

# SECURITY

## & BUSINESS

n.17

AGOSTO 2013

**IN QUESTO  
NUMERO:**

## SPECIALE REPORT ICT SECURITY

**Soluzioni, tecnologie  
e servizi per  
un'efficace protezione  
degli asset aziendali**

### **CYBER WAR: Non c'è password o rete che tenga**

La pressione delle minacce è sempre più elevata. Gli attacchi DDoS sono gli aspetti più evidenti, ma le minacce APT sono probabilmente le più pericolose. Minacce "multiformi" che spesso sottengono ad attacchi mirati.

Ne parliamo nelle pagine della rubrica Cyber War, illustrando anche dei dati italiani ed entrando nel vivo di alcuni meccanismi, grazie all'aiuto di due "white hat hacker" di Stonesoft.

**pag.8-11**

### **SOLUZIONI: IBM Vulnerability Manager**

Cresce il bisogno di intelligence per la sicurezza. I sistemi SIEM si appoggiano agli Analytics e IBM, in particolare, ha esteso il proprio sistema Qradar a vari ambiti. Tra cui spicca la gestione delle vulnerabilità, da sempre modo cruciale nella protezione delle applicazioni e delle reti. La nuova soluzione fornisce ai responsabili della sicurezza una vista complessiva e "prioritizzata" della rete, aiutandoli a rafforzare e consolidare velocemente le loro difese.

**da pag.25**

#### **EDITORIALE**

**pag.03**

• Perdere i dati può diventare un gioco

#### **THE CYBER WAR**

**pag.05**

• Trend Micro svela la diffusione degli APT

**pag.06-07**

• Ogni "record" compromesso costa all'azienda 136 dollari

**pag.08-11**

• Non c'è password o rete che tenga

#### **SPECIALE**

**pag.12-15**

• Introduzione allo Speciale ICT Security

**pag. 16-24**

• Speciale ICT Security

#### **SOLUZIONI**

**pag.25**

• IBM Qradar gestisce le vulnerabilità

**pag.26**

• Sophos semplifica la sicurezza dei dispositivi mobili

**pag.27**

• Trend Micro Worry-free Business Security Services 5.2

#### **NEWS**

**pag.28**

• McAfee Mobile Security

• Servizi HP Cloud Security

• Palo Alto Networks

• WildFire per cloud privati

# È disponibile il libro sulla **SICUREZZA AZIENDALE**

È disponibile il libro "Sicurezza aziendale e continuità del business" realizzato da Reportec. In circa 300 pagine analizza le problematiche di governance e di risk management connesse con i diversi aspetti della sicurezza aziendale: dalla protezione delle informazioni, alla continuità operativa, alla salvaguardia degli asset fisici, non dimenticando di sottolineare le problematiche portate dagli ultimi trend tecnologici, come il cloud computing e la mobility. Completa il volume l'analisi delle soluzioni sviluppate da un ampio numero di primarie aziende del settore.



È anche disponibile il libro  
**UN'IMPRESA SEMPRE PIÙ MOBILE**

Il libro è acquistabile al prezzo di 50 euro (più IVA 21%) richiedendolo a  
**info@reportec.it - tel 02 36580441 - fax 02 36580444**

# PERDERE I DATI PUÒ DIVENTARE UN GIOCO



di  
*Gaetano Di Blasio*

*La perdita o fuoriuscita di informazioni critiche continua a essere un problema per molte aziende. Ci sono casi clamorosi, come quello che ha visto protagonista Edward Snowden, il quale ha rilevato i dati del programma “spia” PRISM della National Security Agency (NSA) statunitense, sottraendoli, pare, tramite una chiavetta USB.*

*Dando per scontato che la NSA disponga di security policy adeguate, c'è sempre il fattore umano da considerare. Non è un caso che gli attacchi mirati comincino tutti con una fase di “esplorazione” e con un'attività di spear phishing. Senza dimenticare il social engineering, che da anni permette ai professionisti dello spionaggio, governativo o industriale che sia, di carpire tasselli di informazione fondamentali.*

*Ancora una volta, dunque, si pone l'accento sulla formazione del personale e sulla diffusione di una cultura della sicurezza, perché si tenga un comportamento accorto. Il problema si complica con la diffusione crescente dei dispositivi mobili e con l'utilizzo di servizi in cloud, non sempre predisposti a una profonda sicurezza.*

*Vengono in aiuto alcuni automatismi sempre più diffusi, che consentono ai sistemi di bloccare le operazioni rischiose, come spedire via mail un file riservato, stamparlo o, appunto, copiarlo su una*

*chiavetta USB. Si tratta di soluzioni fornite dalle ultime generazioni dei sistemi per la DLP (Data Loss Prevention). Ne esistono di diverso livello, che arrivano a includere la crittografia e altre tecnologie come: sistemi di riconoscimento biometrici (a partire dalle impronte digitali), categorizzazione dei dati, sistemi automatici di riconoscimento dei dati all'interno dei file, soluzioni antimalware, sistemi OCR (Optical Character Recognition) per analizzare i testi all'interno delle immagini.*

*I sistemi DLP hanno spesso il difetto di diventare una “scocciatura” per l'utente. Se le procedure di sicurezza sono troppo stringenti, c'è il rischio che si cerchino scorciatoie. In altre parole, occorre applicare il buon senso e catalogare i dati con attenzione, in modo da proteggere quelli realmente critici ed evitare di “svalutare” le politiche di protezione applicandole a qualsiasi dato.*

*Non basta coinvolgere i dipendenti, bisogna anche convincerli, educarli anche attraverso veri e propri test: per esempio, per abituarli a riconoscere i tentativi di phishing. Magari puntando su aspetti ludici organizzando “competizioni” interne.*

*Va coinvolto anche il top management: mostrare gli attacchi bloccati e i rischi corsi, insistere sull'abilitazione di processi che senza la sicurezza non potrebbero essere attuati, serve per ottenere budget.*

# SMAU

INNOVAZIONE DI CASA  
NELLE CITTÀ ★



## SMART CITY ROADSHOW

È L'INIZIATIVA DI SMAU E ANCI DECLINATA IN CINQUE TAPPE SUL TERRITORIO ITALIANO PER VALORIZZARE E METTERE A FATTOR COMUNE LE INIZIATIVE EMERGENTI NEL NOSTRO PAESE, OGGETTO DEL TAVOLO DI LAVORO SMART CITY DELLA CABINA DI REGIA DEL GOVERNO, CHE DIVENTANO COSÌ PATRIMONIO A DISPOSIZIONE DELLA BUSINESS COMMUNITY PER COSTRUIRE LA "VIA ITALIANA ALLE CITTÀ INTELLIGENTI".

A SMAU, UN CICLO DI LABORATORI IN CUI PRESENTARE CASI DI SUCCESSO IN AMBITO SMART CITY, UN PREMIO DEDICATO, UN'AREA START UP E UN EVENTO ISTITUZIONALE PER DELINEARE LO SCENARIO DI MERCATO NAZIONALE E INTERNAZIONALE.

**MILANO**

23-24-25 OTTOBRE 2013

fieramilanocity



Smart City Roadshow porta direttamente "a casa" delle Pubbliche Amministrazioni del territorio progettualità innovative per trasformare le città in chiave Smart City. L'EVENTO È RISERVATO AGLI OPERATORI PROFESSIONALI - IMPRESE, AMMINISTRATORI PUBBLICI, MEDIA -

UN'INIZIATIVA DI

smau



www.smau.it



contact@smau.it



+39.049.8808444



CONTATTI

## Trend Micro svela la diffusione degli APT in Italia

*Da un'indagine condotta in collaborazione con IDC, emerge che il 5,5% delle aziende di grandi dimensioni in Italia ha subito un attacco APT ai propri sistemi negli ultimi 12 mesi*

Si intitola "La diffusione degli attacchi APT in Italia" lo studio sulla sicurezza IT realizzato da IDC e promosso da Trend Micro (scaricabile al seguente LINK) che delinea lo stato rispetto alla penetrazione di queste nuove minacce e al livello di consapevolezza delle aziende del segmento Enterprise sulle misure di protezione da adottare.

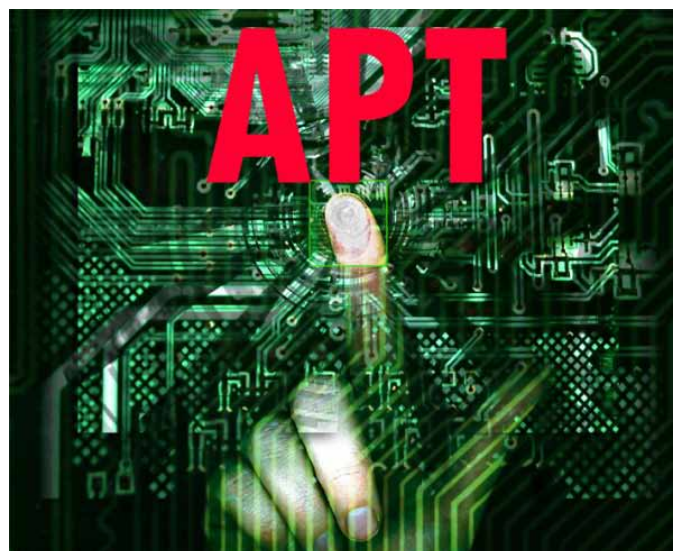
Gli APT (Advanced Persistent Threat) sono processi di attacco sofisticati che seguono schemi precisi e si compongono di una serie continua di tentativi volti a compromettere un obiettivo nel tempo.

Dallo studio emerge che il 57,4% delle aziende di grandi dimensioni in Italia ha subito un attacco occasionale ai propri sistemi negli ultimi 12 mesi. Di queste il 9,6% ha dichiarato di avere subito un attacco APT che, nel 23% dei casi, ha avuto un impatto rilevante sul business aziendale e nel restante 77% è stato neutralizzato in tempo.

Si tratta di un dato probabilmente sottostimato, perché la maggior parte delle imprese non dispone, in realtà, di un sistema di rilevazione per gli APT e, in ogni caso, com'è d'uso in questi casi, prevale la tendenza a tacere gli attacchi.

Tra gli strumenti impiegati tipicamente negli attacchi APT risaltano in modo particolare gli exploit-zero day e i malware zero-day, che coinvolgono tra il 19% e il 39% delle aziende intervistate, mentre soltanto una parte limitata del campione indica le botnet (11%) come una minaccia effettivamente presente.

Altri dati emersi dalla ricerca IDC indicano che il 94,9% delle aziende ritiene che dagli attacchi APT possano risultare im-



patti di assoluta rilevanza, il 46,3% dichiara che la propria organizzazione li teme e che la principale preoccupazione delle aziende è legata alla perdita di dati riservati o finanziari (79,4% dei casi).

L'analisi sulle misure di sicurezza che le aziende hanno adottato o pianificato a 12 mesi indica che la sicurezza IT del segmento Enterprise appare sostanzialmente affidata a tecnologie signature-based, come i firewall e gli antivirus, e le tecnologie di security intelligence risultano ancora limitatamente diffuse.

Rispetto al rischio APT prevale, invece, un atteggiamento reattivo che vede soltanto il 4,4% delle aziende scegliere l'implementazione di almeno una misura di sicurezza in seguito a un attacco APT, sebbene le aziende italiane inizino o programmino di allocare budget dedicati a contrastare queste nuove minacce: il 17% degli intervistati indica che la propria impresa sta implementando o valutando l'implementazione di specifiche misure di sicurezza per ridurre il rischio APT.

*Riccardo Florio*

## Ogni "record" compromesso costa all'azienda 136 dollari

*Il dato emerge dal "2013 Cost of Data Breach Study: Global Analysis", la ricerca commissionata da Symantec a Ponemon Institute. Più basso il costo per le aziende italiane, in media pari a 95 dollari, che sono tra quelle con il minor numero di violazioni*

I costi associati alla violazione dei dati sono elevatissimi. È uno dei principali risultati che emerge dalla versione 2013 dell'annuale ricerca commissionata da Symantec a Ponemon Institute (la ricerca che presenta i risultati per l'anno 2012 è disponibile gratuitamente a questo LINK registrandosi) che ha previsto interviste a 1444 individui che svolgono ruolo di responsabili per l'IT, la compliance o la sicurezza, all'interno di 277 organizzazioni che hanno subito perdite di dati, in 9 Paesi tra cui l'Italia.

Le violazioni dei dati sono risultate causate per il 64% (ma si supera il 70% in settori fortemente regolamentati) da errori umani e problemi di sistema. Tra i primi si annoverano la cattiva gestione dei dati da parte dei dipendenti, mancanza di controlli del sistema e violazioni di policy interne o normative, mentre i guasti di sistema includono errori delle applicazioni, eliminazione involontaria dei dati, errori nel trasferimento dei dati, fallimenti nelle operazioni di identità o autenticazione (accesso illecito), errori di recupero di dati e altro ancora.

Nel 2012 il costo associato a ogni record (informazioni personale e/o aziendale) compromesso da una violazione dei dati è aumentato rispetto all'anno precedente passando da una media di 131 a 136 dollari.

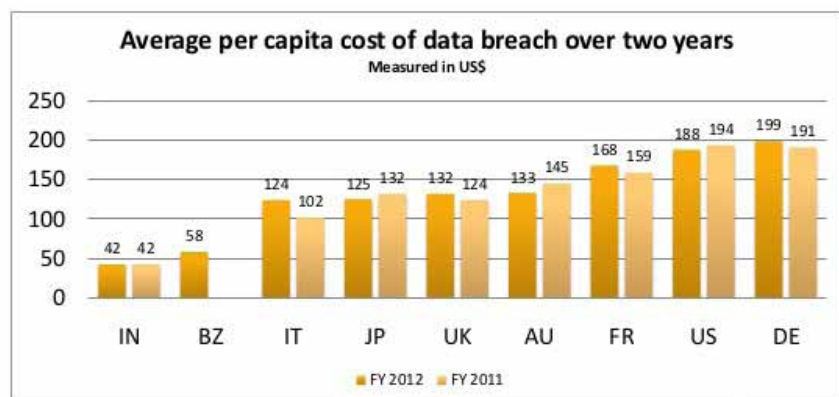
Gli Stati Uniti e la Germania detengono il primato per le violazioni dei dati più costose (rispettivamente 188 e 199 dollari per ogni record compromesso) con un costo annuale medio per azienda

stimato in 5,4 milioni dollari per gli Stati Uniti e in 4,8 milioni di dollari per la Germania. Gli attacchi di tipo criminale causano il 37% delle violazioni dei dati e rappresentano gli incidenti più costosi in tutti i nove Paesi esaminati.

### La situazione italiana

Una volta tanto siamo contenti di trovare l'Italia in fondo a una classifica. Il nostro Paese, infatti, si posiziona all'ottavo posto ovvero tra gli Stati esaminati con il minor numero di record compromessi, e una media di 18.285 record violati, anche se in aumento del 3% rispetto allo scorso anno.

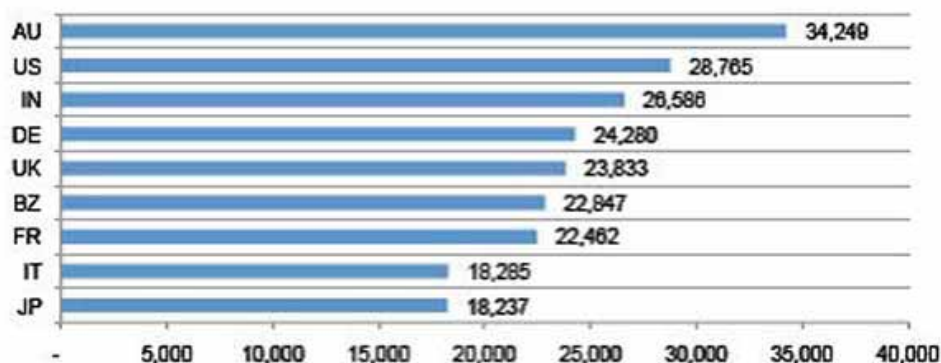
Anche il costo per le violazioni è inferiore alla media seppure



2013 Annual Study: Global Cost of a Data Breach - June 5, 2013



Costo medio per record compromesso



Numero medio di record compromessi per Paese (Fonte: Symantec-Ponemon)

in aumento del 19%: era 78 euro nel 2011 ed è stato di 95 euro nel 2012. Di questi 95 euro, circa il 36% riguarda le spese di rilevamento ed escalation, il 35% deriva dalla perdita di business e il restante 29% si divide tra spese di notifica e risposta.

La componente più rilevante dei costi legati a una violazione dei dati è associata a una perdita di business e nel 2012 il costo medio per azienda è aumentato del 51,5% arrivando alla cifra di 601mila euro. Questi costi dipendono soprattutto dal turnover dei clienti, dalla diminuzione delle opportunità di acquisizione di nuovi clienti e dalla perdita di credibilità.

È interessante notare che, nelle imprese italiane, le cause di violazione dei dati si ripartiscono in modo quasi uguale tra negligenza dei dipendenti (36%), attacchi criminali (32%) e guasto di sistema (32%).

L'indagine ha fornito anche indicazioni relative al livello di efficacia di azioni organizzative al fine di ridurre i costi dovuti alle violazioni. Tra le indicazioni fornite è emerso che:

- le aziende che avevano un piano di risposta agli incidenti hanno avuto un risparmio sui costi di 10 euro per ogni record compromesso;
- le aziende molto forti in sicurezza hanno risparmiato 9 euro per ogni record compromesso;
- le aziende che si avvalgono di un CISO con la responsabilità globale per la protezione dei dati aziendali hanno risparmiato 6 euro per ogni record compromesso;
- le aziende che si sono rivolte a un consulente esterno per gestire gli incidenti hanno avuto un risparmio di 3 euro.

Riccardo Florio

## Toolkit per creare malware per Android

È arrivato sul mercato "underground" il primo toolkit per la creazione di malware per Android. A segnalarlo è Symantec che evidenzia come il processo di commercializzazione di malware per dispositivi mobili e lo sviluppo di toolkit per la creazione di questa tipologia di software sia un segnale del rafforzamento di logiche di criminalità organizzata che dominano ormai su Internet.

L'applicazione identificata da Symantec si chiama AndroidRAT APK Binder ed è acquistabile online consentendo anche a chi ha poca esperienza tecnica di infettare facilmente applicazioni legittime per Android con malware di tipo AndroRAT, di fatto rendendole dei Trojan.

I dati raccolti da Symantec mostrano che le infezioni da AndroRAT sono in questo momento limitate, solo alcune centinaia di casi al mondo, ma in costante aumento.

Il vendor ha anche predisposto un link ([www.symantec.com/connect/blogs/remote-access-tool-takes-aim-android-apk-binder](http://www.symantec.com/connect/blogs/remote-access-tool-takes-aim-android-apk-binder)) all'interno del suo dominio in cui è possibile trovare informazioni di approfondimento del toolkit per AndroRAT disponibile sui network underground.

## Non c'è password o rete che tenga

*Due esperti di Stonesoft, tra cui un ex hacker, spiegano la potenza delle tecniche di evasione e mostrano come sia «facile» crackare password, rubare numeri di carte di credito, prendere possesso del tuo pc o togliere la corrente a una città.*

Potrete anche essere bravi a inventare una password difficilissima, ma se il vostro “vicino di sito” non lo è, allora la vostra bravura è inutile e la vostra password sarà facile preda di un hacker.

Lo afferma, prima di procedere a una dimostrazione pratica, **Olli-Pekka Niemi**, Head of the Vulnerability Analysis Group di Stonesoft, dal 2000 nell'azienda finlandese dove, tra l'altro, ha contribuito allo sviluppo dei sistemi per l'intrusion prevention. Insieme a Olli, **Otto Airamo**, Head of the Security Engine Maintenance Team di Stonesoft, ha preparato “Hack the Lab”, un ambiente in cui praticare “hacking sicuro”. Parte di questo ambiente è un sito che vende musica.

«Il problema – ci spiega Otto - è il livello di sicurezza del sito su cui, sia la password strong sia quella debole sono memorizzati. Il nostro Music Store non lo è particolarmente». Olli e Otto mostrano come possa essere relativamente semplice arrivare a “recuperare” le credenziali di accesso di un utente. Sul sito, come spesso accade nella realtà, gli username sono visibili quali nickname nelle pagine dei commenti o sui forum.

Provando a inserire uno dei nickname come username e digitando una password a caso si ottiene un messaggio d'errore, che fornisce molte informazioni a un utente esperto.

«Un sito sicuro dovrebbe semplicemente comunicare che c'è stato un errore, mentre i messaggi di frequente contengono dettagli tecnici, utili per comprendere o comunque sospettare qual è l'architettura del sistema e progettare il prossimo passaggio».

Un po' di SQL injection e si ottengono altre informazioni di sistema, utili per capire come muoversi, almeno per chi ha rudimenti di system management.

I due esperti, utilizzando software di security progettati per la gestione dei sistemi, quindi impiegabili per ragioni opposte, come “nmap”, e altri decisamente meno innocenti, ma altrettanto efficaci, mostrano come rapidamente si possa “indovinare” una password debole. Ottenute delle credenziali grazie all'ignoranza di un utente o a un suo eccesso di confidenza, diventa relativamente facile (basta lanciare un ulteriore comando) ottenere l'elenco di tutte le password, comprese quelle che, singolarmente, sarebbe stato difficile indovinare.

### Criptare o non criptare?

«Anche se le password fossero crittografate, possiamo scaricarle sul nostro pc e decifrarle», minimizza Otto, passando a una dimostrazione pratica e “crackando” in un solo



Olli-Pekka Niemi di Stonesoft

minuto oltre 4mila password.

Come se non bastasse, dichiara: «In realtà, per un hacker è facile utilizzare una botnet e disporre di grandi capacità di calcolo, impiegando pochi secondi per crackare potenzialmente centinaia di migliaia o milioni di dati».

Un aspetto impressionante è la rapidità con cui operano i toolkit di hacking. Si tratta, infatti di software molto efficienti. Per quanto gli ambienti su cui operavano i due esperti fossero preparati, in realtà i sistemi adoperati erano semplici pc, con potenza di calcolo neanche eccessiva. Questo non significa che la crittografia sia inutile, ma che è necessario incrementare il livello della stessa: quanti più bit sono utilizzati per la codifica, tanti più FLOPS (Floating Point Operations per Second) sono necessari per il cracking. Un anno fa, è stato calcolato che un supercomputer da 10,51 Petaflops, considerato il più potente realizzato fino ad allora, avrebbe impiegato un miliardo di miliardi di anni a decriptare un algoritmo AES (Advanced Encryption Standard) a 128 bit.

Con una cifratura meno potente dell'AES, rischiano di essere pochi anche 128 bit e, comunque, già pochi mesi dopo è stato messo a punto un supercomputer ancora più potente. È difficile stabilire quali potenze possano raggiungere i cluster raggruppabili dagli hacker, ma certamente, sarà una continua rincorsa tra buoni o cattivi e, quantomeno, la crittografia può alzare la barriera d'ingresso e rendere più alto il costo operativo dell'attacco.

## Hacker alla ricerca del ROI

Alzare il livello di protezione aziendale è funzionale proprio per rendere meno conveniente un attacco. Anche gli hacker, infatti, devono ricercare un valido ritorno dagli investimenti. Oggi si trovano a buon mercato diversi tool e servizi di hacking online, ma è comunque un mercato, con le sue leggi legate al profitto.

Anche nell'attacco ipotizzato da Otto e Olli, le password

sono solo un obiettivo intermedio, perché di per se stesse poco interessanti, a meno che non si cercassero specifiche credenziali per

penetrare in un qualche determinato sistema (come vedremo più avanti). Sul sito di musica, però, sono memorizzati i numeri di carta di credito, per accelerare gli acquisti successivi senza dover richiedere i dati. Questi sono gli obiettivi finali di questa prima dimostrazione, che è sembrato veramente semplice ottenere e che a questo punto possono essere utilizzati per commettere frodi, magari clonando le carte, o «semplicemente» essere venduti sul Web a prezzi variabili.

Il valore di questi dati, infatti, cambia in base a diversi fattori, a cominciare dalla data (quanto più è vecchia una carta, tanto più è probabile che sia inutilizzabile) per finire al profilo del proprietario.

In effetti, il mercato online delle "virtual credit card" (VCC) è fiorente. Youtube è pieno di video pubblicitari al riguardo. Olli ce ne mostra uno convincente, che indica anche un link dove acquistare le VCC, pagandole comodamente con carta di credito.

È certo che in molti hanno usato il servizio, senza rendersi conto del paradosso. Addirittura, due anni fa è stato chiuso un sito intermediario per i pagamenti online, dopo che aveva denunciato di aver subito un furto di dati, ma soprattutto dopo aver scoperto che il titolare del sito era un hacker.



*Otto Airamo di Stonesoft*

## Al centro del mirino

Per fortuna, non tutti i siti di e-commerce sono sprovvisti. Per non parlare di altre organizzazioni che pure devono garantire la sicurezza dei dati relativi alla carte di credito. Eppure, vedi Sony, ci sono casi di attacchi andati a buon fine (chiaramente dal punto di vista dell'attaccante).

Sono attacchi mirati che, secondo Stonesoft, sono stati possibili grazie alle cosiddette tecniche di «evasione». Ma questa è una fase successiva.

Come racconta Otto, gli attacchi consistono in più fasi: selezionare il target, effettuare una ricognizione per trovare informazioni utili, realizzare un assessment dei sistemi, condurre l'exploit, sfruttare la vulnerabilità e praticare eventuali passaggi per raggiungere gli obiettivi, compiere ulteriori attacchi.

Il tipico primo passo è recuperare informazioni, accedendo al computer di qualche impiegato. Per questo si comincia a inviare di una mail. Nella demo preparata dagli esperti di Stonesoft, una mail mandata dal Ceo di un'azienda a tutti i dipendenti. Mascherare l'indirizzo reale è facile, così come è facile che venga aperto un messaggio del capo.

Se il messaggio contiene un file chiamato "premi sugli obiettivi", come quello pensato dai nostri esperti il click è altamente probabile.

Il pdf in allegato non si apre, magari dà un messaggio d'errore, comunque subito dopo arriva un secondo messaggio con delle scuse e un allegato che questa volta funziona.

Peccato che il primo file conteneva in realtà un comando con il quale l'hacker può ottenere quello che vuole: per esempio, spiare attraverso la webcam, come hanno fatto Otto e Olli, ma anche prendere il controllo del pc, recuperare credenziali di accesso e passare alla fase successiva.

I due esperti sottolineano che questa procedura può essere realizzata in maniera relativamente facile ed essere usata anche nel "privato", per esempio da uno stalker.

## Tecniche di evasione: non c'è IPS che tenga

Al centro degli attacchi ci sono gli exploit, cioè l'uso di malware per sfruttare le vulnerabilità dei sistemi. Periodicamente i produttori di software pubblicano le cosiddette patch, le "toppe" che consentono di tappare i banchi dei propri sistemi.

Evidentemente, per farlo rivelano la vulnerabilità e gli hacker, ammesso che già non la conoscessero possono sferrare quelli che sono noti come "0 day attack", dove il giorno 0 è proprio quello in cui viene resa nota la vulnerabilità. Per farlo scaricano codici maligni sui sistemi aziendali del target.

C'è però un ostacolo: i sistemi di intrusion prevention (IPS), che sono stati progettati per riconoscere il traffico sospetto e rilevare le intrusioni.

Qui, ci spiegano Otto e Olli, entrano in gioco le tecniche di evasione: «In pratica, consistono "nell'offuscare" il contenuto nocivo, per esempio invertendo l'ordine dei pacchetti trasmessi. Ne esistono di diversi tipi, ma nessun IPS è in grado di rilevarle tutte, anche perché ne esistono a centinaia».

Il fatto è che le evasion technics mascherano il traffico facendolo apparire come pacchetti errati. «Un IPS dovrebbe essere configurato per bloccare tutto quello che non capisce, cosa che potrebbe portare disservizi e normalmente viene sconsigliata», aggiunge Olli.

Francesco Armando, responsabile della tecnologia in Stonesoft Italia, evidenzia che sono stati testati e superati tutti i principali IPS. In particolare, Stonesoft dispone di un tool con il quale permette alle imprese di verificare la propria "resistenza" alle tecniche di evasione.

## Cyber War e cyber terrorismo

Per concludere, Otto e Olli hanno preparato una simulazione di attacco terroristico (o un'azione di Cyber War, visto che il

confine tra le due definizioni è prettamente etico), mostrando quanto potrebbe essere semplice bloccare una centrale elettrica e togliere la corrente a un'intera città.

Basta un minimo di competenza, i tool software giusti, peraltro facilmente reperibili, e una buona dose di pazienza. L'obiettivo è arrivare alla console di gestione della rete elettrica.

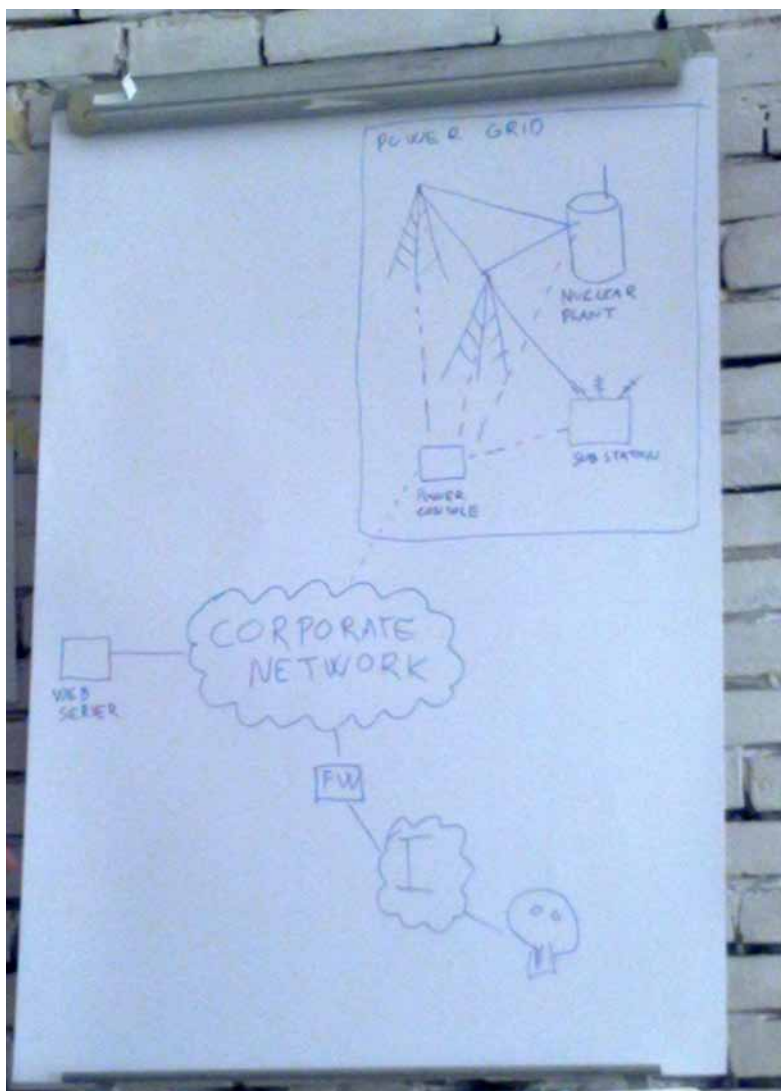
Chiaramente, le policy di sicurezza prevedono che questa, come in tutte le infrastrutture critiche si trovi su una rete isolata. Ma un perfetto isolamento è difficile da realizzare e spesso manca la reale volontà di farlo.

Per esempio, si domanda Otto, com'è

che esiste un'app per iPhone che consente di controllare una rete SCADA da remoto?

Le reti elettriche hanno poi cabine dappertutto, l'unica soluzione, sostiene Otto è una sicurezza dinamica.

Le fasi e le tecniche usate sono in buona parte quelle già viste. Si comincia a fare un po' di ricognizione e si scopre sul sito della compagnia elettrica che vengono cercati



ingegneri con alcune competenze tecniche. È normale segnalare questi dettagli, per fare una preselezione. Ma così facendo si forniscono informazioni preziose sui sistemi installati in azienda. Altre informazioni sono invece contenute nei metadati dei pdf pubblicati sul sito.

Proseguendo con la ricognizione e recuperando dettagli sui sistemi operativi, i protocolli e su altre risorse, i nostri "attacker" arrivano a identificare la vulnerabilità giusta su cui effettuare un exploit, aiutandosi con le tecniche di evasione prima descritte.

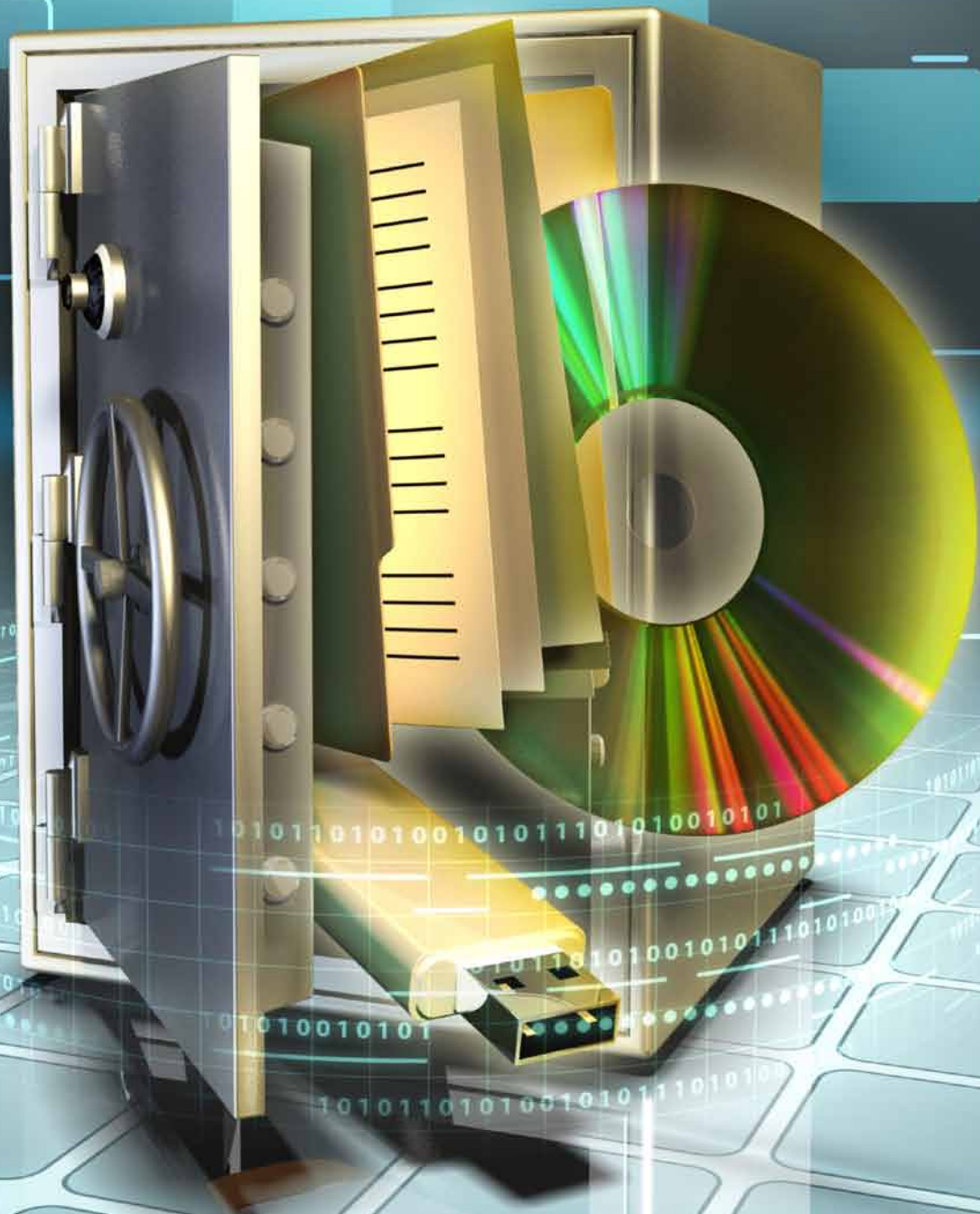
»Una volta dentro – ci rivela Otto –, la visibilità del sistema è tutta

un'altra e arrivare alla power console non è difficile. Poi si aprono diversi scenari di attacco.

Nella simulazione preparata, i nostri hacker prendono possesso prima di un Web server, che era collegato alla rete centrale e poco protetto, essendo giudicato influente. Eppure da un sistema come quello si può riuscire ad arrivare alla console e spegnere la città.

# IL REPORT ICT SECURITY

Soluzioni, tecnologie e servizi per un'efficace protezione degli asset aziendali



**Clicca QUI per la versione più approfondita del report**

È in atto la cosiddetta “business transformation”, che ridefinisce 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, mentre il video ad alta definizione sta cambiando il modo di relazionarsi, riducendo gli spostamenti o permettendo servizi di nuovo tipo.

In questo scenario il tema della sicurezza sta assumendo un'importanza crescente e, in particolare, in un contesto di progressiva convergenza dei servizi di rete sul protocollo IP, quello della network security rappresenta un tema critico.

### **La protezione della rete tra DDoS e Next Generation IPS**

Tra gli ambiti emersi che si sono dimostrati recentemente come i più critici nell'ambito della network security vi sono 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”.

I DDoS, in estrema sintesi, consistono nel “bombardare” un servizio Web con grandi volumi di traffico, fino a metterlo in tilt. Sono diventati noti perché strumento preferito per le azioni dimostrative dei gruppi Anonymous, che hanno avuto

una grande eco mediatica. Negli ultimi dieci anni, gli attacchi DDoS si sono moltiplicati, allargando gli ambiti di impiego e diventando un problema particolarmente serio per le Telco e i service provider.

Crescono, per esempio, gli attacchi mirati di sabotaggio che riguardano soprattutto il mondo aziendale in molti ambiti, dal gaming online al commercio elettronico dove la mancanza di servizio equivale a una temporanea chiusura dell'azienda.

Un altro grande problema per la sicurezza aziendale è costituito dagli attacchi APT (Advanced Persistent Threat), attacchi mirati, costituiti da più fasi, ciascuna condotta con più tecniche di cui almeno una prevede la violazione del sistema, che significa un'intrusione. Gli IPS tradizionali, concentrati sul traffico di rete, possono non essere in grado di rilevare questo tipo di intrusioni così come, allo stesso modo, i firewall di prima concezione non possono contrastare la sofisticazione dei malware più recenti.

Le aziende stanno correndo ai ripari, rilasciando soluzioni cosiddette di “next generation”. Un termine che non trova omogeneità di definizione tra le proposte dei diversi vendor, ma che sottolinea perlomeno l'attenzione a livello applicativo, è l'impiego di meccanismi di analisi e di test statici e dinamici per garantire sviluppo sicuro e identificare, classificare e bloccare il malware senza creare rischi per le aziende. L'analisi del traffico e la scansione della rete sono sempre più necessarie, ma è importante anche predisporre una sicurezza “dinamica” basata su strumenti costantemente ag-

giornati, in grado di analizzare la posta elettronica, le applicazioni, il traffico Web.

Anche il cloud viene incontro a queste esigenze, attraverso offerte di Security as a Service, evoluzione delle tradizionali offerte di Managed Security Service, che consentono di scalare e anche personalizzare, entro certi limiti, i servizi portando anche alle piccola e media impresa un livello di protezione in precedenza economicamente non abbordabile.

### La sicurezza è "mobile"

Un altro aspetto di importanza rilevante nel contesto della sicurezza riguarda i nuovi modelli di lavoro in mobilità che rappresentano lo step finale di quel processo di allargamento del perimetro aziendale cominciato con l'avvento di Internet. La mobilità ha rimosso gli ultimi limiti in termini di spazio e tempo non solo per l'azienda, ma anche per i suoi clienti e fornitori.

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'ambito 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 che raggiungerà, entro la fine del 2013, 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 svilup-

po tecnologico sta rendendo tutto più rapido portando il numero di minacce a crescere costantemente sia in numero sia in pericolosità.

### I rischi del BYOD

Un terzo fondamentale aspetto riguarda le modalità di utilizzo dei dispositivi mobili. È ormai entrata nello slang comune la sigla BYOD che porta con sé i rischi legati un uso promiscuo, personale e aziendale, di dispositivi informatici.

Se le soluzioni software per la protezione degli endpoint hanno messo a disposizione una protezione efficace per evitare di portare all'interno della rete aziendale malware contratti all'esterno, 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. Non è poi insolito l'uso di software o di servizi online (per esempio Dropbox) 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.

## Security as a Service e cloud

Un altro aspetto determinante nel nuovo scenario della sicurezza è quello legato alla crescente diffusione dell'utilizzo di risorse IT sotto forma di servizio o nel cloud. Tra queste vi è anche l'interesse per la Security as a Service che può prevedere sia il demandare in toto gli aspetti inerenti la sicurezza al provider su cloud sia farlo in modo parziale o limitato nel tempo, alimentata 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.

Ai service provider specializzati nel fornire soluzioni di sicurezza a livello applicativo e infrastrutturale e in grado di proteggere i dati sia quando vengono trasmessi o fruiti dalle applicazioni sia quando sono memorizzati in silos informativi o elaborate dai server andrebbero perlomeno richiesti tre requisiti critici.

Il primo è la disponibilità di policy, procedure e standard da adottare e cioè la possibilità di acquistare oltre ai servizi software anche le capacità umane indispensabili per disporre del fondamentale supporto nello sviluppare i servizi necessari sulla base della specificità aziendale, a partire da un'approfondita valutazione delle policy esistenti e della loro efficacia.

Il secondo è 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.

L'ultimo è di fornire adeguati servizi di Security Services Management che permettano di fondere in un unico insie-

me 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 conformità normativa

Strettamente connesso alla sicurezza dei dati nel cloud vi è il tema delle diverse normative delle varie nazioni in cui questi dati possono venirsi a trovare memorizzati fisicamente, che possono essere anche molto differenti tra loro. Per esempio la normativa derivante dall'attuazione del USA PATRIOT ACT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act) del 26 ottobre 2001, prorogato fino a giugno 2015, rende in sostanza obbligatorio per le società statunitensi, nonché per le loro controllate a livello globale, per gli hosting provider americani o hosting provider europei affiliati a società statunitensi, di consentire l'accesso a ogni dato personale da parte delle agenzie di intelligence degli Stati Uniti. In particolare la sezione 215 del Patriot Act e le sezioni 504, 505 e 358 autorizzerebbero le ricerche sia sotto la supervisione di un giudice sia senza. Le disposizioni del Patriot Act risulterebbero incompatibili con la tutela e gli obblighi di riservatezza dell'Unione Europea che ha promulgato leggi per la protezione dei dati personali.

Tra queste la direttiva 95/46/CE del Parlamento e del Consiglio europeo del 24 ottobre 1995, che richiama i principi secondo i quali i sistemi di elaborazione dei dati sono stati sviluppati per servire l'uomo e devono, a prescindere dalla nazionalità e dal luogo di residenza delle persone fisiche, rispettarne la libertà e i diritti fondamentali, in particolare il diritto alla privacy.

# L'EVOLUZIONE DELLA SICUREZZA CHECK POINT

*Un'innovazione dell'offerta e dell'architettura 3D Security che si fonda su nuove tecnologie di threat prevention, prestazioni elevate, security management e mobility*

La strategia e le soluzioni di Check Point Software Technologies continuano a evolvere, puntando all'innovazione. Un'innovazione necessaria che si fonda su quattro pilastri: piattaforme e performance; security management; nuove tecnologie di sicurezza, mobility e dati.

Innovazioni che occorrono per garantire il supporto del business, attraverso la visione Check Point 3D Security, per la quale la sicurezza va considerata quale un processo aziendale come altri. Un processo che parte dalle regole aziendali, coinvolge le persone e si appoggia alla tecnologia che aiuta le persone a rispettare le regole. Gli aggiornamenti più importanti nell'ultimo anno riguardano innanzitutto le piattaforme, che sono state unificate in termini di gestione. Oggi tutte le appliance sono prodotte da Check Point e dispongono di un sistema operativo unificato a partire dalla versione R75.40 del software di Check Point per la sicurezza (oggi alla R76). Tra gli ultimi sistemi presentati, le appliance Check Point 600 e 1100 per le piccole e medie imprese ingegnerizzate. Oltre a queste vanno ricordati i recenti sistemi Check Point 21700 e quelli della serie 13500. Inoltre, la casa israeliana ha aumentato di 3 volte le prestazioni dei sistemi, anche grazie al security accelerator module. Per fornire una visibilità completa e il pieno controllo sull'infrastruttura di sicurezza, Check Point ha unificato la propria piattaforma di security management, che gestisce, dalla stessa console, sia il gateway per la network security sia qualsiasi endpoint. Gestire tutti i sistemi in modo unificato risponde anche al bisogno di collaborazione, necessario per identificare le minacce. Per Check Point la collaborazione "locale", cioè l'integrazione tra i diversi sistemi è altrettanto fondamentale di

quella estesa a tutti i clienti, che consiste nella condivisione delle informazioni raccolte da tutti i sistemi Check Point installati nel mondo, insieme a tutti i dati registrati dalle sonde Check Point e derivanti dalle analisi dei 3D Report, che, senza alterare o modificare in alcun modo l'infrastruttura di un'impresa, ne analizza lo stato della sicurezza. Si ottiene una mole di dati che, attraverso la piattaforma ThreatCloud, aumenta l'intelligenza della sicurezza targata Check Point.

Check Point ha rilasciato una serie di nuove tecnologie che rispondono alle esigenze più sentite nell'ambito della protezione dalle minacce. Tra queste ricordiamo le appliance per rispondere agli attacchi DDoS e la Threat Emulation Software Blade, che integra una tecnologia di sandboxing per emulare il funzionamento dei file che "entrano" nell'infrastruttura aziendale e fronteggiare le minacce APT. Per supportare le strategie BYOD, Check Point ha sviluppato un'App, che è di fatto una bolla applicativa "aziendale", contenente un programma di posta, un'agenda, una rubrica e link a una intranet. Il tutto è completamente separato dal mondo circostante, quindi l'iOS o il sistema Android che rimangono per uso personale. In base alle policy si possono sincronizzare più o meno i due mondi. Quando si chiude l'App viene tutto automaticamente cancellato, oppure, sempre in base alle regole predeterminate, qualcosa viene lasciato in cache. L'App comunica con i sistemi aziendali attraverso un canale criptato VPN. Lo strumento Document Security consente di crittografare il singolo file rendendolo sicuro durante i trasferimenti, ma anche leggibile esclusivamente dallo specifico utente cui è indirizzato, sia che si tratti di un collega aziendale sia egli un esterno.

# FORTINET SPINGE SU PRESTAZIONI E MOBILE

*Tra le principali novità proposte dal vendor vi è FortiOS 5.0, il supporto del BYOD e la protezione dalle APT, sfruttando anche il cloud, con una strategia costantemente rivolta a coniugare protezione ed elevate performance*

Fortinet si mantiene fedele alla propria "mission" sin dalla fondazione: coniugare sicurezza e prestazioni. Questo avviene attraverso dispositivi di ultima generazione che combinano più soluzioni, grazie a un sistema operativo per la sicurezza, e che sfruttano la potenza di circuiti ASIC dedicati.

FortiOS 5.0 consolida i numerosi sviluppi realizzati negli ultimi anni a partire dalla versione 4.0 e le 150 nuove feature sono "solo" aggiunte necessarie. È quanto dichiarato dai responsabili di Fortinet nel presentare l'ultima versione del sistema operativo per i sistemi di sicurezza Fortinet, specificando che le aggiunte indirizzano tre aree: la protezione dalle minacce avanzate di nuova generazione, la sicurezza dei dispositivi mobili in risposta al fenomeno del BYOD (Bring Your Own Device) e una gestione "intelligente" delle security policy e della reportistica.

Scendendo un po' più in dettaglio, il nuovo software di sicurezza aggiunge alle appliance Fortinet capacità avanzate d'identificazione e gestione del comportamento di utenti e dispositivi, inclusi criteri basati sulla reputation, cioè lo stato di sicurezza del dispositivo rispetto alle attività che l'utente effettua. Inoltre, la soluzione si avvale di un nuovo sistema di rilevamento malware (in grado di ispezionare il traffico crittografato), che comprende un motore euristico, basato sul comportamento, sul dispositivo e servizi antivirus basati su cloud, inclusi una sandbox del sistema operativo e un database della IP reputation dei botnet. Il collegamento ai servizi cloud permette di anticipare le minacce, osservando in tempo reale gli eventi sulla Rete mondiale, evidenzia la società, specificando che il sistema applica il profilo adeguato per dispositivo/utente, il tutto in maniera trasparente per

l'utente stesso che non deve fare nulla. Tra le altre novità più recenti, la soluzione Fortinet Secure WLAN fornisce security policy end-to-end, unificando accesso, sicurezza, autenticazione, switching e network management per reti cablate e reti Wireless LAN a vantaggio soprattutto delle imprese distribuite. Parte della soluzione sono i nuovi prodotti per reti cablate e wireless presentati da Fortinet: gli switch Ethernet FortiSwitch-28C e FortiSwitch-348B e gli access point wireless FortiAP-14C e FortiAP-28C. Altro recente aggiornamento dell'offerta è rappresentato dalla famiglia FortiWeb: una serie di appliance firewall per applicazioni Web e XML, che proteggono, bilanciano e accelerano i servizi Web e i database e lo scambio di informazioni tra essi stessi. I sistemi FortiWeb possono ridurre i tempi d'implementazione e le complessità derivanti dall'introduzione e la protezione di applicazioni basate su Web. La ricerca sulle minacce di Fortinet è alla base di tale protezione, migliorando la sicurezza delle informazioni confidenziali e aiutando il mantenimento delle normative, compresa la PCI compliance. Le soluzioni si spingono oltre le funzionalità dei tradizionali Web application firewall, per fornire l'enforcement della sicurezza XML, l'accelerazione delle applicazioni e il server load balancing. Con la versione del sistema operativo FortiWeb 5, compatibile con le appliance precedenti, Fortinet ha introdotto nuove funzionalità con miglioramenti alla sicurezza, inclusa la capacità di identificare in modo accurato l'origine del traffico delle applicazioni Web, per distinguere le fonti legittime da quelle dannose. FortiWeb consente di individuare le richieste legittime dei più noti motori di ricerca, scanner, crawler e altri strumenti basati su soglie.

# LA SICUREZZA INTEGRATA DI HP ESP

*Attraverso la divisione Enterprise Security Product il vendor propone un approccio unificato che riunisce protezione della rete, dei dati, delle transazioni e sviluppo applicativo sicuro*

Per poter affrontare le nuove esigenze di protezione, HP punta a predisporre una strategia complessiva per la gestione del rischio, ponendo le basi per un approccio unificato alla sicurezza enterprise.

Attraverso la divisione Enterprise Security Product (ESP) HP propone i sistemi per prevenire possibili intrusioni (IPS) HP TippingPoint, le soluzioni di 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.

La piattaforma di nuova generazione NGIPS HP TippingPoint, elemento centrale dell'offerta HP per la sicurezza dell'infrastruttura di rete e del data center, permette di filtrare il traffico in ingresso e in uscita sulla rete aziendale, di bloccare i contenuti nocivi e di identificare comportamenti pericolosi o tentate violazioni di policy. Rispetto ai sistemi di Intrusion Detection che provvedono solo a rilevare il traffico indesiderato senza bloccarlo, le soluzioni IPS HP TippingPoint individuano le vulnerabilità presenti sulla rete e intervengono applicando delle "patch" virtuali che ne impediscono lo sfruttamento. Le gamma di soluzioni HP TippingPoint include anche HP Core Controller che estende la protezione IPS basata su tecnologia TippingPoint ai collegamenti a 10 Gbps grazie a 48 porte 1000Base-T e 6 porte 10GbE. Alle esigenze di sicurezza delle infrastrutture data center virtualizzate e del cloud HP ha indirizzato TippingPoint CloudArmour, una combinazione di prodotti progettati per controllare e proteggere il traffico di macchine virtuali all'interno di server host fisici, offrendo piena capacità IPS, che prevede i seguenti componenti: la piattaforma fisica NGIPS, le soluzioni software virtual

Controller (vController), virtual Management Center (vMC) e virtual Firewall (vFW). Con l'appliance TippingPoint SMS HP fornisce una vista globale e la possibilità di amministrazione, configurazione, monitoraggio e reporting nelle situazioni di implementazioni su larga scala di molteplici IPS. Attraverso la piattaforma HP ArcSight il vendor mette a disposizione una suite integrata di prodotti di Security Information e di Event Management (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). La sicurezza applicativa è affrontata attraverso la piattaforma di Security Intelligence and Risk Management HP Fortify. Tra le soluzioni disponibili vi è la Suite HP Fortify Software Security Center che automatizza e gestisce la sicurezza applicativa, mettendo le aziende in grado di testare la sicurezza delle applicazioni e di identificare le vulnerabilità, sia in modalità on-premises sia on-demand. HP Fortify Static Code Analyzer rende sicuro il codice legacy e impedisce di rilasciare sul mercato software insicuro integrando la sicurezza nel software mentre questo viene sviluppato. L'analisi del codice software è disponibile anche in modalità Software as a Service attraverso il servizio HP Fortify on Demand (FoD). Tra le soluzioni di sicurezza di HP ESP figura anche HP Atalla per la sicurezza di pagamenti e transazioni elettroniche, che coniuga il modulo di crittografia hardware HP Atalla Network Security Processor con il sistema sicuro di gestione delle chiavi HP Enterprise Secure Key Manager per garantire una protezione della rete end-to-end, trasparente per l'utente e ad elevate prestazioni.



# LA SICUREZZA «INTELLIGENTE» DI IBM

*Soluzioni e servizi incentrati su strumenti e tecnologie di security intelligence consentono di adottare un approccio integrato che abilita il business nell'era dell'Internet of Things*

Un pianeta sempre più interconnesso, in cui, grazie a Internet aumentano sempre più dispositivi e sensori, reti e sistemi per l'intrattenimento e per il business. Un mondo in cui la sicurezza è necessaria e per la quale IBM ha adottato un'approccio a 360 gradi basato sul concetto di "security intelligence". Guidata dalla piattaforma QRadar, ma supportata da un portfolio molto ampio di soluzioni e servizi, la visione di IBM coniuga esperienze di IT con competenze specifiche sugli aspetti di architettura e di processo. Visibilità, accountability, correlazione degli eventi sono tre dei principali risultati ottenuti dalla piattaforma QRadar, che si riflettono in diversi aspetti della sicurezza. Gli ambiti nei quali si sono concentrate le novità principali di IBM Security sono il cloud, la mobility e i Big Data.

Multiplo l'impegno verso la Cloud Security. In primo luogo. 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: dalla network security alla difesa dell'application server, solo per citare due degli ambiti principali. Il secondo aspetto riguarda le soluzioni stesse di IBM Security Systems, a disposizione di Managed Service Provider interessati a offrire servizi di sicurezza. Infine, la divisione IBM Security Service, attraverso i dieci SOC (Security Operation Center) nel mondo, fornisce servizi gestiti di sicurezza in cloud.

Tra le ultime novità il servizio SIEM, anch'esso basato sulla security intelligence, l'Emergency Response Service (un servizio di consulenza per rispondere agli incidenti) e il servizio di supporto nella realizzazione di un SOC, che può essere in house o ibrido, cioè in parte "appoggiato" ai SOC di IBM.

Per la sicurezza degli ambienti mobili, IBM ha messo a punto un Mobility Framework, che comprende diverse soluzioni per la gestione dei dispositivi, come IBM Endpoint Manager for Mobile oppure IBM Security Access Manager for Mobile (disponibile anche in versione hosted SaaS), che protegge gli accessi alle risorse autenticando gli utenti mobili e i loro dispositivi. Un approccio integrato che comprende anche la sicurezza delle comunicazioni e delle applicazioni, con IBM Mobile Connect e IBM Worklight, che, tra l'altro, fornisce strumenti per consentire agli sviluppatori di crittografare i dati applicativi. A questo si aggiunge Security AppScan, che fornisce una soluzione per la sicurezza dello sviluppo applicativo, consentendo, per esempio di integrare i test della sicurezza delle applicazioni mobili in tutto il ciclo di vita dell'applicazione. IBM ha definito un approccio che permette alle aziende di avvalersi delle funzionalità di analisi dei Big Data per prevenire e rilevare sia le minacce esterne sia i rischi interni. Questa soluzione unisce funzionalità di correlazione in tempo reale, che consentono di realizzare con continuità analisi in profondità (i cosiddetti "insight"), con funzionalità di Business Analytics personalizzate e applicabili a enormi quantità di dati. A questo si aggiungono funzionalità "forensic". Realizzato nei laboratori IBM, IBM Security Intelligence with Big Data unisce le funzionalità di correlazione della sicurezza e di rilevamento delle anomalie in tempo reale della piattaforma IBM QRadar, all'analisi personalizzata di grandi quantità di dati fornita da IBM InfoSphere BigInsights.

Il risultato è una soluzione integrata, che comprende monitoraggio e avvisi intelligenti delle minacce e dei rischi, per analizzare ed esplorare dati di sicurezza in modo innovativo.

# CONNESSIONE SICURA E INTEGRATA DA MCAFEE

*Una strategia che si fonda sull'architettura di riferimento Security Connected per realizzare l'integrazione di più prodotti, servizi e partnership con un controllo centralizzato*

McAfee (società controllata da Intel) è da sempre dedicata alle tecnologie per la sicurezza. Le soluzioni McAfee sono progettate per funzionare insieme e integrano i software di protezione antimalware, antispyware e antivirus con funzionalità di gestione della sicurezza che forniscono visibilità e capacità di analisi in tempo reale, favoriscono il rispetto della compliance e aumentano la protezione Internet.

Le tecnologie di protezione basate sulla reputazione e sul comportamento di McAfee si integrano con una capacità preventiva basata sulle informazioni provenienti dal cloud e raccolte da McAfee Global Threat Intelligence, per proteggere utenti privati e aziende contro le cyber minacce su tutti i vettori: file, Web, messaggi e rete. Elemento cardine della strategia McAfee è l'architettura di riferimento Security Connected che consente l'integrazione di più prodotti, servizi e partnership per una mitigazione dei rischi centralizzata ed efficace. Il framework Security Connected fornisce uno schema di modelli per l'implementazione in grado di adattarsi ai rischi, all'infrastruttura e agli obiettivi che caratterizzano le diverse aziende. McAfee Security Connected copre tutte le funzioni basilari, le tecnologie rinforzate dall'hardware, il white listing dinamico, la scansione intelligente, l'antimalware avanzato, la protezione mobile e altro ancora.

I prodotti e le soluzioni per la sicurezza McAfee intervengono in tutte le principali aree, dalla protezione e-mail e Web, alla sicurezza del database, agli ambienti mobili fino alle soluzioni di Security Information and Event Management (SIEM).

McAfee Security Management fornisce un approccio a 360 gradi alla gestione della sicurezza aziendale e rappresenta il fulcro del framework Security Connected, fornendo l'integra-

zione completa tra i software McAfee ePolicy Orchestrator (che fornisce la gestione unificata di endpoint, rete e sicurezza dei dati), Risk Advisor e le soluzioni McAfee Endpoint. Alla protezione degli endpoint McAfee dedica le suite Complete Endpoint Protection disponibili nelle versioni Enterprise e Business a cui si aggiungono Endpoint Protection-Advanced Suite e Protection Suite, che forniscono una protezione approfondita contro tutto lo spettro delle minacce, dagli exploit zero-day, ai rootkit, alla minacce avanzate persistenti (APT), proteggendo i sistemi Windows, Mac e Linux, oltre che i dispositivi mobili come iPhone, iPad, gli smartphone Android e i tablet. Il tutto attraverso un'unica piattaforma estensibile di gestione della sicurezza. Il vendor fornisce protezione degli endpoint anche in modalità cloud (SaaS Endpoint Protection Suite).

Con le soluzioni Enterprise Mobility Management e Virus-Scan Mobile, McAfee fornisce protezione contro la perdita dei dati conservati sui dispositivi mobili e contro le minacce a smartphone e tablet. Enterprise Mobility Management applica ai dispositivi mobili lo stesso livello di sicurezza e controllo che l'IT applica a laptop e desktop, includendo la capacità di identificare, marcare e assegnare le policy agli apparati di proprietà dei dipendenti o dell'azienda. Le soluzioni per la sicurezza della rete di McAfee si avvalgono delle soluzioni Next Generation Firewall derivanti dalla recente acquisizione di Stonesoft. McAfee dispone anche di un'offerta di sicurezza in forma di servizio erogato direttamente dal cloud su endpoint, e-mail, Web e sulla rete. L'offerta SaaS di McAfee comprende i servizi SaaS Email Encryption, SaaS Email Archiving e SaaS Email Protection and Continuity.

# LA SICUREZZA «AGILE» DI SOURCEFIRE

*Next Generation IPS, Next Generation Firewall e protezione dal malware avanzato sono supportati da un'innovativa tecnologia di passive scanning che conferisce piena visibilità dell'intero ambiente aziendale*

Martin Roesch, il creatore di Snort, ha fondato Sourcefire e insieme ai suoi dirigenti la guida seguendo l'Agile Security Manifesto, secondo il quale bisogna smettere di considerare la sicurezza un problema da risolvere. È una realtà con cui confrontarsi se si vuole sfruttare la tecnologia e l'innovazione per il business.

Poiché gli ambienti e gli scenari in cui sono calati sono troppo mutevoli, l'unico approccio valido è quello appunto "agile". Il primo principio dell'Agile Manifesto, non a caso recita: "Essere più adattativo dei tuoi avversari". Facile a dirsi e a farsi secondo Sourcefire, grazie soprattutto a FireSight, una tecnologia di passive scanning, che consente di ottenere una vista accurata, fino a livello utente, dell'intero ambiente aziendale, aggiornata in tempo reale.

Tre le aree in cui si concentrano le soluzioni di Sourcefire, che sfruttano appunto la potenza di FireSight e del sistema di gestione FireSight Defence Center, grazie ai quali si ottiene una piena contestualizzazione dei dati di sicurezza e si può applicare l'approccio "See Learn Adapt Act". La visibilità completa dello stato architetturale e di quello che avviene sulla rete e alle applicazioni è la base per poter prendere decisioni e agire. Learn, imparare, significa comprendere e valutare i rischi applicando la security intelligence ai dati. Visibilità e comprensione permettono quindi di "adattare" le difese automaticamente e di "agire" in tempo reale.

Pure importanti per l'architettura della sicurezza targata Sourcefire è il supporto del team VRT (Vulnerability Research Team), che contribuisce allo sviluppo delle regole di Snort, ma non solo. Snort è ancora il motore alla base dell'IPS di Sourcefire, che ne sfrutta l'apertura al mondo open source.

Integrando l'attenzione al contesto con l'automazione guidata dalla security intelligence, i Next Generation IPS (NGIPS) di Sourcefire sfruttano le prestazioni delle appliance per fornire protezione efficace dalle minacce.

La funzionalità di application control e di URL filtering permette di mitigare i rischi legati a questo mezzo di penetrazione sempre più utilizzato per evitare i sistemi IPS tradizionali. L'NGIPS è inoltre sempre attento al contesto, grazie a FireSight e può immediatamente rilevare discrepanze rispetto ai valori di riferimento. Al verificarsi di un'anomalia intervergono le regole che sono molto flessibili per incontrare le specificità di ciascun ambiente, come evidenziano presso Sourcefire.

Il controllo applicativo, nel caso di Sourcefire, è una funzionalità realizzata sia dal Next Generation Firewall sia dal NGIPS, che possono essere eventualmente anche integrati. Secondo i casi, però, potrebbe essere sufficiente acquistare solo il NGIPS, mantenendo il firewall tradizionale a realizzare le funzioni tradizionali di gateway e affidando al NGIPS il controllo applicativo.

La soluzione FireAMP, disponibile su appliance, sfrutta il cloud computing e i Big Data forniti e integrati dai sistemi Sourcefire, grazie ai quali classifica i file in ingresso sul sistema aziendale. È disponibile anche una versione per la protezione dai malware sviluppati per dispositivi mobili (Android) o specifici per virtual machine (solo in ambienti VMware). È possibile configurare FireAMP affinché effettui una selezione dei file da esaminare in dettaglio oppure si può decidere di analizzarli tutti. Per garantire le prestazioni, Sourcefire ha realizzato la linea di appliance SourcePower.

# L'IMPATTO DEGLI MSS DI TELECOM ITALIA

*Consulenza pacchettizzata, assessment, gestione delle soluzioni sono gli ambiti in cui si articolano i servizi gestiti, fondati sull'esperienza di chi deve prima pensare alla sicurezza della propria infrastruttura*

Telecom Italia fornisce servizi di sicurezza, perlopiù gestiti, da diversi anni. Recentemente, tra il 2012 e l'inizio del 2013, l'offerta è stata riorganizzata e completata con l'adeguamento di quella che era la proposizione di Managed Security Service (MSS) storica. Nella nuova strutturazione, i servizi forniti da Telecom Italia, direttamente o tramite i propri partner, sono articolate in tre aree: servizi di consulenza, servizi di assessment, security solution.

In tutte le aree si riscontrano i punti di forza dell'offerta di Telecom Italia, che sono le forti competenze interne e l'indipendenza dai produttori di soluzioni per la sicurezza.

Innanzitutto, Telecom Italia ha dovuto sviluppare conoscenze specifiche per garantire la sicurezza della propria infrastruttura. Per questo ha maturato una notevole esperienza, anche nella gestione di più tecnologie diverse. Tecnologie che ha scelto, testato e validato. In altre parole, Telecom Italia gioca un ruolo di "trust advisor" per i propri clienti.

Aldilà della consulenza progettuale, tipicamente di alto livello che risponde a specifiche richieste o addirittura bandi di gara da parte delle imprese, Telecom Italia fornisce servizi di consulenza a medio-grandi aziende per quanto riguarda: risk assessment e il suo trattamento, disaster recovery e impact analysis di business e, infine, Compliant Privacy.

I servizi sono pacchettizzati, cioè le attività definite chiaramente, senza lasciare spazi come nel caso delle quotazioni a giornate uomo.

È l'area che prevede servizi di vulnerability assessment: cioè la ricerca sistematica delle vulnerabilità reali e potenziali dei sistemi. Tali servizi possono essere realizzati sia con tool automatici sia attraverso servizi di penetration test e di analisi

infrastrutturale. In questo modo si ottiene una verifica delle possibilità concrete di sfruttamento delle vulnerabilità per valutarne più direttamente il rischio associato alle stesse in termini di riservatezza, integrità e disponibilità dei dati e delle informazioni.

I servizi di penetration test sono svolti sia in modalità remotizzata, quindi direttamente dal SOC (Security Operation Center) Mercato di Telecom Italia, sia in modalità on-site.

L'area delle Security Solution è quella più ampia e vero cuore dell'offerta di sicurezza da parte di Telecom Italia. Si tratta di un'offerta di MSS che comprende un'ampia gamma di soluzioni per la sicurezza infrastrutturale, le quali rispondono a varie e numerose esigenze. Un fattore comune consiste nel fatto che la gestione del servizio può essere effettuata sia su sistemi installati presso il cliente sia su sistemi residenti presso i data center della società.

Tra gli ambiti di intervento vi è la sicurezza perimetrale, che può essere o meno in bundle con la connettività fornita da Telecom Italia.

Poi è disponibile un servizio di Mail Protection, con antivirus e antispam anche aggiunto al sistema di protezione eventualmente già installato in azienda. Interessante anche il servizio di Host Protection, consistente in una funzionalità di Web Application Firewall fornita in cloud dal data center di Telecom Italia. Importante il servizio di security monitoring, che prevede raccolta, normalizzazione e analisi degli eventi di sicurezza generati da apparati, server, sonde e vari dispositivi sotto monitoraggio. Infine, molto attuale è il servizio di DDoS Protection che viene erogato all'interno della rete di Telecom Italia, sia in modalità reattiva sia proattiva.

# WEBSense UNIFICA LA PROTEZIONE

*Attraverso l'architettura Triton il vendor propone una sicurezza unificata basata su un modello flessibile d'implementazione tramite appliance, in modalità Software as a Service e ibrida*

Per aiutare le aziende ad affrontare le nuove sfide legate alla sicurezza Websense ha sviluppato Triton, un'architettura unificata per la sicurezza dei contenuti che offre protezione di classe enterprise per dati, Web e posta elettronica. Triton mette a disposizione un sistema modulare e scalabile, attivabile con una singola chiave di licenza che consente di decidere come costruire la soluzione di sicurezza intervenendo su tre fronti.

- Analisi unificata dei contenuti che comprende l'analisi delle minacce in tempo reale eseguita da Websense Advanced Classification Engine (ACE).
- 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.
- Piattaforma unificata che consente di scegliere e combinare differenti modalità di implementazione (appliance locale, cloud, ibrida) mantenendo conformità tra le policy a prescindere dalla configurazione del deployment.

La protezione Websense è implementabile in tre diverse modalità. La prima è l'implementazione tramite appliance V-Series, che vengono fornite pre-configurate e pronte all'utilizzo per riunire funzioni di Web Security ed E-mail Security in un'unica piattaforma. Due sono i modelli di appliance disponibili: l'appliance Websense V10000 adatta per le sedi centrali e grandi uffici e la V5000 indirizzata a filiali e aziende di medie dimensioni. Una seconda possibilità di implementazione è tramite servizi SaaS, trasferendo tutti i processi di implementazione e di gestione delle misure di sicurezza ai data center Websense situati nel cloud. I servizi di hosting offerti da Websense, a diffusione globale, hanno ottenuto la

certificazione ISO 270010 e soddisfano i principali standard di sicurezza e di disponibilità. I servizi SaaS per la sicurezza di Web ed e-mail di Websense vengono offerti con una garanzia di operatività e SLA (Service Level Agreement) pari al 99,99%. Websense TruHybrid è il modello di implementazione ibrida che consente l'integrazione di servizi SaaS, piattaforme locali e gestione dell'intero sistema da un'unica console. È possibile, così, disporre dei vantaggi forniti dai servizi SaaS e on-premises (appliance e software), scegliendo la combinazione più indicata per le specifiche esigenze operative. L'implementazione di Websense TruHybrid mette a disposizione appliance o software idonei a soddisfare le esigenze di aziende di grandi dimensioni offrendo i vantaggi dei servizi SaaS per garantire la sicurezza di filiali che non dispongono delle risorse necessarie a sostenere installazioni hardware e per proteggere gli utenti mobili.

Il servizio Web Defensio, fornito attraverso la piattaforma globale Security as a Service di Websense, offre agli utenti e ai proprietari dei siti di social Web protezione personalizzata da commenti spam, malware e altre minacce integrate nei contenuti generati dagli utenti oltre a funzioni di gestione e controllo del contenuto pubblicato su ciascun sito. La piattaforma Defensio consente di combattere le minacce di nuova generazione attraverso le funzionalità di blocco categorie URL, di sicurezza basata sulla reputazione, filtro del dizionario (per rimuovere automaticamente parole specifiche che non si desiderano nei commenti), blocco di script e file eseguibili e protezione della pagina Facebook grazie al monitoraggio in tempo reale e alla rimozione di contenuti indesiderati.

CON IL PATROCINIO DI:

ORGANIZZATA DA:



# Io faccio la corsa giusta

Partecipa anche tu

## alla **INNOVATION RUNNING**

corsa organizzata dalle aziende ICT a sostegno di

B2Blood e AVIS Milano

B2Blood è il progetto di Responsabilità Sociale a favore della donazione di sangue in azienda promosso da AVIS Milano e Assintel



SAVE  
the  
DATE

Domenica 22 settembre 2013  
Arena di Milano



**Campionato provinciale Master maschile & femminile FIDAL**  
Partenza gara competitiva da 10 km - ore 10.00



**TROFEO - CorriMi**  
Partenza corsa non competitiva da 6,5 km - ore 10.10

Per ulteriori informazioni e per iscriversi: [www.innovationrunning.it](http://www.innovationrunning.it)  
E-mail: [info@innovationrunning.it](mailto:info@innovationrunning.it) - Tel. 039.2247435

MAIN SPONSOR:



NILOX



ORACLE

MAIN PARTNER:



SPONSOR PARTNER:



KEY MEDIA

SITECOM



MEDIA PARTNER:

COMPUTERWORLD

ICT4Executive

ZeroUno

NetMediaEurope

DMO datamanager

Corriere delle Comunicazioni

SISTEMI & IMPRESA

PARTNERS

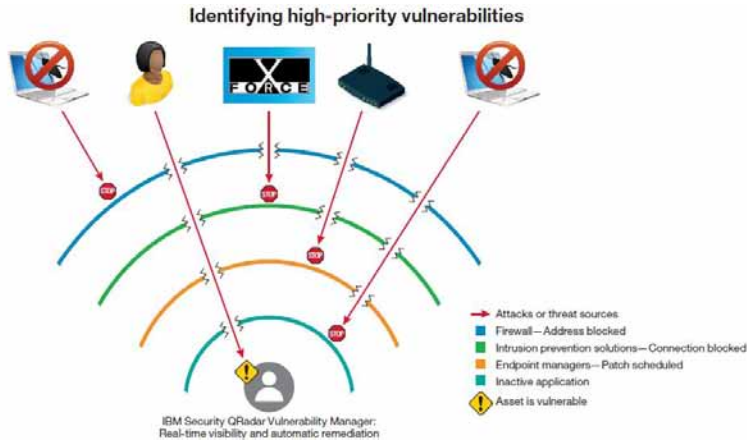
Reportec

01net.



## IBM QRADAR GESTISCE LE VULNERABILITÀ

*Con la security intelligence di QRadar Vulnerability Manager un nuovo software per identificare e prevenire i rischi relativi alla sicurezza*



Gli attacchi informatici aumentano in termini di volume e gravità, rendendo sempre più utile se non necessaria una componente d'intelligence per aiutare le imprese a identificare, selezionare e contestualizzare le minacce. Ibm ha introdotto questo approccio da un po' di tempo e continua a investire in strumenti che ne accrescano l'efficacia. Per gestire e assegnare priorità alle vulnerabilità di rete, Ibm ha sviluppato QRadar Vulnerability Manager, una soluzione di security intelligence integrata, che, a detta dei suoi artefici, contemporaneamente riduce il costo totale dovuto alle operazioni connesse di sicurezza. La soluzione, ci spiegano, fornisce ai responsabili della sicurezza una vista complessiva e "prioritizzata" della loro rete, aiutandoli a rafforzare e consolidare velocemente le loro difese. Raggruppando le informazioni relative alle vulnerabilità in un'unica vista, i team di sicurezza possono esaminare e gestire velocemente i risultati di molteplici scansioni di applicazioni, database, endpoint o reti.

Come parte della Ibm Security Intelligence Platform, QRadar Vulnerability Manager (QVM) esamina le falle nella sicurezza per bloccarle e impedire le azioni di potenziali "exploit", anche di quelli nascosti dietro a firewall, associati ad applicazioni inattive o diversamente irraggiungibili da attacchi esterni. Secondo quanto comunicato da Ibm, attivando una chiave di licenza, il nuovo software può eseguire una scansione automatica e un'analisi della rete.

Un po' più in dettaglio, i responsabili di Ibm evidenziano che QRadar Vulnerability Manager riduce nella mitigazione e remediation delle minacce, riunendo le informazioni sulle vulnerabilità in un'unica vista basata sui rischi e ordinata in base alle priorità. I team di sicurezza possono vedere i risultati provenienti da molteplici scansioni di applicazioni, database, endpoint o reti unitamente ai più recenti alert di X-Force Threat Intelligence e ai report sugli incidenti del National Vulnerability Database. La nuova soluzione include anche un proprio scanner incorporato, certificato PCI, che può essere programmato per funzionare periodicamente o per attivarsi in base agli eventi di rete. L'intelligence di QRadar, inoltre, è stata integrata nel sistema di intrusion prevention Ibm Security Network Protection XGS 5100, che così fornisce un data feed di rete continuo per aiutare a identificare attacchi al Secure Socket Layer (SSL). La piattaforma che si ottiene, evidenziano in Ibm, comprende anche la tecnologia "virtual patch" di Ibm, che fornisce protezione contro le vulnerabilità quando non è ancora disponibile una patch specifica del software. Inoltre, Ibm ha anche annunciato una nuova versione di Ibm Security zSecure Suite, una soluzione di sicurezza integrata con Ibm QRadar Security Intelligence Platform per fornire alle organizzazioni visibilità degli eventi di sicurezza mainframe a livello aziendale. Tale soluzione è supportata da allarmi automatici in tempo reale contro le minacce e reporting della compliance personalizzato.



# SOPHOS SEMPLIFICA LA SICUREZZA DEI DISPOSITIVI MOBILI

*Con Mobile Control 3.5 aumentata la protezione. Annunciata anche la versione SaaS che garantisce la sicurezza per Windows Phone 8 e comprende funzionalità di reportistica e amministrazione*

Sophos ha rilasciato Sophos Mobile Control 3.5, la nuova versione della sua soluzione per il mobile device management (MDM). Disponibile sia on-premise sia in modalità as a service, Sophos Mobile Control 3.5 è stato sviluppato con l'obiettivo di fornire alle PMI una soluzione che semplifichi la messa in sicurezza, il monitoraggio e il controllo dei dispositivi mobili.

La versione è disponibile anche per Windows Phone 8 e mette a disposizione funzionalità che semplificano la reportistica e l'amministrazione, facilitando la messa a punto e l'implementazione di policy BYOD.

Due le considerazioni di Sophos nello sviluppo della soluzione. Nonostante il numero di smartphone e tablet che vengono smarriti ogni giorno sia allarmante, spesso gli utenti non impostano nemmeno una protezione di base tramite password. Il malware trasmesso via mobile e gli attacchi hacker è in costante crescita e molti dipendenti continuano a utilizzare device personali non protetti per accedere ai dati aziendali: ciò rappresenta indubbiamente una seria preoccupazione per le aziende che devono proteggere i dati consentendo contemporaneamente ai dipendenti di lavorare

ovunque vogliono.

Sophos Mobile Control si propone di rispondere a queste criticità e fornire la sicurezza della quale hanno bisogno i responsabili IT al fine di poter sposare la causa della mobilità dei dipendenti in tutta sicurezza.

La nuova versione comprende la protezione a Windows Phone 8 oltre che a iPhone/iPad e Android, con possibilità di registrazione e implementazione self service per gli utenti. I responsabili IT hanno anche la possibilità di gestire l'intero ciclo di vita dei dispositivi, nonché le problematiche derivanti da eventuale furto o smarrimento degli stessi.

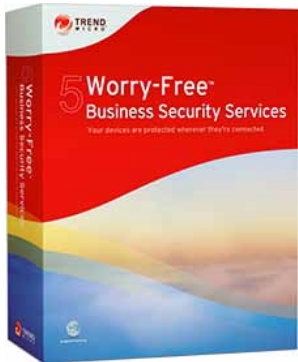
Particolarmente utile, ritiene Sophos, anche la app client semplice da utilizzare, che dà accesso agli status di conformità, ai messaggi e alle informazioni di supporto, garantendo così una reportistica esaustiva e fornendo al reparto IT una visione olistica del parco dispositivi.

*Giuseppe Saccardi*

The screenshot displays the Sophos Mobile Control dashboard. On the left is a navigation menu with categories like Task view, Inventory, Applications, Profiles, Task bundles, Reports, Administrators, Users, Compliance rules, Settings, and About. The main area is titled 'Show device' and features a mobile phone icon. To the right, a table lists device details: Status (Managed), Compliant (Yes), Operating system (iOS 6.1.4), Email access (Yes), Last synchronization (Jun 17, 2013 6:45 PM), Last app synchronization (Jun 7, 2013 3:45 PM), Owner (Employee device), Name (Rogers iPhone), Description (iOS), Phone number (+44...), User (---), Email address (...@sophos.com), Device group (Default), and Device ID (UDID...). Below this is a row of icons representing various management actions. At the bottom, there's a section for 'Installed profiles' with a table containing one entry: 'MDM enrollment profile' with identifier 'com.mdm' and description 'This profile enables your company to manage your mobile device with Sophos Mobile Control.'



## TREND MICRO WORRY-FREE BUSINESS SECURITY SERVICES 5.2



*Gestita in remoto dagli specialisti Trend Micro, la soluzione per le Pmi beneficia dell'architettura in cloud per proteggere dispositivi Windows, Mac e Android*

Nuova release per Worry-Free Business Security Services, la soluzione che, assicurando in Trend Micro, fornisce una protezione di livello Enterprise per i dispositivi Windows, Mac e Android grazie a una console di gestione sicura e centralizzata basata sul Web.

Giunta alla versione 5.2, la soluzione beneficia degli aggiornamenti continuativi forniti dal framework di rilevamento delle minacce Trend Micro Smart Protection Network, che garantisce la protezione costante di pc, laptop e altri dispositivi.

Le nuove funzionalità comprendono: l'amministrazione condivisa, l'audit logging esteso e miglioramenti nella gestione dei dispositivi. Grazie all'aggiornamento automatico alla nuova versione, chi è già cliente di Worry-Free potrà proteggere due dispositivi mobili Android per singola licenza senza costi aggiuntivi.

Smart Protection Network raccoglie e analizza i dati relativi alle minacce, virus e altre forme di malware prima che queste raggiungano i computer degli utenti. Poiché il processo di elaborazione avviene a livello di cloud, Trend Micro Worry-Free Business Security Services minimizza quindi i rallentamenti, consumando quantità minori di memoria e di spazio su disco.

La soluzione è pensata per le aziende con un massimo di 250 endpoint.

È possibile scaricare il data sheet, mentre di seguito riportiamo la descrizione delle principali innovazioni

così come sono state comunicate da Trend Micro:

- Responsabilità di amministrazione condivise.
- Audit Logging esteso – I nuovi registri di controllo catturano gli eventi della console di management, come quelli amministrativi, l'outbreak defence, la gestione di gruppo, la gestione dei dispositivi e gli eventi di configurazione delle policy.
- Visualizzazione - La schermata sul dispositivo comprende ora quattro nuove colonne che permettono di visualizzare la tempistica di avvio e di completamento della scansione pianificata e della scansione manuale.
- Riavvio di una scansione - si possono configurare le scansioni pianificate in modo che, se interrotte per qualsiasi motivo, si riavvino automaticamente.
- Installazione Mac senza richiedere Java.
- Aggiornamento del Device Tree sullo schermo del dispositivo - Cliccando su un'icona di impostazioni del gruppo sul Device Tree è possibile visualizzare il menu pop-up di accesso e selezionare direttamente opzioni come Rimuovi, Rinomina, Replica le impostazioni, Esegui o Interrompi la scansione e Configura le policy.
- La schermata relativa alle licenze visualizza i dispositivi mobile protetti - Anche i dettagli dei dispositivi Android possono essere visualizzati con semplicità sullo schermo del dispositivo cliccando sul collegamento ipertestuale che riporta il nome del dispositivo.

*Gaetano Di Blasio*

## MCAFFEE MOBILE SECURITY

È disponibile una nuova versione di McAfee Mobile Security, che si distingue perché include nuove funzionalità di privacy all'avanguardia, secondo quanto comunicato.

In particolare, i responsabili del prodotto evidenziano la funzione Profile App multi-utente, che consente di creare più profili utente o "zone protette" su un dispositivo con accesso alle applicazioni personalizzato o limitato.

La nuova release del software è distribuito nelle edizioni base o premium. La prima è gratuita e fornisce antivirus, backup e anti-furto, mentre la seconda aggiunge funzionalità di sicurezza all'avanguardia. Più precisamente, la versione base protegge la privacy degli utenti consentendo loro di eseguire il backup, pulire e ripristinare i contatti in remoto attraverso un portale Web e anche di localizzare un dispositivo perso o rubato su una mappa, potendo azionare un allarme sonoro a distanza. La versione premium, invece, è supportata da McAfee Global Threat Intelligence, comprende funzionalità

per la sicurezza delle applicazioni e delle attività telefoniche, tra cui app privacy reporting e un filtro di chiamate e SMS.

Per proteggere i consumatori dalle richieste di permessi abusivi da parte dei malware, McAfee Mobile Security Premium fornisce ora la funzione App Profile multi-utente che consente agli utenti di creare una "zona di sicurezza" per bambini, amici, familiari o anche sconosciuti che possono fare un uso improprio dei loro dispositivi. Inoltre, la versione premium include una funzionalità di rilevamento del malware, Device Admin Detector, che protegge gli utenti da Trojan, come il recentemente scoperto Obad. Questa funzione è inclusa anche in McAfee Mobile Innovations, l'app disponibile su Google Play a costo zero per gli utenti Android.

La soluzione include anche nuove funzionalità di analisi dell'esposizione dei dati personali, che consente agli utenti di verificare di persona il livello di rischio rappresentato dalle applicazioni che hanno installato.

## Servizi HP Cloud Security

HP ha presentato servizi di sicurezza che entrano a far parte della HP Converged Cloud Professional Services Suite.

Si tratta degli HP Cloud Security Risk and Controls Advisory Services, pensati per supportare le aziende nella gestione dei rischi correlati ai dati, nell'identificazione delle vulnerabilità e nel mantenimento della conformità con la governance IT.

Gli HP Cloud Security Risk and Controls Advisory Services prevedono un seminario di un'intera giornata con HP e strumenti online che misurano il grado di maturità dei controlli di sicurezza esistenti e offrono accesso alle best practice e alle tecnologie HP TippingPoint, HP Fortify, HP Atalla e HP Autonomy fornendo una conoscenza approfondita dei rischi di sicurezza cui sono esposte le aziende.

I nuovi servizi cloud di HP si affiancano agli HP Threat and Vulnerability Consulting Services che permettono di definire i protocolli appropriati per la scansione delle vulnerabilità e per le operazioni di test.

R.F.

## Palo Alto Networks WildFire per cloud privati



L'appliance WF-500 di Palo Alto estende alle infrastrutture aziendali

la caratteristica WildFire dei Next Generation Firewall di Palo Alto Networks. Tale funzionalità consente di identificare e analizzare i malware mirati o sconosciuti, attraverso il monitoraggio di 100 comportamenti dannosi. In pratica, attraverso un servizio in cloud, Palo Alto esegue in un ambiente isolato i file, verificandone la natura e classificandoli come malware o file legittimi. Le informazioni vengono poi condivise con tutti i dispositivi della casa madre.

Per chi non vuole usufruire di un servizio in cloud pubblico, magari a causa di policy interne restrittive, Palo Alto ha progettato l'appliance WF-500, che effettua lo stesso tipo di controllo all'interno dell'infrastruttura aziendale del cliente.

Di fatto, come ci spiegano i responsabili di Symbolic, noto specialista italiano della sicurezza, il dispositivo permette di estendere la funzionalità di analisi remota di WildFire creando una sorta di private cloud.

# LA SICUREZZA AZIENDALE E CONTINUITA' DEL BUSINESS

È disponibile il libro **“Sicurezza aziendale e continuità del business”** realizzato da Reportec.

In circa 350 pagine analizza le problematiche di governance e di risk management connesse con i diversi aspetti della sicurezza aziendale: dalla protezione delle informazioni, alla continuità operativa, alla salvaguardia degli asset fisici, non dimenticando di sottolineare le problematiche portate dagli ultimi trend tecnologici, come il cloud computing e la mobility.

Sono tutti elementi connessi con le minacce che alimentano il rischio: spionaggio industriale, sabotaggi, infedeltà dei dipendenti, incendi e altri tipi di incidenti. Questo libro tratta tali temi considerando che il primo problema da affrontare è di tipo organizzativo e il secondo è di mantenere sempre il controllo degli investimenti in chiave

di business. Completa il volume l'analisi delle soluzioni sviluppate per la sicurezza e la continuità del business da parte un ampio numero di primarie aziende del settore.

Il volume è uno strumento unico in Italia per l'ampiezza delle tematiche affrontate e l'opera di sintesi delle soluzioni e dei servizi disponibili sul territorio, consentendo di approfondire gli aspetti strategici, bilanciando i concetti e la teoria con quanto di concreto attualmente esiste.

Conoscere è infatti la condizione sine qua non perché un manager possa decidere. Questo obiettivo è perseguito mediante un esame analitico degli aspetti più importanti, gli economics e le modalità di realizzazione e di adozione di una infrastruttura per la sicurezza.

Per acquistarlo manda un'e-mail a [info@reportec.it](mailto:info@reportec.it) oppure telefona allo **02-36580441**

