

IN QUESTO NUMERO

NEWS

- 6** La sicurezza, in chiave business
- 7** Una minaccia per le posizioni IT
- 8** Symantec cambia pelle
- 10** Sorveglianza via Internet
- 10** Inaz controlla accessi e presenze
- 10** NetApp: "Salviamo di più a meno"
- 12** Pericolo POS per i dati finanziari
- 12** PMI: Trend Micro pensa a Vista...
- 13** ...E Websense le protegge dal Web

COVER STORY

- 16** I risvolti nella gestione delle patch
- 20** IAM: un nodo da sciogliere

24 Outsourcing, ma sicuro...

27 PMI: cambiano le regole

SCENARI

30 Come lavora il cyber crimine

34 Il vecchio phishing è tornato

37 Intervista a Eugene Kaspersky

TECNOLOGIE

42 RFID, i quattro miti da sfatare

TEST

45 Mail server: Kerio MailServer

48 Firewall: Watchguard Firebox X Core 1250e

LA GUIDA PER I RESPONSABILI DELLA SICUREZZA ICT

Direttore Responsabile
PAOLO LOMBARDI (tel. 02/58038.218)

Redazione:
FRANCESCO PIGNATELLI (tel. 02/58038.272)
PAOLO MORATI (tel. 02/58038.246)
(redazione online)

Hanno collaborato a questo numero
FRANCESCO HEMMELER, LUCA RUFO MASONI, ELIO MOLteni

Grafica e Impaginazione
LIA PITARRESI

Responsabile Pubblicità Internazionale e On line
Mauro Buccola (mauro_buccola@nuovaperiodici.it)

Segreteria e Ufficio Traffico Pubblicità:
Margherita Bertocelli
(margherita_bertocelli@nuovaperiodici.it),
Silvia Cardinale (silvia_cardinale@nuovaperiodici.it),
Simona Cattaneo (simona_cattaneo@nuovaperiodici.it)
Tel. 02/580381

Ufficio Commerciale
Emanuela Cella (emanuela_cella@nuovaperiodici.it), Maurizio Dell'Abate
(maurizio_dellabate@nuovaperiodici.it),
Antonio Martinelli (antonio_martinelli@nuovaperiodici.it),
Daniela Parisse (daniela_parissee@nuovaperiodici.it),
Massimiliano Parma
(massimiliano_parma@nuovaperiodici.it),
Maurilio Vitali (maurilio_vitali@nuovaperiodici.it)

Agente per il Lazio e il Centro Sud:
Parisse Pubblicità: via Casal de' Ceveri 8 - 00060 FORMELLO (RM)
Tel. e Fax 06/90405002. (pparissee@iol.it)

Produzione e Servizi Generali
Nilde Meregalli

Marketing e Comunicazione
Claudia Cavallieri, Rosa Guerinoni

Abbonamenti e Diffusione
Enrico Zambetta (Responsabile), Tiziana Parma
Per informazioni sugli abbonamenti:
telefonare allo 02/58038253 o via fax 02/58038306

Una copia 0,52 € - Abbonamento annuo per l'Italia:
45 numeri 23,40 € - (ccp n. 19933209).
Estero: Europa 90 €, - Extraeuropa 97 € (compresa la spedizione)

Direzione, redazione, pubblicità,
sede legale e amministrazione:
Nuov@ Periodici Italia s.r.l.
Via Zante 16/2 - 20138 Milano
Telefono 02/58.038.1 - Telefax 02/58.01.16.70

Registrazione del Trib. di Milano n.193 del 24-4-83

Stampa: CPM Casarile (Milano)
Spedizione in a. p. 45% art.2
Comma 20/B legge 662/96 - filiale di Milano

Computerworld Italia è certificato da ADS -
Certificato ADS n° 5798 del 4/12/2006
Periodo di accertamento dal 1/1/2005 al 31/12/2005

A.N.E.S.
ASSOCIAZIONE NAZIONALE
EDITORIA PERIODICA SPECIALIZZATA
Computerworld® è un marchio registrato
di International Data Group, Inc.



NUOV@PERIODICI

Amministratore Unico
Mario Toffoletti

Direttore Generale
Costantino Ciaffi

Responsabile ufficio Amministrazione e Contabilità
Bruno Agostini

Responsabile ufficio IT
Luca Rufo Masoni

Amministrazione
Elga Legranzi, Grazia Rovati, Katia Trespidi



La sicurezza, in chiave business

Quattro chiacchiere con Alastair MacWillson, managing director Global Security Practice di Accenture. Tra compliance e 'deperimetrizzazione' ecco come le aziende guardano alla sicurezza informatica

a cura di PAOLO MORATI

Abbiamo incontrato Alastair MacWillson, managing director della Global Security Practice di Accenture, per discutere di sicurezza informatica e business, e dell'evoluzione che questa tematica sta avendo sia dal punto di vista dell'approccio delle imprese che delle funzionalità tecnologiche.

A livello organizzativo, com'è percepito oggi dalla dirigenza aziendale il tema della sicurezza informatica, anche alla luce delle richieste normative in termini di compliance e privacy?

Ritengo che l'aspetto della privacy e della compliance abbia avuto un effetto abbastanza forte sulla visibilità del tema della sicurezza in molte organizzazioni. Questo perché le normative in vari Paesi, Italia inclusa, stanno diventando alquanto severe. I dirigenti aziendali stanno di fatto valutando le responsabilità e i rischi legati a tali regole, qualora non vi prestino la dovuta attenzione, e quindi, la sicurezza è diventata un punto di discussione. D'altro canto, non credo che molti di loro stiano guardando a queste cose come a un possibile beneficio per il business

(vedi riquadro), anche se tali tematiche rappresentano comunque una leva per migliorare i controlli di sicurezza sull'intero ambiente dell'organizzazione in cui si opera.

E in questo discorso rientra quindi anche quello dell'automazione, con la possibilità di utilizzare cruscotti che mostrino cosa sta effettivamente accadendo e una strada che chiarisca quali sono i sistemi che non sono effettivamente conformi alle regole. Pensando alle PMI, così numerose in Italia, un fattore di spinta all'adozione delle soluzioni di sicurezza può essere rappresentato dal loro rapporto, in qualità di fornitori, con le grandi aziende. Queste ultime stanno infatti richiedendo che la propria supply chain sia propriamen-

“Si sta andando verso una 'deperimetrizzazione' dell'impresa, con una forma di protezione diversa che si allontana da quella offerta dal solo firewall. Tutto questo richiede però un modo molto sofisticato di pensare la sicurezza”

ALASTAIR MACWILLSON, ACCENTURE



te controllata, per esempio in termini di sistemi di identità. Le grandi realtà stanno insomma cominciando a dettare le regole in tal senso.

Dal punto di vista prettamente tecnologico, quali sono le evoluzioni che vede all'orizzonte in questo settore?

Si sta andando verso una

'deperimetrizzazione' dell'impresa, con una forma di protezione quindi diversa, che si allontana da quella offerta dal solo firewall. Tutto questo richiede un modo molto sofisticato di pensare la sicurezza. Guardiamo ad esempio all'identity & access management, che diventa un grande abilitatore per ogni azienda.

COSA DICONO I RESPONSABILI DEI SISTEMI INFORMATIVI AZIENDALI

Una ricerca compiuta da Accenture a livello mondiale ha individuato quelle realtà che definisce aziende ad 'alte prestazioni' e il loro comportamento nei confronti della tematica della sicurezza. Nel 68% dei casi la sicurezza è posizionata tra le



cinque priorità infrastrutturali nell'agenda dei dirigenti IT. E lo stare al passo con le relative minacce è considerato una delle sfide principali a cui devono far fronte soprattutto in Italia, Giappone e Stati Uniti. D'altro canto, la maggior parte dei responsabili IT sondati fa anche fatica a spiegare il valore di business della sicurezza. E la percentuale sul proprio budget dedicata a quest'area varia dal 9,1% al 11,8%. "La sicurezza va in ogni caso considerata una caratteristica chiave del business dei top performer. Pensiamo, ad esempio, ai fornitori di carte di credito", spiega il managing director della Global Security Practice Alastair MacWillson. "E' un segnale per dire

newsnews

Pensiamo alle SOA, che danno molta agilità e flessibilità. La barriera maggiore alla loro adozione è proprio la sicurezza. Questo perché, se prima un'azienda utilizzava al suo interno applicazioni molto protette, ora deve invece presentarle al di fuori, in una forma differente. Si parla della linfa vitale del business e le capacità di integrazione con il mondo SOA offerte da un sistema di gestione di accessi e identità può favorire un rapido decollo di queste architetture, risolvendo tale preoccupazione.

Cosa può dirmi del fenomeno in espansione del phishing? Quali sono le azioni che devono essere compiute per contrastarlo?

E' un 'fact of life'. Le imprese, comprese alcune banche italiane, stanno facendo un po' di cose per educare meglio i rispettivi clienti, alertandoli regolarmente sull'esistenza del problema. Stanno anche mettendo all'opera sistemi migliori per

“Oggi le aziende, comprese alcune banche italiane, stanno compiendo una serie di azioni per educare meglio i rispettivi clienti, alertandoli regolarmente sull'esistenza di problemi che minano la sicurezza personale, come per esempio il phishing”

identificare e disabilitare gli attacchi di phishing. Si tratta però solo di azioni compiute dopo che il fatto è ormai accaduto. È invece agli operatori telco che bisognerebbe chiedere di risolvere il problema, perché sono loro che trasportano il traffico di phishing e possono quindi sapere dove viene generato, sia direttamente che via proxy. In pratica, le banche possono dire “Noi dobbiamo risolvere il problema dopo l'evento”, ma alle telco possono chiedere “Voi dovete risolverlo prima che [il phishing] arrivi ai clienti”. **nw**

che si tratta di un'azienda valida”.

Un'altra ricerca condotta in Europa e Stati Uniti evidenzia che la maggiore priorità delle organizzazioni è quella di ridurre la complessità della sicurezza e, tra chi valuta regolarmente rischi e minacce, solo il 34% sfrutta tali informazioni per guidare le scelte di budget e pianificazione.

Contemporaneamente, sempre da tale ricerca emerge come il riuscire a misurare il valore della sicurezza sia giudicata un'operazione difficile. “Un'altra statistica ‘scioccante’ vede il 68% dei business executive ritenere la sicurezza come una problematica che riguarda l'IT, il 53% come un male necessario, mentre l'80% non la considera come un abilitatore di business o un elemento che aggiunge valore. E' quindi necessario creare un link tra sicurezza e obiettivi di business e rendere il tema della sicurezza effettivamente accessibile”, conclude MacWillson.

E' anche una minaccia per le posizioni IT

Un'inchiesta rivela che quando si parla di sicurezza la funzione IT non si sente ancora molto tranquilla

Quando si parla di sicurezza informatica in azienda, la funzione IT ancora non si sente tranquilla. Molti professionisti IT, infatti, ritengono a rischio il proprio lavoro nel caso di problemi relativi alla sicurezza. E allo stesso tempo si sentono 'mal equipaggiati' per prevenire perdite di dati personali o aziendali. Lo afferma una recente inchiesta condotta dall'americana King Research.

Nel dettaglio, circa tre quarti di un campione di oltre 250 professionisti IT sono preoccupati di perdere il proprio posto come conseguenza di un'importante breccia nella sicurezza dell'azienda per cui lavorano. “I dipartimenti IT stanno lavorando senza sosta per combattere e minimizzare le problematiche relative alla sicurezza. Ma nonostante l'ampia gamma di strumenti in cui le organizzazioni hanno investito, esistono ancora dei gap a livello di sicurezza”, commenta Diane Hagglund, analista di King Research.

Circa due terzi dei professionisti IT del campione intervistato dichiarano che la responsabilità associata a tali breccie va a colpirli perso-

nalmente. E mentre l'87% si dice fiducioso della propria capacità di reagire ad attacchi compiuti via virus, spam, spyware e malware, solo il 35% ritiene di essere in grado di gestire la perdita di da-

Circa il 65% dei professionisti IT appartenenti a un campione di 250 ritiene a rischio il proprio lavoro nel caso di problemi relativi alla sicurezza

ti personali o aziendali.

Circa la metà dei professionisti IT considera la conoscenza e l'integrazione di applicazioni differenti di system & security management come il problema maggiore da superare per cercare di proteggere tutti i dispositivi aziendali.

Quasi il 100% ha un anti-virus, oltre l'80% software antispyware e di patch management, e circa il 70% ha installato aggiornamenti software automatizzati. Tuttavia, pochi hanno riportato di avere prodotti di configurazione automatica del desktop (50%) e di scansioni delle vulnerabilità dei cosiddetti 'end-node' (35%). **nw**

COVER STORY



Uno degli aspetti più significativi nel complesso mondo della sicurezza delle informazioni consiste nell'individuare e gestire le vulnerabilità che affliggono la maggior parte dei software utilizzati per processare tali informazioni.

Chiunque si occupi di informatica sa che il software è, per sua natura, soggetto a errori di programmazione e tali errori - i quali normalmente vengono scoperti durante il processo di sviluppo e di

patch

test, ma possono anche rivelarsi successivamente nei prodotti rilasciati - possono essere causa di vulnerabilità specifiche e quindi, se sfruttati da malintenzionati, essere veicoli per la conduzione di attacchi ai sistemi informatici di qualunque dimensione e tipologia.

LE DIMENSIONI DEL PROBLEMA

Le statistiche del CERT indicano che il numero di vulnerabilità identificate è passato dalle 3.784 del 2003 alle 8.064 del 2006 e che il trend è evidentemente in crescita.

La sfida dei responsabili informatici e della sicurezza di tutto il mondo è quella di intervenire con rapidità per risolvere le vulnerabilità che vengono scoperte e poi rese pubbliche.

Questa battaglia può essere vinta solo attraverso l'impegno dei produttori di software, chiamati a rila-

Foto: IBM

I risvolti economici nella gestione delle patch

Molti CSO ritengono le vulnerabilità un problema in realtà non risolvibile, ma non effettuano neanche una accurata valutazione dei costi associati

coverstory

sciare aggiornamenti funzionali e di sicurezza (patch) in tempi sempre più brevi.

Ciononostante, l'impegno che ogni organizzazione deve mettere in campo per gestire tale problematica cresce esponenzialmente all'aumentare della tipologia e numerosità dei sistemi utilizzati. Tale difficoltà spinge, il più delle volte, a considerare illusoria la risoluzione del problema, lasciando aperte breccie preferenziali per violare la sicurezza dei propri sistemi.

In una recente ricerca condotta da IPSOS, che ha coinvolto diverse centinaia di manager IT e della sicurezza a livello di media-grande azienda europea, il problema è indicato con particolare enfasi, principalmente per la sua complessità e i suoi costi, in particolare per le grandi aziende.

In media un intervistato del campione su quattro spende alcune ore al giorno alla ricerca di vulnerabilità e nell'installazione di patch, quota che per l'Italia sale a uno su tre. Il lungo tempo necessario alla gestione del problema (dalla scoperta della vulnerabilità alla disponibilità della patch da parte del produttore del software e successivamente alla sua implementazione) comporta che la cosiddetta "finestra di vulnerabilità" resta troppo ampia, durando a volte settimane e anche mesi. Sempre nella stessa ricerca è indicato che oltre un quarto degli

In Italia la finestra di vulnerabilità può arrivare ad alcune settimane e anche mesi

intervistati impiega almeno tre giorni dal rilascio della patch alla totale implementazione, mentre per un'azienda europea su cinque è necessaria fino a una settimana o oltre per l'implementazione.

Ragionando in termini di costi, accade spesso che il problema economico venga sottovalutato, in quanto non è direttamente misurabile il costo diretto da esso generato. Volendo fare un esempio, nella tabella a pagina 19 è ipotizzata l'incidenza dei costi complessivi legati alla gestione del problema sul budget di spesa della funzione IT. L'ipotesi si riferisce ad una realtà di media-grande dimensione, tra 50 e 100 dispositivi infrastrutturali (server, dispositivi di rete, etc.) e un massimo di 500 utenze client. L'ipotesi inoltre non tiene conto dei costi non misurabili. Infatti la prevenzione di un incidente potrebbe aggiungere un valore fuori scala.

Ne consegue come non sia economicamente sostenibile per la singola azienda affrontare in modo autonomo la problematica del patching. A questo scopo esistono enti di ricerca, aziende specializzate e organizzazioni che rendono disponibili servizi e informazioni inerenti gli attacchi e le relative contromisure. In conclusione (la fonte è sempre IPSOS) la maggior parte delle organizzazioni ritiene di dover dedicare più risorse alla gestione del problema in futuro, anche perché direttamente collegato alla "compliance" rispetto a specifiche normative (nazionali e di settore), in Italia per esempio il D.Lgs 196/03 - codice in materia di protezione dei dati personali.

IL CICLO DI VITA DELLE VULNERABILITÀ

Le informazioni caratterizzanti una vulnerabilità seguono un percorso evolutivo che risulta piuttosto

UN DIBATTITO IN CORSO

Periodicamente si tengono "gare di hacking" in cui ricercatori e appassionati più o meno noti vengono sfidati a trovare e sfruttare delle nuove vulnerabilità, talvolta con ricchi premi in palio. Questo modo di trovare vulnerabilità critiche e i relativi exploit rende davvero più sicure le reti aziendali, o crea al contrario maggiori rischi perché crea un mercato per gli hacker più o meno etici? Alcuni, come Gartner, sostengono che le gare di hacking non siano il modo appropriato di portare avanti le ricerche di vulnerabilità, perché non danno modo ai produttori colpiti dalla vulnerabilità di porvi rimedio prima dell'annuncio pubblico della vulnerabilità stessa. (f.p.)

complesso. Una nuova vulnerabilità fa inizialmente la sua comparsa sotto forma di argomento di discussione su un newsgroup di Internet, come alert specifico su un sito Web, come messaggio su una mailing list o come entry in una newsletter. Le informazioni non sono necessariamente strutturate secondo un formato standard comprensibile e utilizzabile da chiunque, né tantomeno concentrate in un unico luogo.

Una vulnerabilità è quindi una realtà dinamica, che evolve rapidamente con l'aggiunta nel tempo di nuove informazioni, sempre più dettagliate. Filtrare le miriadi di informazioni disponibili sulle vulnerabilità, trovare ciò che è rilevante per la propria organizzazione, valutarlo, testarlo e intraprendere la giusta azione correttiva richiede uno sforzo notevole in termini di tempo, denaro e manodopera qualificata.

A seguito di questa fase si registra quindi la nascita di strumenti che sfruttano la vulnerabilità facilmente reperibili in Internet (i cosiddetti exploit).

Quando la vulnerabilità ha raggiunto un sufficiente livello di maturazione, cominciano a fare la loro comparsa le soluzioni alla vulnerabilità stessa, prima quelle provvisori-



SCENARI



Se in passato gli hacker hanno sferrato i loro attacchi spinti soprattutto dalla voglia di notorietà, oggi le motivazioni alla base del loro agire stanno cambiando e, sempre più spesso, ciò che sta dietro le loro operazioni è essenzialmente una questione di denaro. Il cyber crimine è diventato ormai infatti una vera professione - potremmo addirittura parlare di un modello di business - e la tipologia del criminale informatico sta cambiando di conseguenza: dall'immagine classica dell'individuo che non esce mai dalla propria camera, alla figura più tipica del criminale organizzato, molto simile a quella del trafficante di droga, coinvolto in attività di estorsione e riciclaggio di denaro.

analisi

NON SERVE ESSERE TECNICI

Anche l'immagine dell'hacker come grande esperto tecnico sta lentamente tramontando: persone con conoscenze informatiche minime oggi possono infatti rubare migliaia di euro ogni giorno, senza allontanarsi dalla propria abitazione. Di fatto, l'unico momento in cui il criminale deve allontanarsi dal proprio pc è quando deve ritirare il denaro, e a volte nemmeno in quel caso.

La cosa sorprendente è che il guadagno è spesso più elevato di

Fonte: Oracle

Come lavora il cyber crimine: una realtà molto variegata

Strumenti informatici alla portata anche dei non esperti, reti internazionali di collaborazione, guadagni elevati a fronte di rischi ridotti rispetto al crimine 'fisico'

Pariscenaris

quanto sia possibile ottenere con una massiccia produzione e vendita di eroina di classe A (e con un rischio molto inferiore).

In ogni impresa, i modelli di business efficienti si basano sia sulla divisione orizzontale di processi di produzione, servizi professionali e canali di vendita (ciascuno dei quali richiede abilità e risorse specializzate), sia su una buona strategia di commercializzazione a seconda delle forze della domanda e dell'offerta del mercato. Il cyber crime non è diverso; vanta un mercato internazionale vivace costituito da competenze, tool e prodotti finiti. Ha perfino una propria moneta.

GLI STRUMENTI E LE SOLUZIONI

Il cyber crime è cresciuto parallelamente all'aumento delle transazioni con le carte di credito sul web e al proliferare dei conti correnti bancari on line. Una volta che ci si è impossessati delle informazioni finanziarie relative a un conto e a una carta di credito, non solo si può rubare senza essere scoperti, ma anche – attraverso un processo automatizzato guidato da virus – ipoteticamente per un numero infinito di volte.

Esistono molti e diversi metodi attraverso i quali è possibile ottenere i dati delle carte di credito e dei conti correnti. Ognuno di essi comporta naturalmente una propria combinazione di rischi, spese e abilità. La cosa più semplice è acquistare il "prodotto finito" e in questo caso useremo come esempio un conto corrente on line. Il prodotto è rappresentato dalle informazioni necessarie per ottenere un controllo "autorizzato" su questo conto corrente a sei cifre. Il costo per ottenere queste informazioni ammonta a

IRC
Forma di comunicazione istantanea su Internet, sia tra due utenti che interi gruppi

circa 400 dollari (la valuta con cui sempre trattano i criminali informatici trattano sempre in dollari). Sembra una cifra irrisoria, ma considerando il poco lavoro necessario a ottenere i dati e il basso rischio che si corre, si tratta di denaro facile. Inoltre, dobbiamo ricordare che questo è un

offshore e possono essere creati on line e trasferiti a conti di "denaro reale" in modo anonimo.

I diversi protagonisti nella comunità del crimine informatico ricoprono ruoli di diversa importanza e che richiedono differenti specializzazioni. Possiamo dividerli - in linea di massima - nei quattro gruppi che elenchiamo nella prossima pagina. ▷



Fonte: Panda Software

commercio internazionale; molti cyber criminali di questa categoria provengono da Paesi poveri dell'Europa dell'Est, Sud America o dell'Asia Sud-Est per i quali si tratta comunque di una somma economica significativa.

Il probabile luogo dove avviene questo tipo di transazioni sarà una chatroom **IRC** (Internet Relay Chat) nascosta e la "quota" di 400 dollari verrà facilmente trasformata in una qualche forma di denaro virtuale. I conti con denaro virtuale infatti non sono regolati da alcuna legislazione, sono registrati in Paesi

LA GUERRA INFORMATICA

Gli attacchi informatici che a maggio dalla Russia sono stati portati all'Estonia sono stati lo spunto che il Commissario europeo alla Giustizia, Franco Frattini, ha usato per spingere verso una maggiore collaborazione dei Paesi UE nella lotta al cybercrime. L'attacco degli hacker ostili russi sembra una ritorsione contro l'eliminazione di un mausoleo in memoria dei caduti russi che si trovava a Tallinn, capitale dell'Estonia. Fonti ufficiali del Governo estone affermano che gli attacchi ai siti Web estoni sono stati tracciati e provengono da server governativi russi. "In Estonia - ha spiegato Frattini - ci sono stati 128 diversi attacchi durante le prime due settimane di maggio... Sono stati attacchi coordinati contro una nazione, non solo contro un ministero. In situazioni come queste dobbiamo cooperare e sviluppare una strategia di prevenzione", ha aggiunto. Bruxelles sarà a novembre sede di una conferenza specifica: "Il suo scopo - ha spiegato Frattini - è semplicemente quello di sradicare il cybercrime". (f.p.)

TECNOLOGIE

I quattro miti da sfatare della tecnologia RFID

Limiti e problemi hanno ridimensionato le promesse e rallentato l'adozione di questa tecnologia come arma sicura nella lotta alla contraffazione dei farmaci

Da un paio di anni a ogni singola boccetta del medicinale OxyContin della Purdue Pharma consegnato ai distributori viene apposta una etichetta speciale. Nascondo nell'etichetta si trova un tag di identificazione in radiofrequenza (RFID) appositamente disegnato per consentire all'azienda farmaceutica di tenere traccia del percorso compiuto dal farmaco attraverso la catena di fornitura. L'intento è quello di permettere ai distributori che ricevono le confezioni di verificare rapidamente, con degli appositi lettori, l'autenticità delle boccette di medicinale, leggerne la provenienza e respingere alla casa farmaceutica quelle senza le indicazioni corrette.

“Un sistema efficiente, accurato, che fa quello che a noi serve dal punto di vista della sicurezza e senza creare rallentamenti nel sistema distributivo” afferma il CSO della Purdue Pharma.

Non si tratta certo di novità eclatanti, visto che se ne parla da anni. Il CSO non può neppure fornire particolari dettagli sui risultati ottenuti nella lotta alla contraffazione del farmaco visto che la sua casa farmaceutica non ha avuto mai problemi di questo tipo.

Per contrastare davvero la contraffazione dei farmaci occorrerebbe un sorta di sistema centralizzato ti-



po ‘camera di compensazione’ che consenta a ogni distributore e a ogni farmacia di controllare e validare il ‘pedigree’ di ogni farmaco. Un obiettivo assai più complesso, evidentemente, che non il tracking di un solo tipo di farmaco indirizzato verso due differenti distributori, che è quanto sta facendo Purdue Pharma.

La necessità di prevenire la contraffazione dei farmaci è molto sentita. L’Organizzazione Mondiale della Sanità ha quantificato il volume d'affari prodotto dalle vendite di farmaci contraffatti nel 10% del

totale prodotto da questo business, attribuendo a queste contraffazioni la responsabilità di alcune migliaia di decessi l'anno.

Il problema è che decenni dopo l'invenzione della tecnologia RFID questa tecnologia resta ancorata allo status di “più promettente tecnologia anti contraffazione”.

Secondo i responsabili del Vulnerability Assessment Team dei Laboratori di Los Alamos “per quanto riguarda la sicurezza, guardare alla tecnologia come a qualcosa di miracoloso - si prende un'etichetta in radiofrequenza, la si applica a un og-

tecnologie

getto e si pensa che in qualche modo questo produca maggior sicurezza – è radicalmente sbagliato”. Perché? Ci sono almeno 4 ragioni che hanno radici in altrettanti miti sulla tecnologia RFID.

MITO N. 1: LE ETICHETTE RFID SONO DISPOSITIVI ANTICONTRAFFAZIONE

Abbiamo parlato con i responsabili dei test sull'RFID di alcuni tra i maggiori distributori di medicinali negli USA.

Da loro stessi le etichette RFID sono considerate anzitutto un dispositivo per il tracking, non per la sicurezza. Gli stessi produttori di etichette RFID sono tutto tranne che operatori in ambito sicurezza. Il semplice fatto di leggere informazioni su un'etichetta applicata a un prodotto non garantisce che quel prodotto sia autentico.

MITO N. 2: LA TECNOLOGIA RFID PUÒ ESSERE USATA PER 'MARCARE' PILLOLE E COMPRESSE

Quando i sostenitori dell'RFID la presentano come “la soluzione alla contraffazione dei medicinali”, il CSO di Novartis risponde subito che non sono i medicinali ad essere ‘marcati’ con l'RFID ma le confezioni. “Noi abbiamo visto medicinali contraffatti in confezioni originali, e medicinali genuini in confezioni contraffatte. Ma la confezione non è la cosa più importante”.

E comunque, di regola, i prodotti farmaceutici vengono riconfezionati sia negli USA che in Europa, per cui se un'azienda investe quattrini per inserire dispositivi di sicurezza nelle confezioni, i prodotti potrebbero essere legalmente spostati in confezioni prive di dispositivi di sicurezza.

Per questo il CSO di Novartis ritiene che cambiare le regole che governano la distribuzione (anche semplicemente rafforzando le pen-

pecuniarie per i trasgressori) potrebbe essere più efficace che usare le attuali tecnologie RFID per sconfinare la contraffazione dei medicinali.

MITO N. 3: L'RFID CONSENTIRÀ AI CONSUMATORI DI VERIFICARE CHE HANNO ACQUISTATO PRODOTTI ORIGINALI E NON CONTRAFFATTI

L'obiettivo ultimo di chi impiega l'RFID è quello di dare ai consumatori la sicurezza che i medicinali che hanno nel cassetto di casa sono autentici e non dei falsi.

Per il momento nessuno – non la FDA e neppure i diversi progetti pilota avviati dall'industria privata – è in grado di proporre un sistema capace di garantire ai consumatori la possibilità di validare come originali i prodotti di cui dispongono. In effetti è frequente il fatto che le etichette RFID vengono disabilitate prima che i medicinali raggiungano il cassetto di casa dei consumatori. Questo per le preoccupazioni che i grandi magazzini possano usare le informazioni presenti nelle etichette RFID per sapere quale confezione di quale medicinale è in possesso di un determinato consumatore. L'unica reale garanzia per il consumatore resta ad oggi in uno strumento che... più tradizionale non si può: la sua fiducia nella propria farmacia e nel fatto che il proprio farmacista acquisti soltanto prodotti assolutamente originali e non contraffatti.

MITO N. 4: L'INDUSTRIA FARMACEUTICA È ORMAI VICINA A UN'ADOZIONE COMPLETA DELL'RFID

Con tutti questi limiti non sorprende che, dopo essere stata indicata da anni come ‘LA’ soluzione per l'industria farmaceutica, la scelta di adottare la tecnologia RFID per rendere sicura la fornitura di medicinali abbia subito dei rallentamenti. La Federal Drug Admini-

DALLA PRIVACY ALLA SECURITY

‘Sebbene a livello normativo vi sia ormai una adeguata tutela contro utilizzi inammissibili delle tecnologie RFID l'enfasi si sposta dalla privacy alla security ovvero verso le modalità con cui ci si può tutelare dalla violazione (hacking) dei sistemi Rfid e il conseguente furto di informazioni riservate a scopi illeciti. (. . . .). Oggettivamente questo tema non è ancora compiutamente sviluppato. Nei casi in cui il tag contiene informazioni direttamente fruibili si stanno affacciando nuove soluzioni per ridurre o eliminare il rischio di violazione. Queste soluzioni possono essere classificate in base alla tipologia di intervento e suddivise in tre classi: interventi sui tag, interventi sui reader e, infine, interventi sul protocollo di comunicazione tra tag e reader. La numerosità delle leve tecnologiche disponibili mostra il grado di attenzione che i produttori stanno prestando a questa tematica. Molte di queste soluzioni sono tuttavia, allo stato attuale, solo immaginate e deve ancora essere intrapreso un processo organico di standardizzazione e diffusione delle migliori contromisure, ciascuna nell'opportuno contesto di adozione. Un processo che richiederà ancora del tempo’.

Da ‘Rfid: alla ricerca del valore’, Politecnico di Milano
Dipartimento di Ingegneria Gestionale 2007

stration, dopo aver rinviato per anni l'ora X per l'adozione dell'RFID ha pensato bene di darsi un'altra scadenza.

“Nel 2004 - spiega il responsabile FDA per il settore farmaceutico – pensavamo che nel 2007 l'RFID avrebbe avuto un pieno utilizzo. Non è stato così, ed ora, piuttosto che fissare noi un'altra scadenza, preferiamo lasciare la decisione agli operatori interessati”. In ogni caso la FDA continua a ritenere che l'RFID sia “la tecnologia più promettente per l'autenticazione dei medicinali”.

Forse, alla fine, sia i sostenitori dell'RFID sia gli scettici potranno convenire sul fatto che la tecnologia RFID potrebbe essere la strada più promettente, ma solo per attenuare un problema che al momento appare praticamente impossibile da risolvere. **nw**

TEST CENTER

Il mail server trasversale

Come funziona il server di posta elettronica di Kerio, nato con particolari funzioni di sicurezza e di gestione della messaggistica mobile

Quando si parla di posta elettronica, il panorama dei software server disponibili anche per piattaforme che non siano semplicemente Microsoft Windows non è poi così vasto. In questo ambito Kerio MailServer si è conquistato una sua fetta di utenti Windows, Linux (Fedora SuSE, Red Hat) e Mac OS X puntando sulla semplicità d'uso e sulla affidabilità del software nella gestione delle minacce informatiche, oltre che su un prezzo contenuto e sulla localizzazione in italiano, che non guasta mai.

L'installazione del mail server è semplice: chi vuole lo può scaricare dal sito del produttore e provarlo direttamente per un po'. Successivamente si decide se prenderlo in licenza definitivamente o se rimuoverlo dal proprio server.

L'amministrazione del software avviene da una console unica e separata dal mail server vero e proprio. Le opzioni di amministrazione sono raggruppate in quattro sezioni (Configurazione, Impostazioni dominio, Stato, Registri) di cui la

più importante è la prima. Le altre tre servono rispettivamente a gestire gli utenti e i gruppi di utenti che scaricheranno e invieranno mail, a controllare lo stato del mail server (statistiche del traffico, connessioni attive, eccetera) e a consultare i log di sistema per vedere cosa è successo durante il funzionamento del software.

QUESTIONE DI DNA

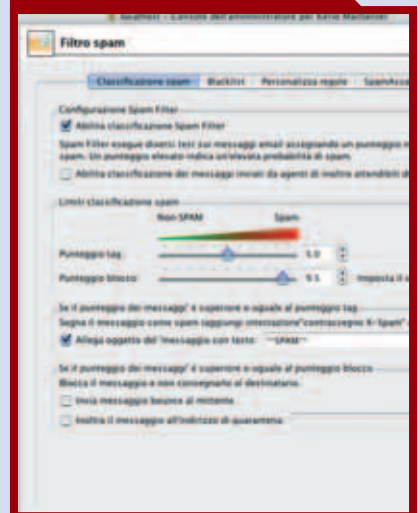
Nella parte di Configurazione si evidenzia il fattore di distinzione principale di Kerio MailServer, ossia l'attenzione alla sicurezza delle comunicazioni via mail. In effetti, storicamente Kerio nasce come software house dedicata alla sicurezza e si è interessata alla posta elettronica solo in seguito. Il suo mail server mostra chiaramente questa sorta di codice genetico.

Sono conseguentemente ben strutturate le funzioni di antispam, antivirus e controllo dei contenuti. Nel primo ambito il software Kerio adotta alcune forme di protezione classiche (la valutazione di un indice di spam, l'adozione di "black list" dei mittenti, l'integrazione con SpamAssassin) e altre meno banali come il controllo della "reputazione" del mittente tramite i protocolli Sender ID o SPF. C'è anche una importazione che indica a Kerio MailServer di comportarsi come un server SMTP lento per "scoraggiare" chi ha deciso di inviare fraudolentemente centinaia di migliaia di messaggi di spam utilizzando a nostra insaputa il mail server aziendale.

La parte antivirus è delegata a un motore interno (di McAfee) o si aggancia a diversi antivirus esterni (Avast, AVG, eTrust, NOD32, Sophos, Symantec). Utile anche



MAIL SERVER



L'interfaccia di Kerio MailServer è essenziale ma completa: adatta per l'utenza a cui si rivolge

