

SOPHOS

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

secured.

SOPHOS

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

Anno 2 N°1 Marzo/Aprile 2007

Sommario

editoriale	attualità	cultura
education	pubblica amministrazione	impresa
service provider	operatori ICT	numero 1

Editoriale

"Tenere la difesa alta". Mutuando il linguaggio del mondo del calcio, abusato ma spesso efficace, questo è lo scenario che si sta determinando nel mercato della sicurezza informatica. Se, in passato, si pensava fosse sufficiente proteggere solo l'endpoint, in pratica fare "catenaccio", oggi il confine della sicurezza si sta spostando sempre più all'esterno: sul perimetro dell'organizzazione e oltre.

Fuor di metafora è evidente che le minacce per le imprese oggi provengono anche dall'esterno del perimetro aziendale, coinvolgendo la comunità di business: fornitori, partner, clienti, tele-lavoratori, dipendenti che si connettono alla rete aziendale da remoto. Come verificare che gli accessi seguano le politiche aziendali? Come assicurarsi che per distrazione o dolo chi entra nel network non diffonda malware? In soccorso ci viene la tecnologia NAC (Network Access Control), che classifica il traffico che tenta di entrare nel network, lo compara con le policy definite e si assicura che sia compliant alla tipologia di accessi consentiti: le barriere di protezione si spostano sempre più verso l'esterno. E questo, nell'era del web, non è cosa da poco.

Rossella Lucangelo
Direttore Secured.

IN QUESTO NUMERO:**NAC: i nuovi confini della sicurezza****Case history: il Comune di Bologna****Quanto è sicuro Vista?**

Maxi operazione dei Carabinieri di Roma e di Europol contro il pedoweb: si chiama "Flashpoint" ed ha portato al sequestro di un sito italiano utilizzato da una folta community per la distribuzione di materiale pedo-pornografico. Si è conclusa il 16 febbraio scorso

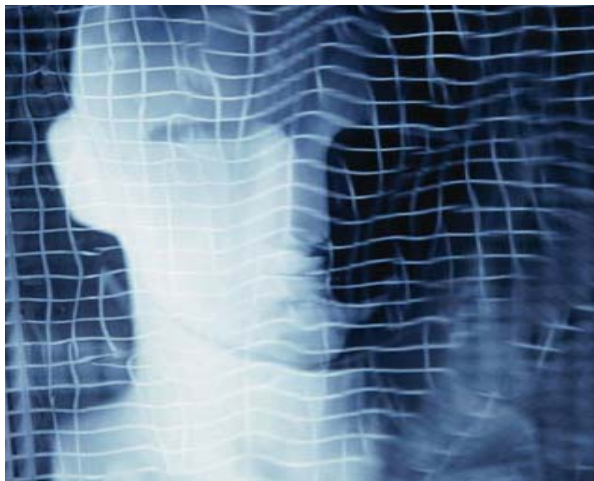
con l'arresto di un romano e la denuncia di 24 persone in Italia e di 15 in Romania, Svizzera e Slovenia, accusate di detenzione e divulgazione di contenuti pedo-pornografici. Sono stati individuati quasi 3.000 contatti sul sito e sequestrati 48 pc,

quasi 1.400 tra dvd e cd, 242 videocassette e 11 smart card fotografiche. La community si proteggeva spostando i contenuti da un provider all'altro e controllando rigidamente l'accesso al sito, del tutto privo di riferimenti pornografici.

attualità e cultura

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

Chi sono gli hacker? L'analisi di "Hacker's Profiling Project"



È con l'invio di un questionario a circa 600 hacker in tutto il mondo, che ha preso il via "HPP- Hacker's Profiling Project", una ricerca finalizzata a tracciare l'identikit degli hacker del 2000.

Uno degli autori è l'ex-hacker Raul Chiesa, oggi a capo di una società di sicurezza informatica. Quanto emerge dallo studio, che ha utilizzato la metodologia impiegata nelle indagini sui crimini

di matrice violenta e sessuale, è la giovane età dell'ultima generazione di hacker. Si parte dai 9, 10 anni, per arrivare ai "veterani", figure esperte di 40, 50 o 60 anni. Obiettivi e comportamenti eterogenei, oltre alle differenze d'età, fanno dell'hacker una figura tutt'altro che univoca. La ricerca ne individua 8 tipologie: Wannabe Lamer (l'incapace), Script Kiddie (il ragazzino degli script), Cracker (il distruttore), Ethical Hacker (l'etico), Quiet, Paranoid & Skilled Hacker (il paranoico), Cyber Warrior (il mercenario), Industrial Spy (la spia industriale), Military Hacker (arruolato per com-

battere "con un computer"). Sopravvive la figura dell'hacker etico, che sfrutta la sua conoscenza per scoprire e denunciare frodi e truffe, ma è molto meno diffusa rispetto al passato a causa delle pressanti richieste della criminalità organizzata che oggi assolda hacker per fini di spionaggio industriale, furto di credenziali di accesso bancarie o identità personale, danni ai sistemi ecc. È stato inoltre rilevato che gli hacker spesso non temono le conseguenze legali delle loro azioni, nonostante l'asprezza, nella maggior parte dei casi, delle legislazioni contro il cybercrime.

ISAC: un'efficace risposta a tutela della sicurezza informatica secondo il Clusit

Le numerose vulnerabilità della rete nazionale stanno incrementando la consapevolezza dell'urgenza di misure efficaci contro i crescenti danni causati dalle minacce informatiche. **Il Clusit (Associazione Italiana per la sicurezza informatica) ha ribadito come la debolezza della rete sia da correlare alla cronica mancanza in Italia di una cultura diffusa della sicurezza.** Secondo il Clusit, gli investimenti tecnologici non bastano da soli a risolvere questi problemi: occorre sviluppare strutture efficaci deputate alla ricerca, all'analisi e allo scambio di informazioni. Il modello citato è quello degli ISAC, rete di centri di analisi, attiva da tempo negli Stati Uniti, per la condivisione di dati e per la produzione di valutazioni e istruzioni volte a rafforzare la protezione delle infrastrutture. La costituzione di una rete ISAC, sottolinea il Clusit, è sicuramente auspicabile anche per l'Italia. Essa richiede tuttavia l'abbattimento di barriere di natura finanziaria e l'eliminazio-



ne della storica diffidenza tra aziende nazionali, comportando l'investimento in nuove risorse e una forte collaborazione anche tra competitor. Indipendenti dalle istituzioni pubbliche, gli ISAC infatti si reggono sui finanziamenti delle organizzazioni che ne fanno parte e sono guidati da una logica fortemente sinergica, pur tutelando la riservatezza dei dati sensibili scambiati. Solo in tale prospettiva sarà possibile inaugurare un approccio alla sicurezza in grado di rispondere in modo coordinato alle emergenze e alle minacce e capace di fornire nuove misure preventive nella lotta contro il malware.

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%

	attualità	cultura

ultura



cultura della sicurezza

E-mail sollecita pagamenti di verbali? È una truffa

Si moltiplicano i cittadini a cui è pervenuta, via e-mail, la minaccia di sanzioni e ingiunzioni per pagamenti non effettuati. Segnalando uno studio legale o un servizio di riscossione con cui mettersi in contatto, i messaggi giocano sulla tensione dell'utente per mettere a segno truffe finalizzate alla propagazione di virus o a rubare i dati forniti dal malcapitato a scopo di lucro.

I nemici che possono riuscir pericolosi sono sempre abbastanza scaltri per non esporsi al pericolo. (Napoleone Bonaparte)

Insegnante vittima dell'adware: rischia il carcere

Julie Amero, condannata per aver sottoposto dei minori a pop up pornografici, rischia 40 anni di carcere. La dichiarazione di colpevolezza ha suscitato reazioni discordanti: ipotesi probabile è che l'insegnante, inesperta di computing, sia caduta vittima di un adware all'interno del pc. (Punto Informatico -16/04/07)

Il lato oscuro del web al centro di un convegno di Assintel sul cybercrime

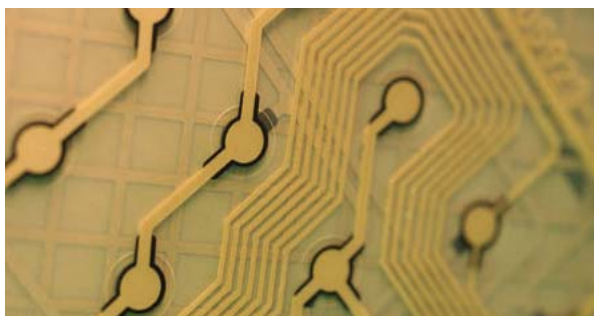
Cresce da parte del mondo industriale l'interesse verso una riflessione a 360 gradi sui rischi per la sicurezza informatica generati dall'uso di internet e delle nuove tecnologie mobili. Per contribuire alla sensibilizzazione su questo tema, Assintel, Associazione Nazionale delle imprese ICT, ha promosso il convegno "Crimini informatici e sicurezza della navigazione: un problema globale", svoltosi il 7 febbraio scorso durante la fiera Infosecurity.

Ha aperto l'incontro il presidente dell'Associazione Giorgio Rapari, che ha sottolineato l'esigenza che istituzioni, aziende e cittadini sviluppino una cultura condivisa della sicurezza, alla luce della necessità di strumenti normativi, strategici e operativi in grado di arginare gli allarmanti fenomeni del cybercrime e della pedo-pornografia on line.

Sono intervenuti al convegno esperti autorevoli del settore, tra cui Yolanda Arevalo Torres, Project Officer del Programma "Safer Internet Plus" promosso dalla Commissione Europea, che ha sottolineato l'esigenza di una maggiore conoscenza delle ripercussioni di tali crimini anche a livello sociale, oltre che tecnologico ed economico.

Relativamente al crescente fenomeno della pedo-pornografia on line, lo scenario delineato da Torres rivela infatti che oltre il 40% dei bambini di 11 anni o di età inferiore usa internet, e che stanno crescendo inoltre i rischi connessi all'uso dei dispositivi mobili, che consentono l'accesso a materiali multimediali e la loro pubblicazione.

Torres ha descritto alcune delle iniziative della Comunità Europea come il "Safer Internet Plus", Programma per la promozione di un uso più sicuro di Internet e delle tecnologie on-line. Ha ribadito inoltre l'importanza di una maggiore diffusione di strutture di riferimento per gli utenti: l'esempio riportato è quello degli hotline, che rilevano le segnalazioni fatte dai cittadini, molto utili per le procedure di indagine finalizzate alla lotta ai contenuti illegali e indesiderati.



L'angolo della sicurezza

L'adware (contrazione di advertising-supported software, software sovvenzionato dalla pubblicità) è un programma che prevede come licenza d'uso la trasmissione di messaggi pubblicitari durante il suo utilizzo che possono essere banner o finestre pop-up.

Presenta lo svantaggio di rallentare la navigazione e in generale le operazioni informatiche. Non è di per sé dannoso ma può rappresentare una minaccia se si installa direttamente sul PC senza consenso dell'utente, se installa applicazioni diverse da quelle di origine, se cambia le impostazioni del browser e se raccoglie ed invia a terzi informazioni riservate.

+ 3% di visitatori a Infosecurity 2007

Infosecurity edizione 2007 chiude con un bilancio molto positivo: 5.500 visitatori, ovvero con un incremento del 3% rispetto alla precedente edizione. Segnale che l'evento milanese dedicato alla sicurezza IT continua ad essere un punto di riferimento per addetti ai lavori e operatori del mondo dell'informazione.

La tre giorni, che ha animato Fieramilanocity dal

6 all'8 febbraio, ha proposto un palinsesto particolarmente ricco. Oltre ad un selezionato parterre di espositori (170 aziende, +13% rispetto all'edizione 2006) che hanno presentato al salotto milanese le loro ultimissime soluzioni e tecnologie, la manifestazione ha offerto un interessante e seguitissimo programma di convegni, incontri, dimostrazioni e talk show.

education

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

Insolita azione di hacking a Downing Street

Una singolare indagine resa pubblica dal Telegraph: i consulenti informatici di Scotland Yard, a caccia di prove su un presunti compensi abusivi, sono penetrati nei sistemi informativi del governo britannico, utilizzando software simili a quelli impiegati per realizzare truffe complesse. (Punto Informativo - 23/01/07)

Palermo: frode al fisco

Sono dodici le ordinanze di custodia cautelare per ipotesi di corruzione, frode informatica, accesso abusivo a un sistema informatico e falsità materiale a carico di commercialisti e funzionari tributari, introdotti illecitamente al sistema informatico tributario per fare avere indebiti sgravi fiscali per 1,5 milioni di euro. (Repubblica.it - 16/01/07)

La cultura della sicurezza s'impura sui banchi di scuola



Il dato è preoccupante. Dall' Hacker Profiling Project, il progetto del CLUSIT - Associazione Italiana per la Sicurezza Informatica - teso ad analizzare e tracciare l'identikit del cyber-criminale del 2000, è emerso che l'età degli hacker sta drammaticamente scendendo. Spesso si inizia verso i nove, dieci anni. A volte anche prima. Ecco perché diventa fondamentale sensibilizza-

re e diffondere la cultura della sicurezza anche all'interno delle scuole. Già dalle elementari.

Un tema, quello della sicurezza informatica, che poi riguarda la scuola anche come ente utilizzatore. Con l'introduzione dell'Informatica, infatti, anche i Dirigenti Scolastici hanno dovuto affrontare le problematiche legate alla protezione e alla tutela delle informazioni riservate. **Per chi usa i computer a fini didattici, la sicurezza è uno dei valori a cui prestare maggiore attenzione, insieme ovviamente alle finalità di studio, all'appropriatezza dei contenuti e alla correttezza dell'impiego.** La tutela delle infrastrutture è un punto imprescindibile, in particolare per chi ha un ruolo formativo. La cultura della sicurezza infatti, oltre ad implicare l'utilizzo di software aggiornati, è soprattutto una questione di policy e di corrette abitudini... da imparare. Dove meglio che a scuola dunque?

Non accettate web caramelle dagli sconosciuti

Mai come in questi ultimi mesi, il binomio adolescenti e Internet desta allarme e preoccupazione nei genitori. La cronaca certo non aiuta, attenta come è a mettere sotto i riflettori i casi eclatanti e a puntare il dito sugli abusi. Ma come può regolarsi un genitore in questo scenario?

Di certo, se i figli sono nella prima scolarità la classica regola del non navigare da soli è più che mai valida. **Non si tratta semplicemente di assistere il bambino, evitandogli "cattivi incontri", ma di garantirgli un vero e proprio supporto per insegnargli a navigare meglio, indicandogli le regole di comportamento, i rischi, i pericoli, ma anche le opportunità.**

Diverso è il caso di genitori con figli adolescenti. Il rischio più evidente è quello

di cadere nei due eccessi opposti: negare il problema, oppure esasperarlo al punto da impedire al ragazzo l'utilizzo di strumenti come servizi di messaggistica istantanea, blog, chat e persino le più semplici ricerche. È chiaro che in entrambi i casi siamo di fronte a un'esasperazione che non aiuta l'adolescente ad avvicinarsi a un utilizzo consapevole della rete. Per questo motivo è importante concordare con lui alcune semplici regole di uso e di comportamento. In primo luogo, soprattutto per i più giovani non è male fissare dei limiti orari, per evitare fenomeni di assuefazione e di straniamento dalla vita reale. **È poi importante verificare che sul suo computer siano installati programmi di protezione (antivirus, firewall, anti-**

spamming, antiphishing), raccomandandogli di mantenerli regolarmente aggiornati. La salute del suo pc dipende anche da queste semplici precauzioni. I servizi di messaggistica istantanea hanno sostituito le lunghe ore al

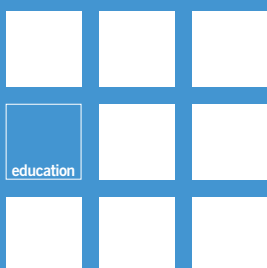
vige la vecchia regola del non accettare caramelle dagli sconosciuti. Generalità reali, indirizzi, numeri di telefono, scuola o palestra frequentate sono informazioni da non rilasciare, men che meno ai primi incontri.



telefono degli adolescenti di venti anni fa: nessun problema, dunque, ma chiedete di poter controllare periodicamente la sua buddy list. Chat e forum spaventano sempre un po': dietro un nickname si può nascondere chiunque. E le cronache lo testimoniano. In questo caso,

Quanto ai blog, sono l'ultima passione degli adolescenti. Se possibile, fate in modo che utilizzino una piattaforma che consenta l'accesso al blog ai soli membri autorizzati e non a chiunque.

Maria Teresa Della Mura



pubblica

amministrazione



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

Il Comune di Bologna come esempio di evoluzione in sicurezza della Pubblica Amministrazione

Il Comune di Bologna oggi si avvale di 5.000 dipendenti, gli utenti internet sono 3.600 e vengono utilizzate 4.000 caselle di posta elettronica nelle 85 sedi del Comune, con un volume di e-mail che varia dai 30.000 ai 40.000 messaggi al giorno. Fino al 2005 il Comune di Bologna affrontava le problematiche legate allo spam e alla protezione della navigazione web con soluzioni realizzate in casa. Tali metodologie, con il tempo, si sono rivelate insufficienti. È nata

quindi l'esigenza di utilizzare un servizio specifico per gestire con maggiore efficacia sia la protezione dei messaggi di posta elettronica che la protezione dei contenuti e della navigazione dei siti internet. Per tale motivo, il Comune ha indetto un bando di gara per acquisire il servizio. Il capitolato ha

definito in modo dettagliato i livelli di servizio attesi: la fornitura è stata aggiudicata alla Secure Group Srl, azienda certificata ISO 27001 che si occupa di sicurezza informatica da più di dieci anni. Per il Comune di Bologna Secure Group ha scelto Sophos PureMessage per la protezione della posta elettronica. Il servizio identifica fino al 98% di spam e protegge gli utenti dalle e-mail contenenti virus e malware, sia per i messaggi in uscita che per quelli in entrata. L'infrastruttura tecnologica utilizzata prevede server bilanciati e ridondati ed è in grado di proteggere tutti i domini di posta del Comune. I messaggi sospetti vengono inseriti in aree di quarantena gestite direttamente dall'utente finale in modo semplice ed intuitivo. La combinazione Proxy Squid e Websense Enterprise è stata scelta per gestire la navigazione web. Websense aggiorna ogni 5 minuti il proprio database, dove vengono censiti i siti internet. Tale database classifica i siti internet in più di 90 categorie: ogni il database contiene

oltre 15 milioni di siti censiti. Tutti gli utenti navigano tramite i proxy aziendali interfacciati con i server di Websense, entrambi ridondati e bilanciati. L'infrastruttura è gestita da remoto 24 ore su 24 attraverso il Security Operation Center di Secure Group. Una scelta vincente per garantirsi un servizio efficiente senza investimenti in prodotti e con un ridotto coinvolgimento del personale tecnico del Comune. "Aver scelto di affidare in outsourcing la gestione della sicurezza della posta elettronica e della navigazione web ci ha permesso di ottenere in breve tempo un miglioramento della produttività dell'utente finale e una maggior semplificazione del lavoro per la direzione tecnica", ha spiegato l'Ingegnere Massimo Carnevali, Responsabile Esercizio dei Sistemi Informativi e Telematici del Comune di Bologna. "L'alto livello di soddisfazione degli utenti finali ha fatto in modo che questo venisse considerato uno dei progetti chiave in termini di miglioramento della produttività aziendale e della riduzione dei costi gestionali".

"L'alto livello di soddisfazione degli utenti finali ha fatto in modo che questo venisse considerato uno dei progetti chiave in termini di miglioramento della produttività aziendale e della riduzione dei costi gestionali"

Chi gode d'una ferma autorità presto apprende che la sicurezza, e non il progresso, è la più grande lezione nell'arte del governo. (James Russell Lowell)

Proteggi le tue applicazioni web da accessi indesiderati!

Infoklix ha sviluppato una soluzione innovativa finalizzata a **garantire la sicurezza delle applicazioni web**, che unisce la potenza di **Linux** alle tecnologie per la sicurezza di **Sophos**.

Già da oggi puoi elevare gli standard di sicurezza proteggendo le tue applicazioni web da attacchi di tipo **SQL injection** e **Cross Site Scripting** e **bloccare file infetti** prima ancora che vengano caricati sui server.

La soluzione avanzata di Infoklix per proteggere le applicazioni di e-commerce, intranet/extranet, web-mail e web-portal.



INFOKLIX SPA
MILANO - TORINO - CUNEO

Infoklix unisce la trentennale esperienza nel mercato ICT con competenze specifiche di integrazione in ambito IT Security, IT Infrastructure e High Availability & Business Continuity.

www.infoklix.it



sage per la protezione della posta elettronica. Il servizio identifica fino al 98% di spam e protegge gli utenti dalle e-mail contenenti virus e malware, sia per i messaggi in uscita che per quelli in entrata. L'infrastruttura tecnologica utilizzata prevede server bilanciati e ridondati ed è in grado di proteggere tutti i domini di posta del Comune. I messaggi sospetti vengono inseriti in aree di quarantena gestite direttamente dall'utente finale in modo semplice ed intuitivo. La combinazione Proxy Squid e Websense Enterprise è stata scelta per gestire la navigazione web. Websense aggiorna ogni 5 minuti il proprio database, dove vengono censiti i siti internet. Tale database classifica i siti internet in più di 90 categorie: ogni il database contiene

service

provider



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

Minori nel mirino della pedo-pornografia on line

Allarmante un rapporto di Telefono Azzurro, secondo il quale quasi la metà dei bambini italiani (48,2%) naviga in rete e nel 33,6% dei casi da solo. Il 20,5% di quelli tra i 7 e gli 11 anni ha incontrato on line un adulto che ha dato loro fastidio, percentuale che scende al 17,6% per la fascia dai 12 ai 19 anni. (Helpconsumatori.it - 20/12/06)

La vera intelligenza dell'uomo consiste nel rendere intelligente la sua società.
(Pierre Lévy)

Gestivano milioni di PC infetti: 2 anni di carcere

Due truffatori olandesi in possesso di numeri di carte di credito e informazioni riservate sono stati condannati dal tribunale di Brera a due anni di reclusione e al pagamento complessivamente di 13mila euro. Avevano utilizzato il worm W32/Codbot, sfruttando anche la sua capacità di registrare i tasti premuti sulle tastiere. (Punto Informatico - 02/02/07)

Nuovi sistemi di filtraggio della navigazione internet contro la pornografia infantile



È stato pubblicato in G.U. il 29 gennaio scorso il nuovo decreto varato dal ministro delle Comunicazioni Paolo Gentiloni che ha imposto agli ISP l'attivazione, entro marzo 2007, di sistemi di filtri in grado di oscurare i siti responsabili di diffondere, distribuire o commerciare immagini pedo-pornografiche. Il decreto nasce con il contributo del ministero all'Innovazione nella PA, della Polizia Postale e

delle Comunicazioni e delle stesse associazioni degli Internet Provider. Affida al Centro Nazionale per il contrasto della pedo-pornografia on line, istituito presso il Ministero degli Interni, il compito di raccogliere le segnalazioni relative a siti che diffondono sulla rete tale materiale. **Gli ISP dovranno inibire i siti entro 6 ore dalla comunicazione, intervenendo sia a un livello di nome a dominio sia, entro maggio 2007, a**

livello di indirizzo IP laddove segnalato dal Centro. Saranno poi sottoposti, ogni 6 mesi, al controllo delle tecnologie impiegate e dei risultati ottenuti.

Per limitare efficacemente la diffusione dei contenuti incriminati, i filtri dovranno essere applicati a qualsiasi tipologia di codifica di caratteri utilizzati e impedire l'accesso e le modifiche non autorizzate all'elenco dei siti inibiti.

Il decreto è stato definito dal mondo politico e dall'associazionismo pro-infanzia un passo importante verso una più efficace cooperazione internazionale per la repressione della pedo-pornografia.

Sono state tuttavia sollevate dai Provider perplessità in relazione ad ostacoli riguardanti il metodo di applicazione dei filtri e la loro efficacia. Per quanto riguarda gli interventi a livello dell'indirizzo IP, il blocco potrebbe

comportare l'oscuramento di numerosi siti ospitati nel medesimo host di quello incriminato, pur non avendone nulla in comune. In caso di indirizzo IP dinamico, inoltre, potrebbero venir segnalati erroneamente siti a cui è stato attribuito lo stesso indirizzo appartenente in precedenza ad un sito pedo-pornografico. Sebbene giudicato positivo nel ridurre l'accesso casuale ai siti di questo genere, il decreto poi non riuscirebbe a frenare l'azione dei pedofili sufficientemente esperti di informatica. Per quanto riguarda l'intervento a livello minimo di nome a dominio, infatti, la legge fa ipotizzare un intervento del filtro al livello DNS (Domain Name System), metodo in grado di ostacolare l'accesso non intenzionale, ma non l'intervento di utenti "abili", che potrebbero aggirare i filtri tramite intervento manuale di re-impostazione del DNS.

Nuove norme per la vigilanza e controllo sui gestori di PEC

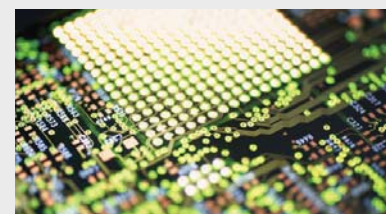
Massime garanzie per la posta elettronica certificata: lo ribadisce la circolare emessa dal CNIPA (Centro Nazionale per Informatica nella Pubblica Amministrazione), pubblicata il 21 dicembre 2006 in G.U., relativa alla vigilanza sui gestori di PEC. Questi avranno l'obbligo di effettuare verifiche, mediante una "suite di test" di riferimento indicate dal CNIPA, sull'interoperabilità dei propri sistemi, e di fornire tempestivamente informative relative a

eventuali malfunzionamenti.

Sono inoltre previsti controlli sulle forme di commercializzazione del servizio per garantire l'unicità del rapporto tra titolare e gestore, e sopralluoghi presso le strutture operative utilizzate dal gestore per verificare la conformità del sistema PEC.

Attraverso tali norme il CNIPA intende certificare ulteriormente uno strumento che, pur già del tutto collaudato, stenta diffondersi ampiamente sul mercato.

Ad oggi risulta infatti che tale servizio è sottoscritto solamente dal 32% degli uffici della PA, dal 20% tra le banche e le assicurazioni, dal 18% tra le altre aziende e dal 12% delle Camere di commercio.



Impresa

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

Sempre più silenzioso il malware del futuro

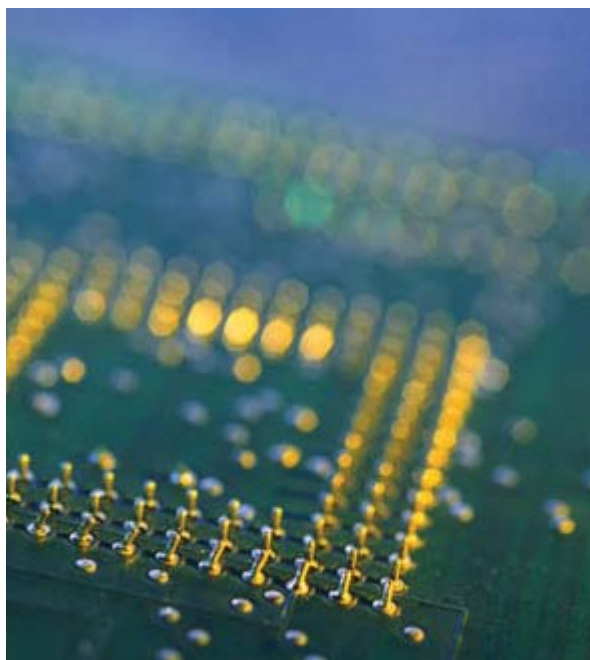
Secondo una ricerca di Gartner, entro la fine del 2007 il 75 % delle aziende sarà affetto da una tipologia di malware silente ma mirata, alimentata da precise motivazioni finanziarie: una minaccia targetizzata e automatizzata, capace di replicarsi in molteplici varianti. (Week.it - 05/02/07)

Il telelavoro tra i bersagli del malware

Secondo un'indagine, in Italia il 47% dei telelavoratori usa il proprio computer aziendale per fare acquisti su Internet. Il 31% consente ad altri di impiegarlo: uno su due "non vede niente di errato in questo comportamento". Solo il 29% ha equipaggiato il computer con un software di sicurezza. (Punto Informativo - 16/01/07)

La tecnologia NAC sposta i confini della sicurezza della rete aziendale

Con l'evolvere della tecnologia, il perimetro delle reti aziendali si è esteso fino a comprendere dispositivi mobili con funzionalità avanzate e sempre più connesse tra loro. La capillare diffusione di notebook, smartphone, terminali wireless e palmari ha aperto efficaci modalità operative ma anche nuovi orizzonti per potenziali intrusioni e comportamenti a rischio, pericolosi per le organizzazioni. Bluetooth e altre tecnologie wireless che collegano i dispositivi mobili, ad esempio, sono diventati facile bersaglio per il malware costituito da virus, worm, cavalli di troia, spyware, e così via. Le mutate frontiere del cybercrime impongono quindi un nuovo equilibrio tra accesso alla rete e sicurezza. In



questo contesto, **assume un'importanza fondamentale il controllo degli endpoint attraverso cui personale, collaboratori, partner commerciali o ospiti accedono sempre più facilmente alla rete aziendale.** Tale esigenza

trova una risposta efficace nella tecnologia NAC (Network Access Control), che consente agli amministratori IT di controllare se i device utilizzati dispongono di un antivirus, qual è il relativo livello di upgrade, il

sistema operativo in uso e il grado di patching. **Si tratta di una soluzione che permette di autorizzare l'accesso, negarlo, mettere in quarantena il client o forzare l'aggiornamento, implementando efficaci criteri di sicurezza per il controllo della rete aziendale.**

La gestione avviene indipendentemente dal tipo di dispositivi utilizzati e dalle modalità di accesso dell'utente: remoto, cablato, wireless, tramite LAN, da endpoint registrato o non registrato. Controllando lo stato di protezione (patch installate, presenza di virus...) dei device che si connettono alla LAN, si può stabilire infine a quali dati e applicazioni fornire l'accesso, rifiutando gli endpoint non autorizzati ancora prima che entrino in rete.

Tele-lavoratori?

Sì, ma con una maggiore cultura della sicurezza

Tele-lavoratori e sicurezza: un binomio tutt'altro che rassicurante, almeno secondo quanto emerge da una recente analisi condotta dal prestigioso istituto di ricerca Insight Express. Dal nutrito campione di tele-lavoratori intervistati è emerso uno scenario davvero preoccupante: molti di questi, infatti, pur credendo di operare in piena sicurezza, spesso agiscono in modo imprudente e potenzialmente pericoloso.

Il 47% dei tele-lavoratori italiani interpellati ha ammesso di usare il PC aziendale ed internet anche per scopi personali come acquisti on line, credendo che tale attività non dia fastidio al datore di lavoro. Il 31% consente anche ad altre persone di impiegare il computer, senza tener conto dei rischi per la



sicurezza derivanti da tali comportamenti. Ma non solo. Il 71% ha dichiarato di non avere antivirus o altri software di sicurezza installati sui proprio computer. Non manca poi chi apre normalmente le email anche se di provenienza sconosciuta (34%) e chi sfrutta connessioni wireless di un vicino per il proprio tele-lavoro (18%).

operatori ICT

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

PC Zombie: 2 milioni nel mondo

Nel mondo i pc controllati a distanza da hacker all'insaputa dei loro proprietari sono aumentati repentinamente arrivando nel 2006 a quota 2 milioni. L'allarme botnet è esploso anche in Italia, dove si stima che le macchine infettate siano già diverse decine di migliaia (Repubblica.it - 06/01/07)

È con la cultura che si innesca il progresso, perchè senza di essa l'uomo è condannato a vedere nell'altro sempre e solo un nemico.
(K.F. Allan)

Spam island-hopping

In seguito all'aumento del dominio di primo livello .st usato per le località Sao Tome e Principe, è stata individuata una categoria di spammer che utilizza per i propri attacchi nomi di dominio di piccole isole come link a siti Web, difficilmente rilevabili poiché sconosciuti ai filtri spam. (Toptrade - 12/06)

Quanto è sicuro Windows Vista?

Rende più affidabili e stabili e le infrastrutture, ma non ne garantisce la protezione totale. Questa la critica sollevata da molte software house focalizzate sull'IT, security sul pacchetto di sicurezza di Windows Vista, il nuovo sistema operativo recentemente rilasciato da Microsoft. Dotato di un centro di sicurezza che monitora lo stato del software di protezione del computer, **Vista possiede un account per prevenire il malware, Firewall e Antispyware e PatchGuard per impedire al codice malevolo di effettuare modifiche indesiderate al kernel del sistema operativo.**

Internet Explorer 7 di Vista include inoltre funzioni per prevenire phishing e spoofing.

Secondo alcuni maggiori vendor del settore, il nuovo sistema operativo

sarebbe comunque vulnerabile ad attacchi virali in mancanza di protezioni complementari a quelle già presenti. La posizione fortemente "dominante" di Microsoft in questo segmento di mercato, inoltre, frenerebbe l'innovazione nella protezione del sistema. Secondo Sophos, Vista offre sicuramente un certo grado di sicurezza ma va migliorato nei servizi di supporto del sistema operativo e di gestione centralizzata.

Il dubbio che Microsoft non possa competere con la velocità e l'efficacia delle soluzioni fornite da società specializzate in risposta alla rapida evoluzione del cybercrime, ha sollevato perplessità sul suo livello di protezione anche presso i responsabili di sicurezza di molte aziende, preoccupati dalla complessità dei problemi che si verrebbero a creare

in caso di vulnerabilità ad un attacco. **Microsoft ribadisce che il sistema è protetto e in grado di avvisare l'utente ogni volta che incorre in un pericolo, ma consiglia anche di installare una suite di sicurezza di un altro fornitore,** precisando inoltre che è possibile, per chi lo desidera, disabilitare le protezioni di Vista. Con riferimento al seg-

mento dei clienti "consumer", tali affermazioni presuppongono però un utente sufficientemente esperto da intervenire sulle impostazioni di sicurezza, e non chiariscono le ambiguità su quanto sia vitale per la protezione del potenziale acquirente preoccuparsi di installare un antivirus una volta adottato Vista.



Vista: Microsoft e Security Vendor a confronto

Con la nascita di Vista, si è aperto un confronto tra la corporazione di Redmond e i security vendor, da sempre abituati ad una piena libertà d'azione



nella ricerca di soluzioni contro le vulnerabilità di

Windows. Secondo alcuni l'ingresso di Microsoft nel mercato della sicurezza è guidato da un approccio chiuso e non collaborativo. Si è assistito a

una forte presa di posizione da parte di alcuni ven-

dor di sicurezza sulla riluttanza di Microsoft a rilasciare le specifiche tecniche per consentire lo sviluppo di soluzioni di supporto o alternative alle proprie. Numerose le critiche sulla chiusura dell'accesso al kernel del sistema operativo a causa della presenza del programma "Patch Guard", che impedisce ai software di terze parti di dialogare efficacemente con Vista.

Contro tale presunto atteggiamento anticoncorrenziale e i rischi di un'offerta sul mercato destinata a limitare la scelta dei consumatori, è intervenuta anche la commissione europea, davanti alla quale Microsoft si è impegnata a fornire le Api (Application Programming Interface) del proprio sistema operativo ai security vendor.