

SOPHOS

Protecting business against viruses, spyware, adware, spam and policy abuse.

secured.

SOPHOS

Protecting business against viruses, spyware, adware, spam and policy abuse.

Anno 1 N°2 Novembre/Dicembre 2006

Sommario

editoriale	attualità	cultura
education	pubblica amministrazione	impresa
service provider	operatori ICT	numero 2

Editoriale

Da utenti, magari un po' ingenui, a ricettatori senza passare dal via. È questa la fine che molti sprovveduti hanno fatto, e rischiano tuttora di fare, perché all'oscuro dei nuovi modi di agire dei cyber-criminali.

La breaking news che leggete in questa stessa pagina è sintomatica di un fenomeno che sta crescendo vertiginosamente e sfrutta, ancora una volta, la scarsa cultura sulla sicurezza informatica della maggior parte degli utenti.

Pur di racimolare spiccioli facili, si accetta di fornire informazioni riservate, come i propri numeri di conto corrente, per farvi transitare per via telematica fondi di cui, secondo il messaggio degli scaltri criminali, si potrà trattenere una parte. Risultato, si diventa riciclatori di denaro sporco e si rischia la galera. C'è qualcuno che ancora pensa che la sicurezza informatica non sia una priorità?

Rossella Lucangelo**IN QUESTO NUMERO:****La protezione dei dati nelle pubbliche amministrazioni****Dal database la sicurezza dell'azienda****Posta elettronica certificata**

Lo scorso luglio è stata emanata dal Tribunale di Milano **la prima condanna per phishing in Italia** per due truffatori appartenenti ad un'organizzazione criminale internazionale. Dotati di documenti falsi, i due avevano creato società fasulle intestandovi dei conti bancari per un'attività di riciclaggio in apparenza legittima. Utilizzavano l'esca del phishing per ricevere pagamenti che dopo essere stati versati sul conto corrente di altri individui coinvolti nella truffa, venivano trasferiti alle società fasulle e stornati su conti all'estero attraverso dei bonifici. I due truffatori dovranno scontare rispettivamente 4 anni e 4 anni e 6 mesi di reclusione e pagare una sanzione di 4000 euro.

attualità e cultura

L'evoluzione delle minacce informatiche, l'analisi degli esperti, il ruolo della tecnologia, la

Gli scenari futuri del mercato della sicurezza secondo IDC

Il mercato della sicurezza informatica continua a mostrare elevati tassi di crescita, decisamente superiori rispetto al mercato IT nel suo complesso: **IDC stima che in Italia nel periodo 2004-2009 la spesa in hardware, software e servizi di sicurezza cresca del 13% medio annuo, passando da 450 a più di 1000 milioni di Euro di spesa annua.**

Si tratta di un settore in continuo rinnovamento, per quanto riguarda sia le minacce che le tecnologie di prevenzione e risoluzione dei problemi, le metodologie per implementare piani di sicurezza e le norme che definiscono una corretta gestione dei sistemi.

Non a caso **secondo IDC i settori della sicurezza e della Business Continuity sono considerati tra i "Best Performer Markets" in termini di crescita attesa della spesa delle aziende nei prossimi 4-5 anni.**

In parte si tratta di una conseguenza della necessità di mantenere aggiornato l'esistente: non a caso le aziende continuano a investire in soluzioni ormai ampiamente presenti in azienda (firewall, antivirus ecc.) per far fronte alle nuove minacce che quotidianamente si manifestano, sia all'esterno che all'interno della loro struttura. Anzi è proprio dall'interno dell'organizzazione che spesso si originano i maggiori problemi per la

sicurezza, a causa di comportamenti dolosi o colposi (ovvero non finalizzati a nuocere ma comunque in grado di provocare danni) dei dipendenti.

Nuove minacce continuano ad emergere, spesso legate alle soluzioni ICT più innovative, come ad esempio le applicazioni IT che si appoggiano a servizi di accesso wireless. Le istituzioni poi sempre di più si preoccupano delle implicazioni per gli utenti e richiedono che i sistemi, utilizzati sia nell'ambito pubblico che in quello privato, offrano completa garanzia di sicurezza.

Tra gli elementi che modificheranno in futuro la domanda di soluzioni di sicurezza:

- soluzioni puntuali come antivirus e firewall, in grado di rispondere a singole problematiche, faranno

sempre più spesso parte di un disegno complessivo della sicurezza aziendale e si trasformeranno in soluzioni "unificate" in grado di estendere sia le funzionalità che le prestazioni originarie.

- i servizi, sia di gestione (in particolare per la componente dei Managed Security Services) che per aspetti di consulenza, come il Vulnerability Assessment, saranno maggiormente richiesti a corredo delle tecnologie di sicurezza, in rispondenza della maggiore complessità e della necessità di compliance normativa.

- in un contesto competitivo, **i clienti premieranno sempre di più i vendor in grado di rispondere a molteplici requisiti, con competenze complete e multi-piattaforma, una posizione finanziaria solida e refe-**

renze significative.

A fianco di queste evoluzioni vi è poi una trasformazione profonda non solo delle soluzioni, quanto del concetto stesso di sicurezza, che da difesa puntuale di problemi chiaramente identificabili (attacchi esterni, accessi non autorizzati ecc.) diventa un elemento integrato nelle piattaforme applicative e di rete, meno visibile ma non per questo meno importante. Ma c'è di più. In questo percorso evolutivo la sicurezza esce dall'ambito delle soluzioni specializzate e si confonde con altre aree applicative, di cui sfrutta i modelli e le funzionalità per migliorare la difesa dell'azienda fino agli aspetti più "intimi", ovvero i comportamenti, strutturati e non, dei singoli.

Editore:

Sophos S.r.l.
Via Senigallia 18/2
20161 Milano, Italia
Tel: +39-02-6628100
Fax: +39-02-66281099
e-mail: info@sophos.it
www.sophos.it

Direttore Responsabile:

Rossella Lucangelo

Caporedattore:

Enrico Salsi

Redazione:

Via Rainaldi 5
40139 Bologna, Italia
Tel: +39.051.6545658
e-mail:
redazionesecured@pragmatika.it

I testi sono realizzati con il contributo del Comitato Scientifico

Grafica e impaginazione:

Conte Oggioni & Partners

Stampa:

Venturini DMC S.p.A

Costo di una copia ai soli

fini fiscali: 1,00 euro

Titolare del trattamento dati

(D. Legislativo 196/03):

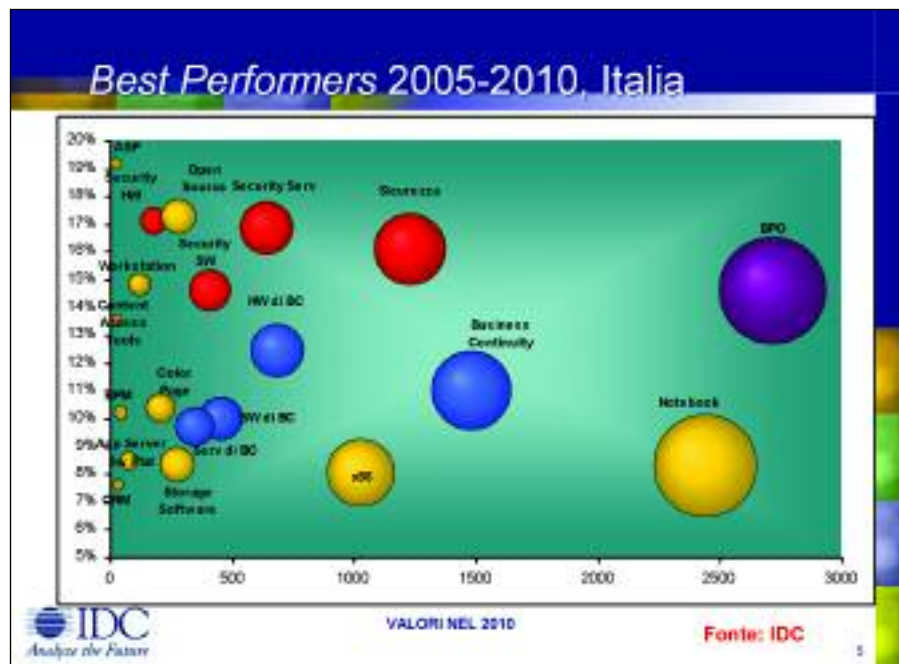
Sophos S.r.l.

Testata registrata al Tribunale

di Milano con il numero 450
il 3 luglio 2006

Contenuto pubblicitario

non superiore al 45%



cultura



cultura della sicurezza

Comitato scientifico:

Leonardo Valcamonici - CASPUR
Piero Caporale - CNIPA
Luisa Franchina - Ministero delle Comunicazioni
Stefano Pasquini - Ufficio Internet della Santa Sede
Francesco Marino - Top Trade Informatica
Marco Gatti - Week It
Dario Colombo - Linea EDP e Searchsecurity.it
Valerio Mariani - Computer Dealer & Var
Pieraugusto Pozzi - Forum per la tecnologia dell'informazione
Marco Masoni - Masobit Corporation
Michele Bianco - Bull Italia
Valeria Severini - FreeData
Roberto Mastropasqua - IDC Italia
Bruno Fiammella - Ass. Intern. di Criminologi e Centro Studi Informatica Giuridica
Massimo Melica - Centro Studi Informatica Giuridica
Andrea Ardizzone - ASSINTEL
Alessandro Musumeci - Comune di Milano
Cinzia Villani - ASSOCERTIFICAZIONI c/o Telecom Italia
Marco De Luca Saggese - Esercito Italiano, Comando Trasmissioni e Informazioni
Maurizio La Puca - Stato Maggiore Marina Militare, Comparto ICT & Sicurezza
Marco Strano - Polizia di Stato, Centro di Neurologia e Psicologia Medica
Giuseppe Russo - Sun Microsystems
Marco Chan - CNA IT
Francesco Palmieri - Università degli Studi di Napoli Federico II, CSI
Lucilla Mancini - Business-e
Giuseppe Cattaneo - Università di Salerno - Dip. Informatica e Applicazioni

Lo sviluppo dell'offerta di security nel mondo IT ha sinora sempre avuto analogie con i bisogni di sicurezza delle altre istituzioni. **Inizialmente si protegge il perimetro da attacchi provenienti dall'esterno:** firewall, antivirus, IDS e IPS, sono esempi classici. **In secondo luogo si adottano meccanismi per la prevenzione da minacce interne,** il che si traduce nell'implementazione di soluzioni che tutelino l'organizzazione dalla fuoriuscita non autorizzata d'informazioni rilevanti. **Infine, si cerca di investigare all'esterno della struttura organizzativa per identificare e prevenire minacce capaci di danneggiare l'organizzazione** direttamente, o indirettamente toccando gli interessi degli sta-

keholders. Fenomeni di frode, utilizzo illecito di marchio, di canali non autorizzati per le vendite, sono esempi di minacce di questo tipo.

I primi due bisogni sono stati soddisfatti da un numero sempre crescente di soluzioni in continua evoluzione; il terzo richiede, oggi, nuovi approcci di difesa che consentano di analizzare un vasto numero d'informazioni al di fuori del perimetro aziendale, in diversi formati, su molteplici canali di comunicazione, siano esse esplicite o latenti.

Un modo nuovo ed economicamente efficiente di dare risposta a questo bisogno sta portando l'offerta a re-inventare un prodotto, nato per altri scopi, orientandolo alla soddisfazione di bisogni di sicurez-

za. Strumenti di content e knowledge management, hanno intrinsecamente le potenzialità per essere usati in questo ambito. I loro motori, provvedendo alla ricerca d'informazioni e contenuti mediante avanzate tecniche d'analisi linguistica, possono essere impiegati per attività d'intelligence. L'uso dello stesso strumento all'interno del perimetro aziendale permette inoltre di tutelare l'organizzazione da minacce interne, rispondendo contemporaneamente ad un'ulteriore esigenza della domanda, ossia, maggiore integrazione fra i prodotti.

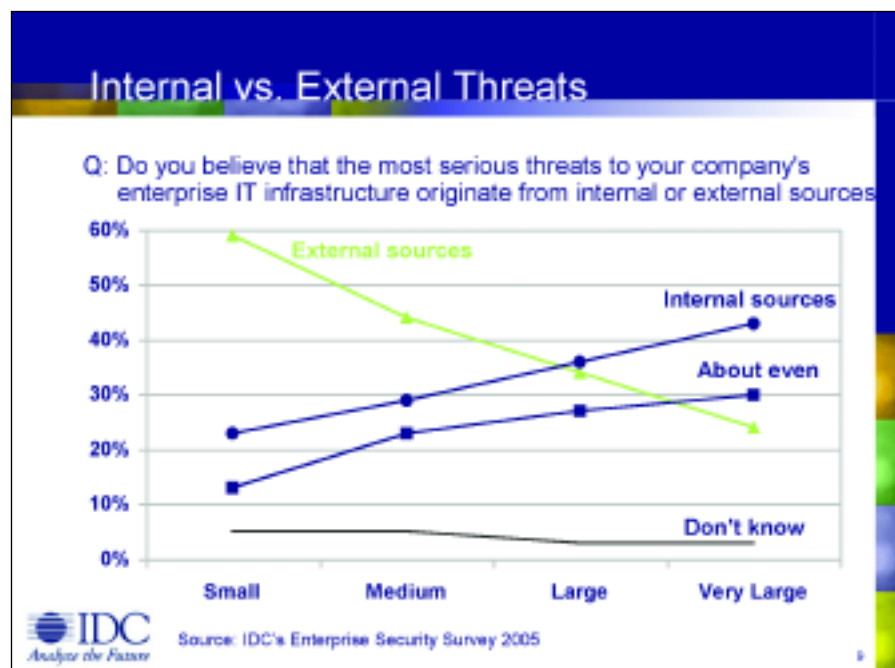
Roberto Mastropasqua
Research Director IDC Italia
(ha collaborato Andrea Negri)



Da hacker a cracker: l'evoluzione del cyber-crime

Se una volta i pirati informatici creavano virus per una sfida intellettuale, stimolati dalla ricerca di fama e celebrità, adesso l'elemento economico ha preso il sopravvento e la visione romantica si è trasformata nella più pragmatica ricerca del facile guadagno. In questa trasformazione sta la differenza tra hacker a cracker.

L'**hacker** usa la propria profonda conoscenza delle reti e dei sistemi informatici per affrontare sfide intellettuali aggirando e superando creativamente le limitazioni che gli vengono imposte. Il **cracker** è il vero cyber-criminale, colui che sfrutta le proprie conoscenze tecnologiche per scopi di lucro. Entra abusivamente in sistemi altrui per danneggiarli, rubare informazioni e perpetrare frodi.



education

L'innovazione nella formazione, l'eccellenza nella ricerca, la cultura della sicurezza

Le "nuove frontiere del cyber-crime" al centro di un convegno ospitato dall'Università di Napoli

Falle nei software: +40% in un anno

Nell'ultimo semestre sono state riscontrate 1.896 nuove vulnerabilità nel software commerciale. Nel 2005 queste sono aumentate del 40% rispetto al 2004.

(Prontoconsumatore 18/09/2006)

DoS

Negli ultimi 6 mesi gli attacchi tipo 'Denial of Service' sono aumentati del 51% rispetto al semestre precedente, raggiungendo una media di 1.402 al giorno.

(Anti-phishing.it 05/09/2006)

Il saggio impara molte cose dai suoi nemici.
(Aristofane)

Il mondo accademico, l'industria e la Pubblica Amministrazione sono oggi tre attori che sempre più sentono la necessità di dialogare e cercare strade comuni sul terreno della sicurezza della rete informatica.

La diffusa esigenza di affrontare "a più voci" la problematica dei nuovi crimini informatici ha portato Sophos Italia, impegnata costantemente nel fornire soluzioni tecnologiche a contrasto del fenomeno malware, ad organizzare, con il contributo dell'Università degli Studi di Napoli "Parthenope", un convegno dal titolo "*Le nuove frontiere del cyber-crime*". L'evento si è svolto il 28 settembre scorso presso il Centro Congressi Villa Doria D'Angri a Posillipo.

Il filo conduttore dei vari interventi, introdotti da Vito Pascazio, vicepresidente della Facoltà di Ingegneria dell'Università Parthenope, è stato la "**cultura della sicurezza**", intesa come **convergenza di innovazione tecnologica, ricerca scientifica e servizi orientati a salvaguardare la rete digitale e lo sviluppo della società dell'informazione**.

Tra i relatori, Luigi Romano, professore associato dell'Università Parthenope, si è focalizzato sull'importanza di un approccio progettuale - anziché un tantum - alla sicurezza.

Romano ha sottolineato l'esigenza della messa in campo di risorse e compe-

tenze eterogenee e di un impegno puntuale e preventivo, funzionale all'analisi dei rischi e delle contromisure necessarie per realizzare un vero "ciclo della sicurezza". Essenziale in tale direzione, ha precisato Romano, è la creazione di sinergie tra università, aziende e PA, di modo che

Dopo solo 10 minuti, un PC non protetto ha il 40% delle possibilità di essere infettato. Tale percentuale sale addirittura al 94% dopo 60 minuti.

la ricerca scientifica possa essere trasferita al settore ICT e da qui alle aziende e alle risorse umane.

Nel corso del convegno è intervenuto Maurizio Masciopinto, Direttore della Divisione Investigativa del-

la Polizia Postale e delle Comunicazioni, che ha ricordato come **la salvaguardia della sicurezza richiede una dettagliata conoscenza delle nuove tipologie di attacchi informatici**, nel contesto delle norme vigenti e degli strumenti tecnologici e logistici a disposizione.

Masciopinto ha quindi tracciato **l'attuale volto del cyber-crime: una minaccia nuova rispetto ai crimini tradizionali, dinamica e in continuo mutamento, caratterizzata da una connotazione transnazionale e priva di coordinate geografiche**. Ha descritto, inoltre, sulla base del quadro legislativo, le principali azioni di contrasto portate avanti dalla Polizia Postale, sottolineando come la loro efficacia sia soggetta anche al progresso tecnologico, ad una ricerca scientifica mirata e ai servizi delle aziende del settore ICT.

Sophos, attraverso l'intervento di Andrea Scattina, Sales Engineer, ha fornito il suo contributo sottolineando come la tutela della sicurezza sia oggi una priorità per tutte le organizzazioni: dopo solo 10 minuti, un PC non protetto ha il 40% delle possibilità di essere infettato. Tale percentuale sale addirittura al 94% dopo 60 minuti. Da qui la necessità di introdurre **soluzioni di protezione integrate, sempre aggiornate e facili da gestire, che tutelino le aziende sia a livello endpoint sia gateway**. Non solo. Fondamentali sono anche la disponibilità di servizi quali lo zombie e il phishing alert, per essere tempestivamente aggiornati sui rischi incombenti e, naturalmente, una campagna di sensibilizzazione che faccia cultura sulla reale consistenza del cyber-crime.





Il dialogo con il cittadino, le potenzialità dell'e-government, la cultura della sicurezza

La protezione dei dati nelle pubbliche amministrazioni

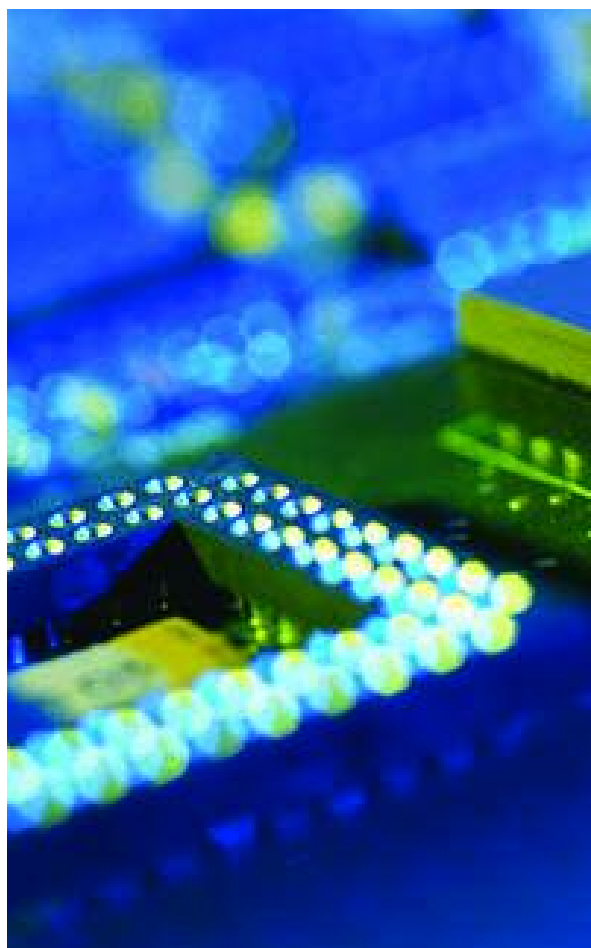
La protezione delle informazioni sensibili sta diventando una delle problematiche di maggior rilievo nelle pubbliche amministrazioni; basti pensare alle recenti disposizioni legislative che limitano la diffusione dei dati personali, ampiamente utilizzati e memorizzati ad ogni livello negli archivi delle pubbliche amministrazioni e al tempo stesso alla crescita esponenziale dei servizi on-line offerti dai portali di pubbliche amministrazioni centrali e locali. Per poter conciliare queste due esigenze apparentemente in contrasto fra loro, stanno rapidamente diffondendosi tecniche di protezione dei dati:

- 1) basate sulla trasmissione delle informazioni tramite Reti Private Virtuali (VPN) che permettono di inviare, in modalità cifrata, informazioni su rete pubblica in modo assolutamente riservato;
- 2) fondate su sistemi di posta certificata, che, previsti nel recente codice della pubblica amministrazione digitale, consentono di dare validità giuridica ai documenti scambiati fra pubbliche amministrazioni e fra queste e i cittadini;
- 3) imperniate sull'uso di carte di autenticazione digitale, basate su smart card, accoppiate o meno a un PIN di protezione. In quest'ambito vanno annoverati anche gli utilizzi delle carte RFID, ovvero basate su tecniche di ricezione passiva del segnale e di ritrasmissione di opportuna codifica.

Esistono già molteplici esempi dell'uso di tali sistemi nella pubblica amministrazione italiana; ad esempio nel Ministero della Pubblica Istruzione **è utilizzata dalle scuole una rete a larga banda (che connette l'86% delle Istituzioni Scolastiche pubbliche), che consente la trasmissione e la ricezione sicura di documenti, non solo fra istituzioni scolastiche, ma anche fra queste e le famiglie e con altre pubbliche amministrazioni.**

Tale rete è anche ampiamente utilizzata per la ricezione del cedolino dello stipendio in forma elettronica, che interessa ormai oltre 600.000 fra dirigenti scolastici, docenti e personale amministrativo di ogni ordine e grado.

Presso gli uffici del Ministero della Pubblica Istruzione, inoltre, è in fase di sperimentazione, in collaborazione con il CNIPA, un sistema di posta certificata, in grado di dare piena validità giuridica ai documenti scambiati fra gli uffici, riducendo il flusso cartaceo all'interno dell'amministrazione e abbassando



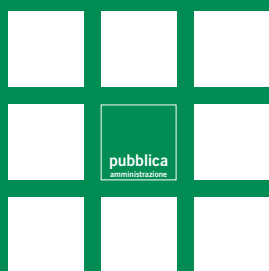
in modo rilevante costi di trasmissione e di archiviazione delle informazioni.

Presso altre amministrazioni, come ad esempio il Comune di Milano, è in fase di sperimentazione l'accesso ai servizi disponibili sul portale (come ad esempio il pagamento dell'ICI o la stampa dei certificati anagrafici direttamente presso la propria abitazione), tramite la Carta dei Servizi distribuita gratuitamente dalla Regione Lombardia a tutti i cittadini.

Questi pochi esempi dimostrano come si possano conciliare con successo due esigenze fondamentali: il diritto alla "privacy" dei cittadini e la loro necessità di usufruire di servizi evoluti, utilizzando le moderne tecnologie che stanno cambiando in modo radicale l'organizzazione della nostra società.

Alessandro Musumeci

Direttore Sistemi Informativi, Comune di Milano



Phishing

Una mail ogni 119 è una mail di 'phishing'.
La media giornaliera è di oltre 8 milioni di attacchi.

(Tuttoconsumatori.it
05/09/2006)

PC nel mirino dei Bot

Negli ultimi mesi sono stati identificati circa 9.130 nuovi PC al giorno infetti da particolari virus detti 'Bot'.

(01NET 06/09/2006)

service

provider



L'affidabilità delle infrastrutture, la continuità del servizio, la cultura della sicurezza

Posta Elettronica Certificata



La Posta Elettronica Certificata (PEC) è un servizio di Posta Elettronica che permette al *Mittente* di ottenere la garanzia di ricevimento del messaggio da parte del *Destinatario*.

In Italia l'invio di una e-mail certificata è equiparato a tutti gli effetti di legge alla spedizione di una Raccomandata cartacea con Avviso di Ricevimento (art. 48 D.L. 07/03/2005, n°82). Ai fini della normativa, il messaggio si considera consegnato al destinatario quando è accessibile nella sua casella di posta (Si veda DPR 11/02/2005, n°68 in G.U. 28 aprile 2005, n°97).

Il meccanismo consiste nel fatto che il gestore della PEC, nel momento in cui prende a carico l'e-mail del mittente, gli spedisce una ricevuta di accettazione che certifica l'avvenuto invio. Quando il messaggio è depositato nella casella del destinatario, invia al mittente una ricevuta di consegna che certifica anche l'avvenuta ricezione. Sia la *ricevuta di accettazione* che quella di consegna sono in formato elettronico

co e ad esse è apposta la firma digitale del gestore. Se la mail non viene depositata nella casella del destinatario, al mittente viene invece inviata una ricevuta di mancata consegna.

Nel caso in cui il mittente smarrisca le ricevute, la traccia informatica delle operazioni svolte, *conserva-*

ta per legge per un periodo di 30 mesi, ne consente la riproduzione con lo stesso valore giuridico.

I gestori di PEC sono soggetti privati che devono possedere una pluralità di requisiti stabiliti dalla legge (requisiti di onorabilità previsti per l'attività bancaria, capitale sociale non inferiore a 1 milione di

euro, etc.) e possono operare solo se autorizzati dal CNIPA (www.cnipa.gov.it). L'elenco dei Gestori Autorizzati è presente alla pagina web:

www.cnipa.gov.it/site/filles/Elenco_Pubblico.pdf

Il Decreto Ministeriale contenente le "Regole Tecniche" per la formazione, la trasmissione e la validazione, anche temporale, della PEC, è stato pubblicato nella G.U. del 15/11/2005, n°266.

Marco Masoni
General Manager,
Masobit Corporation Srl

File in ostaggio

Sono in rapido aumento i virus Ransomwares, malware che infettano i computer a scopo di lucro, danneggiando in prima persona il singolo utente. Il capostipite di questa famiglia è PGPCoder, che non minaccia di cancellare i file memorizzati ma si limita a criptarli.

(Win Magazine 31/10/2006)

Boom di frodi finanziarie

Oggi il 15% dello spam - a gennaio 2005 questa percentuale era lo 0,8% - è rappresentato da e-mail fraudolente che tentano operazioni finanziarie di pump-and-dump allo scopo di gonfiare i prezzi delle azioni e permettere facili guadagni agli spammer.

(CSO 30/09/2006)



Servizi e Soluzioni contro Spam, Phishing, Spyware e Virus. Sicurezza delle applicazioni. Gestione e manutenzione hardware e software. Ottimizzazione della banda.

LIBERA IL PERCORSO ALLE INFORMAZIONI

Secure Group protegge la Continuità del Servizio dei sistemi informatici



SECURE GROUP S.r.l.
C.so Svizzera 185 - 10149 Torino
Tel. 011 0700900 - fax 011 0700032
info@securegroup.it

service
provider

Impresa

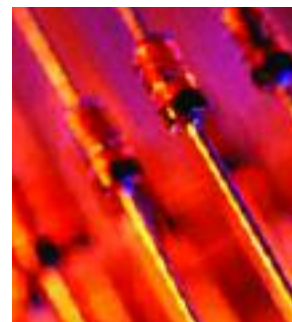
La protezione del business, la capacità competitiva, la cultura della sicurezza

Dal database la sicurezza dell'azienda

Settembre, mese della sicurezza. Almeno per Gartner, uno dei più grandi analisti (insieme a Idc e Forrester Research) del panorama It al mondo, che al proprio summit mondiale di Londra tenuto sul tema (l'It Security Summit), ha stilato un capitolato delle operazioni che le aziende dovrebbero fare per mettersi al sicuro da perdite di dati accidentali. Si tratta, generalmente, di garantirsi da rischi generati dall'apertura delle reti aziendali verso l'esterno. Ossia, per essere concreti, generati dalle attività di comunicazione, tramite posta elettronica e dalle transazioni di dati fatte attraverso Internet. Gartner ha delineato cinque passi che tutte le aziende dovrebbero seguire per stabilire le condizioni migliori per la sicurezza delle proprie informazioni. Vediamoli uno per uno, facendoci delle semplici domande che sorgono da un sano scetticismo. Dapprima l'analista raccomanda l'installazione di una soluzione cosiddetta di Content Monitoring and Filtering. Con ciò allude alla creazione di un sistema di filtro dei contenuti che transitano da e verso l'azienda. Qualcosa che controlli il traffico di rete e generi allarmi in relazione alle attività sospette. Giusto. La domanda dello scettico: dato che si tratta di controllare posta elettronica, instant messaging, traffico Internet (Ftp,

Http, la Web mail), a chi affidare il controllo? A personale interno o esterno? Il secondo step concerne la crittazione dei contenuti sui dispositivi di storage, dai nastri ai dischi. Lo scopo, evidente, è quello di evitare furti di dati e conseguenti frodi. Osservazione: i dispositivi di crittazione, per funzionare bene, devono essere usati da tutti. Va, quindi, predisposta un'azione culturale, tesa a insegnarne l'uso e ad assicurarsi che tutti i dipendenti aziendali mettano in atto le pratiche di encryption. Basta anche un solo disobbediente e la falla potenziale si crea. Il terzo passo riguarda le singole postazioni di lavoro, che devono essere messe in sicurezza totale. Qui si parla anche di ridurre i computer domestici che accedono alla rete aziendale (notoriamente in situazione "anarchica") e la neutralizzazione dei dispositivi di storage portatile di tipo Usb. Osservazione: ancora di più che al punto precedente, è necessario agire sul fronte culturale, indirizzando dipendenti e non, che accedono al sistema informativo dell'azienda tramite Internet, a comportarsi correttamente. Il quarto step concerne i computer portatili, vera mina vagante, letteralmente. Chi lavora in mobilità, per definizione, sfugge facilmente alle policy di sicurezza.

Domanda: bisogna mettere in atto delle forme di "polizia territoriale" per tenere sotto controllo i lavoratori mobili? Oppure sono sufficienti delle solide policy di accesso alla rete aziendale? Il quinto e ultimo passo riguarda la costituzione di un sistema che tenga traccia di tutte le attività, lecite e illecite, che vengono fatte su un database, che è il vero centro delle informazioni di un'azienda. **Sapere cosa accade nel database significa sapere cosa accade nell'azienda.** Da più parti del mondo in quest'ultimo periodo arrivano notizie che riguardano proprio la figura professionale del DbA, ossia del database administrator, che lo dipingono come un bene scarso. Meglio: di DbA se ne trovano, quello che è difficile è trovarne



uno buono. Ecco allora che, forse, un investimento sul futuro per sé, per la propria azienda, e anche per la comunità economica e tecnologica in cui si è inseriti e si lavora, è investire sulla creazione di un valido database administrator. Un investimento fatto oggi, per lavorare meglio domani.

Dario Colombo
Linea EDP e
Searchsecurity.it

SearchSecurity.it (www.searchsecurity.it) è il sito verticale dedicato alla sicurezza del network TechTarget Italia, realizzato da Editoriale Gpp in partnership con la media company statunitense TechTarget, che ha una directory di 28 siti specializzati dedicati a specifiche comunità di professionisti operanti nel mondo ICT. SearchSecurity implementa un modello di formazione-informazione per l'utente, che mette a disposizione dei decisori d'acquisto dell'It aziendale "centri risorse" specializzati, costituiti da banche dati di suggerimenti, consigli di esperti, White Paper e altri strumenti formativi. Il tutto in lingua italiana. Linea EDP, inviata ogni settimana a 39.000 referenze It in Italia, è la rivista dedicata ai CIO, al personale di staff e ai professionisti It in ambito aziendale.

Il crimine è una cosa comune. La logica è rara. Tuttavia è sulla logica che dovresti insistere.
(Arthur Conan Doyle)

Un listino per gli spammer

Un tariffario russo dello spamming offriva per 500 dollari la distribuzione di messaggi a undici milioni di indirizzi e-mail russi. Per 50 dollari era possibile ordinare l'invio di messaggi a un milione di indirizzi e-mail in qualsiasi paese.

(CSO 30/09/2006)

VoIP: allarme falsi call center

Cresce il fenomeno del "vishing", pratica analoga al phishing che utilizza i servizi di telefonia VoIP allo scopo di indirizzare gli utenti verso fantomatici call center per estorcere dati bancari e farne uso illecito.

(Prontoconsumatore
29/08/2006)

operatori ICT

La risposta al mercato, la fidelizzazione del cliente, la cultura della sicurezza

Il mercato della sicurezza: la necessità di una visione olistica

Secondo una ricerca di Morgan Stanley sulle prime 100 aziende di Fortune, la sicurezza è un tema prioritario per i CIO delle aziende americane. In questi ultimi anni infatti la diffusione di malware, phishing, virus e trojan si è moltiplicata, in parte anche grazie all'evoluzione delle tecnologie mobili e alle connessioni senza fili (prime fra tutti Bluetooth e Wi-Fi). Un'indagine di PricewaterhouseCoopers su 8000 aziende in tutto il mondo ha indicato tempo fa che circa l'11% del budget destinato all'IT dalle aziende sarà destinato alla sicurezza informatica.

Anche in Italia il mercato della sicurezza informatica è in crescita rispetto agli altri settori dell'IT. Tuttavia, spesso le aziende sono mosse ad investimenti in sicurezza più dalle normative che dai pericoli reali, come ad esempio la legge sulla privacy o, nel settore del credito, le normative emanate da Bankitalia. Quello che ancora manca in Italia è probabilmente una "cultura" della sicurezza informatica, che vede in un Security Manager la figura di riferimento in azienda. Il nostro tessuto industriale è fatto di piccole e medie aziende dove questa cultura stenta ad affermarsi e quindi il problema della sicurezza informatica viene spesso affrontato limitandosi ad apparecchiature hardware o software di base (firewall, router, ecc...).

Affrontare la sicurezza informatica significa invece analizzare a fondo le implicazioni che comporta, individuare le proprie necessità e le necessarie implicazioni fra hardware, software e servizi fino ad arrivare a poter stimare il ritorno sugli investimenti in sicurezza IT così come si è abituati a valutarlo per gli altri investimenti aziendali. In questo senso anche lo scenario dell'offerta di

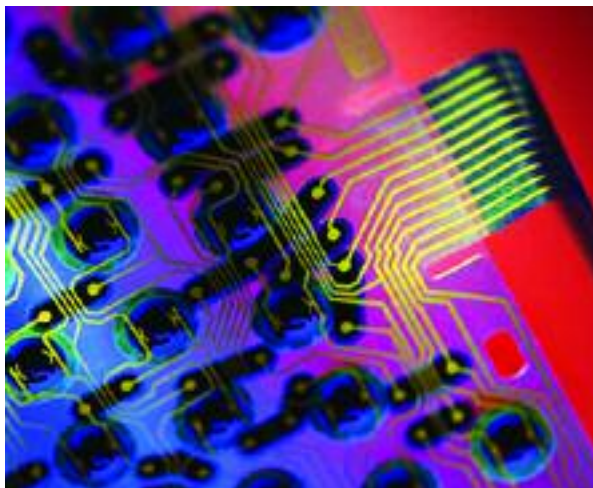
La sicurezza IT è in realtà qualcosa che coinvolge tutta l'azienda, le sue funzioni, i suoi dipendenti, i suoi clienti, i suoi fornitori ed, in definitiva, il suo business



soluzioni di sicurezza IT si sta evolvendo in Italia, cercando di offrire soluzioni che vanno da quelle che richiedono il minimo di personalizzazione per le piccolissime imprese a quelle più complesse dove il concetto di "cultura" della sicurezza comincia a farsi strada. Vengono così proposte non soltanto soluzioni hardware e software, ma anche corsi per il personale, strumenti di simulazione dei danni che possono deri-

vare da falle nella sicurezza, metodi per valutare il ritorno degli investimenti. Legato poi al concetto di sicurezza IT in senso lato c'è il concetto di tutela dei dati che porta con sé esi-

genze sempre più sofisticate in termini di storage hardware e di software per il backup e la loro gestione. In particolare riveste un ruolo importante per l'azienda la gestione dei dati dei propri clienti (di nuovo fa leva la legge sulla privacy) ma anche i rapporti con i propri fornitori o, nelle aziende più grandi, il rapporto con il proprio canale di vendita. Da questo si capisce quindi come la sicurezza IT sia in realtà qualcosa che coinvolge tutta l'azienda, le sue funzioni, i suoi dipendenti, i suoi clienti, i suoi fornitori ed in definitiva il suo business. Solo questo cambio di ottica può portare un'azienda ad investire non solo sull'onda delle normative, ma come azienda utente "evoluta". Lo scenario dell'offerta di soluzioni di sicurezza in Italia è ancora molto eterogeneo ed in definitiva, nonostante un mercato in crescita, gli investimenti delle aziende sono abbastanza lontani dal quell' 11%.



Italia: cresce il Cybercrime

Nel 2005 in Italia le frodi informatiche sono aumentate del 35,9% rispetto al 2004: coinvolti nelle truffe 30 siti nazionali e circa 600 persone e aziende.

(Quarantasettesima conferenza sul "Computer Crime" organizzata a Roma dalla polizia postale 5/09/2006)

Cybercrime, USA e UE vicini

Il Governo statunitense ha deciso di ratificare il protocollo sul cybercrime redatto dall'Assemblea parlamentare del Consiglio d'Europa. La normativa estende i poteri di polizia e di indagine e rende più agevoli le attività di cooperazione fra i diversi paesi.

(Punto Informatico 04/10/2006)

