McAfee

Webank www.webank.it

inLineaNet

L'INTERNET BANKING NELL'ERA DELLA SICUREZZA

UN PERCORSO VERSO LA SICUREZZA TOTALE

Da McAfee e Banca Popolare di Milano il vademecum per imparare a proteggersi in rete.

BPM Gruppo Bipiemme

Sicurezza in rete: lo scenario corrente

Danilo Bruschi - Dipartimento di Informatica e Comunicazione, Università degli Studi di Milano

La diffusione delle tecnologie dell'informazione e della comunicazione a cui abbiamo assistito in questi anni, è stata caratterizzata, tra le altre cose, dalla diffusione di un fenomeno degenerativo rappresentato dagli attacchi o intrusioni informatiche. Gli attacchi informatici sono attività svolte da terze parti che, sfruttando errori commessi nella fase di progettazione e realizzazione dei suddetti strumenti, riescono ad accedere, a nostra insaputa, ai nostri computer ed alle informazioni in essi memorizzate. Sono molto rare le tecnologie informatiche e i prodotti software che in questi ultimi anni non siano stati fonte di nuove tecniche di intrusione. Tutti gli esperti sono tra l'altro concordi nell'affermare che questo stato di cose perdurerà ancora per molto tempo, sicuramente per alcuni decenni.

Gli attacchi informatici di questo ultimo periodo sono stati caratterizzati da un cambio di prospettiva particolarmente interessante. Se sino ad un paio di anni fa il principale obiettivo degli attacchi informatici erano i server di grosse organizzazioni e le informazioni in essi contenute, gli attacchi informatici di questi ultimi due anni sono stati mirati ad acquisire informazioni e sistemi del singolo utente. Le ragioni di questo cambio di prospettiva sono diverse: i sistemi degli utenti sono mediamente molto meno protetti di quelli di un'azienda e quindi più facili da attaccare con successo, i sistemi di utenti finali contengono comunque informazioni particolarmente utili, e con la diffusione della banda larga anche un singolo PC diventa una macchina sufficientemente potente per l'effettuazione di attacchi.

Lo scenario contemporaneo è dominato da diverse forme di attacco tutte mirate ad un unico obiettivo: il furto dell'identità digitale. Dove per identità digitale si intendono tutte quelle informazioni usate da un utente per dimostrare la propria identità in tutte le transazioni svolte in rete. Ad esempio il codice utente e la password usate per accedere ad un servizio di e-banking, i dati della carta di credito usati per effettuare commercio elettronico, codice utente e password per accedere ai PC aziendali, ecc.ecc. Le tecniche più usate per il furto di identità digitale sono il phishing e lo spyware. Con il phishing si dirotta un utente su un sito civetta del tutto simile a quello usato dall'utente per svolgere alcuni particolari servizi (solitamente si tratta di servizi di home banking o e-commerce), e lo si invita a svolgere alcune operazioni tra cui la digitazione dei codici di accesso, che saranno opportunamente intercettati, per poi essere illegalmente utilizzati.

Lo spyware, invece, è un programma che viene occultato all'interno di altri programmi o attachment di posta elettronica. Quando un utente scarica questi programmi o apre inavvertitamente questi attachment, lo spyware si attiva automaticamente e da questo momento è in grado di intercettare tutte le operazioni che un utente esegue sul proprio PC. Informazioni che provvede ad inviare in rete ad una destinazione ben definita. Sia lo spyware che il phishing sono attacchi basati su un'unica assunzione: gli utenti finali sono molto a digiuno di competenze informatiche ed in questo ambito è facile raggirarli. Il successo che questi attacchi stanno riscuotendo dimostra che l'assunzione è corretta.

Ovviamente il mondo della ricerca ha individuato le necessarie contromisure per poter far fronte a questi attacchi, soluzioni queste che dovrebbero essere adottate sia da parte degli utenti che da parte di chi realizza i servizi di rete. Vediamo brevemente quali sono questi strumenti sia lato utente che lato azienda, incominciando dai primi. Gli strumenti realizzati e disponibili per gli utenti finali sono: antivirus, antispyware e personal firewall. Il corretto uso di questi strumenti consente, nell'ordine: di rilevare in tempo reale la presenza di virus sul computer e provvedere alla loro eliminazione, di rilevare in tempo reale la presenza di spyware sul computer e provvedere alla loro eliminazione e di individuare attività anomale svolte sul computer e quindi prevenire forme di attacco diverse da virus e spyware.
Con il ricorso a queste tecnologie, il computer di un utente può godere di un livello di protezione più che soddisfacente; il problema è che l'utente medio o non le usa, perché inconsapevole del problema, o le usa male (non effettua gli aggiornamenti periodici, non predispone adeguatamente le configurazioni, li disabilita e poi si dimentica di riabilitarli, ecc. ecc.) perché si tratta comunque di tecnologie troppo complesse per l'utente medio.

Questo significa che nessun affidamento può essere fatto sull'utente finale per la messa in sicurezza di un servizio web, almeno finché non si è proceduto con un massiccio programma di formazione e sensibilizzazione mirati a rendere consapevoli tutti gli utenti di servizi informatici dei rischi legati all'uso degli stessi.

In questa fase storica, ancora caratterizzata da un forte tasso di analfabetismo informatico, è quindi insensato richiedere all'utente finale ogni contributo significativo nella soluzione dei problemi di sicurezza della rete, anche se indubbiamente lo stesso va coinvolto ed “educato” all'uso corretto dei servizi, la responsabilità in questo senso deve quindi essere presa a carico da chi realizza e offre questi servizi.
In questo contesto sono stati individuati una serie di strumenti tecnologici che possono contribuire a rendere molto più difficile l'effettuazione di attacchi quali il phishing, anche se questi attacchi potranno essere completamente elusi solo quando si riuscirà ad ottenere la fattiva collaborazione degli utenti finali.

Quali sono questi strumenti? Sostanzialmente tutti gli strumenti che rendono inutilizzabili, da parte di chi le carpisce, le informazioni raccolte durante gli attacchi di phishing e spyware. In questo contesto stanno assumendo una certa rilevanza i codici di accesso one-time, cioè utilizzabili una sola volta. Il principio su cui è basato tale meccanismo è il seguente. Ogni utente di un sistema viene fornito di un generatore di codici di accesso della dimensione di un portachiavi, che genera un diverso codice di accesso ogni 60 secondi. Quando un utente si collega ad un servizio dovrà inserire il codice di accesso generato in quel momento dal suo “portachiavi”, è ovvio che se anche qualcuno riuscisse a carpire questo codice non potrà usarlo in alcun modo.

Estremo interesse stanno suscitando anche le tecniche biometriche che consentono di associare i codici di accesso ai servizi, agli attributi fisici di una persona quali il viso, la voce, l'iride, la retina, l'impronta digitale, la geometria della mano, la firma manoscritta. In questo modo l'accesso ad servizio è vincolato “fisicamente” al legittimo utente. I progressi fatti in questo settore negli ultimi anni sono davvero molto impressionanti, sia dal punto dei costi che della precisione. Sono oggi presenti sul mercato tecnologie il cui costo si aggira sulle poche decine di euro e che sono in grado di garantire risultati molto precisi con percentuali di errore molto ridotte (che si aggirano su un errore ogni milione di casi considerati).

Queste soluzioni, faranno molto presto l'ingresso nel mondo dei servizi di rete in particolare nel mondo dell'home-banking, che non solo è tra i settori più minacciati da queste nuove forme di attacco ma è anche tra i settori più attenti all'adozione di tecniche e strumenti di contenimento. Se l'adozione di questi strumenti diminuirà di molto la probabilità di successo di un attacco di furto di identità, questo non significa che il problema debba essere considerato risolto.

Sono recentemente apparse in letteratura alcune tecniche di intrusione che se venissero implementate con successo riuscirebbero a consentire il superamento, sia di credenziali one-time che di tecniche biometriche. Ci riferiamo al Hijacking (dirottamento), una tecnica, teoricamente nota da molto tempo, che consentirebbe ad un attaccante di intromettersi in una comunicazione tra due parti, ad esempio un utente e la propria banca, e sostituire l'utente dopo che la banca lo ha correttamente riconosciuto. In questo caso il furto d'identità diventa inutile perché l'utente viene sostituito dopo che si è fatto riconoscere. La tecnica è ancora in fase di perfezionamento e ad oggi è usabile solo in contesti molto particolari, va ovviamente studiata ed osservata attentamente perché una sua generalizzazione alla rete Internet metterebbe a repentaglio la stragrande maggioranza dei servizi di rete oggi disponibili.
In questo contesto emerge con forte evidenza la rilevanza di una componente fondamentale di ogni strategia di sicurezza ICT, troppo spesso trascurata nel nostro paese, lo studio e la ricerca. La sicurezza informatica è una continua lotta tra chi da una parte individua nuove tecniche di intrusione e dall'altra chi cerca le contromisure per annullarne gli effetti, solitamente vince chi ha il maggiore know-how.

L'evoluzione di Internet, della sicurezza e dei servizi on line.

Sempre più aziende e famiglie italiane oggi stanno adottando Internet quale mezzo di comunicazione - e di lavoro - a fianco dei media tradizionali. Ciò conferma quanto sia aumentata la fiducia nei confronti della Rete, e quanto l'informatica sia sempre più alla portata anche dei non addetti ai lavori. La crescente familiarità con l'innovazione tecnologica, in Italia, è facilmente riscontrabile analizzando i dati aggiornati al mese di Ottobre 2004 del Federcomin/DIT - Osservatorio permanente della Società dell'Informazione, disponibili sul sito del Ministero per l'Innovazione e le Tecnologie (http://www.innovazione.gov.it).

L'utenza aziendale che si affaccia sul World Wide Web costituisce circa la metà del totale delle imprese italiane. Il dato è significativo perché copre trasversalmente grandi, medie e piccole realtà imprenditoriali; inoltre, una parte consistente delle realtà prese in considerazione ha anche sviluppato servizi basati sul web in grado di recare valore aggiunto a dipendenti, clienti e fornitori. Il che significa che intranet e siti web non sono più solo mezzi di comunicazione ma strumenti a supporto della produttività. Una percentuale di poco inferiore di cittadini, sul totale della popolazione, percepisce Internet, per la praticità dei servizi messi a disposizione, alla pari di un comune elettrodomestico. Inoltre osservando le percentuali di penetrazione della cultura Internet nelle famiglie italiane, più dell'80% del totale degli home Personal Computer è connesso alla Rete.

Crescono, in sintesi, l'offerta e la fruizione di servizi erogati via web. Alcune delle attività quotidiane dei cittadini - anche quelle che costituivano le cosiddette "seccature", ovvero code e tempo perso - sono state virtualizzate e possono essere fatte on line in modo valido ed efficace. Lato fornitori di servizi, la crescita di aziende con accesso a Internet ha una duplice chiave di lettura: alla necessità di fornire informazioni tramite una "vetrina elettronica" si è affiancata la diffusione di una piattaforma flessibile - Internet, appunto - in grado di integrare la gestione di numerose - se non illimitate - applicazioni per la produttività aziendale e per l'offerta di servizi rivolti ai clienti.

In questo scenario si constata solo una, ma corposa, conseguenza negativa: la crescita, direttamente proporzionale, del desiderio di sfida e l'ampliamento dell'orizzonte di conquista di hacker e criminali informatici. La posta in gioco è, d'altronde, sempre più alta: le reti trasferiscono dati sensibili. Fortunatamente sono in aumento anche tutti i fattori che contribuiscono a migliorare la sicurezza dei navigatori, su diversi fronti. La tecnologia, innanzitutto. Grazie agli sforzi congiunti di produttori di dispositivi di networking e dei maggiori marchi di software antivirus, anche gli operatori più sensibili agli attacchi quali le realtà bancarie e finanziarie hanno a disposizione una base tecnologica più solida su cui impostare la sicurezza propria e dei clienti. La protezione da attacchi non è più solo una esigenza aziendale, ma ha assunto i toni di una questione legale prioritaria. Parallelamente, sembra prendere corpo una maggior consapevolezza del mezzo Internet e dei rischi che una "rete tentacolare" comporta. Più minacce, ma maggior informazione e attenzione da parte del navigatore nei confronti dei contenuti - e non solo - che la rete e la posta elettronica propongono.

Il panorama mondiale, europeo e italiano.

A vent'anni di distanza dai primi virus trasmessi via floppy-disk, e 10 anni dopo l'epidemia del primo worm diffusosi via Internet, l'evoluzione dell'informatica continua a doversi confrontare con l'evoluzione delle minacce alla sicurezza dei PC e dati in esso contenuti. Ne è una prova la velocità con cui, nel Gennaio 2004, il virus Mydoom si diffuse in rete: la rapidità fu notevolmente superiore rispetto a quella del virus mass mail Sobig.f, risalente ad appena un anno prima.

Mentre servizi all'avanguardia di e-government e Internet Banking si stanno sempre più consolidando tra le abitudini di cittadini e utenti Internet, c'è quindi chi ha colto la sfida di ricavare benefici tramite attività illecite, attirato dai dati sensibili e confidenziali che quotidianamente transitano in Internet, come numeri di carte di credito, username e password di conti on line, caselle di posta elettronica private. Questo non deve spaventare e scoraggiare coloro i quali colgono la comodità di accedere a un mondo di servizi comunicando tramite la tastiera del proprio PC.
Le aziende costruttrici di tecnologia stanno collaborando con i marchi dei più noti software di sicurezza informatica per fare fronte comune contro tutti gli sviluppi dei crimine informatico. Questo però non è sufficiente, se manca l'informazione. Come qualsiasi altro pericolo non virtuale, è fondamentale conoscere i rischi per poterli prevenire, e anche nell'ambito della sicurezza informatica una delle strategie di difesa più efficaci è il buon senso.

Le aziende: un mondo a rischio.

Per dare un'idea delle dimensioni del fenomeno, gli esperti informatici hanno denominato il 2003 “L'anno del Worm”. Lungo i 12 mesi di un annus horribilis per la security, numerose infezioni digitali si sono diffuse tramite Internet intasando le reti, bloccando i computer e paralizzando le attività delle aziende.

Nel gennaio 2003, il worm Slammer si è insediato su 75.000 server in soli 10 minuti, intasando le reti bancomat e causando ritardi sporadici nei voli.
Poco dopo entra in azione il worm Blaster, che si diffonde sfruttando una falla di Windows, mentre in Agosto il worm Sobig.F esplode in modo ancor più virulento: nell'apice della diffusione, un messaggio e-mail ogni 17 contiene una copia di Sobig.f (Fonte: Dati Interni McAfee® Security).

In questi stessi anni, le aziende hanno raggiunto un elevato livello di dipendenza da Internet, dalle comunicazioni wireless, dalle connessioni remote e dal mobile working. In Europa esistono 13.8 milioni di piccole aziende (da 10 a 49 dipendenti), di cui l'81% utilizza la posta elettronica e il web per portare avanti le attività quotidiane (Fonte: Just Numbers, Numbers on Internet use, electronic commerce, IT and related figuresfor the European Community, Gennaio 2001).

Le aziende con meno di 50 dipendenti giocano un ruolo centrale nella crescita e prosperità dell'Europa; le stesse, attualmente, sono costrette ad affrontare problematiche derivanti da codice maligno, virus, worm, hacker e spam esattamente come le grandi aziende. La differenza è che molto spesso le piccole aziende non dispongono di esperti informatici che sviluppano policy per le loro reti e computer contro la crescente minaccia del crimine informatico. Molte non possono permettersi di affrontare un attacco, e quando lo subiscono il danno economico è ingente. Uno studio McAfee® Security (“Counting the Cost of Cybercrime”) rivela il reale impatto dei crimini informatici sull'economia europea e del costo correlato sulla sua crescita. Lo studio riguarda piccole aziende con meno di 20 dipendenti di 6 Paesi europei: Regno Unito, Francia, Germania, Paesi Bassi, Spagna e Italia.
La ricerca rivela che le piccole aziende si sentono più vulnerabili ma rifiutano di considerare seriamente le minacce perpetrate via Internet, malgrado milioni di persone siano state infettate dal più alto numero di virus in circolazione mai registrato. L'atteggiamento verso la sicurezza on line varia a secondo dei Paesi europei. Tali atteggiamenti si riflettono nelle azioni che le varie nazioni intraprendono per consolidare le loro difese contro le minacce on line come virus e hacker. Per esempio, in Francia, Regno Unito, Spagna e Italia un numero elevato di piccole aziende assegna un livello di “priorità elevata” alla sicurezza on line mentre in Germania e nei Paesi Bassi questa viene considerata una priorità di livello “basso”.

La posta elettronica e il web si confermano gli strumenti più utilizzati all'interno delle aziende, il modo più economico per comunicare e operare sul mercato. Malgrado ciò, quasi un terzo degli intervistati ha confessato di non sapere che informazioni personali quali i codici pin delle carte di credito e le password di sistema potrebbero essere rubate e utilizzate a loro insaputa.
Si tratta di un dato particolarmente preoccupante dal momento che i Trojan più recenti installano una "backdoor" elettronica sui computer infetti che può essere poi utilizzata per accedere a qualsiasi file - inclusi i dettagli relativi alle carte di credito e ai dati bancari. Gli hacker possono anche inviare enormi quantità di messaggi spam dal computer infetto a tutti coloro inclusi nella rubrica degli indirizzi.

Il cyber-spying è un'altra forma di crimine informatico di cui un terzo delle piccole aziende in Francia, Regno Unito e Paesi Bassi ignorava l'esistenza.
Le aziende in Spagna e Germania sono risultate le più informate circa la possibilità di furto delle informazioni personali e delle tecniche di cyber-spying.

Un'altra nuova forma di truffa volta a colpire gli utenti Internet è il dirottamento della connessione telefonica. I ladri informatici deviano una connessione telefonica locale a una linea telefonica con tariffa maggiorata. L'utente riceve così una bolletta telefonica esorbitante per quella che pensava essere una tariffa di connessione locale. Il livello di conoscenza delle tecniche di dirottamento delle connessioni telefoniche si è dimostrato generalmente basso tra tutte le nazioni intervistate, con quasi una su due aziende che ignorano il pericolo in Germania, Regno Unito e Paesi Bassi. Le aziende del Sud Europa in Spagna e Italia sono invece quelle con il più elevato livello di conoscenza.

Vecchi e nuovi orizzonti del cybercrime.

In principio era il Virus... La storia dei pericoli informatici (e dei conseguenti problemi di sicurezza) inizia così, ovvero con un file di programma in grado di allegarsi ai dischi del PC o ad altri file e di replicarsi ripetutamente, a insaputa dell'utente. Ecco le principali tappe attraverso le quali le minacce informatiche si sono sviluppate parallelamente alla tecnologia.

1948 John Von Neumann dimostra matematicamente la possibilità di costruire una macchina o un programma in grado di replicarsi autonomamente.

1959 Il concetto di programma auto-replicante viene per la prima volta implementato in un gioco ideato da un gruppo di programmatori dei Bell Laboratories della AT&T.

1983 Ken Thompson, autore del sistema operativo UNIX, rimuove il velo di omertà che ricopre i programmi auto-replicanti. Nel frattempo il primo esempio di virus viene mostrato nel corso di un seminario sulla sicurezza dei computer. La teoria dei programmi auto-replicanti è ormai di dominio pubblico.

1986 Un programmatore di nome Ralf Burger sperimenta la possibilità che ha un programma di replicarsi attaccando una sua copia a un altro file. Le sue simulazioni suscitarono un interesse tale da convincerlo a pubblicare un libro. Contemporaneamente in diverse parti del mondo la produzione di virus è in continua crescita. A Tel Aviv, Israele (altre fonti dicono in Italia), un programmatore sperimenta e crea uno dopo l'altro Suriv-01 (virus al contrario), Suriv-02, Suriv-03.

Il quarto virus di questa serie, conosciuto come Jerusalem, si diffonde rapidamente al di fuori dei confini di Israele. Nell'altro emisfero, in Nuova Zelanda, un giovane programmatore crea un virus che si diffonde molto rapidamente. Il virus, denominato Stoned, visualizza sullo schermo il messaggio "Your PC is Stoned" quando il computer viene avviato da un dischetto infetto. In Italia, all'università di Torino, un programmatore (probabilmente un docente) crea un nuovo virus: se viene effettuato un accesso al disco alla mezz'ora esatta, una pallina si visualizza sullo schermo e rimbalza ogni qual volta raggiunge il bordo. Per questo suo effetto a tale virus venne assegnato il nome di virus italiano o Ping Pong virus.
Simpatico e per fortuna innocuo.

1987 Un programmatore tedesco scrive un virus complesso, Cascade, così battezzato a causa dell'effetto che provoca sul testo presente sullo schermo. Cascade incorpora una nuova idea: la maggior parte del codice del virus è crittografato. Stoned, Cascade e Jerusalem sono tuttora i tre virus più diffusi nel mondo.

1988 Appaiono sul mercato i primi prodotti anti-virus a basso prezzo se non freeware, perché il problema non è ancora così sentito. Contemporaneamente il worm Morris infetta le macchine collegate a Internet, diventando così il primo worm a diffondersi in tutto il mondo.

1989 Sia la produzione dei virus che la ricerca di efficaci prodotti anti-virus sono guidate dalla Gran Bretagna. Nello stesso anno anche da Bulgaria e Unione Sovietica si propagano nuove minacce. A seguito della comparsa di un nuovo virus, denominato Datacrime, IBM decide di commercializzare un programma anti-virus scritto inizialmente per uso interno. Datacrime, ridenominato Columbus day virus, si dimostra un virus poco pericoloso, tanto da essere praticamente scomparso.

1990 Il nuovo decennio segna la comparsa, ad opera di Mark Washburn, di un nuovo virus: l'intero codice è crittografato in modo variabile, la parte del virus che si incarica della de-crittografazione può assumere diverse forme, per questo motivo viene detto virus polimorfico. Nello stesso anno si ha in circolazione un gran numero di virus di produzione bulgara. Il loro produttore, che si identifica come Dark Avenger, introduce i propri virus sui BBS (l'antenato di Internet) di numerose nazioni, infettando anche i programmi anti-virus shareware.
Nel dicembre dello stesso anno sono in circolazione circa 150 virus, e la Bulgaria divente il leader nella loro produzione.

1991 Il problema diventa commercialmente interessante: nuovi prodotti anti-virus entrano nel mercato. Ma la vera novità del 1991 è la comparsa di un virus ottenuto modificando alcune istruzioni di un virus già esistente, in modo da renderlo irriconoscibile da parte dei prodotti anti-virus in commercio. Si verifica infatti l'attacco di Tequila, il primo virus polimorfico.
Il virus arriva dalla Svizzera e si auto-modifica ogni volta che lancia un'infezione in modo da evitare il rilevamento da parte dei software anti-virus. Il numero di virus in circolazione aumenta enormemente.

1992 Dark Avenger rilascia il suo Self Mutation Engine (MtE), contenente il codice sorgente di un semplice virus, ovvero il fai-da-te del pirata informatico. Inoltre commercianti senza scrupoli vendono interi CD-Rom pieni di virus già pronti o in formato sorgente. Ma è "Michelangelo" il primo virus a ottenere l'attenzione delle cronache. Un allarme mondiale viene inviato allertando sulla possibilità di enormi danni, anche se poi in realtà il tutto è molto ridimensionato.
Lo stesso anno, il Dark Avenger Mutation Engine (DAME) divenne il primo toolkit che può essere utilizzato per trasformare qualsiasi virus in un virus polimorfico. Inoltre, sempre nello stesso anno il Virus Creation Laboratory (VCL) realizza il primo kit per la creazione di virus reali.

1999 Lo sviluppo della tecnologia informatica ha nel frattempo subito una forte accelerazione, e la pirateria sembra tenere il passo e alza la mira. Si manifesta il worm Melissa che ha come obiettivo Microsoft Word e i sistemi che utilizzano Outlook. Il virus genera un aumento del traffico Internet, e durante l'estate del 2001 il worm Code Red attacca i Microsoft Internet Information Server, ma conquista la celebrità per aver attaccato il sito web della Casa Bianca.

2003 Due worm denominati Sobig e Blaster lanciano un attacco ai computer basati su Microsoft Windows provocando così i maggiori danni mai registrati in termini di downtime e costi associati a rimuovere l'infezione. Molte aziende richiedono un intervento del governo.

2004 Mydoom si diffonde a partire dal mese di Gennaio, e attualmente detiene il record per il worm Internet a più rapida diffusione della storia.

L'evoluzione del crimine informatico.

Agli albori della diffusione dei computer, “crimine informatico” significava introdursi in un PC e appropriarsi di informazioni. Oggi, il termine include un'ampia gamma di reati in rapida evoluzione. Generalmente parlando, il cybercrime può essere suddiviso in due categorie. Da una parte si sono diffusi nuovi crimini che possono essere perpetrati solo on line. In questa categoria rientrano i reati contro la riservatezza, l'integrità e la disponibilità di computer e informazioni. L'hacking è il metodo più conosciuto e studiato, ma sviluppi più recenti includono l'elaborazione “parassita”, dove i criminali utilizzano una serie di computer remoti per effettuare operazioni improprie, tra cui memorizzare dati illegali, dalle immagini pornografiche al software copiato illegalmente.

Ci sono però crimini vecchio stile che sfruttano il mondo on line: sistemi informatici e di telecomunicazione vengono utilizzati per attaccare interessi legali protetti da leggi penali, attraverso attività di estorsione e frode. Il crimine informatico in Europa si è evoluto, passando da semplici fanatici informatici, meglio conosciuti come “geek” - gli “smanettoni” di una volta - a vere e proprie bande criminali organizzate che sfruttano Internet in modo sistematico e professional per perpetrare azioni illegali.

Gli esperti di tutta Europa concordano sulla crescita del fenomeno del crimine informatico nell'area. Il Professor Ulrich Sieber del Max-Planck-Institute for Foreign and International Criminal Law di Friburgo, Germania, afferma che “il crimine informatico rappresenta la categoria di reato in più rapida crescita in Europa”.
Gran Bretagna, Olanda, Francia, Germania, Italia e Spagna sono state identificate come i principali obiettivi dei criminali informatici. Oggi, il numero delle nuove minacce potenzialmente dannose rilevate mensilmente dai ricercatori McAfee è salito a 1.500. Il crimine informatico riflette le tradizionali attività criminali offline, con circa il 70% del software doloso (malware) che viene creato puramente per profitto. Purtroppo il cybercrime è in fase di evoluzione, e guarda al futuro per identificare le minacce che queste attività comportano per i PC di casa, per le infrastrutture della pubblica amministrazione e per i sistemi informatici dei settori finanziario e sanitario.

Dagli hacker solitari alle bande criminali organizzate.

La maggior parte dei crimini informatici nel 2000 venivano commessi dai criminali informatici "solitari". Le motivazioni di questi hacker solitari erano principalmente pubblicità e notorietà.
Gli hacker sono solitamente giovani, maschi e socialmente emarginati, come conferma John Suler, esperto di psicologia del cyberspazio alla Rider University, Lawrenceville, NJ: "Alcuni sono affascinati dalla sfida e dall'eccitazione di avventurarsi in territori proibiti. Traggono un senso di realizzazione, supremazia e potenza dal fare quello che altri non possono fare. Impressionare altri utenti, specialmente gli altri hacker, è una fonte di auto-stima. Introdursi nel sistema delle "istituzioni" riflette un atteggiamento provocatorio nei confronti dell'autorità. Un hacker si sente spinto a dimostrare di essere migliore e più intelligente di chiunque altro. Il gioco del gatto e il topo per battere il sistema diventa una ricerca implacabile e inesorabile per mettere alla prova sé stessi[1]".

1 - Suler, John. Techno-Crimes (Hacking): Managing deviant on line behavior, Part5. Disponibile on line sul sito http:// www.enotalone.com

Virus e spam sono sempre stati uno dei rovesci della medaglia di Internet. Ma il crimine organizzato si è velocemente adattato al nuovo mondo dell'hi-tech; le gang criminali tradizionali stanno iniziando a utilizzare Internet non solo per comunicare ma anche come strumento per commettere reati "classici" - estorsioni, truffe, riciclaggio di denaro, intimidazione e furto - in modo più efficiente e con meno rischi e per entrare in nuovi campi del crimine. Grazie alla portata globale di Internet, la tentazione è elevata - e la portata del problema è imponente.
La crescita dell'e-business e dell'utilizzo di Internet come parte delle attività quotidiane ha reso ancora più semplice per le bande criminali compiere reati e nascondere le loro attività illegali. Il denaro può essere movimentato rapidamente, con pochi semplici click del mouse; e per la polizia non è semplice monitorare e seguire le transazioni finanziarie di bande criminali internazionali. Inoltre, la creazione di "identità virtuali" garantisce un maggior anonimato alle attività del crimine organizzato. Computer e stampanti semplificano la produzione di documenti falsi di maggior qualità, più difficili da identificare.

Un'indagine realizzata per l'Octopus Programme del Council of Europe identifica quattro paesi Europei dove il crimine organizzato tradizionale è già entrato nel mondo on line: Danimarca, Portogallo, Romania e UK, seguito a ruota dalla Russia. Il Ministro degli Affari Interni russo ha conteggiato 7.053 casi di crimini informatici nel 2003, circa il doppio del 2002 (3.782); nel 2004 tale numero è aumentato drasticamente, con 4.995 casi registrati nella prima metà dell'anno[2].

2 - Dati forniti da Vladimir Golubev in una intervista rilascata alla rivista "Hacker", disponibile on line sul sito http:// www.crime-research.org/ interviews/computer_crimes/ (1-10-2004)

Inoltre, proprio a San Pietroburgo è stato localizzato il primo esempio significativo di crimine informatico organizzato. Vladimir Leonidovich Levin, nel 1997, ha trasferito 3,7 milioni di dollari dal Sistema di Gestione dei Contanti di Citibank a New York su conti che appartenevano alla sua rete criminale negli Stati Uniti, Olanda, Finlandia, Germania e Israele. I complici furono arrestati mentre effettuavano prelievi a San Francisco e in Olanda. Vladimir Leonidovich venne arrestato durante un soggiorno a New York e incarcerato.
In Germania, il numero di crimini informatici registrati è quadruplicato passando da 15.000 nel 1993 a 60.000 nel 2003[3].
C'è anche una crescente testimonianza di organizzazioni criminali che operano in Finlandia, Olanda, Italia, Spagna e Svezia.

3 - Polizeiliche Kriminalstatistik 2003. Bundesrepublik Deutschland. Disponibile on line sul sito http://www.bka.de (31-08-2004)

Rispetto alle gang criminali tradizionali molto compatte e legate, le reti on line possono spesso essere alleanze libere. Internet sta modificando il modo in cui i delinquenti si organizzano per perpetrare i crimini. Il cybercrime non richiede controllo su un territorio geografico e necessita di minori contatti personali, e non rende necessarie relazioni tra criminali che si basino sulla fiducia e la disciplina. In breve, non è necessaria un'organizzazione formale. La rete può favorire quelle organizzazioni criminali che sono già basate su una rete a struttura lineare.

Come i criminali organizzati guadagnano con Internet.

Il fine principale del crimine organizzato è quello di fare soldi. Gang organizzate e truffatori professionisti sfruttano Internet per guadagnare - ovunque ci sia l'opportunità di arricchirsi. E colpiscono sia le aziende che i singoli individui, indifferentemente.

Tra i crimini della vecchia scuola che sono stati portati a nuova vita su Internet vi sono, per esempio, i racket di estorsione e protezione, che hanno avuto una nuova svolta nel 21° secolo con la comparsa dei "bots", da robot, ovvero armi informatiche progettate per ricattare le aziende. I computer infettati da un Trojan vengono anche chiamati zombie; vari zombie infetti con lo stesso Trojan costituiscono una bot-net o rete di bot. Le bot-net possono essere controllate da remoto da un unico computer affinché eseguano gli stessi comandi, come un esercito di decine di migliaia di robot dannosi.

Si è registrato un massiccio aumento nella richiesta di questo tipo di estorsioni negli ultimi due o tre anni, con una crescita nel numero di reti controllate da remoto da criminali. Ne è un esempio l'azione di sicurezza dell'Internet provider Norvegese Telenor, che nel settembre 2004 ha chiuso una rete di bot-net di circa 10.000 macchine. La bot-net era sul punto di lanciare attacchi denial-of-service e tentativi di intrusione su vari computer e reti. In ogni caso, lo staff di Telenor non riuscì a determinare esattamente il computer host della bot-net che stavano cercando. Così, mentre spegnevano il server che controllava gli zombie (i computer in ostaggio nella rete bot-net), gli hacker dietro le quinte della bot-net avevano già rilanciato le loro attività dannose assegnando a un altro server il nome dell'host che il sistema bot-net ricercava[4].

4 - Telenor avdekker internasjonal sikkerhetsrisiko. Disponibile on line sul sito http://www.telenor.no (10-09-2004)

Il Regno Unito è stato uno dei primi paesi Europei a evidenziare il problema. Len Hynds, Capo del NHTCU, afferma: "Diventando sempre più forte dopo ogni attacco, creando beni illeciti per sovvenzionare altre aree della criminalità, e acquisendo esperienza e competenza con cui contaminare attività legittime - il crimine organizzato è sia una minaccia che un concorrente, e il mondo industriale non può più ignorare il problema[5]".

5 - Fonte: articolo tratto da una intervista rilasciata da Len Hynds, fornito da Felicity Bull, Corporate Communications Manager, NHCTU (07-09-2004)

Non a caso, il livello di preoccupazione è stato tra i motivi che hanno portato alla creazione del Serious Organised Crime Agency (SOCA), un'agenzia specializzata operativa dal 2006. Il suo Direttore Generale sarà Bill Hughes, attualmente a capo del National Crime Squad. Sir Stephen Lander, un responsabile dell'ex-MI5, assumerà il ruolo di Chairman. Il SOCA riunirà una serie di esperti, inclusi specialisti di tecnologia e finanziari e coloro con capacità investigative e competenze criminali, per combattere contro il crimine organizzato del 21° secolo.

La truffa delle carte di credito rappresenta una vasta area di attività anche per il crimine organizzato. In Germania le frodi con carte di credito rappresentano circa i due terzi dei casi di crimini informatici riportati, le frodi tramite computer contano per il 16% e circa il 10% dei casi coinvolge l'accesso fraudolento ai servizi di telecomunicazione, inclusi i dialer.

A causa dell'inacessibilità dei sistemi informatici delle grandi aziende, più frequentemente gli attacchi vengono perpetrati ai loro clienti, con attività di "phishing" per impossessarsi dei dettagli bancari.

Vengono creati finti siti web falsi e vengono inviati messaggi e-mail contraffatti che chiedono ai clienti di condividere i numeri di conto corrente. I conti possono poi essere saccheggiati. Nel maggio 2004 la polizia Spagnola effettuò una serie di arresti collegati a una truffa di phishing internazionale.

Questa operazione internazionale coinvolse l'unità Cyber Crime dell'Interpol a Lione, l'FBI, l'NHTCU inglese, la Guardia Civil e il GDT. Gli attacchi di phishing sono iniziati negli Stati Uniti nel Dicembre 2003, con un tasso di crescita mensile di circa il 50%. Nel Gennaio 2004 gli attacchi si manifestarono anche nel Regno Unito e in Australia, a Luglio in Brasile e Germania e in Agosto in Francia. Sempre in Agosto, dei kit fai-da-te per lanciare attacchi di phishing fecero la loro apparizione su Internet. Le fonti degli attacchi condussero a sedi negli USA e in Corea del Sud e più tardi in Russia e Asia. Due terzi di tutti i siti web legati al phishing hanno sede negli Stati Uniti, nella Corea del Sud e in Cina. Almeno il 15% del phishing si verifica in Europa, in particolare in Olanda e Turchia, ma anche in Croazia, Polonia, Portogallo, Spagna, Svezia e nel Regno Unito.

Per coloro che non cadono vittime delle frodi di phishing, e sono protette da firewall e software anti-virus, è in agguato una forma di truffa ancor più pericolosa. Le truffe d'identità, ovvero l'utilizzo di dati personali per ottenere carte di credito o addirittura assumere l'identità altrui, sono in aumento. Recentemente, 28 persone sono state arrestate dopo che il servizio segreto Statunitense ha scoperto un circolo di siti web truffa incriminato di aver venduto 1,7 milioni di numeri di carte di credito, passaporti e certificati di nascita.

Le minacce: cosa sono, come difendersi.

I primi pericoli che hanno attirato l'attenzione di studiosi ed esperti si sicurezza hanno nomi quali Trojan Horse, cavalli di troia, che come lo stratagemma di Ulisse sono programmi nefasti che si spacciano per applicazioni benevole. E l'onomastica rende ancora l'idea con i worm, altri programmi parassiti che si replicano ma, a differenza dei virus, non infettano altri file di programma. I worm possono creare copie sullo stesso computer, o inviare le copie ad altri computer tramite una rete.

Alcuni virus si attaccano ai file in modo che quando il file infetto viene eseguito, anche il virus va in esecuzione. Altri virus risiedono nella memoria del computer e infettano i file nel momento in cui il computer apre, modifica o crea i file. Non necessariamente le "infezioni" si manifestano tramite "sintomi", ma le conseguenze sono spesso poco piacevoli e vanno dai file danneggiati a danni irrecuperabili sul sistema. Il numero del software doloso attualmente in circolazione è stimato intorno alle 57.000 differenti tipologie.

A differenza di altri programmi dannosi per computer e reti, è necessario l'intervento - involontario - di un utente per dare inizio all'infezione e alla propagazione di un virus. Oggi, con l'obsolescenza dei floppy disk, storico veicolo di contagio, i virus si diffondono via e-mail e Internet. Occorre, quindi, prestare la massima attenzione agli allegati della posta in arrivo.

Ugualmente seccanti sono i falsi virus, o "hoax". In genere si tratta di messaggi elettronici voluti o non intenzionali che avvisano le persone di un virus o altro software doloso. Alcuni hoax causano tanti problemi quanto un virus provocando enormi quantità di e-mail non necessarie.
Gli hoax possono contenere avvertimenti su nuovi presunti virus e i danni conseguenti oppure richieste di inoltro dell'avviso al maggior numero possibile di persone, "informazioni" pseudo-tecniche che descrivono il virus, unite a falsi commenti da parte di enti ufficiali (FBI, produttori di software, agenzie).

Ma le minacce, oggi, si sono notevolmente evolute.

Phishing

È facile inviare una e-mail fingendosi qualcun altro; è possibile infatti spedire messaggi di posta elettronica provenienti, in apparenza, da mittenti legittimi e, a prima vista in tutto simili per impostazione e aspetto grafico a messaggi autentici. Lo scopo è ovviamente criminoso: spingere i destinatari a svelare dati personali e sensibili (numero di carta di credito, password e login di accesso personali ecc...) da utilizzare per attività fraudolente.

La miglior difesa per truffe di questo genere è il buon senso e l'informazione. Banche e aziende di e-commerce non chiedono mai ai propri clienti dati confidenziali al di fuori delle sessioni di transazione protette, tanto meno tramite comunicazioni via e-mail.
È fondamentale, quindi, essere a conoscenza dei criteri di comunicazione dei propri fornitori di servizi di e-banking e commercio elettronico e non esitare a mettersi in contatto con i mittenti per verificare l'autenticità delle e-mail.

Anche se nessun utente in Internet può considerarsi al sicuro da frodi tutt'altro che virtuali, le aziende di tutto il mondo stanno moltiplicando i propri sforzi per mettere al sicuro i propri clienti. Ad oggi anche i grandi colossi dell'e-commerce hanno dovuto fare i conti con false e-mail spedite a loro clienti. Perfino l'FBI può essere enumerata fra le vittime delle tecniche di phishing.

Secondo un'analisi dall'Anti-Phishing Working Group, un'associazione industriale internazionale che combatte furti d'identità e frodi simili, ben il 5% delle richieste contenute in e-mail fraudolente sono andate realmente a buon fine riuscendo a carpire informazioni confidenziali al destinatario.

È necessario quindi prestare attenzione a messaggi contenenti inviti a visitare un sito web, oppure alla richiesta di scaricare un file che potrebbe contenere un elemento pericoloso, come un virus o un trojan. Conviene diffidare da e-mail contenenti messaggi generici di richiesta di informazioni personali per motivi non ben specificati, come scadenza della carta di credito o problemi tecnici sospetti.

È importante adottare sistemi di protezione informatici per difendersi da tutti gli elementi pericolosi ai fini del phishing, come rilevatori di spamming e software antivirus.

Spyware

Uno spyware è un software che è in grado di installarsi a insaputa dell'utente sul PC durante normali sessioni di navigazione in Internet o in aggiunta ad altre applicazioni. Lo spyware raccoglie informazioni sull'utente, le trasmette via Internet e le utilizza per trarne profitto. Carpendo l'indirizzo di posta, per esempio, l'utente potrà essere fatto oggetto di invii indesiderati (vedi Spam).

Non tutti gli spyware, però, sono illegali. In questa categoria, infatti, si collocano anche tutti i programmi per la raccolta di dati e installati con il consenso dell'utente, consapevole quindi di quali dati e a quali condizioni siano raccolti. Trattandosi di applicazioni installate sul PC, è opportuno impostare il proprio browser con un livello di sicurezza tale da impedire il download automatico di file (è il modo più semplice per "contrarre infezioni").
È comunque opportuno diffidare da software e utility offerte gratuitamente tramite finestre di pop-up invasive, e non è difficile trovare spyware agganciati ai più diffusi programmi per la condivisione di musica: una volta installati, è difficile eliminarli. Poiché i criminali informatici sono sempre più orientati verso attività redditizie, lo spyware verrà utilizzato sempre più per i cosiddetti furti d'identità.

Non a caso sono in aumento i casi di utilizzo di dati personali per ottenere carte di credito o commettere reati con identità altrui. Le strutture investigative di tutto il mondo, specializzate in crimini informatici, sono già passate all'attacco per bloccare siti web truffa specializzati nella vendita di numeri di carte di credito, passaporti e certificati di nascita.

Un motivo più che sufficiente per rinunciare ad un download sospetto sul PC e per correre ai ripari. Esistono programmi anti-spyware nei prodotti di protezione del PC, in grado di rilevare le talpe indesiderate. È possibile inoltre verificare, attraverso il Task Manager Windows, tutte le applicazioni (.exe) in attività nel proprio computer, confrontandole con le liste, disponibili in Internet, degli spyware più pericolosi.

Spam

Se una minaccia informatica ha preso il nome della carne in scatola fornita all'esercito americano - Spam, ovvero Spiced Ham - la dice tutta sulla "sostanza" propagata dall'imponente mole di e-mail non desiderate, quantificato nel 48% del traffico di posta elettronica mondiale. Ma è stato un celebre sketch dei Monty Python - un cameriere tenta di propinare la suddetta pietanza in ogni proposta del menu ad un gruppo di improbabili avventori vichinghi - a far sì che il termine Spam fosse associato a qualcosa di onnipresente.

Lo Spam è un fenomeno in continuo aumento che interessa allo stesso modo sia le aziende che i navigatori di tutto il mondo. Milioni di e-mail pubblicitarie, se non di contenuto offensivo, spedite a raffica a tutti gli indirizzi e-mail resi pubblici che, oltre ad intasare le caselle di posta, diventano anche pericolosi veicoli per altre minacce - virus, phishing ecc...
Bloccare lo Spam e la sua fonte è una delle possibilità per fermare il fenomeno mediante l'utilizzo della funzione di blocco degli ISP spammer conosciuti. È stato anche suggerito di rimandare lo spam agli spammer, ma ciò non farebbe altro che paralizzare gli Internet Service Provider autorizzati, che non potrebbero far fronte alla richiesta di banda extra per rimandare milioni di messaggi e-mail.
Dal momento che si ritiene che lo spam provenga da 200 fonti principali, il software anti-spam è il modo più efficace per identificare gli spammer conosciuti e l'attività di spamming ed evitare che entri in rete.

Un software di questo tipo può utilizzare diversi metodi proattivie reattivi per rilevare lo Spam. Può creare liste di indirizzi e-mail "buoni" e "cattivi". Può escludere gli indirizzi e-mail inclusi nelle "liste nere" dalle caselle di posta elettronica in ingresso degli utenti. Può utilizzare regole integrate nel prodotto per fornire rilevamento euristico e analisi di integrità di ciascun messaggio. Il software anti-spam più efficace si basa su un sistema di regole che forniscono diversi metodi di rilevamento proattivo e reattivo. D'altronde, le statistiche parlano chiaro(fonte McAfee interna): 1/4 (24%) delle piccole aziende italiane riceve fino a 5 messaggi spam ogni settimana e una su cinque (19%) ne riceve più di 50.
Questo significa che gran parte della posta che si riceve è indesiderata. Il metodo migliore per limitare la quantità di spam nella propria casella di posta è... creare una casella di posta alternativa, qualora si voglia partecipare a forum, blog, o inserire annunci in rete, limitando così la divulgazione di indirizzi e-mail personali.

Bot-net

Si dice che le disgrazie non vengano mai da sole. Lo spam, che già di per sé fa perdere tempo a tutti gli utenti di posta elettronica, è tra le principali cause della diffusione dei Trojan, le applicazioni che infettano i computer senza creare sospetti. I Trojan, a loro volta, sono il mezzo per far penetrare, nei sistemi operativi dei PC presi di mira, programmi che permettono a terzi il controllo del PC, chiamati "bot".

Il computer colpito, a questo punto, si trasforma in un "robot" controllato da manovratori occulti. I criminali telematici possono, quindi, controllare numerosi PC contemporaneamente attraverso questo sistema, creando delle vere e proprie reti (o bot-net) pronte a lanciare attacchi di vasta portata.

I sistemi di difesa sono gli stessi per le altre minacce invasive (virus, trojan horse ecc...): è fondamentale proteggersi attraverso software antivirus e usare il buon senso prima di scaricare file da Internet o aprire allegati su e-mail, sospette e non. Utilizzando migliaia di computer in tutto il mondo che sono stati infettati con codice doloso, i criminali possono schierare "eserciti di bot-net" per bombardare i siti web aziendali con migliaia di e-mail false al secondo, bloccando tutte le transazioni genuine e le comunità. I criminali quindi inviano un'e-mail richiedendo un riscatto e minacciando nuovi bombardamenti. Tale attività minaccia la reale vitalità di un'azienda on line: se il suo sito web non funziona, non può fare affari.

Si tratta della la nuova frontiera del crimine on line. Si è registrato un massiccio aumento nella richiesta di questo tipo di estorsioni negli ultimi due o tre anni, con una crescita nel numero di reti controllate da remoto da criminali. Una fonte all'interno di Scotland Yard afferma: "Piccoli gruppi di giovani creano una risorsa di 10.000 fino a 30.000 computer collegati in rete tra loro e la affittano a chiunque abbia i soldi". La tariffa attuale sembra essere pari a $100 all'ora.
Ci sono inoltre prove che gli indirizzi IP di queste macchine sono venduti nelle chat room. Autori di virus e intermediari gestiscono il pagamento attraverso conti anonimi. I criminali organizzati possono utilizzare tali reti per sferrare vasti attacchi denial-of-service o distribuire spam con virus che rubano carte di credito e/o dati bancari a utenti ignari.

Keylogging

Il keylogging è una forma di crimine informatico che consiste nella registrazione dei tasti che un utente di PC preme quando scrive. Gli hacker analizzano poi le battute sulla tastiera per recuperare i dettagli relativi a nomi utente, password o conti bancari.
La memorizzazione può avvenire tramite un piccolo componente hardware installato tra la tastiera e il PC - dispositivi non illegali e facilmente acquistabili Internet per poco più di 50 Euro - oppure in modalità remota tramite l'installazione sul PC di un software. Alcuni programmi di key-logging evoluti sono in grado di aspettare il momento in cui l'utente si collega a un sito specifico di una banca per iniziare a registrare le battute sulla tastiera.

I programmi software di key-logging normalmente arrivano sui PC tramite messaggi e-mail o via internet, tramite virus o "Trojan horse": file che sembrano innocui, contengono uno scherzo o un'immagine, ma che nascondo nell'allegato un altro programma che si installa e inizia a girare sul PC, causando solo un lieve rallentamento nelle prestazioni del computer.

Anche in questo caso, la migliore difesa consiste nel dotarsi di un programma antivirus che fornisca una protezione automatica e sempre attiva, in grado di aggiornarsi via internet costantemente; tali applicazioni, oltre a controllare cosa entra in un computer da Internet monitorano l'eventuale verificarsi di attività sospette che esulano dalle normali attività di sistema del PC.

Recentemente, la Polizia inglese ha sventato a fatica un piano ad opera di criminali informatici architettato al fine di rubare 220 milioni di sterline dagli uffici di Londra della banca giapponese Sumitomo Mitsui, cercando di introdursi nei sistemi informatici della banca. Direttamente da casa a colpi di click, gli hacker avevano ottenuto l'accesso ai sistemi della banca utilizzando un software di keylogging che teneva traccia di ogni tasto premuto sulle tastiere dei computer della banca.

Questo è solo uno dei numerosi casi di crimine informatico, e testimonia l'evoluzione del crimine organizzato che si sta indirizzando verso frodi e truffe on line, attraverso cui gli hacker possono conseguire enormi guadagni accedendo a reti riservate. È sufficiente qualche piccolo accorgimento (ancora una volta identificabile con il senno) per non cadere delle trame dei malintenzionati, evitando, per esempio, di scaricare screensaver o vignette animate da siti web sconosciuti. Inoltre, essendo il sistema operativo Microsoft Windows particolarmente soggetto agli attacchi poiché è quello più comunemente utilizzato, è bene assicurarsi di aver caricato e implementato le patch di sicurezza più recenti rilasciate da Microsoft per combattere le minacce degli hacker.

Dialer

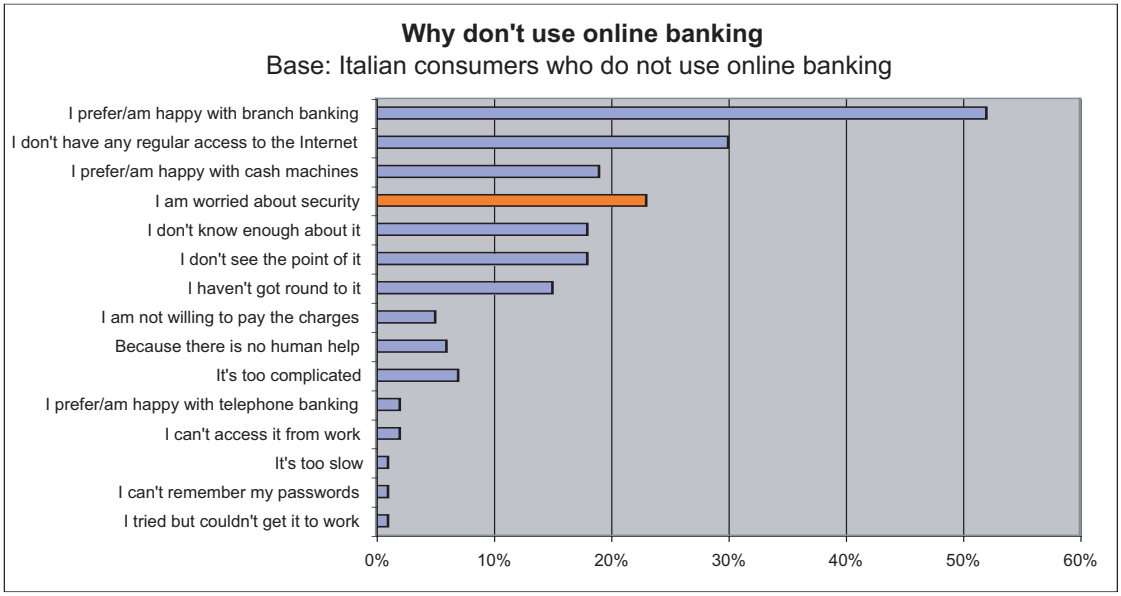
Un dialer è un programma che - all'insaputa dell'utente - reindirizza le connessioni Internet dei PC su cui riesce ad installarsi verso un Internet Service Provider diverso da quello dell'utente, con lo scopo di addebitare i costi di connessione per collegamenti ad una terza parte. L'attacco al PC avviene a livello di impostazioni di sistema, per cui le attività di navigazione in Internet si svolgono apparentemente in totale normalità. La differenza la si coglie soltanto con la notifica della successiva bolletta telefonica.

Tra i cosiddetti spyware, il dialer è uno dei più subdoli, in quanto mira alla vera e propria truffa economica ai danni dell'utente. Anche in questo caso, è bene non scaricare (e installare) programmi attraverso Internet, o ricevuti via e-mail, se non si ha l'assoluta certezza dell'autenticità.

E se l'operatore telefonico di fiducia sembra aver aumentato eccessivamente i prezzi della connessione Internet, prima di recedere dal contratto e passare alla concorrenza è bene accertarsi di non essere vittima di una truffa informatica. Il dialer è un raggiro doppiamente seccante, perché colpisce non solo il navigatore/utente ma anche il cittadino consumatore. Occorre pertanto controllare le impostazioni di connessione, per accertarsi di non essere sotto controllo di un dialer. È possibile inoltre chiedere al proprio operatore la disattivazione di numeri telefonici aventi prefisso utilizzato per chiamate a tariffa speciale.

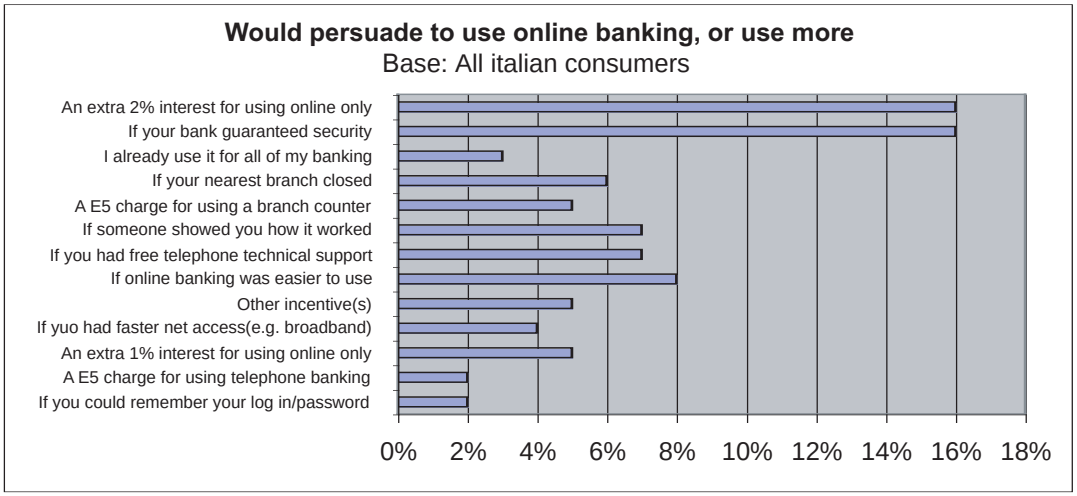
L'unione fa la sicurezza.

Il seguente grafico evidenzia che ben il 23% degli utenti italiani non utilizza servizi di internet banking perchè preoccupato del livello di sicurezza durante le transazioni.



Fonte: Forrester Research, Inc., 16 Marzo 2005,
Why Banks Must Tackle Net Users' Security Fears
Net Users' Trust In Online Security Decides Whether They Bank Online

E, come si evince dalla stessa ricerca, un elevato livello di sicurezza sarebbe uno dei principali motivi di diffusione dei servizi on line.



Fonte: Forrester Research, Inc., 16 Marzo 2005,
Why Banks Must Tackle Net Users' Security Fears
Net Users' Trust In Online Security Decides Whether They Bank Online

Applicando le necessarie misure di protezione, è possibile usufruire di servizi bancari e non in tranquillità. Se da una parte gli utenti sono tenuti ad essere informati su sicurezza e privacy on line, gli "sportelli virtuali" degli istituti di credito devono adottare procedure operative di elevata affidabilità e soluzioni tecnologiche in costante aggiornamento.

Tecnologia d'avanguardia...

La protezione dell'ambiente operativo è il primo livello di protezione di cui un serio (e sicuro) servizio finanziario on-line deve essere dotato. Alla base di transazioni virtuali devono essere presenti dispositivi di firewalling a più livelli in grado di creare un vero e proprio scudo a difesa di chi utilizza i servizi on line. Un ulteriore elemento che mette al riparo da accessi non autorizzati alla rete è costituito dai sistemi di monitoraggio delle intrusioni, o IDS (Intrusion Detection System).
Tali controlli devono essere effettuati costantemente.
Altri accorgimenti possono essere applicati durante le operazioni stesse, per fornire maggiori criteri di sicurezza. Le sessioni di connessione devono essere temporizzate e devono essere impedite operazioni, come i bonifici, di vasta entità.
Attraverso l'indicazione nell'home page dell'area privata dei dettagli dell'ultimo accesso, l'utente è in grado di verificare eventuali accessi irregolari.

La registrazione dei dati delle transazioni è un altro procedimento indispensabile a garantire un elevato livello di sicurezza. Attraverso l'archiviazione di accessi e operazioni, è possibile avere il controllo di tutto ciò che accade nell'ambiente operativo e risalire agli indirizzi IP e i POP dei computer che hanno effettuato l'accesso. Naturalmente, per la vigente normativa sulla privacy e protezione dei dati, la raccolta di tali informazioni deve essere autorizzata dall'utente che sottoscrive il contratto di utilizzo dei servizi.

...e buon senso dell'utente.

Gli strumenti per difendersi da tutti i tipi di minacce (virus, worm, trojan horse, backdoor) sono alla portata di tutti: è importante adottarli, e soprattutto utilizzarli correttamente.

In commercio esistono numerosi programmi antivirus, alcuni dei quali possono anche essere acquistati via Internet. L'antivirus va attivato ogni volta che si accende il computer (è possibile impostare questa funzione automaticamente) e deve assolvere la funzione di controllo dei file ricevuti in allegato alla posta elettronica, tutti i supporti utilizzati (come floppy e cd rom) e tutto il materiale scaricato da Internet.

In aggiunta all'antivirus, esistono strumenti di protezione - i Personal Firewall - che creano una vera e propria barriera in grado di filtrare la trasmissione di dati verso il nostro computer, per bloccare i flussi provenienti da indirizzi web potenzialmente pericolosi. Il programma anti-virus, per funzionare in modo proattivo, deve essere quotidianamente aggiornato. Nuovi virus e minacce diverse invadono la rete ogni giorno, e le case produttrici di software antivirus rilasciano giorno per giorno gli aggiornamenti per far fronte ai pericoli in continuo mutamento.
Aggiornare l'antivirus è semplice: in genere basta collegarsi al sito della casa produttrice e scaricare gli aggiornamenti. In alcuni casi, è possibile acquistare una sorta di "abbonamento" che provvede a compiere l'operazione automaticamente ad ogni connessione ad Internet, oppure a scadenze fisse.
Inoltre l'antivirus è in grado di controllare il contenuto dei dischi del computer attraverso la scansione completa del sistema, anch'essa programmabile in automatico.

Tanto più si utilizzano Internet e posta elettronica, tanto maggiore dovrà essere l'attenzione ai pericoli di "infezione". La diffusione e la praticità della comunicazione via e-mail, infatti, fa della posta elettronica il mezzo più utilizzato e più semplice a disposizione degli hacker.
Per questo motivo occorre fare estrema attenzione ai file allegati, diffidare delle e-mail sospette o provenienti da indirizzi sconosciuti, non rispondere mai a e-mail che chiedono di comunicare dati sensibili o personali.

Anche i browser sono adatti a proteggere il proprio computer, perché sono compatibili con le tecnologie di protezione adottate da servizi on line di natura finanziaria (per esempio le banche), da siti di e-commerce e da tutti gli altri siti internet che utilizzano la cosiddetta "connessione sicura" (protocollo https).
È importante quindi scaricare e installare sul proprio computer gli aggiornamenti che vengono messi a disposizione dalle case produttrici dei browser sul loro sito internet.

Allo stesso modo, è importante aggiornare il sistema operativo del computer che si utilizza: ogni nuova versione proposta è generalmente migliore della precedente in quanto a strumenti di protezione e sicurezza. Inoltre, anche per i sistemi operativi vengono rilasciati aggiornamenti (detti "patch") di specifiche funzioni, in seguito a segnalazioni di debolezze o problemi rilevati dagli utenti.

Infine è importante che alcuni comportamenti diventino la norma per l'utilizzo di Internet e dei servizi erogati via web in sicurezza:

- non fornire mai a nessuno i codici segreti che si usano per accedere ai servizi di natura finanziaria e bancaria
- custodire i codici segreti separatamente.
- modificare di frequente le password che si utilizzano.
- scegliere password non prevedibili (nomi di parenti, date di nascita ecc.)
- non lasciare mai incustodito un computer connesso all'area privata di siti internet di natura economica/finanziaria o personale. Ricordarsi, allo stesso modo, di disconnettersi (fare log out) una volta terminato l'uso del servizio.
- servirsi sempre di computer di cui si conosce il livello di protezione e sicurezza, in particolar modo quando si tratta di macchine utilizzate da un gran numero di persone.

Gli strumenti legislativi: il caso dell'Italia.

La protezione delle informazioni, le politiche di controllo degli accessi e dell'integrità dei dati, sono ora obbligo di legge. Da un anno è in vigore il nuovo Testo Unico sulla Privacy, che impone il rispetto di normative specifiche relativamente alla sicurezza informatica, da poco meno le aziende hanno dovuto adeguarsi alle nuove misure.

Il Decreto 30/07/2003 n. 196 che sostituisce la legge n. 675/1996, amplia le normative che regolano la protezione dei dati personali per chiunque, nel rispetto di tre concetti di base: i dati personali devono essere protetti, la protezione deve essere correlata ai diritti e alle libertà fondamentali dell'interessato e dei dati, dei quali deve essere garantita la riservatezza.
Da ora, l'utilizzazione dei dati personali e dei dati identificativi dovrà essere ridotta al minimo e quindi riservata soltanto ai casi nei quali non si possa procedere attraverso dati anonimi o non si possa ricorrere a modalità che consentano di identificare diversamente l'interessato.

Per utenti e aziende diventa così prioritario dotarsi di applicativi sempre disponibili, per ottenere contemporaneamente la garanzia di un livello di sicurezza adeguato alla difesa sia delle risorse tecnologiche (reti e sistemi) sia dei dati da proteggere, risultati dai processi produttivi. Proteggere le informazioni da intrusioni e difendersi da furti di dati personali equivale a tutelarsi legalmente. Come a suo tempo la 626 per gli obblighi di sicurezza, il Testo Unico sulla Privacy - o “Codice in Materia di protezione dei dati personali” prevede una serie di misure per garantire i diritti e le libertà fondamentali delle persone in materia informazioni personali partendo dal presupposto che i dati vengano gestiti attraverso l'IT.

La normativa

Il testo della legge conferisce particolare importanza alla definizione delle figure che operano nell'ambito del trattamento dei dati personali, ovvero il Titolare, il Responsabile e l'Incaricato, da parte del soggetto che va a raccogliere i dati, in quanto gli obblighi e le responsabilità inerenti sono differenti a seconda della figura. Il Titolare, qualora sia un trattamento effettuato da una persona giuridica, dalla pubblica amministrazione, un ente privato o pubblico, un'associazione profit o non profit, costituisce l'entità nel suo complesso. La titolarità del trattamento è necessaria.

Il Responsabile ed eventuali Incaricati possono essere nominati dal titolare, individuando soggetti che per capacità, affidabilità, responsabilità, esperienza siano in grado di dare migliore e più completa esecuzione alla legge sui dati personali. Si possono designare anche più responsabili, che dovranno eventualmente agire in base a compiti predefiniti e permettere una più efficace attivazione interna o esterna per qualunque tipo di riferimento in merito a quel dato.

Quindi le operazioni di trattamento possono essere effettuate da incaricati che operino sotto la diretta autorità del Titolare o del Responsabile e attendendosi alle istruzioni impartite. Si crea quindi gerarchicamente una scala di osservanza della legge che consenta di rispettare pienamente i principi alla base del testo unico.

Le figure responsabili devono avere la visibilità adeguata sullo stato di sicurezza dell'azienda o dell'organizzazione nella quale operano, in modo che le soluzioni adottate siano intraprese con piene visibilità della struttura e delle funzioni aziendali. Le informazioni raccolte dai responsabili e incaricati del trattamento sono necessarie per permettere di avere un'efficace strategia e azioni opportune in tema di trattamento dati, oltre a consentire la presentazione adeguata degli eventi relativi a eventuali attacchi con la produzione della reportistica necessaria.

Per cui, i requisiti di base evidenziati nell'adeguamento al testo unico relativi alla protezione dell'integrità dei dati, al controllo degli accessi, alle risorse del sistema informativo e alle modalità di utilizzo dei dati, sono soddisfatti con sistemi di sicurezza caratterizzati dalla visione globale dei possibili attacchi all'intero sistema informativo, con particolare attenzione per quelli che potrebbero avvenire sfruttando vulnerabilità non note.

Di fatto il trattamento dei dati con strumenti elettronici viene consentito solo se sono adottate misure di base: l'autenticazione informatica e l'adozione di procedure di gestione dell'autenticazione stessa. Ciò richiede che le credenziali dell'autenticazione vengano adottate tramite procedure di gestione per evitare che l'autenticazione possa essere eseguita da soggetti che non hanno l'incarico o la responsabilità per farla. Un'attività così strutturata di autenticazione informatica, autorizzazione al trattamento dei dati, sicurezza, ripristino dei dati ecc... richiede pertanto un impegno tecnologico e un know how specifico.

Inoltre sarà necessaria l'adozione di tecniche di cifratura codici identificativi per eventuali trattamenti dei dati sensibili in modo che proteggano i dati dall'accesso dai non autorizzati sia interni che esterni all'azienda o al titolare stesso. Infine, in merito allo spamming, il testo unico, con riferimento alle comunicazioni elettroniche indesiderate, dispone che l'uso di sistemi automatizzati di chiamata debba essere anche esso regolato, cioè possibile soltanto previo consenso dell'interessato.

UK National Hi-Tech Crime Unit (NHTCU)
L'inglese National Hi-Tech Crime Unit (NHTCU), fondato nel 2001, è una delle unità più efficienti nel suo genere in Europa. Len Hynds, Capo dell'NHTCU, afferma: "Il successo della sua attività pionieristica è stato tale che ora viene esaminato e accolto dall'Europol e dall'Interpol come modello di best practice da seguire[6]".
Le principali attività dell'NHTCU sono focalizzate su hacker e autori di virus, estorsioni correlate a attività di hacking, spoofing, DDoS, crimini on line legati al mondo della droga e frodi nelle aste on line. Nel 2003 un'analisi ha riportato che gli attacchi di virus erano la forma principale di crimine informatico, con un danno stimato del valore di 27,8 milioni di Sterline.
Altri attacchi hanno riguardato meno del 20% degli intervistati.

5 - Fonte: articolo tratto da una intervista rilasciata da Len Hynds, fornito da Felicity Bull, Corporate Communications Manager, NHCTU (07-09-2004)

OLANDA Korps landelijke politiediensten (KLPD)
La lotta contro il crimine informatico in Olanda è attualmente suddivisa tra il KLPD e sette squadre regionali, ma si prevede di creare un centro nazionale. Come risultato, gli Olandesi non sono in una posizione solida rispetto ad altri paesi per combattere il crimine organizzato. Nel 2002 il governo Olandese fondò il Computer Emergency Response Team, "GOVCERT.NL," per supportare il mondo industriale e i consumatori. Nel 2003 venne creato il Waarschuwingsdienst per supportare in particolare le piccole e medie aziende. È focalizzato su come le aziende possono proteggere i loro computer contro attacchi tecnici e ha prodotto un manuale sul crimine informatico di facile lettura. Fino ad oggi in Olanda la focalizzazione è stata su tecniche specifiche di cybercrime quali spam, virus, dialer e spyware.

GERMANIA - Bundeskriminalamt (BKA)
La Germania ha diverse organizzazioni, una specializzata nel crimine organizzato, l'altra nei crimini correlati all'informatica e alle telecomunicazioni. Il ZaRD (Zentrale anlassunabhängige Recherche in Datennetzen) venne creato nel 1999 come agenzia specializzata per controllare l'attività su Internet, piuttosto che investigare su incidenti specifici. Fa parte del BKA. La pornografia minorile rappresenta la maggioranza delle attività illegali di cui si occupa lo ZaRD. Solo una piccola percentuale dei casi segnalati sono tentativi diretti di hacking o correlati a virus, Trojan horse e spyware. Comunque, gli specialisti del BKA affermano: "Riteniamo esista un enorme numero di casi sconosciuti per queste minacce, perché le aziende non sempre segnalano questi attacchi alla polizia. La maggior parte degli attacchi rivendicati dagli hacker non sono stati segnalati dalle vittime[7]".
Ancora, la principale area di attività per il BKA è la pornografia minorile, su base nazionale e internazionale, oltre a pirateria on line di musica e film. Purtroppo, in termini di utilizzo di Internet da parte del crimine organizzato, sia il BKA che lo ZaRD non hanno controllo su cosa sta accadendo o è in fase di sviluppo. Sembrano essere lenti a reagire alle nuove minacce e vengono a patti solo con forme di cybercrime di vecchia data. Uno dei motivi è la confusione su chi è responsabile di sorvegliare il crimine quando riguarda sia il mondo reale che il cyberspazio.

7 - Intervista telefonica con Herr Köhner del BKA

FRANCIA - Office Central de Lutte Contre la Criminalité Liée aux Technologies de l'Information et de la Communicationì (OCLCTIC)
L'OCLCTIC è stato creato nel 2000 dal Ministero degli Interni Francese.
È focalizzato sui fenomeni di hacking, truffe, in particolare frodi di carte di credito nell'e-business, e contraffazione del software. Coopera con l'"Institut de Recherche Criminelle de la Gendarmerie" (IRCGN, Istituto per la Ricerca Criminale della Polizia Nazionale). Entrambe le istituzioni riceveranno ulteriori fondi e personale nei prossimi tre anni. "Il nostro scopo è dimostrare che il cyberspazio non è una zona senza legge," afferma un portavoce. "Dal momento che dobbiamo proteggere lo spazio terrestre, marittimo e aereo, ora esiste un quarto spazio - lo spazio dell'informazione - che non può eludere la legge[8]"

8 - Tratto da una intervista con Christophe Guillermin per ZDNet France, disponibile on line sul sito http://www.zdnet.fr (08-09-2004)

L'attività principale è focalizzata sulla pedofilia, l'anti-semitismo e i crimini razziali, terrorismo e pirateria del software. In una recente azione repressiva contro la pirateria software, cinque Internet service provider hanno firmato un accordo con il governo Francese impegnandosi a chiudere o sospendere gli abbonamenti di coloro che scaricano software illegalmente.
Lo scambio di software illegale, musica e video su reti peer-to-peer (P2P), rappresenta un grande problema in Francia. In Gennaio, il Ministro Francese per l'Industria, Nicole Fontaine, ha lanciato la campagna "Danger: Counterfeit". François d'Aubert, presidente del Comité National Anti-Contrefaçon (Cnac, Comitato Nazionale Contro la Contraffazione) ha affermato: "Il P2P è una minaccia in particolare per l'equilibrio finanziario della produzione cinematografica[9]".
Il Cnac è anche preoccupato dai beni contraffatti venduti su Internet, in particolare medicinali. "Questi prodotti possono essere pericolosi perché non hanno una certificazione in linea con gli standard Europei," ha affermato d'Aubert.

9 - Tratto da una intervista con Christophe Guillermin per ZDNet France, disponibile on line sul sito http://www.zdnet.fr (08-09-2004)

ITALIA - Gruppo Anticrimine Tecnologico - GAT
Il GAT è stato creato in Italia nel Luglio 2000 e ha avviato le operazioni nel 2001. Fa parte della Guardia di Finanza e opera a stretto contatto con altri gruppi specializzati della forza di polizia generale, quali l'Unità Centrale di Sicurezza della Polizia e il Gruppo Investigativo Speciale dei Carabinieri.
Altre aree di attività includono la pirateria del software e attività di stampo politico. Anche gli attacchi a server di organizzazioni pubbliche sono sotto stretta osservazione degli specialisti del GAT. In Marzo, l'Italia ha introdotto una nuova legislazione contro la distribuzione illegale di materiale audiovisivo su Internet. In Novembre, la polizia ha perquisito varie abitazioni in tre città principali in un'azione repressiva contro la pirateria musicale e cinematografica. A un congresso sulla pirateria in Internet tenutosi recentemente, Umberto Rapetto, Direttore del GAT, ha affermato: "La gente deve essere educata - non solo i più giovani ma anche coloro che lavorano a contatto con i giovani: educatori, insegnanti, genitori spesso ignorano l'avanzato livello di conoscenza di Internet dei ragazzi[10]"

10 - Tratto da una intervista rilasciata a Network World Italia, http://www.nwi.it (03-08-2004)

SPAGNA - Grupo de Delitos Telemáticos (GDT)
Il Gruppo Delitos informáticos (Crimini informatici) della Guardia Civile opera sin dal 1996. Nel 2003 è stato oggetto di riorganizzazione e ampliamento e, attualmente, si chiama Grupo de Delitos Telemáticos (GDT, Gruppo Crimini Telematici). Il suo impegno principale è la ricerca dei crimini informatici, per la cui conduzione si avvale di personale altamente qualificato.
Juan Salom, Responsabile del GDT, commenta: "È difficile quantificare i cibercrimini commessi ogni anno ed in materia esistono pochi studi affidabili.
Probabilmente, viene denunciato solo il 20% di questi crimini, in quanto le vittime non sono consapevoli della loro condizione di vittime o temono ripercussioni per la loro immagine istituzionale" e prosegue:
"Secondo la Guardia Civile, ogni anno il numero di crimini di hacking, frode e pornografia infantile raddoppia[11]".
IL GDT si occupa dei crimini informatici più importanti come la frode, la pornografia infantile, i virus, l'hacking e la pirateria del software. "Questi sono i crimini da noi perseguiti, anche se ne esistono molti altri tipi che, per essere perpetrati, si avvalgono delle nuove tecnologie e di Internet," spiega Salom.[12]

11 - Tratto da una intervista rilasciata a Agencia EFE disponibile on line sul sito http://abc.mynewsonline.com (25-07-2004)

12 - Tratto da una intervista rilasciata a Agencia EFE disponibile on line sul sito http://abc.mynewsonline.com (25-07-2004)

L'ABC della sicurezza on line

Ecco alcuni suggerimenti di base per proteggersi dagli attacchi di hacker e virus.

- **Non aprire mai allegati di posta di mittenti sconosciuti, e accertarsi, laddove sia possibile, di aprire file in arrivo da indirizzi di posta "amici". Ci sono virus, infatti, che si auto-trasmettono via e-mail ai destinatari presenti nella rubrica di posta. In generale, un file in allegato avente estensione .exe è sempre dannoso.**
- **Sarebbe meglio evitare di aprire l'e-mail stessa (e non solo l'allegato) se proviene da un mittente sconosciuto. Molti programmi per la gestione della posta, inoltre, permettono di impostare la modalità di visualizzazione dei messaggi in arrivo; evitando l'anteprima delle e-mail ricevute, il livello di sicurezza aumenta.**
- **Prima di scaricare file da Internet, assicurarsi che la fonte sia legittima e rispettabile. I siti contenenti materiale illecito e pornografico spesso installano automaticamente, sul computer del visitatore, programmi per attività illegali.**
- **È bene rinunciare alla curiosità e cancellare messaggi tipo catena di Sant'Antonio, richieste di aiuto economico e posta spam in genere. Oltre alla possibilità di attivare un virus, l'inoltro di questi messaggi è considerato attività di spamming ed è perseguibile legalmente.**
- **È fondamentale dotarsi di un programma di sicurezza, o anti-virus, che deve essere sottoposto a costante aggiornamento. Esistono oltre 80.000 virus conosciuti e ogni mese ne appaiono 500 nuovi. Sono presenti in commercio numerosi software e servizi anti-virus che aggiornano regolarmente le informazioni sui virus e il motore di scansione.**
- **Il principale danno dei virus è la distruzione dei file. Fare regolarmente il back-up dei file e mantenere la copia di back-up in un luogo diverso da quello dei file utilizzati, preferibilmente non sull'hard disk del Pc.**
- **Accertarsi che il sistema operativo del proprio computer sia aggiornato visitando regolarmente il sito web del produttore (per esempio Microsoft)**
- **L'immissione dei dati della carta di credito o di altri dati personali deve avvenire solo nei siti la cui sicurezza è certificata.**