche a disposizione sistemi di Application Control che, una volta installati su macchine SCADA, chiedono all'amministratore di selezionare le applicazioni che possono girare, evitando l'installazione non solo di applicazioni potenzialmente nocive, ma anche di quelle inutili.

Tra le soluzioni che sono state sviluppate da Trend Micro figura anche Portable Security; si tratta di una soluzione ospitata su una chiavetta USB che, all'atto dell'inserimento su macchine SCADA con sistema Windows embedded, effettua automaticamente una scansione certificando la macchina prima di metterla nuovamente in linea. *

La roadmap di Symantec per sconfiggere le minacce avanzate

Il vendor punta sul concetto di integrazione nella sua offerta di Advanced Threat Protection e si prepara al rilascio di nuove soluzioni e servizi nel corso dell'anno

Nel 2013 secondo i dati riportati nell'Internet Security Threat Report di Symantec si è assistito a un aumento del 62% del numero di violazioni dei dati rispetto all'anno precedente, che ha determinato la compromissione di oltre 552 milioni di identità. Una crescita che dimostra come i crimini informatici siano una minaccia reale e pericolosa sia per gli utenti consumer sia per le aziende. Lo studio di Symantec ha anche evidenziato come sia in atto un significativo cambiamento nel comportamento dei criminali informatici, i quali, prima di sferrare un attacco di vasta portata, tramano e pianificano per mesi. Inoltre, sempre nell'anno passato, gli attacchi mirati sono aumentati del 91% e hanno avuto una durata media tre volte superiore rispetto a quelli del 2012.

Tra le figure professionali prese di mira ci sono stati assistenti personali e professionisti delle pubbliche relazioni: per gli autori di crimini informatici rappresentano il primo passo verso obiettivi di più alto profilo, come manager aziendali.

Proteggere la rete aziendale da nuove tipologie di minacce sempre più avanzate comporta la necessità di sviluppare un approccio integrato e completo. È il concetto alla base dell'offerta di Advanced Threat

Protection di Symantec che quest'anno sarà aggiornata con nuovi servizi e soluzioni tra cui Symantec Managed Security Services-Advanced Threat Protection e Symantec Advanced Threat Protection Solution, che combinano avvisi e intelligence all'interno di diverse tecnologie di sicurezza per offrire una prevenzione completa degli attacchi. Con l'aumento degli attacchi mirati le aziende hanno la necessità di proteggersi da intrusioni che possono avvenire in diversi punti di ingresso della rete. Symantec si propone con un'offerta di protezione end-to-end, che integra l'intero portfolio ed è fruibile sotto forma di servizi grazie al proprio ecosistema di partner. Inoltre il portfolio di soluzioni integrate ATP di Symantec è alimentato dalla piattaforma Symantec Global Intelligence Network, e da un team di oltre 550 ricercatori nel mondo, che raccoglie giornalmente i dati di milioni di clienti e sensori, sviluppando strategie predittive e proattive di difesa.

Disponibile da giugno il nuovo servizio gestito Symantec Managed Security Services-Advanced Threat Protection (MSS-ATP), riduce il tempo necessario per rilevare, attribuire



una priorità e rispondere a incidenti di sicurezza, consentendo anche l'integrazione con prodotti di sicurezza di terze parti.

Inoltre, entro i prossimi sei mesi, Symantec introdurrà due nuovi servizi chiave: il primo servizio interamente nuovo di Incident Response, che fornisce ai clienti con un accesso immediato alle funzionalità critiche, conoscenze e set di abilità durante scenari di risposta agli incidenti; un secondo servizio di Intelligence, che fornisce visibilità e analisi delle minacce, offrendo feed di dati e servizi basati sull'Intelligence, così come il Managed Adversary Information che fornisce un report avanzato sugli attori della minaccia.

La nuova soluzione di Advanced Threat Protection che Symantec porterà sul mercato sarà, invece, disponibile entro i prossimi 12 mesi. Si tratta di una soluzione end-to-end che offrirà un'avanzata protezione dalle minacce, integrando endpoint, e-mail e gateway per fornire capacità di rilevamento e risposta critiche in tutti i punti di controllo. In più due nuove tecnologie saranno alla base dell'elevata capacità di rilevamento e di risposta della soluzione: Dynamic Malware Analysis Service di Symantec, un ambiente sandbox basato sul cloud e Synapse, che consente la comunicazione fluida tra endpoint, e-mail e gateway per migliorare la risposta. *

I firewall Dell Sonicwall per le esigenze enterprise

Una gamma di modelli di nuova generazione che si caratterizzano per la presenza di processori specializzati multicore e la tecnologia brevettata Reassembly-Free Deep Packet Inspection

Attraverso la serie di dispositivi E-Class Network Security Appliance (NSA), Dell Sonicwall mette a disposizione una soluzione di firewall e intrusion prevention di nuova generazione indirizzata a grandi aziende, enti governativi e università.

Questa gamma di soluzioni sfrutta la tecnologia brevettata **Reassembly-Free Deep Packet Inspection (RFDPI)** che effettua scansione del traffico su tutte le porte e su oltre 50 protocolli con l'obiettivo di identificare e prevenire le avanzate tecniche di evasione utilizzate per nascondere attacchi tradizionali a tutti i livelli dello stack di rete. La capacità di categorizzare il traffico applicativo consente di estendere la protezione anche al livello di applicazione.

Alla tecnologia RFDPI, le appliance di rete **NSA Serie E** affiancano microprocessori multi-core specializzati per fornire funzionalità di gateway antivirus, anti-spyware, prevenzione delle intrusioni basate su firma e Application Intelligence ad alta velocità.

L'**Application Intelligence Service** di Sonicwall fornisce una serie di strumenti di protezione personalizzabili per il controllo del traffico di rete che consentono di automatizzare la gestione dell'ampiezza di banda, controllare gli accessi Web interni ed esterni, limitare il trasferimento di file e documenti

specifici, scansionare allegati e-mail tramite criteri configurabili dall'utente e supportare le firme dei clienti.

La gamma NSA Serie E prevede i tre modelli siglati E8500, E6500 ed E5500 che si differenziano essenzialmente per le prestazioni e il numero massimo di connessioni. Nella modalità firewall le prestazioni (throughput) dei modelli E8500, E6500 ed E5500 sono, rispettivamente, di 8 Gbps, 5 Gbps e 3,9 Gbps (che si dimezzano circa per le VPN 3DES/AES) con un numero massimo di connessioni simultanee pari a 1 milione e mezzo, 1 milione e 750mila. Il throughput DPI/Gateway AV/Anti-Spyware/IPS per i tre modelli è rispettivamente di 2,2 Gbps, 1,59 Gbps e 850 Mbps.

Alle esigenze delle reti aziendali distribuite a livello globale, dei grandi centri dati, delle Telco e dei service provider più esigenti si indirizzano le soluzioni **SuperMassive Serie 9000 e Serie E10000**.

La serie SuperMassive 9000 (dispo-

nibile nei tre modelli 9200, 9400 e 9600) mette a disposizione 4 porte SFP+ 10-GbE, 8 porte SFP 1-GbE e 8 porte 1-GbE a cui si aggiunge un'interfaccia di gestione da 1 Gbps. Le prestazioni dichiarate da Sonicwall prevedono un throughput fino a 20 Gbps in modalità firewall, di 9,7 Gbps in modalità Intrusion Prevention con controllo applicativo e di 5 Gbps nella protezione antimalware.

I dispositivi SuperMassive E10000 (disponibili nelle versioni E10100, E10200, E10400, E10800) sono stati progettati per fornire bassissima latenza nelle operazioni di analisi dei pacchetti e mettono a disposizione fino a 240 Gbps of ampiezza di banda "nonblocking".

Lo chassis del firewall SuperMassive E10000 include 6 porte SFP+ 10-GbE e 16 porte SFP 1-GbE e inoltre prevede alimentatore e moduli di ventilazione ridondanti e hot swappable.

È in grado di scalare fino a 96 core di elaborazione con un throughput dichiarato dall'azienda pari a 40 Gbps come firewall, 30 Gbps come Intrusion Prevention con analisi applicativa e 10 Gbps nella protezione antimalware. *



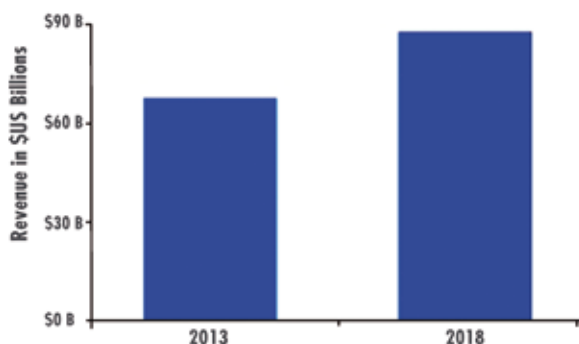
Il firewall Dell Sonicwall SuperMassive E10100

SERVIZI VOIP IN AMBITO BUSINESS SEMPRE PIÙ UTILIZZATI ANCHE GRAZIE AL CLOUD

Una ricerca di Infonetics conferma che la fruizione di servizi VoIP in ambito business è ormai una prassi comune che si orienta in misura crescente verso modelli cloud

Secondo una recente ricerca di Infonetics l'adozione di servizi VoIP in ambito aziendale ha superato da tempo la fase iniziale che vi vedeva coinvolte per lo più le aziende di medie o grandi dimensioni. In sostanza, oggi la fruizione del VoIP nelle aziende risulta una prassi comune, spinta dalla disponibilità globale di servizi di SIP trunking e piattaforme per la telefonia ospitate nel cloud.

Infonetics riporta in proposito una crescita dell'8% del mercato globale dei servizi VoIP erogati sia in ambito residenziale sia business nel 2013 e prevede un giro d'affari di 88 miliardi di dollari su scala mondiale entro il 2018.



Mercato globale dei servizi VoIP e UC per l'utenza residenziale e business (Fonte: Infonetics Research)

La richiesta di **servizi di SIP trunking**, attraverso cui gli operatori forniscono servizi voce ai clienti dotati di propri centralini IP è letteralmente esplosa nello scorso anno, con un tasso di crescita del 50% negli Stati Uniti. L'analista prevede un ampio contributo dell'area EMEA per il 2014.

La domanda di centralini IP hosted e di servizi di Unified Communications erogati via cloud è cresciuta del 13% di pari passo con l'erogazione di servizi VoIP gestiti: circa il 10-20 % delle nuove linee VoIP sono commercializzate come parte di un pacchetto di servizi gestiti o nel quadro di contratti di outsourcing. Infonetics, indica che l'adozione di massa del VoIP in ambito aziendale è stata favorita proprio dalla crescente disponibilità a livello globale di servizi di SIP trunking e di piattaforme per la telefonia ospitate nel cloud, e che la possibilità di avvalersi di soluzioni complete per le Unified Communications via cloud viene vista con crescente interesse da parte di aziende di medie e grandi dimensioni che attualmente considerano lo spostamento di servizi e applicazioni nel cloud o stanno già migrando le proprie infrastrutture. *

VIDEO TRASFERTE IN PIRELLI, BASTA VIAGGI

Per migliorare il lavoro dei team e risparmiare Pirelli dice addio alle trasferte e le sostituisce con la videocomunicazione di Cisco

Con 22 stabilimenti nel mondo e una presenza commerciale in 160 Paesi, l'azienda ha trovato nelle soluzioni Cisco un'alternativa alle riunioni di persona e, rivolgendosi a Dimension Data, partner di Cisco, ha portato avanti un progetto che è stato la base di un rinnovamento dell'intera infrastruttura, pensata per mettere a disposizione di Pirelli una piattaforma di collaborazione che tenesse conto di elevati parametri di qualità, disponibilità e sicurezza.

La rete aziendale è stata realizzata utilizzando switch **Catalyst serie 6509** per funzionalità di routing layer 3 e con switch **Catalyst serie 3750, 3500 e 2900** nel layer per la distribuzione. Si tratta di un'infrastruttura in grado di supportare una rete wireless comprensiva di più di 1000 access point in tutto il mondo, gestita da Wireless LAN Controller Cisco serie 5500 e un'ampia gamma di endpoint per la videoconferenza.

Questi includono gli endpoint video Cisco TelePresence System serie EX90 e EX60, i Quick Set C20 e SX20, i Codec C40, C60, e C90 e gli IP Phone Cisco adatti alla video comunicazione, gestiti dalla Multipoint Control Unit Cisco TelePresence MCU serie 5300.

Cisco Unified Communications Manager consente il controllo delle chiamate. La soluzione è completata da 10 virtual meeting room Cisco WebEx e da un Cisco Secure Access Control Server per l'autenticazione e l'autorizzazione.

Gli uffici, spiega la società, possono invece fruire di una migliore interconnessione e attraverso la TelePresence e WebEx è possibile avere interazioni più efficaci tra la forza commerciale e la produzione. *



Switch Cisco Catalyst serie 6509

IPSWITCH PORTA ALLE PMI IL MONITORAGGIO DI RETE ENTERPRISE

Nel mondo interconnesso in cui stiamo vivendo e con il quale devono fronteggiarsi le imprese, l'importanza delle tecnologie di rete è seconda solo a quella del network management. Infatti, la rete è fondamentale perché fornisce un supporto, ma garantirlo non è banale, soprattutto da quando i budget sono stati ridotti all'osso.

I grandi applicativi di network management tanto popolari negli anni Novanta, del resto, non erano famosi per i costi contenuti.

A tal proposito, Chiara Ornicotti, Business Development manager Southern Emea per la Network Management Division di Ipswitch, sostiene: «Per anni è stata diffusa la percezione di un grosso gap di funzionalità e performance tra le soluzioni di monitoraggio IT a basso costo indirizzate alle piccole e medie realtà e quelle delle "big four", i cui prezzi partono da sei cifre per salire rapidamente».

Cifre che non tutti possono permettersi, come nel caso di un **ateneo britannico con 6000 studenti**, di cui ci parla Ornicotti, che aveva la necessità di creare mappe di rete che coprissero le sue sette sedi e, quindi, monitorare la rete distribuita per garantirne il massimo uptime e poter spegnere correttamente tutti i server nel caso in cui si fosse verificato un black out di durata superiore a quella gestibile dai sistemi UPS.

Dopo avere condotto alcune ricerche sugli ultimi trend nei prodotti per il monitoraggio IT, i responsabili IT capirono che non sarebbe stato necessario investire cifre spropositate, per garantire a professori, studenti e personale la massima operatività.

«Fino a poco tempo fa - sostiene la manager italiana - l'assenza di consapevolezza delle capacità e scalabilità dei prodotti di monitoraggio

IT rivolti alle piccole e medie realtà portava organizzazioni di medie dimensioni, come l'università, a spendere ben **oltre 100mila dollari** per prodotti di classe enterprise. Negli ultimi anni le soluzioni di monitoraggio IT indirizzate al mercato delle piccole e medie imprese hanno ampliato in modo significativo funzionalità e scalabilità, tanto da poter soddisfare oggi anche le esigenze di organizzazioni più grandi ed esigenti. Mentre le soluzioni più costose tipicamente offrono le funzioni che le grandi organizzazioni si aspettano di trovare, tali funzionalità aggiuntive non necessariamente sono richieste dalla maggior parte delle altre organizzazioni e non ne giustificano il prezzo più alto».

Ornicotti riassume dunque le caratteristiche fornite dalla suite integrata **WhatsUp Gold di Ipswitch** che hanno determinato la scelta dell'ateneo britannico:

- visione unificata di tutti i servizi IT, compresa la possibilità di mappare l'intera rete fino a livello dei singoli dispositivi;
- monitoraggio integrato che comprende ogni aspetto, dal livello applicativo fino ai singoli componenti dei singoli dispositivi;
- disponibilità avanzata dei servizi IT conformemente ai Service Level Agreement;
- risoluzione dei problemi ridotta da giorni (o settimane, o mesi) a minuti;
- dashboard e report facili da personalizzare;
- velocità di installazione e integrazione dell'ambiente di produzione;
- profili applicativi di facile personalizzazione;
- automatizzazione degli interventi facilmente personalizzabile. *



Chiara Ornicotti, Business Development Manager Southern Emea per la Network Management Division di Ipswitch

Con la suite WhatsUp Gold un'università inglese risparmia cifre a cinque zeri, grazie a una soluzione integrata che, tra l'altro, consente di ottenere una visione completa della rete, risolvere rapidamente anomalie, automatizzare le procedure e personalizzare i profili delle applicazioni

di Gaetano Di Blasio



di Gaetano Di Blasio

L'allineamento catartico tra IT e business

Si è sempre parlato di allineamento tra IT e business, ma in impresa si è poco praticato a causa di resistenze su entrambi i fronti. Solo alcuni IT manager illuminati compresero già una decina d'anni fa che la collaborazione con gli altri dirigenti era ineluttabile.

D'altro canto, in molti aleggiava un senso di superiorità nel saper governare i computer, ritenendo così di gestire un potere assoluto. Dall'altro lato, la frustrazione del manager costretto ad aspettare i tempi apparentemente infiniti dell'IT per implementare un nuovo servizio, nonché il senso di esclusione, rendeva il dialogo pressoché impossibile.

Oggi lo scenario è totalmente cambiato grazie a due fenomeni che si sono affermati. Il primo consiste nell'evoluzione di quello che dieci anni fa veniva chiamato Web 2.0 e che, passando per Facebook e i social network, è oggi rappresentato da un nuovo modo di relazionarsi tra individui.

Il secondo è il cloud. Quest'ultimo, in particolare, ha portato l'IT manager a riflettere sul proprio ruolo, nel momento in cui i business manager hanno cominciato a trovare servizi chiavi in mano sul Web. Pronti in pochi click, anche se standard e con molti limiti di adattabilità alle esigenze delle imprese.

L'incontro tra cloud pubblico e virtualizzazione sta accelerando i processi IT e, contemporaneamente, il boom della "social enterprise" sta accelerando i processi decisionali e di business.

Come ormai pare chiaro, anche da quanto emerge in numerosi convegni, le best practice suggeriscono di riorganizzare l'impresa.

Le maggiori imprese, da Procter & Gamble a Fiat, da Unicredit a ENI, stanno ripensando l'approccio all'IT. Il CIO sta diventando un service broker e deve promuovere questa impostazione, favorendola con l'adozione degli strumenti di Unified

Communication e Social Collaboration adatti, in tutta l'impresa. Solo in questo modo vedrà il proprio acronimo diventare Chief Innovation Officer e solo così potrà contribuire in maniera significativa allo sviluppo della propria impresa.

Non dimentichiamo che il Web 2.0 è alle spalle. Oggi si parla di Internet of Things e la rivoluzione tecnologica riguarderà non solo l'organizzazione e i processi decisionali, ma anche quelli produttivi e commerciali.

*Diverse aziende lo hanno compreso, soprattutto all'estero. Almeno secondo quanto comunicato da IDC, i cui ricercatori ritengono che il mercato della Unified Communication & Collaboration è al centro degli investimenti delle imprese per la loro capacità di migliorare i processi aziendali e abilitare il lavoro da remoto e in movimento. **

DATA CENTER PIÙ DISPONIBILE CON IL SISTEMA DI REFRIGERAZIONE DI EMERSON

Emerson Network Power ha annunciato con orgoglio **Liebert AFC**, un nuovo sistema di raffreddamento per data center che l'azienda sostiene sia in grado di fornire risparmi energetici annuali fino al 30 per cento.

L'elevato livello di efficienza energetica fornito è una conseguenza dell'utilizzo della tecnologia "free-cooling adiabatica", che si avvale dell'evaporazione dell'acqua per abbassare la temperatura dell'aria che attraversa la batteria di condensazione e di raffreddamento. Questa tecnologia, secondo Emerson, permette di preservare al massimo la disponibilità del raffreddamento, anche nelle condizioni più critiche come, per

esempio, in presenza di fluttuazioni dell'alimentazione elettrica, carenza d'acqua o di elevate temperature dell'aria esterna.

Grazie a queste caratteristiche il produttore rivendica un indice di efficienza **Power Usage Effectiveness (pPUE) di 1,08**.

Secondo le stime fornite da Emerson Network Power, in un data center a pieno carico da 1,4 MW localizzato in centro Europa, un sistema di "free-cooling" tradizionale consumerebbe circa 963mila kWh all'anno rispetto ai 645mila kWh con un Liebert AFC, con un risparmio stimabile in circa 50mila Euro all'anno (assumendo un costo energetico di 0,15 €/kW). *



Il "chiller" Liebert AFC di Emerson Network Power

Il produttore ha sviluppato Liebert AFC pensato per massimizzare efficienza e disponibilità raggruppando tre tecnologie di raffreddamento in una singola unità

CON FUJITSU VSHAPE ED ETERNUS FAI PIÙ CON MENO

L'architetture vShape con ETERNUS, ideata per infrastrutture virtualizzate, è disponibile a livello mondiale e integra storage ETERNUS e server PRIMERGY

Fujitsu ha introdotto una nuova architettura di riferimento vShape completamente virtualizzata che, osserva la società, è stata sviluppata per fornire prestazioni più elevate e un ritorno più rapido degli investimenti.

La soluzione integra il sistema di storage Fujitsu **ETERNUS DX S3**, le unità Fujitsu Server **PRIMERGY RX300 S8**, i nuovi switch Brocade Fibre Channel e il software di virtualizzazione Microsoft Hyper-V in alternativa al software VMware.

Più in particolare, ha spiegato Fujitsu, l'ecosistema vShape privilegia più elevati livelli di disponibilità tramite nuove funzionalità di backup basate sullo storage ETERNUS CS800 Data Protection Appliance, in combinazione con il software Symantec Backup Exec V-RAY.

Tramite il supporto della tecnologia di deduplicazione, ETERNUS CS800 supporta anche backup e un ripristino molto rapidi, con una riduzione della capacità

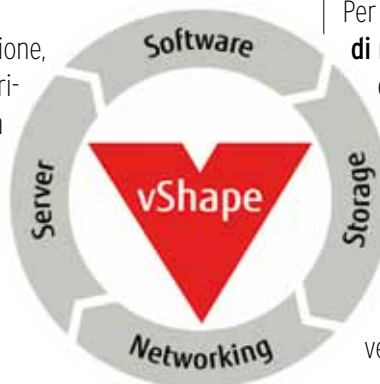
necessaria per il backup su disco che evidenzia come possa arrivare fino al 95%.

Allo stesso tempo, continua l'azienda, Backup Exec V-Ray fornisce una sicurezza molto ampia per gli ambienti virtuali con VMware o Hyper-V. In questo caso, il processo di ripristino di macchine virtuali può essere finemente regolato su vari livelli - per file singoli, oggetti Active Directory, email di Exchange o anche documenti di SharePoint.

Per aziende con esigenze specifiche **l'architettura di riferimento vShape** è modulare e i diversi pacchetti possono essere adattati secondo necessità.

Le aziende hanno anche la possibilità di aggiungere nuovi prodotti e servizi.

Tra le validazioni ottenute, quella per le infrastrutture desktop virtuali (VDIs) fornisce agli utenti di telefonia mobile un accesso sicuro ai dati e alle applicazioni sulla rete aziendale attraverso una varietà di dispositivi. *



CON F5 E VMWARE PIÙ SICURI I DESKTOP VIRTUALI

Le aziende uniscono le forze per un accesso sicuro ai desktop virtuali e Desktop-as-a-Service ad alte prestazioni per l'era del "mobile cloud"

F5 Networks e VMware hanno annunciato il rafforzamento della collaborazione per garantire il controllo dell'accesso sicuro per l'implementazione dei desktop virtuali. Le nuove offerte delle due aziende introducono funzionalità per il Mobile Cloud e per gli utenti finali che accedono ai loro desktop e alle applicazioni da vari dispositivi mobili.

Va premesso che F5 ha portato sul mercato nuove versioni della sua soluzione **BIG-IP Access Policy Manager (APM)** che è stata sviluppata su misura al fine di fornire un accesso sicuro e prestazioni ottimizzate per VMware Horizon View.

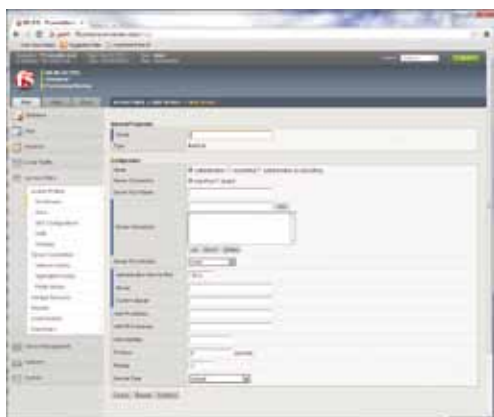
Disponibile con diverse opzioni di throughput e di accesso di utenti simultanei, queste nuove offerte garantiscono un significativo risparmio di costi e forniscono la tecnologia leader per l'accesso sicuro.

Inoltre, F5 ha introdotto una iApp dedicata e un'architettura di riferimento per accelerare in modo significativo la distribuzione e fornire indicazioni prescrittive su come queste nuove soluzioni supportano le tecnologie VMware.

Sviluppate sulla base di una collaborazione tecnologica di lunga data, l'abbinamento di **soluzioni EUC VMware** con le tecnologie per applicazioni intelligenti di F5 si propone di fornire soluzioni sofisticate e sicure per garantire la mobilità della forza lavoro, pur mantenendo il controllo e la sicurezza.

Da parte sua VMware fornisce l'accesso alle API e estensioni del protocollo di accesso remoto che consentano a F5 di estendere le proprie soluzioni per aggiungere il controllo dell'accesso ad ambienti Horizon View.

Con questa integrazione, osserva la società, gli utilizzatori possono esercitare un controllo più granulare basato su dispositivo, ubicazione, e altre variabili di accesso, e sono in grado di reindirizzare gli utenti ad applicazioni o cloud diversi in una distribuzione globale. *



F5 BIG-IP Access Policy Manager

SOFTWARE AG MIGLIORA LA GESTIONE MOBILE

L'acquisizione di Metaquark aggiunge nuove funzionalità alle piattaforme Intelligent Business Operations e webMethods del produttore tedesco

Software AG, azienda con una storia quarantennale che fornisce soluzioni tecnologiche in merito a big data, integrazione e processi di business, ha annunciato il completamento dell'acquisizione di Metaquark e la contestuale integrazione delle funzionalità per il mobile sviluppate da quest'ultima all'interno delle piattaforme di **Intelligent Business Operations (IBO)** e di **webMethods Business Process Management**.

L'utilizzo della tecnologia sviluppata da Metaquark consente la gestione unificata di utenti, dispositivi e profili di sicurezza in ambito mobile, fornendo, inoltre, una serie di funzionalità di monitoraggio con la generazione di report e statistiche.

Queste caratteristiche la rendono un elemento di completamento sinergico alle funzionalità mobile di Software AG che permettono di creare un'unica versione di un'applicazione nativa mobile che può essere utilizzata con qualsiasi dispositivo iOS, Android, BlackBerry e Windows Mobile.

La tecnologia mobile di Metaquark è stata integrata anche alla piattaforma webMethods Business Process Management di Software AG.

«Con la piena integrazione di metaquark nel portafoglio dei prodotti IBO di Software AG, gli sviluppatori possono ora realizzare, testare e gestire da una singola piattaforma, applicazioni per diversi sistemi operativi - ha precisato John Bates, responsabile della linea di business Intelligent Business Operations di Software AG - . Una funzionalità interessante riguarda la visual analytics in real-time: questa, generata con applicazioni IBO-enabled, può essere applicata a diversi dispositivi mobile o wearable». *



L'EUROPA ACCELERA SULLA FATTURAZIONE ELETTRONICA

Il Parlamento Europeo ha sostenuto la proposta della Commissione relativa alla creazione di uno standard comune a tutta l'area europea per l'e-invoicing nell'ambito del procurement pubblico. Si tratta di un passo ulteriore verso la creazione di un mercato digitale unico in Europa.

La fattura elettronica nei rapporti economici tra pubblica amministrazione e fornitori mira ad una semplificazione delle procedure amministrative in un'ottica di trasparenza, monitoraggio e rendicontazione della spesa pubblica.

Anche l'Italia, da parte sua fa passi avanti. Il Decreto Ministeriale n. 55 del 3 aprile 2013, entrato in vigore il 6 giugno 2013, ha reso operativo quanto stabilito dalla Finanziaria 2008 in merito all'obbligo di emissione, trasmissione, conservazione e archiviazione in forma elettronica delle fatture nei rapporti con le PA. Ministeri, Agenzie fiscali ed Enti nazionali di previdenza e assistenza sociale dovranno essere i primi ad adeguarsi al Decreto (entro 12 mesi stabilisce l'art. 6 c. 2 ovvero dal prossimo 6 giugno) mentre le altre PA (art. 6 c. 3) avranno tempo fino al 6 giugno 2015. Affinché la Commissione riesca entro il 2020 a rendere l'e-invoicing la forma di fatturazione prevalente in Europa appare però necessario agire in un'ottica paneuropea. Il **Parlamento europeo** ha approvato in proposito un pacchetto di investimenti dell'ammontare di 1 miliardo di euro per supportare progetti digitali paneuropei e reti a banda larga ad alta velocità. Questo progetto fa parte del meccanismo per collegare l'Europa (Connecting Europe Facility), un piano sviluppato dalla Commissione Europea per migliorare le reti europee di trasporto, energia e digitali. Il problema di base è che sino a questo momento lo sviluppo di standard relativi alla fatturazione elet-

tronica è avvenuto a livello di singolo Paese e questo, da un lato, ha limitato l'interoperabilità e, dall'altro, si è tradotto in un aumento dei costi per le aziende con attività di fatturazione elettronica cross-border.

Non sorprende quindi il fatto che l'adozione dell'e-invoicing in Europa sia stata fino a questo momento piuttosto limitata: le fatture elettroniche rappresentano solo **dal 4% al 15% del totale** delle fatture inviate. La frammentazione degli standard porta a inefficienze e rappresenta un ostacolo a una diffusione più ampia dell'e-invoicing in particolare per le piccole e medie imprese.

Rimangono, tuttavia, delle sfide da superare. Da una ricerca di Ricoh è, difatti, emerso come il 63% delle aziende europee sia ancora lontano dalla trasformazione digitale. Il prossimo passo per le imprese sarà quello di rivedere e innovare le modalità operative, le tecnologie e i processi. Secondo Ricoh uno dei principali aspetti da considerare è rappresentato dalle modalità con cui passare dal cartaceo al digitale, un passaggio che non può avvenire dall'oggi al domani, ma che richiede diversi step strutturati e per il quale risulta fondamentale considerare l'intero processo di fatturazione e non semplicemente l'output finale. *

Si profila uno standard comune a tutta l'area europea per l'e-invoicing nell'ambito del procurement pubblico

di Giuseppe Saccardi



MICROSOFT CLOUD PLATFORM: NUOVI SERVIZI DA DIMENSION DATA

Un nuovo servizio Private CaaS che permette di migrare le applicazioni Microsoft su una piattaforma cloud ibrida sicura

Dimension Data ha annunciato la disponibilità di un servizio di private cloud basato su Microsoft Cloud Platform che permette alle aziende di sviluppare e ospitare applicazioni Microsoft all'interno di un ambiente cloud dedicato.

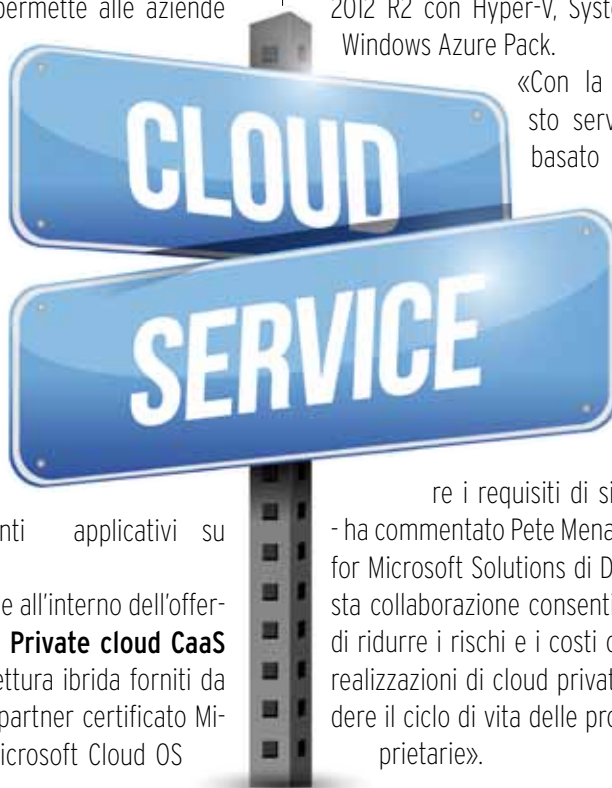
L'annuncio rientra nella strategia del fornitore globale di soluzioni ICT volta a fornire integrazione dei sistemi, migrazione dei dati e servizi cloud pubblici e privati con l'obiettivo di supportare le organizzazioni a migrare i complessi ambienti applicativi su cloud.

Il nuovo servizio si inserisce all'interno dell'offerta più ampia di **servizi di Private cloud CaaS** caratterizzati da un'architettura ibrida forniti da Dimension Data che è un partner certificato Microsoft Certified Gold e Microsoft Cloud OS

Network. Questa nuova offerta di servizi supporta la Microsoft Cloud Platform basata su Windows Server 2012 R2 con Hyper-V, System Center 2012 R2 e Windows Azure Pack.

«Con la disponibilità di questo servizio di private cloud basato su Microsoft Cloud Platform, Dimension Data e Microsoft saranno in grado di indirizzare le esigenze dei clienti che richiedono un ambiente cloud dedicato per soddisfa-

re i requisiti di sicurezza e conformità - ha commentato Pete Menadue, general manager for Microsoft Solutions di Dimension Data -. Questa collaborazione consentirà alle organizzazioni di ridurre i rischi e i costi operativi associati alla realizzazioni di cloud privati in-house e di estendere il ciclo di vita delle proprie applicazioni proprietarie». *



DA IBM UN MARKETPLACE PER IL CLOUD D'IMPRESA

Attivato un portale per accedere ai software e ai servizi cloud offerti da IBM e i suoi partner

Un nuovo marketplace per il Cloud è stato realizzato da IBM per promuovere il proprio portafoglio di funzionalità cloud e i servizi di terze parti verso sviluppatori, responsabili IT e business leader.

All'interno di un unico portale è possibile provare e acquistare i software e i servizi cloud di IBM che comprende oltre **100 applicazioni SaaS**, servizi com-

ponibili di Platform as a Service IBM BlueMix e di Infrastructure-as-a-Service SoftLayer. Per i partner di IBM questo marketplace rappresenta un'ulteriore opportunità per raggiungere imprese in tutto il mondo e per collaborare con tutto il canale.

Il marketplace cloud di IBM è organizzato in **tre componenti** indirizzate ai professionisti delle linee di business, agli sviluppatori e ai reparti IT. I contenuti vengono forniti in base al ruolo professionale e le pagine dei servizi permettono un accesso intuitivo agli utenti interessati a start-up, mobile, gaming e altro. «Nelle aziende gli utenti cloud, sia che appartengano alle divisioni di business, che all'IT o allo sviluppo, cercano sempre più un accesso agevole a una vasta gamma di servizi - ha osservato Robert LeBlanc, senior vice president, IBM Software & Cloud Solutions -. Il marketplace cloud IBM porta ai nostri clienti tutto il potenziale "as-a-Service" di IBM e del nostro ecosistema». *



È disponibile il libro sul **CLOUD COMPUTING**

In oltre 280 pagine analizza gli economics e le strategie alla base dell'adozione del Cloud come strumento per rendere l'IT più efficace, razionale e meno costoso, nonché gli aspetti connessi ai nuovi paradigmi dell'IT e del cloud. Tra questi l'Hybrid Cloud, i Big data e il Software Defined Data Center. Completa l'opera l'esame della strategia e della proposizione di primarie aziende dell'IT internazionale che hanno fatto del Cloud uno degli elementi portanti del proprio portfolio di soluzioni e servizi.



**PRENOTA
L'EDIZIONE 2014
IN USCITA
A GIUGNO**

Cloud Computing e IT as a Service

Hybrid Cloud, Big Data, Software Defined Data Center
e Servizi per un'azienda agile e competitiva

Giuseppe Saccardi
Gaetano Di Blasio - Riccardo Florio

Reportec

Sono anche disponibili i libri

- UN'IMPRESA SEMPRE PIÙ MOBILE
- STORAGE e
- SICUREZZA AZIENDALE
E CONTINUITÀ DEL BUSINESS

Il libro è acquistabile al prezzo di 50 euro (più IVA) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444

MOBIZ

MOBILITY FORUM 2014

Facing the Mobility Diversity

Milano, 18 Giugno 2014 · Hotel Melià

Gli studi IDC hanno evidenziato un'evoluzione dalla fase 'passiva' della consumerizzazione a quella 'attiva' del mobile first. Molte aziende infatti hanno invertito l'approccio al fenomeno mobility: dal semplice tamponamento dei problemi ci si focalizza sempre più a sviluppare strategie aziendali che promuovano i benefici di business derivanti dall'inserimento della mobility all'interno della cultura IT aziendale. Diventa pertanto sempre più importante approfondire e discutere di questi aspetti e lo faremo nel corso di Mobiz Mobility Forum 2014 di IDC, giunto alla quarta edizione, che presenta le principali best practice in ambito di enterprise mobility.

Tra i Keynote speaker

Daniela Rao, TLC Research & Consulting Director, **IDC Italia**

Nick McQuire, CEO, **The Global Enterprise Mobility Alliance (GEMA)**

Fabio Biancotto, Executive IT Manager, **Air Dolomiti**

e con l'esclusiva partecipazione di:

Giovanni Maistrello, Location Manager, **Car2Go Italia**

Platinum Sponsor



Gold Sponsor



Contributor



 #IDCMobizMI14

PER INFORMAZIONI

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

http://idcitalia.com/ita_mobiz_14