

THE CYBER WAR

CRONACA VERA: VIRUS INFORMATICO INFETTA UN UMANO

IN QUESTO
NUMERO:

> **pg.01**

- Cronaca vera: virus informatico infetta un umano

> **pg.02**

- Cambiano le minacce secondo Ibm X-Force

> **pg.05**

- Sapio riduce i costi di storage e centralizza la gestione dati con Sinergy

> **pg.06**

- L'ICT corre per sostenere AVIS

> **pg.07**

- Il backup di Symantec fa un passo in avanti
- Le sorprese del BYOD secondo Fortinet
- Nuova generazione per i sistemi UTM di SonicWall

> **pg.08**

- Kaspersky protegge il network casalingo
- La strategia per una sicurezza completa secondo Check Point

> **pg.09**

- G-Data protegge pc, smartphone e tablet
- Sicurezza degli ambienti cloud con Trend Micro

> **pg.10**

- Il nuovo libro "Sicurezza aziendale e continuità del business" di Reportec

Il titolo è meno provocatorio di quanto si possa pensare. Si tratta, infatti, di una possibilità concreta che potrebbe verificarsi anche in un futuro molto vicino. Esistono apparati medicali impiantati nelle persone che contengono chip programmabili e, pertanto, "infettabili" da un malware. Al momento è un'ipotesi teorica, ma il fatto che non si conoscano esperimenti in tal senso non significa che non siano stati effettuati. Del resto è facile immaginare che controllare tali dispositivi via wireless possa essere utile per determinate terapie o per consentire il recupero di disabilità fisiche. Raggiungere quindi il circuito elettronico con un segnale "apre" la strada a un qualche tipo di exploit maligno e il "gioco" è fatto. Lasciamo che siano gli sceneggiatori di Hollywood a costruire i tanti scenari, terroristici e non, che si possono prefigurare. Come già detto in passato, Cyber War con la maiuscola, intesa come guerra tra stati sovrani, e quella con la minuscola, intesa come minacce per gli individui e le aziende, s'intrecciano. In un mondo sempre più interconnesso, in cui si contano 13 miliardi di dispositivi collegati in rete, la "vita" digitale equivale a quella fisica, almeno per il mondo industrializzato. Un attacco software, in altre parole, può mettere a repentaglio la vita di tutti i giorni, cioè le relazioni umane e di affari, come oggi vengono concepite. Questi

scenari li lasciamo alla politica, che dovrebbe tornare a progettare la società, occupandoci di segnalare l'evoluzione delle ultime minacce, in particolare con l'aiuto del rapporto 2011 di Ibm X-Force (si veda la pagina seguente) e con un bollettino di Websense. Quest'ultima, in particolare, ci avvisa che è stata rilevata un'ondata di malware APT (Advanced Persistent Threat), cioè di codice maligno che si annida silenziosamente sui computer per raccogliere dati e/o utilizzarne le risorse.

Chiamato Flame (ma noto anche come Flamer o Skywiper) questo malware si pensa sia in circolazione già dal 2010, ma solo a maggio 2012 è stato identificato. La funzione principale è raccogliere informazioni in diversi modi, tra cui registrare file audio, catturare screenshot, compilare una lista dei dispositivi Bluetooth presenti nelle vicinanze e molto altro. Infatti, le funzionalità integrate sono tante, con numerosi moduli quali, decompressione, librerie, database SQL e virtual machine LUA, cosicché, a differenza di altri sistemi APT "nascosti", che difficilmente arrivano a 1 MB, Flame pesa 20 MB circa. Al momento sembra che le vulnerabilità sfruttate da Flame per mantenere la presenza e spostarsi sulle reti infette siano le stesse utilizzate da Stuxnet e Duqu (appunto diffusi nel 2010), rispetto ai quali appare però molto più avanzato.

il 36% delle vulnerabilità software sono rimaste senza patch nel 2011 rispetto al 43% del 2010.

Hacktivism e cyber-criminalità

Se, da un lato, migliora la protezione verso certi tipi di attacco, dall'altro ne nascono di nuovi. Per esempio, «è più che raddoppiato l'utilizzo di tecniche di tipo shell command injection contro i server Web – spiega Panada -. Questo potrebbe essere considerato una risposta ai tentativi, coronati da successo, di bloccare altri tipi di vulnerabilità delle applicazioni Web».

Mentre gruppi di cosiddetti "hacktivist", come gli Anonymous, causano dei Denial of Service (che continueranno ad aumentare colpendo organizzazioni governative e aziende "simbolo"), realizzando operazioni cui danno forte risalto, dall'altro lato il crimine informativo segue le "mode" e inaugura nuove frontiere: «Tra i nuovi attacchi, rilevate da Ibm X-Force, gli exploit per il mobile, il guessing automatico delle password e un forte aumento degli attacchi di phishing», rimarca Panada.

Questi ultimi, in particolare, denunciano ancora una scarsa cultura della sicurezza. Come si legge nel report, infatti, la presenza di password (e delle relative policy) non sufficientemente robuste ha svolto un ruolo decisivo in una serie di violazioni di alto livello nel corso del 2011. Attacchi cosiddetti "a forza bruta", contro siti SSL e SSH, hanno avuto un significativo successo nella seconda metà del 2011.

Il phishing, invece, sfrutta l'ingenuità degli utenti e, nella seconda metà del 2011, il volume di email riconducibili al phishing ha raggiunto dimensioni cui non si assisteva dal 2008. Molte di queste email appaiono arrivare da popolari siti di social network e servizi di corriere espresso e invogliano le vittime a cliccare su link a pagine Web che possono tentare di infettare i loro pc grazie all'utilizzo di malware. Una parte di queste attività può essere attribuita anche al fenomeno del click fraud pubblicitario, nel quale gli spammer utilizzano messaggi di posta elettronica ingannevoli per indirizzare il traffico verso siti web di vendita.

Nuovi pericoli per il mobile e il social

I siti social, del resto, sono una fonte di informazione utilissima per gli attacchi di phishing, che attraverso i dati raccolti sui profili degli utenti possono creare messaggi email molto più accurati e personalizzati. Aumentano, infatti, gli attacchi mirati a specifici target. Altro aspetto "nuovo" riguarda la crescita delle minacce per il mondo mobile, che va di pari passo all'esplosione nella diffusione di questi dispositivi, come osserva Panada, che, sollecitato al riguardo commenta: «Il BYOD (Bring Your Own Device) crea qualche problema in più e porta il tema del mobile device management sui tavoli di tutti i CISO (Chief Information Security Officer). Il primo passo da effettuare in azienda, è quello di adottare una strategia chiara per la gestione, per esempio, obbligando i dipendenti a installare un tool di management e ad accettare determinate condizioni o firmare liberatorie».

Uno dei problemi è che le soluzioni per la sicurezza di apparati come smartphone e tablet sono ancora immature. Soprattutto, però, e torniamo al tema della gestione «non esiste un processo di patching strutturato per gli strumenti mobile», evidenzia Panada. Il mondo Apple non è immune neanche sul fronte Mac: la diffusione dei pc con la Mela, infatti ha portato allo sviluppo di minacce ad hoc, come MacDefender, che simulava un antivirus, invece era un malware, alcuni trojan e altri codici maligni per Mac OS.

Si assiste ancora a una crescita delle APT (Advanced Persistent Threat), guidata da un aumento delle botnet. Nascono e muoiono come funghi anonymous proxy, mentre gli stessi fornitori delle soluzioni di sicurezza sono bersagli mirati: vengono sottratti codici sorgente, riporta Panada, preoccupato di quello che ciò potrebbe significare.

A rischio, infine, sono anche le infrastrutture critiche di un paese, dopo Stuxnet: «È stato dimostrato come sia possibile effettuare un attacco di tipo DoS persino sui televisori IP. In un mondo sempre più interconnesso, la sicurezza diventa una questione fondamentale».

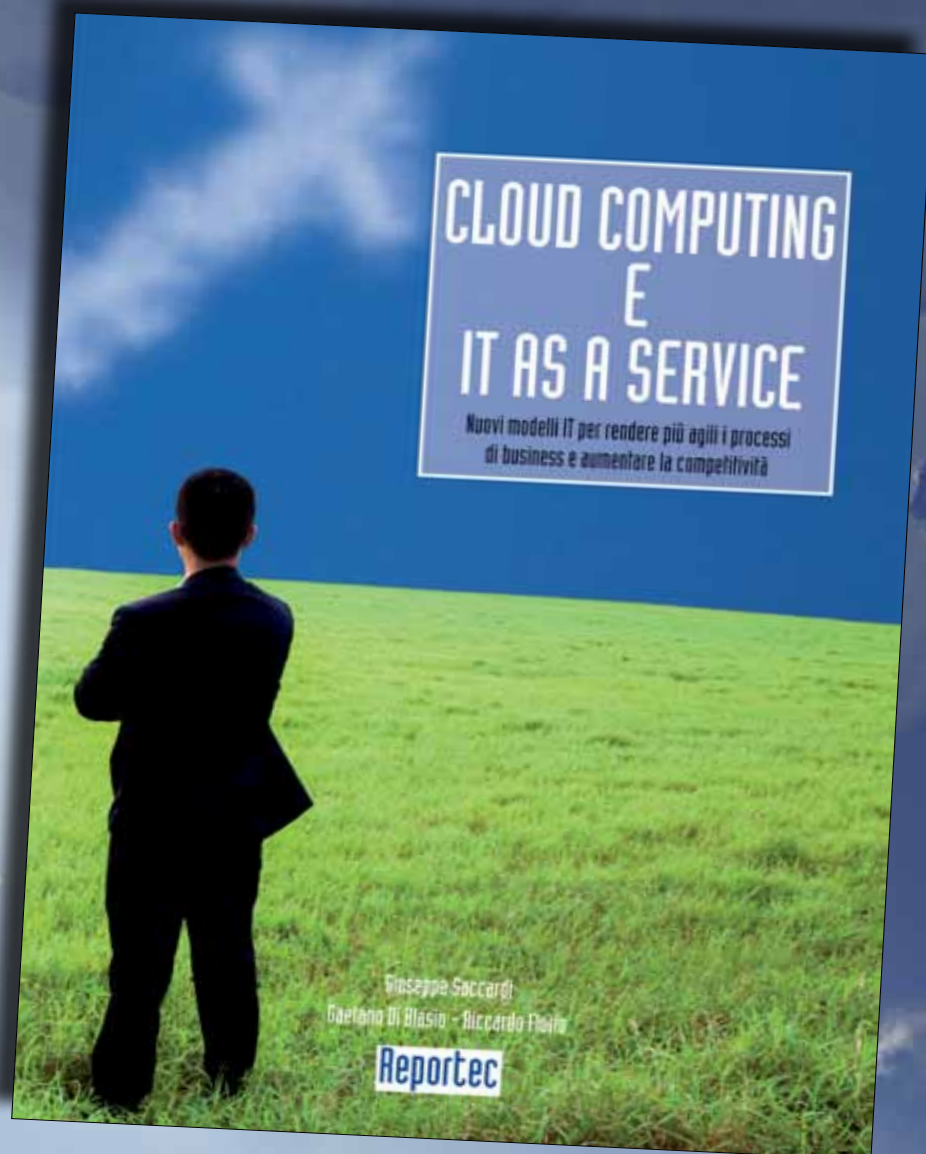
È disponibile il libro sul **CLOUD COMPUTING**

Realizzato da Reportec, in oltre 350 pagine, analizza i prodromi del cloud computing, le modalità di fruizione e i benefici che derivano dall'adozione di questa innovativa possibilità di utilizzo del più avanzato IT, senza dover immobilizzare ingenti capitali.

Completa il volume l'analisi delle soluzioni sviluppate per il cloud computing da parte di un ampio numero di primarie aziende del settore attive nel campo delle infrastrutture, delle applicazioni e dei servizi.

Il volume è uno strumento unico in Italia per affrontare le tematiche del cloud computing e approfondire gli aspetti, bilanciando i concetti e la teoria con quanto di concreto attualmente esistente.

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 un'infrastruttura cloud computing.



È anche disponibile il libro
UN'IMPRESA SEMPRE PIÙ MOBILE

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

Sapio riduce i costi di storage e centralizza la gestione dati con Sinergy

Con l'introduzione di tecnologie Symantec, l'azienda, attiva nel settore dei gas tecnici e medicali, ha conseguito un maggior controllo dei costi, riducendoli fino al 20%

Sapio, tra i gruppi leader in Italia nel settore dei gas tecnici e medicali, ha trasformato la propria infrastruttura tecnologica adottando soluzioni innovative di automazione e virtualizzazione con lo scopo di ridurre i costi e aumentare parallelamente la qualità del servizio in tutte le aree dell'azienda.

Per rispondere alle esigenze di evoluzione della propria infrastruttura Sapio, in collaborazione con il Partner Sinergy, ha implementato e integrato una suite di tecnologie Symantec, comprendenti archiviazione, gestione e protezione delle informazioni. Sinergy è dal 1994 tra i principali System Integrator del panorama italiano ICT ed affianca clienti in tutti i settori del mercato fin dalla fase iniziale di assessment dell'infrastruttura, offrendo soluzioni tecnologiche d'avanguardia e servizi "full life cycle" di Advisory, Design, Implementazione, Integrazione e Gestione delle soluzioni. «Abbiamo affiancato il Gruppo Sapio sin dalla fase di valutazione del progetto di evoluzione dell'architettura - ha dichiarato Pietro De Lorenzi, Account Manager Sinergy - proponendo soluzioni innovative, in linea con l'esigenza del cliente. Lavorando con il team Sapio e mettendo a disposizione le nostre competenze e le solide conoscenze in ambito Data Center si è creato un vero e proprio knowledge transfer a vantaggio dell'efficacia complessiva».

Sapio ha trovato in Symantec un portafoglio unificato di soluzioni che rispondevano alle proprie esigenze. Symantec Enterprise Vault ha conferito un approccio intelligente all'archiviazione, gestione e reperimento dei dati nel sistema e-mail Exchange, nell'ambiente file server e nella piattaforma di colla-



borazione SharePoint. Symantec Backup Exec è stato altrettanto efficace nella protezione dei dati in Windows e, utilizzato per salvaguardare i dati sui 30 server fisici di Sapio distribuiti tra le varie sedi italiane, ha centralizzato la gestione di questi server, consentendo di estendere la propria infrastruttura di backup a tutto l'ambiente distribuito dell'azienda e alle sedi remote e di gestire la protezione dei dati di server e desktop direttamente da Monza nella fase di sviluppo del business in Italia.

Ghost Solution Suite ha completato questa strategia integrata di protezione dei dati e gestione delle informazioni supportando la distribuzione remota, la gestione dei sistemi e il processo di "imaging" dei computer di più di 100 filiali distribuite in tutto il territorio italiano. «Le soluzioni di Symantec hanno offerto a Sapio un modo flessibile e conveniente per gestire un ambiente di storage Exchange in crescita, un'ampia dotazione di funzionalità e facilità d'uso - ha spiegato Stefano Ferrari, Responsabile IT del Gruppo Sapio -. Riusciamo a proteggere più dati utilizzando meno storage, risparmiando tempo e denaro, e abbiamo gestito la migrazione a Windows 7 da una singola finestra di gestione. I risultati sono stati eccellenti e Symantec Enterprise Vault ha contribuito a ridurre del 20% i costi di storage dei dati utilizzando una combinazione di archiviazione intelligente di Exchange, file system e SharePoint, mentre Symantec Backup Exec sta proteggendo in modo affidabile i dati critici su più di 30 server distribuiti. Inoltre, Symantec Ghost Solution Suite ha aiutato a ridurre di quasi il 50% il tempo necessario per migrare mille pc a Windows 7»



L'ICT corre per sostenere AVIS



L'iniziativa Innovation Running vuole essere un momento di sport e condivisione per sensibilizzare sull'emergenza sangue, con le aziende dell'ICT in prima linea



Si svolgerà domenica 10 giugno, presso la bellissima cornice naturale del Parco delle Cave a Milano, la prima edizione di INNOVATION RUNNING: una giornata di gare di corsa aperta a tutti coloro che desiderano contribuire alla raccolta fondi a favore di Avis.

Con il patrocinio di Regione Lombardia, Provincia di Milano e Comune di Milano, l'evento sportivo fa parte delle iniziative di B2Blood, il primo progetto italiano di responsabilità sociale a livello di associazione di categoria ideato da AVIS Milano e Assintel (Associazione Nazionale Imprese ICT), con il supporto di quattro grandi multinazionali come CA Technologies, Esprinet, Oracle e SAP. Altre importanti realtà dell'Information Technology in Italia, Altea, Hitachi Data Systems, Intel, Realtech e Reply, si sono attivate a sostegno della manifestazione.

Una giornata all'insegna dello sport, del divertimento e della condivisione che si pone l'obiettivo di sostenere i progetti di donazione sangue e prevenzione di AVIS Milano e rilan-

ciare lo sviluppo dell'iniziativa B2Blood, una proposta per la sensibilizzazione civica di Avis Milano e Assintel per promuovere la raccolta del sangue all'interno delle aziende ICT.

L'evento prevede una gara competitiva a staffetta aperta a tutti coloro che sono nati prima del 31 dicembre 1994: ogni azienda, associazione, gruppo organizzato potrà iscrivere le proprie squadre, che si sfideranno lungo un percorso di 10 km. Una corsa non competitiva da 5 km sarà, invece, aperta a tutti senza alcun limite di età. In entrambi i casi, i partecipanti correranno lungo un anello immerso nel verde del meraviglioso Parco delle Cave, con partenza e arrivo presso il lago in Via Cancano. Con questa iniziativa le imprese dell'innovazione italiana si pongono al servizio della comunità, promuovendo la diffusione della cultura aziendale alla sensibilità civica e alla responsabilità sociale.

Tutte le informazioni sul regolamento di gara e le modalità di partecipazione sono disponibili sul sito: www.innovationrunning.it.

Il backup di Symantec fa un passo in avanti

Arrivano sul mercato Backup Exec 2012 e NetBackup 7.5, le nuove release delle diffuse soluzioni Symantec per la protezione e il ripristino dei dati. Le nuove versioni prevedono una serie di miglioramenti che si inseriscono all'interno dei tre punti chiave che definiscono la proposta di Symantec per affrontare con successo il backup: controllo della crescita dei dati, unificazione delle piattaforme, semplificazione.

Backup Exec 2012 è la nuova versione della soluzione per la protezione in ambienti Windows. Integra la tecnologia di deduplicazione, prevede il supporto per la protezione di ambienti VMware e Microsoft Hyper-V ed è disponibile in versione con agente (per un backup più granulare) oppure agentless per incrementare al massimo le prestazioni.

I miglioramenti apportati, invece, alla nuova soluzione NetBackup 7.5, consentono di ridurre i tempi di backup, di coniugare il meglio della tecnologia snapshot all'interno dei processi di backup e di evitare backup infiniti di informazioni inutili, grazie a un'indicizzazione e catalogazione dei dati in base al loro valore. Tra le novità: l'introduzione di NetBackup Accelerator, NetBackup Replication Director e NetBackup Search.

Continua online



Le sorprese del BYOD secondo Fortinet

Inarrestabile, il fenomeno del BYOD (Bring Your Own Device) impone alle aziende l'uso di dispositivi personali, tipicamente mobili, per il lavoro. Di fatto, il dipendente è soddisfatto e la sua produttività aumenta, senza contare che si sobbarca il costo del dispositivo. Le aziende ne traggono beneficio ma non considerano alcuni "effetti collaterali". Le sorprese del BYOD, secondo Fortinet, partono dalla sicurezza: poche aziende implementano policy per proteggere adeguatamente tali dispositivi. Anzi, in molti casi, trovano conveniente lasciare al dipendente tutta la gestione dell'apparato anche in caso di guasti. Senza le adeguate policy, però, i dati aziendali sono a rischio e i responsabili delle aziende perseguibili anche penalmente in base alla legge sulla protezione dei dati. Senza le policy adeguate, in altre parole, le aziende dovrebbero bloccare il BYOD e rinunciare a tutti i suoi benefici. Nella realtà, il dipendente lo utilizzerà comunque, mettendo a rischio l'impresa. Il problema è che, come evidenziano i responsabili di Fortinet, questi dispositivi

sono privi delle più elementari funzionalità di sicurezza, come antivirus e password, per cui applicare le security policy classiche potrebbe essere difficile. Fortinet suggerisce tre strategie:

- Implementare opportune policy mobile, stabilendo, per esempio, a quali dipendenti sarà consentito usare questi dispositivi; quali applicazioni sono necessarie e quali non consentite e a chi consentire l'accesso in base a profili il più possibile granulari.
- Utilizzare un software di gestione remota per poter applicare la gamma di funzioni di sicurezza di base, come l'antivirus, e poter gestire alcune funzioni sul dispositivo, come rimuovere i dati, aggiornare il sistema operativo con le patch e impedire che qualsiasi vulnerabilità esistente venga sfruttata per attacchi mobili.
- Bloccare i dispositivi non compatibili, adottando, di fatto, un compromesso con gli utenti che saranno costretti ad accettare di installare software per la sicurezza e di delegare almeno in parte il controllo dell'apparato all'azienda.

Nuova generazione per i sistemi UTM di SonicWall

La brevettata tecnologia d'ispezione dei pacchetti Reassembly-Free Deep Packet Inspection di SonicWall è alla base dei dispositivi firewall UTM di nuova generazione TZ 105 e TZ 205, in grado di supportare la forza lavoro mobile con un client di accesso remoto SSL VPN nativo per dispositivi Apple iOS, Google Android, Windows, Mac OS e Linux, pur essendo "dimensionati" per piccole e medie imprese o sedi distaccate di grandi aziende.

Grazie alla protezione completa da virus, trojan, key-logger e altri malware per attacchi a livello appli-

cativo, i nuovi apparati si differenziano dai prodotti di fascia consumer utilizzati da molte aziende di piccole dimensioni, poiché integrano funzionalità avanzate quali anti-malware, prevenzione delle intrusioni, filtraggio dei contenuti/URL e controllo delle applicazioni. L'esclusivo motore Reassembly-Free Deep Packet Inspection di

SonicWall, integrato nella serie TZ, garantisce una protezione completa della rete senza introdurre latenza, un problema frequente in altri firewall, che ostacolano così la produttività aziendale nei momenti di massimo traffico.



Kaspersky protegge il network casalingo

Kaspersky Pure, la soluzione di sicurezza di Kaspersky Lab, arriva sul mercato nella nuova versione 2.0 caratterizzata dalla denominazione Total Secure che si indirizza alla protezione dei pc e dei beni digitali comunemente presenti all'interno del network casalingo.

Questa soluzione si basa sul Kaspersky Security Network che implementando un approccio ibrido sfrutta sia le tecnologie di controllo cloud predisposte da Kaspersky Lab, sia motori di sicurezza installati sul pc, ponendo un'attenzione particolare a temi quali il controllo parentale, il backup e la gestione delle password.

In più Kaspersky Pure 2.0 prevede una nuova interfaccia grafica all'interno della quale sono inclusi i moduli di protezione che svolgono funzioni di protezione da malware, scansione in tempo reale del traffico Web, controllo delle applicazioni, sandbox (la tecnologia che consente di emulare il comportamento delle applicazioni in un ambiente virtuale), controllo sulle operazioni effettuate a livello di sistema operativo, anti-virus per Instant Messaging, firewall, blocco degli attacchi di rete. Possibile anche cifrare le informazioni collocate all'interno di una parte del disco rigido, con accesso controllato da password.

Continua online



La strategia per una sicurezza completa secondo Check Point

La 3D Security del vendor spiegata dal country manager Rodolfo Falcone. Policy, People ed Enforcement le parole chiave

C'è molta confusione nelle aziende: ancora oggi, come in passato, sono troppe in Italia quelle che approcciano la sicurezza introducendo una soluzione in risposta a uno specifico problema. La pensa così Rodolfo Falcone, country manager di Check Point, che afferma: «Si fanno tante discussioni, ma poi non si trova una direzione strategica sul tema security, non si prendono decisioni. Noi ne consigliamo una molto semplice, ma estremamente efficace: consolidare! Oggi le imprese, nelle loro infrastrutture hanno soluzioni di 4 o 5 vendor di sicurezza. Questo comporta spese maggiori in tecnologia e soprattutto in conoscenza e competenze, che se non possiedi all'interno devi acquistare fuori». Oggi, secondo il manager italiano, non si può continuare a ragionare in termini di singole soluzioni, ma occorre un approccio unificato: «La sicurezza deve essere integrata e gestita centralmente ed è inutile nascondere che sussiste un problema di budget. Consolidando è possibile ottimizzare la spesa per la sicurezza: con una o, massimo, due soluzioni è possibile coprire tutte le esigenze e, quindi, risparmiare sia sui costi delle licenze e sulla gestione dei contratti, sia sulla manutenzione e sull'amministrazione della sicurezza. Rendendo, inoltre, il sistema più efficiente, perché si può gestire tutto da un'unica console, senza doverne usare quattro o cinque».

Oltre che integrato, l'approccio deve essere strategico, per questo, invece che il classico punto di

Check Point propone di guardare la sicurezza da tre angolazioni diverse, lasciando solo per ultima la tecnologia

vista focalizzato sui prodotti, Check Point propone di guardare la sicurezza da tre angolazioni diverse, lasciando solo per ultima la tecnologia: «Una volta che ho definito quali sono le policy, qual è quindi l'obiettivo che devo perseguire, e quali sono le aree critiche, sulle quali faccio formazione. A questo punto posso stabilire quale tecnologia è necessaria per fare "enforcement", quali strumenti e software servono per aiutare gli utenti ad applicare le policy. La tecnologia è l'ultimo tassello: prima devo riflettere. Numeri alla mano, abbiamo dimostrato a molti clienti come questo significa ottimizzare e risparmiare», continua Falcone. È la strategia della 3D Security, che contempla appunto tre dimensioni: policy, people ed enforcement. Come spiega il country manager di Check Point:

«Il primo passaggio da compiere in azienda è definire le policy per la sicurezza, disciplinando l'uso delle risorse. Tanti si spaventano, ritenendo la definizione delle policy un lavoro molto grande. Eppure possono bastare anche tre paginette con quattro regole ben scritte. Un buon vendor di sicurezza – prosegue Falcone – deve aiutare i propri clienti a definire le policy, allineandole alle normative e alle esigenze aziendali. Una volta definite le regole è necessario renderne edotti gli utenti, che sono il classico anello debole. Diffondere la cultura della sicurezza è fondamentale: riguarda le aziende e, più in generale, la società, perché l'informatizzazione cresce».

Leggi online l'intervento di Falcone



Rodolfo Falcone di Check Point

G-Data protegge pc, smartphone e tablet

La crescita di minacce sempre più varie e G-data, spinta da questi scenari dinamici, ha rinnovato la propria offerta per il consumer con la nuova line up 2013. Elevato detection rate (99,7%, certificato da una comparazione indipendente come primo) e minimo impatto sulle risorse del pc, dichiarato dal costruttore, sono le caratteristiche distintive della nuova suite, il cui prodotto di punta è G-Data TotalProtection, confezione Oro, che fornisce una protezione completa anche contro la perdita dei dati grazie al modulo di backup integrato. La novità principale, però, riguarda tutta la suite e consiste nel numero di licenze incluse in ogni prodotto: due licenze per PC con l'aggiunta gratuita dell'antivirus per smartphone e tablet con sistema operativo Android. Il costo rimane invariato rispetto alla versione precedente con una sola licenza. Subito sotto TotalProtection, troviamo G Data InternetSecurity 2013, confezione Argento, che protegge contro tutti i rischi della rete e include la protezione della navigazione dei bambini. Infine, G Data AntiVirus 2013 protegge il pc dagli attacchi di virus, trojan e altri malware, grazie a una moderna tecnologia intelligente che si basa sulla combinazione di due motori di scansione, tecnologia cloud e protezione proattiva.

Sicurezza degli ambienti cloud con Trend Micro

Il vendor propone soluzioni per ambienti virtuali e cloud che si stanno diffondendo nelle aziende, conquistando una posizione di rilevanza nel mercato

TechNavio, società indipendente che valuta i prodotti IT, ha stimato un giro d'affari per il mercato globale della sicurezza cloud pari a 241 milioni di dollari nel 2010. Entro il 2014 lo studio "Global Cloud Security Software Market" stima una crescita composta aggregata (CAGR) del 41,4%, per un traguardo atteso di 963,4 milioni di dollari. Sempre secondo i dati emersi in questo studio di TechNavio, Trend Micro, tra i quattro principali protagonisti del settore sicurezza, è quello con la maggiore quota di tale segmento.

Più precisamente, la ricerca evidenzia la diversificazione geografica ottimale, la base di clienti ben consolidata e una brand reputation affermata, tra le ragioni del successo, dovuto anche all'alleanza con il leader

della virtualizzazione, VMware, e agli accordi con altri importanti vendor dell'IT, quali HP, Cisco, Dell, Microsoft, Oracle e Wipro.

Secondo TechNavio gli elementi che contribuiscono maggiormente al rapido sviluppo del mercato della Cloud Security sono il crescente utilizzo dei servizi cloud per la memorizzazione dei dati critici, ma anche il rapido incremento degli attacchi mirati ai danni del cloud stesso. In generale, sempre più imprese scelgono di trasferire i loro dati sul cloud per le sue carat-

teristiche di flessibilità, riduzione dei costi e disponibilità.

Stefano Volpi, country manager di Trend Micro Italy, commenta: «La presenza dominante di Trend Micro nella cloud security, deriva dalla focalizzazione e dall'impegno a supporto di progetti innovativi. Approccio che ci ha permesso di estendere il raggio di azione della nostra infrastruttura cloud globale, massimizzando la sicurezza, abbattendo le complessità e favorendo una migliore user experience».

Le soluzioni Trend Micro per gli ambienti virtuali e cloud sono Trend Micro SecureCloud, che garantisce la protezione dei dati negli ambienti virtuali VMware vSphere e nei cloud pubblici e privati, utilizzando funzioni crittografiche con gestione policy-based delle chiavi e convalida

dei server, e Trend Micro Deep Security, che fornisce sicurezza a livello di sistema e di applicazioni in ambienti fisici, virtuali e in the cloud.

Deep Security risponde alle tipiche problematiche di sicurezza operativa e compliance che caratterizzano l'attuale data center dinamico, coniugando funzioni di rilevamento e prevenzione delle intrusioni, web application protection, firewall, monitoraggio dell'integrità, ispezione dei log e anti-malware in un'unica soluzione gestita centralmente.

Secondo uno studio di TechNavio, Trend Micro è uno dei quattro protagonisti a livello mondiale del settore della sicurezza



Contenuti esclusivi sul sito di Reportec

Registrandovi gratuitamente su

www.reportec.it/registratori

potrete accedere ai contenuti esclusivi, analisi, report, opinioni, documenti di approfondimento su tecnologie e strategie ICT.

È in stampa 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.

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.



Una sintesi dei contenuti:

capitolo 1. Una strategia per la sicurezza e la continuità del business

capitolo 2. I nuovi rischi per la sicurezza:

capitolo 3. La gestione del rischio aziendale e la compliance

capitolo 4. Data center, sicurezza e business continuity

capitolo 5. La sicurezza delle reti

capitolo 6. Gestione delle minacce e data protection

capitolo 7. Il binomio sicurezza logica e sicurezza fisica

[clicca per vedere il sommario completo](#)

Il libro è in vendita al prezzo di 50 euro (più IVA) ed è prenotabile scrivendo a info@reportec.it o contattandoci via tel. 0236580441 e fax 0236580444

**Security
&
Business**

Numero 08 - Maggio-Giugno 2012 - Tutti i marchi sono di proprietà delle relative società
Editore: Reportec Srl - Direttore responsabile: Gaetano Di Blasio In redazione: Giuseppe Saccardi, Riccardo Florio, Paola Saccardi - Registrazione al tribunale n°585 del 5 Novembre 2010 Immagini da: www.dreamstime.com - www.security-business.it

Reportec

Reportec Srl. - Via Marco Aurelio 8 - 20127 Milano - Tel. 0236580441 - Fax 0236580444 - www.reportec.it