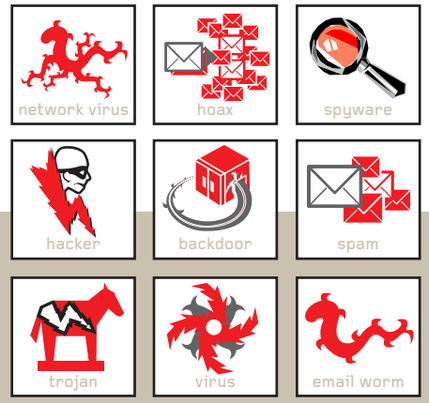
TREND MICRO ITALY - Via Donat Cattin, 5
20063 Cernusco sul Naviglio (Mi)
Tel. +39 02 925931 - Fax +39 02 92593401
www.trendmicro-europe.com



La nostra visione:

Creare un mondo sicuro
per lo scambio di informazioni digitali

La nostra missione:

Assicurare la continuità operativa
contro le minacce imprevedibili

La nostra strategia:

Fornire aggiornamenti tempestivi
per la gestione delle minacce,
tramite l'integrazione
con il flusso di informazioni in rete

sicurezza

Una guida alla sicurezza

per le imprese

Una guida alla sicurezza
per le imprese in crescita

INDICE

INTRODUZIONE

Perché la sicurezza informatica è necessaria?

La sicurezza informatica non è mai stata così importante come oggi.

La maggior parte delle imprese fa un tale affidamento sulla tecnologia informatica (information technology –IT) che potrebbe a stento rinunciarvi nel proprio lavoro. Ma con la crescita dell'uso di internet e della posta elettronica, aumenta anche la minaccia esterna, rappresentata dai virus e dagli hacker, per non parlare dei danni arrecati, per errore o per dolo, dal personale interno.

Tuttavia, mentre secondo il vecchio adagio il 90% dei problemi di sicurezza erano causati da personale interno all'impresa, il cambiamento nel modo di condurre gli affari ha mutato la natura dei rischi.

In risposta a queste crescenti minacce, la Trend Micro ha promosso una ricerca sulle questioni fondamentali di sicurezza che le piccole e medie imprese devono affrontare. La ricerca della Trend Micro, condotta in Europa e negli USA, ha avuto come oggetto le aziende con meno di 500 dipendenti. Il risultato del sondaggio ha mostrato che se il 77,5% del campione adotta procedure di sicurezza, il 56% è stato vittima nell'ultimo anno di un attacco da virus.

Secondo un rapporto del Department of Trade and Industry (DTI) e di PricewaterhouseCoopers (PwC) del 2004, anche se solo il 27% delle aziende britanniche, siano esse piccole, medie o grandi, ha subito incidenti gravi, come un crollo improvviso del sistema o la manomissione dei dati, tuttavia, addirittura il 74% del campione è incorso in un qualche episodio di violazione della sicurezza.

Non ha importanza da dove provenga la minaccia, se da dentro o fuori l'azienda, essa costa ogni anno alle imprese britanniche milioni di sterline. Come ha evidenziato lo studio, il 68% delle aziende ha subito almeno una violazione dolosa della sicurezza, mentre il costo per rimettersi in sesto dopo un incidente grave varia dalle 10.000 alle 120.000 sterline, a seconda delle dimensioni dell'impresa. Una cifra non da poco.

Di tutte le minacce alle quali è esposta la vostra impresa, il singolo pericolo più grande è rappresentato dai virus, che sono responsabili del 70% di tutte le infrazioni gravi alla sicurezza e che hanno colpito qualcosa come il 50% delle aziende britanniche.

Oltre ai virus, le imprese sono oggi chiamate ad affrontare il problema dello spayware, il software che spia e può rubare informazioni. Uno studio condotto da Trend

Micro nel luglio 2005, che ha coinvolto 1.200 utenti finali di aziende di ogni dimensione situate in Germania, Stati Uniti e Giappone, ha rilevato numerose particolarità inerenti le percezioni e i comportamenti degli utenti finali sul luogo di lavoro, molte delle quali legate al crescente problema dello spyware. Secondo lo studio, la diffusione dello spyware sta aumentando specialmente nelle aziende di piccole e medie dimensioni. Dalla ricerca si evince come lo spyware sia presente soprattutto negli Stati Uniti, dove il 40% degli utenti interpellati ha affermato di esserne stato colpito sul lavoro contro il 14% del Giappone e il 23% della Germania. In tutti questi tre Paesi gli utenti appartenenti alla PMI hanno subìto un numero di attacchi superiore a quello dei loro colleghi inseriti in aziende più grosse.

Secondo i dati rilasciati a Gennaio 2006 dall'Antiphishing Working Group, il 2005 può essere a pieno titolo considerato l'annus horribilis per il phishing. Nel solo mese di novembre, citano i report, sono stati segnalati 16.882 attacchi singoli, che facevano riferimento a 93 marchi differenti. Una cifra record, che supera il tetto dei 15.820 attacchi di ottobre e che raddoppia la cifra registrata 12 mesi prima.

Altri problemi in aumento sono gli attacchi di Denial of Service e gli attacchi di pirateria individuale contro siti web. Qualsiasi computer collegato a internet viene di regola scansito diverse volte al giorno dai pirati elettronici in cerca di punti deboli da sfruttare per danneggiare il sistema.

Secondo lo studio del DTI/PwC del 2002 (la ricerca è ripetuta ogni due anni), solo un'azienda su venti era stata vittima di un attacco informatico. Nel 2004 lo è stata una su quindici!

Tutto ciò dimostra come il problema si aggravi di anno in anno e non sia chiaramente destinato ad alleviarsi col passare del tempo.

Stiamo prendendo sul serio i problemi di sicurezza?

Nonostante molte imprese considerino le informazioni e i dati aziendali un loro patrimonio inestimabile e sappiano perfettamente di non poter lavorare senza di esse, molte non fanno semplicemente abbastanza per salvaguardare queste preziose risorse e i computer sui quali sono archiviate.

Secondo il rapporto DTI/PwC del 2004, sebbene le spese per la sicurezza dipendano ovviamente dalle singole realtà aziendali, una buona regola approssimativa prescriverebbe di spendere nel settore tra il tre e il cinque per cento del budget dedicato all'IT. Tuttavia il dato preoccupante è che il 18% delle imprese campione non spende nulla, il 35% meno dell'1% del budget dedicato all'informatica e l'11% non ha idea di quanto spenda in sicurezza.

La questione fondamentale è che la sicurezza informatica è concepita dalla gran parte delle imprese britanniche come un costo, piuttosto che come un investimento. Troppe non riescono a capire che in realtà le aiuta a fare soldi, non alzando i profitti o tagliando i costi, ma esentandole da future spese.

Una sicurezza inadeguata costa alle imprese molti soldi sotto forma di spese per il ripristino dei sistemi informatici, perdita di produttività, danni potenziali derivanti dal deterioramento dell'immagine e del marchio aziendale o, il che è più grave, dall'assoluta impossibilità di lavorare.

Cosa possono fare le aziende per proteggersi più efficacemente?
La salvaguardia dagli attacchi informatici richiede una strategia basata su tre fronti – le persone, le procedure, la tecnologia, in quest'ordine. Impiantare un firewall per proteggere la vostra rete aziendale funziona solo fino ad un certo punto e non vi fornirà adeguata tutela contro tutta quella serie di minacce (vedi pp. 5-11) che siamo chiamati ad affrontare sempre più spesso.

Procediamo con ordine – le persone. La vostra impresa è sicura quanto è sicuro il suo anello più debole, e l'anello più debole è spesso un uomo. La maggior parte della gente non vi causerà problemi intenzionalmente, ma se una persona non sa bene quel che deve fare o non è consapevole di svolgere un ruolo fondamentale nel mantenimento della sicurezza può, senza volerlo, causare della falle nel sistema.

Per affrontare questo problema ed assicurarsi che tutti capiscano chiaramente le proprie responsabilità, è essenziale stabile una politica aziendale in materia di sicurezza (vedi pp. 16-19), che esponga, in modo facilmente comprensibile, cosa ci si aspetta da ognuno, così che possa facilmente attenervisi ed essere ritenuto responsabile in caso di mancato adempimento.

Il secondo fattore riguarda le procedure aziendali. Di nuovo, le linee di condotta aziendali hanno un ruolo importante nell'indirizzare il personale IT e gli utenti finali, affinché operino in un modo il più possibile orientato alla sicurezza e sappiano cosa fare nel caso si apra una falla nel sistema.

La terza categoria, invece, riguarda la tecnologia e quei prodotti per la sicurezza (vedi pp. 12-15) che sono necessari per rinforzare le misure messe in atto a livello di personale e di procedure. Le esigenze e le priorità variano da azienda ad azienda, ma, ai giorni nostri, si ritiene comunemente che l'installazione di un firewall, di un software antivirus, uno di antispam ed uno di antispyware siano comunque il minimo indispensabile.

II. DEFINIZIONE DELLE PRINCIPALI MINACCE

Attacchi Denial of Service

Il Denial of Service, o DoS, è un programma che interrompe od ostacola il normale flusso dei dati da e verso il sistema. La maggior parte degli attacchi DoS impegna le risorse di sistema, di modo che, nel giro di poco tempo, il computer bersagliato è reso inutilizzabile. Un'altra forma di attacco DoS consiste nell'invio simultaneo e ripetuto di molte richieste d'accesso ad un sito Web, impedendo così ad altri sistemi di accedere al servizio e di recuperare dati da esso.

Un esempio recente di attacco DoS, che ha avuto larga pubblicità, è avvenuto all'inizio del 2004. Il sito della SCO.com è stato chiuso per un mese dopo essere caduto vittima del worm MyDoom. Questo worm installò un backdoor all'interno di numerosi PC, utilizzandolo per lanciare un attacco ai server della compagnia durato dall'1 al 12 febbraio e protrattosi in seguito per qualche altro giorno, poiché gli orologi interni di molti computer infettati non erano tarati correttamente.

Backdoor

Una backdoor ("porta di servizio") è un programma che apre un accesso segreto al sistema ed è spesso usato per aggirare la sicurezza. Un backdoor non infetta i file del computer ospite, ma quasi tutti i programmi di questo tipo modificano il registro di sistema (registry).

Una backdoor consente a chiunque di vedere, modificare o distruggere i dati e il software del computer ospite, senza bisogno di passare attraverso un'autorizzazione. Una backdoor permette agli individui malintenzionati di prendere il controllo della vostra macchina e di utilizzarla per scaricare informazioni, accedere ai dati personali, o di usarla per distribuire materiale come la pornografia infantile o lo spam senza che sia possibile risalire fino ad essi.

Le backdoor possono essere introdotti sul sistema anche installando inavvertitamente un Trojan Horse dopo aver aperto un allegato di posta elettronica infetto. Un esempio è il worm Bugle, che permette al suo creatore di controllare a distanza il vostro computer.

Bot (net)

Le Botnet sono un insieme di PC connessi ad Internet colpiti da software robots, o bots, che funzionano autonomamente ed in maniera invisibile. Un creatore di

botnets può controllare questi PC remotamente, di solito attraverso comandi tipo IRC, solitamente per scopi criminali o a fini di lucro.

Digital Snooping

Il "ficcanasare digitale" consiste nel monitoraggio del network aziendale per scoprire le password ed altri dati riservati, compiuto generalmente dal personale interno. Il digital snooping può verificarsi anche quando semplici messaggi di testo sono usati incautamente per trasferire informazioni riservate via internet.

Hackers – Cracks/Hacks

Si ha un'azione di hackeraggio quando qualcuno ottiene un accesso non autorizzato al vostro computer. Mentre i crackers sono coloro che entrano in un computer estraneo con intenzioni ostili (ad esempio: per scaricare informazioni, per accedere a dati personali, come il numero di carta di credito, per sfruttare le debolezze del sistema operativo e compilare un worm, un virus o un Trojan Horse che inserisce un backdoor), gli hackers aderiscono ad un codice etico di comportamento e hanno come obiettivo l'individuazione dei problemi relativi alla sicurezza e l'esplorazione delle funzionalità del computer.

Siano cracker o hacker, accedono in ogni caso senza autorizzazione al vostro computer.

A complicare le cose, il termine Black Hat Hacker ("hacker dal cappello nero") è a volte usato per riferirsi ai "cattivi" (i cracker), mentre l'espressione White Hat Hacker ("hacker dal cappello bianco") si applica ai "buoni" (gli hacker veri e propri).

Malware

Il malware – il software "maligno" – è un qualsiasi programma o codice dagli effetti dannosi o indesiderati. Non tutti i programmi e i codici "maligni" sono virus. I virus, però, insieme ai worm (i "bachi" informatici), sono a tutt'oggi la forma più diffusa di malware.

Dato i molti tipi di programmi "maligni" in circolazione, l'espressione collettiva "malware" aiuta a non fare confusione. Ad esempio, un virus con le caratteristiche di un Trojan Horse può essere definito malware.

Social Engineering

Il termine è usato per indicare in generale tutti quei metodi non-tecnici usati da individui malintenzionati per indurre le vittime a consegnare informazioni, aprire messaggi e-mail e file che contengono malware, o comunque a trasgredire le normali procedure di sicurezza.

Un esempio tipico è la tecnica usata dai creatori del virus Netsky. Le vittime ricevono una mail infetta che ha come oggetto un frase opportunamente scelta dagli autori del virus. I titoli variano, ma hanno tutti un'aria innocua, come "Protected Mail Request" o "Mail Authentication". Nel corpo del messaggio sono riportate delle affermazioni, attribuite a sedicenti produttori di software di protezione, secondo cui l'e-mail inviata è sicura e non contiene virus. In questo modo il destinatario, tratto in inganno da tutti questi elementi, viene indotto ad aprire l'allegato infetto.

Pharming

Simile al phishing negli scopi, compromette il sistema o il DNS server dell'utente per deviare il traffico verso un sito pirata. Attraverso le tecniche di "DNS poisoning" o "URL hijacking", anche URL digitati correttamente possono essere dirottati con successo verso siti illegali - spesso un eccellente rifacimento del sito originale - nel tentativo di carpire informazioni personali dalle vittime.

Phishing

Il phishing è il fenomeno di manipolazione sociale per cui la gente è indotta con l'inganno ad inviare dati personali via e-mail.

Un esempio sono quei messaggi di posta elettronica, che, all'apparenza, risultano inviati da istituti bancari di prestigio e che richiedono di fornire informazioni riservate sul proprio conto. Alle vittime viene chiesto, cliccando su un indirizzo internet codificato per apparire del tutto identico a quello della vera banca, di accedere ad un sito web fraudolento progettato per essere simile a quello autentico. I dati personali vengono quindi inseriti direttamente sul sito truffa.

Rootkit

Il nome "rootkit" deriva dal termine "root", in altre parole la figura del "superuser" nei sistemi operativi appartenenti alla famiglia UNIX. Negli anni Ottanta gli hacker erano soliti penetrare all'interno di macchine UNIX per installare un programma che, di fatto, apriva una backdoor al loro interno consentendo di rientrarvi in qualunque momento con tutti i privilegi di "root". Il termine "rootkit" è ora usato in modo similare dai moderni ricercatori anche programmi basati su Windows. Un rootkit potrebbe nascondere la presenza di programmi pericolosi attivi nel sistema così come qualunque elemento del registry modificato per i propri scopi. Ecco perché i rootkit stanno diventando così popolari tra gli autori di malware: come minimo, garantiscono loro un manto d'invisibilità.

Spam

Lo spam è la posta-spazzatura non richiesta, che di solito pubblicizza prodotti o servizi. Alcuni messaggi di spam hanno un contenuto sconveniente e indecoro-

so e/o collegamenti a forme di malware. La cancellazione della posta indesiderata fa sprecare del tempo, oltre ad impegnare le linee della rete, e può anche sovraccaricare i server di posta elettronica provocandone l'arresto.

Spimming

Lo spimming è lo spam inviato tramite gli Instant Messanger (IM), le applicazioni che permettono in tempo reale di mandare e ricevere messaggi da un serie di contatti e-mail selezionati dall'utente. Data la crescente diffusione degli IM, lo spimming ha già da qualche tempo iniziato ad attirare l'attenzione dei media.

Secondo un recente studio della Ferris Research, nel 2007 ci saranno 182 milioni di persone che useranno un IM. Sempre secondo la ricerca, gli spimmers stanno sviluppando tecniche avanzate che permettono di inviare messaggi contemporaneamente a milioni di utenti.

Spoofing

Lo spoofing ("camuffamento") consiste nell'inserirsi in un network fingendo che il computer abbia i privilegi di accesso speciali di un'altra macchina presente nella rete; in questo modo malintenzionati possono accedere a tutti gli altri sistemi del network.

Il termine si usa anche in ambito internet. In questo caso, si parla di spoofing quando il pirata informatico cha ha preso il controllo della vostra macchina attraverso un backdoor, la utilizza per distribuire materiali come la pornografia infantile o lo spam, senza che si possa in alcun modo risalire a lui.

Ciò può evidentemente avere conseguenze disastrose, non solo perché tiene impegnate le risorse del computer e ha un impatto sulla produttività, ma anche perché il vostro indirizzo e-mail potrebbe finire su una lista nera di mittenti indesiderati, il che vi impedirebbe di continuare a spedire messaggi di posta elettronica – a chiunque.

Lo spoofing via e-mail, invece, consiste nel modificare l'intestazione del messaggio in modo da far sembrare che a spedirlo sia stato qualcuno diverso dal vero mittente. Questo tipo di e-mail contiene spesso spam o malware.

Secondo le statistiche della Trend Micro, circa il 60% del malware scoperto nell'aprile 2004 conteneva un backdoor.

Spyware

E' un'applicazione software che registra le abitudini e le informazioni personali

dell'utente e le invia a terze parti senza che l'utente abbia concesso l'autorizzazione o ne sia a conoscenza.

Uno spyware raccoglie segretamente informazioni su di voi e sulle pagine che visitate via internet, a vostra insaputa e sfruttando la vostra connessione. Le informazioni così raccolte vanno dai vostri indirizzi e-mail, alle password, ai numeri di carta di credito e sono di solito usate per scopi pubblicitari.

Lo spyware funziona in modo analogo ad un Trojan Horse nel fatto che l'utente ignora di averlo installato. E' dannoso non solo perché ruba le vostre informazioni personali, ma anche perché impegna la linea quando le rigira al creatore del programma, il tutto tramite la vostra connessione internet. Ciò può provocare instabilità nel sistema o causarne l'arresto, perché impegna la memoria e le risorse del computer.

Trojan

Un Trojan è un malware che esegue operazioni indesiderate e non autorizzate, spesso con intenzioni ostili. La differenza più importante tra un virus e un Trojan è che quest'ultimo non è in grado di replicarsi. I Trojan provocano danni, comportamenti di sistema inattesi e compromettono la sicurezza, ma non si replicano. Se un Trojan si replica, allora è più corretto definirlo un virus.

Un Trojan (il nome deriva dal Cavallo di Troia della mitologia greca) è all'apparenza innocuo, ma nasconde delle insidie all'interno del codice. Quando un Trojan viene eseguito, gli utenti vanno di solito incontro a problemi nell'uso del sistema e talora alla perdita di dati preziosi.

Un esempio famoso di Trojan Horse è Xombe, che colpisce i sistemi operativi Windows XP, 95, 98, ME, NT, 2000 e 2003 Servers. Esteriormente, si presenta come un allegato e-mail contenente un aggiornamento fondamentale per Windows XP, ma, quando viene aperto, scarica un backdoor da internet.

Virus e tipi di virus

Un virus informatico è un programma – un pezzo di codice eseguibile – che ha la caratteristica unica di replicarsi. Come i virus biologici, i virus informatici possono diffondersi velocemente e sono difficili da debellare. Possono attaccarsi a quasi ogni tipo di file e diffondersi quando il file infetto viene copiato e inviato da una persona all'altra.
Oltre alla replicazione, alcuni tipi di virus hanno un'altra caratteristica in comune: una routine dannosa che libera la parte attiva del virus. Può, ad esempio, far semplicemente apparire sul monitor messaggi o immagini, ma potrebbe

anche distruggere file, riformattare l'hard disk o causare altri tipi di danni. Se il virus non ha un routine dannosa, può causare comunque dei problemi, perché occupa spazio sul disco e in memoria e quindi riduce le prestazioni generali del sistema.
Molti anni fa i virus si trasmettevano soprattutto via floppy disk, ma internet ha cambiato il meccanismo di propagazione. Ora che la posta elettronica è diventata uno strumento fondamentale di comunicazione per le imprese, i virus si stanno diffondendo più che mai. I virus allegati ai messaggi e-mail possono infettare un'intera impresa nel giro di pochi minuti e costare alle aziende milioni di dollari ogni anno in termini di produttività persa e di spese di ripristino.
I virus non scompariranno presto: ne sono stati identificati più di 60.000 e ne vengono creati 400 nuovi ogni mese, secondo quanto rilevato dalla International Computer Security Association (ICSA). Di fronte a cifre del genere, si può tranquillamente affermare che la maggior parte delle imprese sarà periodicamente infettata da un virus. Nessun utente di computer è immune dai virus.
I virus possono provocare gravi danni, cancellando file o persino l'intero hard disk o manomettendo i dati. Tuttavia, a differenza dei worms, i "bachi", i virus non si replicano automaticamente e devono venir attivati dagli utenti, il più delle volte aprendo un allegato e-mail infetto.

Ci sono molti diversi tipi di virus, per maggiori informazioni si veda: http://it.trendmicro-europe.com/consumer/security_info/overview.php

Oltre ai soliti, sono in circolazione dei virus di nuovo tipo in grado di provocare danni su vasta scala. Questi virus sfruttano le novità tecnologiche. Due di essi meritano un descrizione più dettagliata in virtù della loro pericolosità: i Blended Threats e Network Virus.

Blended Threats

Questi virus "misti" hanno caratteristiche derivate dai worm, dai virus tradizionali, dai Trojan e da altre forme di malware e utilizzano i server e i punti deboli di internet per espandersi velocemente. Combinando tecnologie e codici diversi, possono causare danni di grandi proporzioni.

Per proteggersi efficacemente contro i Blended Threats è necessario un sistema di sicurezza articolato, basato su livelli multipli di difesa e meccanismi di risposta adeguati.

Network virus

Un virus di rete è un programma (o una serie di programmi) in grado di auto-

duplicarsi, in tutto o in parte, attraverso un network, quale ad esempio internet. La propagazione avviene di solito attraverso le risorse condivise, che possono essere dischi o cartelle, o altri porte e servizi del network. I virus di rete non prendono unicamente la forma di file o allegato e-mail, ma possono anche risiedere unicamente nella memoria del computer (si parla allora di Memory-only Worms). In molti casi i virus di network sfruttano le falle del sistema operativo o di altri programmi installati sul computer. Alcuni virus di rete in circolazione hanno la capacità di diffondersi attraverso porte di rete valide, come le porte 80 (http), 1434 (SQL) o 135 (DCOM RPC).
Una volta che un virus di rete ha infettato il sistema, si mette spesso in cerca di altri obiettivi potenziali e va a caccia dei punti deboli all'interno della rete. Quando ne trova uno, il virus cerca di infettarlo.
Alcuni virus contengono al loro interno delle routine dannose, ad esempio possono lanciare un attacco di Denail of Service. Quando viene portato un attacco del genere, il computer infetto invia continue richieste di accesso al sistema bersaglio, fino al punto di renderlo mal funzionante. Esempio: il virus MSBLAST ha sferrato un attacco DoS contro l'indirizzo internet: www.windowsupdate.com. I più noti virus di network sono quelli della famiglia Sasser, CodeRed, Nimda, SQLSlammer e MSBLAST.

Worm

Un "baco" informatico è un programma (o una serie di programmi) autosufficiente in grado di autoduplicarsi, in tutto o in parte, diffondendosi su altri sistemi. La propagazione avviene di solito attraverso le connessioni del network o tramite gli allegati e-mail.

Un esempio di worm è il Mydoom, che si diffonde all'apertura di allegati e-mail infetti, generalmente file con un'estensione di tipo .zip. Il file ha spesso nomi come message.zip, o readme.zip. Se l'allegato viene aperto, il worm installa un codice nocivo sul computer e invia copie di se stesso a tutti gli indirizzi che trova sulla rubrica del vostro programma di posta. Installa anche un Trojan Horse sulla macchina ospite, consentendo, almeno potenzialmente, ad individui ostili di manipolarla.

III. I PRODOTTI PER LA PROTEZIONE DEI COMPUTER E DEL NETWORK

Filtraggio dei contenuti

Questi prodotti confrontano, basandosi su regole predefinite, i contenuti provenienti da una quantità di fonti diverse, come e-mail, web e ftp. Le regole di filtraggio possono venir stabilite su misura (a seconda delle politiche aziendali) o fissate centralmente (è il caso dei filtri antispam, antipishing, antipharming).

I programmi di filtraggio possono risiedere su un PC, su un server o sul gateaway del network. Generalmente, si ritiene che il gateaway sia la sede migliore per questo tipo di programmi, tuttavia va tenuto presente che in questo caso i contenuti che girano all'interno della rete aziendale, non passando attraverso il gateaway, non vengono sottoposti a filtraggio.

Firewall

I firewall restringono il flusso dei dati in entrata e in uscita del network, proteggendolo in questo modo dall'attacco degli hackers o dei virus. Alcuni tipi di firewall controllano le applicazioni e sono in grado di esaminare il contenuto dei file in traffico e di scoprire il malware.

I firewall di norma risiedono o sul vostro PC o sul gateway del vostro network. Comunque, è possibile installare il firewall su qualsiasi punto del sistema in cui i dati in entrata possono costituire una minaccia. Generalmente, tuttavia, si ritiene che siano più efficienti se installati sul getaway, visto che è questo il punto di accesso alla rete.

Gestione delle identità e degli accessi

I prodotti di questo tipo permettono agli amministratori di sistema e di rete di assegnare e gestire le identità degli utenti, di modo che ogni membro del personale disponga di un diverso livello di accesso ai computer e agli altri sistemi presenti sul network. Questi programmi sono usati anche per gestire le password e per fornire al personale sistemi di autenticazione che permettano di sapere con certezza l'identità di chi cerca di accedere al sistema.

Gestione delle prestazioni della sicurezza.

E' una postazione singola che, a livello centrale, raccoglie tutti i segnali d'allarme provenienti dai vari punti del network in caso di uso improprio o non auto-

rizzato del sistema. Tiene anche un registro cronologico in cui sono elencati tutti i tentativi di violazione del software di protezione, come gli antivirus o gli IDS.

Polizia scientifica informatica

L'indagine di polizia scientifica applicata ai computer è l'insieme degli strumenti e delle tecniche usato per esaminare e analizzare scientificamente i dati custoditi sugli strumenti di archiviazione informatica, di solito gli Hard Disk, così che le informazioni ricavate in seguito all'analisi possano venir utilizzate, se necessario, come elementi di prova in tribunale.

Altre forme di indagine possono avere come oggetto i dati grezzi del network e analizzare se e in che modo il software e gli strumenti di sicurezza sono stati modificati a seguito di errori di configurazione o di bug presenti sul network o a causa di sottrazione dei dati e di infrazioni in materia di linee guida sulla sicurezza.

Sistemi di individuazione delle intrusioni

I software IDS (Intrusion Detection Systems) controllano il comportamento del traffico di rete e lo confrontano con registri di sicurezza e dati di verifica per individuare, identificare e isolare i tentativi da parte di estranei di entrare nel sistema senza autorizzazione.

Software antivirus

E' un software progettato per individuare le varie forme di malware e proteggere da esse la rete. Può risiedere sul PC, sul programma di posta elettronica, su un server gateway e, sempre più spesso, viene installato anche su altri nodi del network, come i router. Tradizionalmente, il posto migliore in cui installare l'antivirus è il gateway, ossia il principale punto d'accesso al network. In futuro, gli antivirus verranno fatti risiedere anche sulle componenti infrastrutturali del network (router, switch...) per fornire un ulteriore livello di protezione alla rete.

Software di codifica cifrata

Questo software fornisce gli strumenti per codificare e decodificare sistematicamente i vostri dati aziendali, così che se qualcuno se ne appropria senza autorizzazione, non sia in grado di decifrarli. Si possono codificare e-mail, dati provenienti da apparecchi mobili, come i telefoni cellulari, e strumenti usati dagli sviluppatori di programmi. Generalmente viene installato o su un server del network o localmente sul computer di un addetto specifico che, a richiesta, può distribuire l'informazione decifrata.

Le applicazioni di Public Key Infrastructure (PKI) sono una forma diffusa di

software di codifica usata nelle transazioni via internet, come l'acquisto di beni tramite carta di credito. Si basano su dei certificati digitali e sulla verifica, fornita da apposite autorità di registrazione, che entrambe le parti sono effettivamente chi dichiarano di essere.

Antispam

E' un programma progettato per individuare e bloccare le mail indesiderate prima che raggiungano l'utente finale. A seconda del produttore del software, possono funzionare sulla base di tecnologie come l'analisi del comportamento e i motori euristici che filtrano le mail spazzatura e riducono il carico sul server di posta, aumentando la produttività dei dipendenti.

Antispyware

Queste applicazioni controllano la memoria, il registro, gli hard disk, i supporti di memoria removibili ed ottici alla ricerca di spyware e lo rimuovono dal computer.

Strumenti di pianificazione della continuità aziendale

Si tratta di programmi informatici concepiti per creare, mantenere e revisionare un piano di Continuità Aziendale. L'obiettivo di tale piano è fare in modo che l'azienda continui a funzionare anche in caso di disastro improvviso, come un incendio e un'alluvione.

Strumenti di valutazione e analisi dei rischi

Questi programmi consentono di determinare quali sono i rischi potenziali cui è esposta la vostra azienda e quali siano i principali punti deboli del sistema di sicurezza in un dato momento. Sulla base di queste informazioni potete quindi farvi un'idea precisa di quali misure di sicurezza sia necessario introdurre, stilando un ordine di priorità in linea con il vostro budget.

Valutazione dei punti deboli e gestione delle configurazioni

Un software di questo tipo crea un inventario di quali server, software di sicurezza e dispositivi di network , come gli switch, avete sul vostro network e li confronta con le ultime versioni in circolazione.

Quindi, formula delle raccomandazioni su quali aggiornamenti sarebbe opportuno apportare alle varie configurazioni e, in alcuni casi, li effettua automaticamente. I software di questo tipo gestiscono anche le patch, gli aggiornamenti periodici che rimediano ai bug scoperti col tempo all'interno del software. In questo modo potete essere certi che le nuove patch, man mano che si rendono disponibili le versioni più recenti, vengano installate su tutti i sistemi della rete.

I software di gestione della configurazione di solito forniscono un livello di auto-

mazione superiore alle applicazioni di valutazione delle dei punti deboli e vi permettono di programmare nel tempo i cambiamenti con maggiore precisione. Generalmente includono anche un repository ("deposito") in cui sono archiviati i parametri di tutte le configurazione ottimali.

Inoltre, il software di gestione della configurazione permette di generare dei rapporti e aiuta gli sviluppatori a controllare la versione del programma cui stanno lavorando, in modo da avere a disposizione un registro di tutte le modifiche apportate.

Virtual Private Network

Un VPN è un network costruito usando connessioni pubbliche per collegare due nodi – solitamente via internet. Il software VPN usa un sistema di codici cifrati e di autenticazione per essere certo che solo gli utenti autorizzati possano accedere ai nodi e che i dati non possano venir letti se intercettati. I VPN sono usati in genere dagli uffici decentrati o dal personale che lavora da casa.

UTM (Amministrazione Unificata delle Minacce)

Gli appliance "Unified Threat Management", sono dei dispositivi che consolidano molteplici caratteristiche di sicurezza in una singola piattaforma hardware. Solitamente questi dispositivi sono in grado di controllare codici maligni e contenuti Internet, il contenuto delle mail e lo spam, la navigazione internet, dispongono di un firewall, di un sistema di Intrusion Protection / Prevention, una VPN e sono adatti alle PMI.

IV. GUIDA INTRODUTTIVA ALLA CREAZIONE DI UNA POLITICA AZIENDALE SULLA SICUREZZA

Perché è importante fissare una politica aziendale sulla sicurezza?

Fissare per iscritto delle linee di condotta valide per tutti è la chiave di volta dell'intero sistema di sicurezza della vostra azienda perché getta le fondamenta sulle quali costruire tutto il resto. "Tutto il resto" sono le procedure di verifica sullo stato della sicurezza e di intervento in caso di violazione e le tecnologie messe in campo per proteggere l'infrastruttura IT dagli attacchi.

Si tratta in pratica di un piano d'azione, che stabilisce quali sono le risorse informative decisive per l'impresa e come debbano essere protette. Risorse di questo tipo sono i computer, il network e tutte le informazioni aziendali.

L'obiettivo è fissare regole e procedure che si applichino a chiunque voglia accedere alle vostre risorse informative, sia esso un membro del personale, del management o una parte terza autorizzata. In questo modo potete essere certi che le risorse mantengano la loro integrità, rimangano confidenziali e siano disponibili quando ce ne è bisogno.

Le linee di condotta in materia di sicurezza dovrebbero quindi stabilire precisamente gli ambiti di responsabilità del personale e del management, concedendo contestualmente ai tecnici IT l'autorizzazione a svolgere il loro lavoro. E' anche opportuno fissare le procedure da attuare in caso di attacchi alla sicurezza. In ogni caso, il linguaggio deve evitare il gergo tecnico, così che tutti possano capire le regole e, quindi, seguirle.

Come approntare una politica aziendale di sicurezza

Il primo passo è intraprendere un progetto di Analisi dei Rischi, il che significa farsi un quadro preciso di come funziona il vostro business, se non lo sapete già.

Ma un progetto di analisi dei rischi definisce anche quali sono le risorse informative dell'azienda nel suo complesso, cosa fanno, quanto sono importanti (in modo da poter stabilire una scala delle priorità in materia di sicurezza) e a quali rischi possano essere soggette.

Sebbene ci siano dei software che vi aiutano ad analizzare la vostra situazione, bisogna tener presente che ci sono anche altre fonti di rischio, come il manca-

to aggiornamento periodico delle patch di sicurezza del sistema operativo o l'utilizzo da parte del personale di programmi insicuri, come gli Instant Messanger, per chattare con colleghi o amici.

In poche parole, il fine ultimo è capire che cosa volete proteggere, da chi state cercando di proteggerlo e come intendete farlo. Per quest'ultimo aspetto, può essere utile intraprendere un analisi del divario (gap analysis) che vi fornirà un quadro dei punti deboli delle procedure di sicurezza e di come farvi fronte installando nuovi prodotti.

Dopo aver svolto questo lavoro preparatorio, il passo successivo è stendere per iscritto una dichiarazione d'intenti sulla sicurezza informatica che trasmetta ai lettori il senso di quelli che sono gli obiettivi della politica aziendale in quest'ambito. E' importante anche render chiaro che la sicurezza è una responsabilità di tutti, e non il compito di un paio di tecnici.

La dichiarazione dovrebbe, se possibile, fare da paragrafo introduttivo ad un documento più articolato che deve essere facilmente disponibile a tutti i membri dell'azienda, o in forma cartacea o come file di testo elettronico, reperibile via intranet o network.

La seconda parte di questo documento deve individuare i ruoli e le responsabilità di tutti coloro che hanno accesso alle risorse informative. L'obiettivo è in questo caso ridurre il rischio di potenziali infrazioni alla sicurezza dovute ad errore umano e assicurarsi che il personale e il management non finiscano per violare le prescrizioni legislative come quelle regolate dalla legge 675/96 in materia di tutela dei dati personali.

Di conseguenza, il documento dovrebbe includere delle linee guida che stabiliscano, ad esempio, in che termini è consentito usare internet o la posta elettronica, quali sono le procedure per ottenere l'accesso al network, quali sono le restrizioni all'installazione di nuovo software o di nuovo hardware. E' importante anche fissare delle regole su come scegliere e usare le password, che costituiscono spesso l'anello più debole nella catena della sicurezza.

Un'altra sezione del documento, invece, dovrebbe dare indicazioni su come la politica aziendale di sicurezza sarà fatta valere e su come le infrazioni e i comportamenti negligenti saranno sanzionati.

La responsabilità principale nel mettere in atto e nel far valere le linee guida spetta in linea di massima a coloro che si occupano di IT o di sicurezza all'in-

terno dell'azienda. Ad essi dovrebbe essere demandata anche la responsabilità di approvare o meno le richieste, comunque motivate, di esenzione dalle norme di sicurezza fissate nel documento. Anche le procedure per ottenere il nulla osta dovrebbero venir delineate nel documento.

Un'altra sezione del documento dovrebbe regolamentare l'uso dei dispositivi fisici del network, come i PC e gli switch, e stabilire degli standard e delle procedure su come renderli il più sicuri possibile.

Ciò significa anche verificare che i parametri di configurazione di default forniti dal produttore hardware vengano cambiati, perché sono i più facili da violare. La configurazione dovrebbe essere fatta in linea con le esigenze dell'azienda e i servizi non necessari disabilitati o rimossi dal sistema.

Da ultimo, un piano di "back-up e recupero" o di continuità aziendale è fondamentale affinché l'impresa continui a funzionare in caso di catastrofe. Per lo meno, i nastri di back-up dovrebbero venir archiviati fuori dal sistema di modo che se esso va in crash, viene violato da un pirata o alcuni dei file in esso contenuti vengono rimossi per sbaglio, si possa accedere rapidamente alle copie e ripristinarlo.

Anche se sarebbe meglio delineare le norme aziendali sul "back-up e recupero" in un documento apposito, se ne dovrebbe far menzione anche in quello che fissa le linee guida sulla sicurezza.

Come esser certi che la politica aziendale sulla sicurezza funzioni

Dopo aver steso il documento sulla sicurezza, il passo successivo è metterlo in pratica, il che è spesso il compito più difficile.

Ciò significa innanzitutto assicurarsi che tutti abbiano accesso al documento e contestualmente vuol dire anche impiegare tempo e risorse nell'educazione e nell'addestramento del personale, affinché capisca cosa stabilisce il documento e ognuno sia reso consapevole del suo ruolo fondamentale nel mantenimento complessivo della sicurezza.

La tecnologia viene in aiuto all'applicazione delle politiche di sicurezza grazie ai sistemi di "Policy Enforcement", una componente applicativa che verifica i diritti di autorizzazione o la sicurezza minima prima di accordare l'accesso a risorse protette, in particolare dai cosiddetti endpoint. Per esempio, un'application server deve verificare che un utente presenti credenziali di autorizzazione sufficienti ad accedere una data pagina web, modificare un record di

database, oppure i dispositivi di rete devono permettere l'accesso ad un PC solo se ha l'antivirus aggiornato all'ultima versione disponibile.

Un ultima cosa da tenere ben presente è che il documento sulla sicurezza è qualcosa di vivo, che cresce e cambia insieme all'azienda.

Deve essere perciò flessibile e adattabile, e non scolpito una volta per tutte nella pietra, e tenere in dovuto conto i cambiamenti apportati da nuove tecnologie e da nuovi processi. Questo significa che il documento non dovrebbe venir archiviato a prender polvere in un cassetto, ma che deve venir rivisto periodicamente per assicurarsi che sia conforme alle vostre esigenze.

Un punto che vale la pena ricordare è che una politica aziendale di sicurezza ha sempre due scopi. Uno è mantenere la sicurezza. L'altro è assicurare la fruibilità. Temperando queste due esigenze, l'impresa sarà produttiva, efficiente e protetta.

V. COME ALLESTIRE E GESTIRE UNA STRUTTURA DI NETWORK SICURA

I problemi in gioco

Il problema principale è che la sicurezza è un bersaglio in continuo movimento. La Trend Micro ha analizzato più di 2.200 nuove forme di malware nel solo gennaio 2005 e, inoltre, ogni mese vengono scoperti nuovi exploit (bug o difetti di configurazione), nuovi bug nel software e si registra un'enorme crescita della spam, che, oltre ad essere irritante, costa soldi alle imprese.

Ogni azienda è poi diversa e ha le sue esigenze peculiari, le sue procedure e i suoi sistemi informatici. La varietà delle priorità e dei problemi implica che ogni impresa deve configurare il suo network in maniera leggermente diversa dalle altre.

Da dove cominciare?

La prima cosa da fare è fissare delle linee guida sulla sicurezza (si veda sopra) che definiscano quali sono le risorse informative principali dell'azienda e come difenderle. Dopo aver delineato processi e procedure per la gestione della sicurezza su base quotidiana e per la difesa da potenziali violazioni, il passo successivo è valutare quali strumenti tecnologici siano necessari per proteggere il network e l'infrastruttura IT.

Il modo migliore per procedere in questo senso è individuare i rischi più importanti a cui può essere esposta l'azienda, esaminare le falle che espongono il sistema agli attacchi, e stabilire quali prodotti possano "tapparle" al meglio. Insieme alle linee guida, tutto questo aiuta a definire un'impostazione complessiva della sicurezza aziendale, che sarà la base a partire dalla quale acquistare le tecnologie necessarie.

La maggior parte degli esperti sono d'accordo nel ritenere che un firewall è un buon punto di partenza, un livello base di protezione dai tentativi dolosi di penetrare nel vostro network. Un software antivirus/antispyware e uno antispam o un programma di filtro dei contenuti vanno anch'essi installati, perché salvaguardano il PC dai danni provocati dai virus e fanno in modo che la produttività non subisca un calo a causa dello spam.

Un livello di protezione ulteriore è fornito dai sistemi di IDS, che cercano di prevenire attivamente le intrusioni di esterni nel network, e dai sistemi di VPN, che

fanno in modo che gli utenti a distanza possano accedere in tutta sicurezza alla rete aziendale.

I software gestionali sono molto utili per aiutarvi a sfruttare al meglio le strutture di sicurezza presenti sul network. Si crede a volte che questo tipo di software sia costoso, e perciò non viene usato dalle PMI. In realtà, ci sono molti software di gestione ottimi e a un costo ragionevole. E' una buona idea dare un'occhiata ai pacchetti integrati di software gestionale disponibili presso il vostro rivenditore.

La cosa migliore che possiate fare per orientarvi nell'acquisto è valutare i vari prodotti e compilare una prima selezione, in base alle prestazioni, ai requisiti richiesti, alla facilità d'uso, alla disponibilità di un servizio di assistenza tecnica in loco e ai costi.

E' buona norma indirizzarsi verso prodotti di facile installazione, progettati per essere subito pronti all'uso. I prodotti per la sicurezza progettati apposta per soddisfare i bisogni delle PMI.

Come esser certi che il vostro network sia sempre sicuro

Una volta che avete installato i prodotti di vostra scelta, una delle cose più importanti è ricordarsi di non abbandonarli lì come sono. E' di vitale importanza che siano sempre aggiornati e questo vale per ogni aspetto della politica aziendale di sicurezza.

I prodotti per la sicurezza contengono spesso una funzione di aggiornamento automatico. Assicuratevi che questa opzione sia sempre attivata, quando è possibile, visto che in questo modo risparmierete tempo e fatica.

Contemporaneamente, è importante accertarsi che il personale e il management capiscano le linee guida sulla sicurezza informatica e le mettano in pratica effettivamente. Non serve a niente stilare un documento se poi finisce dimenticato in una cassetto o su un computer. Una politica aziendale di sicurezza deve essere fatta valere attivamente.

A questo proposito, è necessario che il piano di sicurezza sia rivisto periodicamente ed eventualmente verificato da esterni, per monitorarne costantemente l'efficacia.

Per una valutazione tecnica esterna può essere utile rivolgersi ad un rivenditore locale qualificato che possa darvi consigli ulteriori sui test di penetrabilità e

di vulnerabilità e possa formulare raccomandazioni precise in seguito ad un analisi completa dei test svolti.

VI. DOVE VA LA SICUREZZA INFORMATICA DEL FUTURO?

Le minacce alla sicurezza cambiano in continuazione. Mentre le tecnologie di sicurezza si fanno sempre più sofisticate, crescono anche i modi di aggirarle. I vari Script Kiddies, Crackers e Black Hat Hackers si divertono un mondo a far vedere a tutti quanto sono bravi a creare problemi.

I virus di rete, ad esempio, usano sempre più strumenti di attacco che aggirano i normali antivirus propagandosi all'interno della memoria del computer. Questi virus, come i worms e il malware che circolano e si diffondono via internet, possono avere effetti devastanti. Un esempio di virus di network è Sasser, che ha colpito gli utenti nel maggio 2004.

Per quanto riguarda worms come Nimda, Code Red, WORM_SLAMMER e WORM_MSBLAST o WORM_SASSER, si propagano senza bisogno di vettori come la posta elettronica, il web o i file condivisi. Chiunque sia connesso ad internet con un sistema operativo senza patch è un possibile bersaglio del worm SASSER.

L'attuale tendenza dei worm sembra orientarsi verso i Bot. I Bot – programmi che operano come un agente a favore di un utente o un altro programma – sono perlopiù visti come malware e tengono sotto attacco un numero sorprendentemente alto utenti insospettabili.
Al giorno d'oggi tutti i worm bot sono costruiti in modo modulare. Questo significa che chi crea il programma può scegliere tra un numero differente di metodi d'attacco, incluso lo sfruttamento delle vulnerabilità, gli invii massicci di posta elettronica, la propagazione punto-punto come anche tutti i parametri per ogni modalità. Il risultato è un worm ad hoc, specificatamente progettato per raggiungere i propri obiettivi: rubare le informazioni e tenere sotto controllo i computer infetti.

Dobbiamo accettare il fatto che le tradizionali soluzioni antivirus da sole non possono fronteggiare queste nuove minacce, che fanno ricorso a sistemi di propagazione diversi – alcuni dei quali non richiedono alcun tipo di intervento da parte dell'utente. Le aziende sono chiamate ad elaborare "soluzioni di sicurezza olistiche" per combattere le minacce odierne.

La Trend Micro ha scoperto che il 60% del nuovo malware scoperto nell'aprile

2004 era costituito da backdoor – il che segna una inversione di tendenza decisiva nel panorama dei virus.

La crescita di backdoor mostra chiaramente che i compilatori di virus hanno alzato il tiro. Fino ad oggi, la maggior parte dei programmatori di virus scriveva i suoi codici con l'intento di attirare l'attenzione dei media, quasi una sorta di "gioco". Tuttavia, nel complesso, il numero di codici veramente nocivi, che potevano arrecare realmente gravi danni al sistema, era molto basso. Ora, il rilascio di così tanti backdoor ha cambiato il volto del mondo del malware.

Con la crescita dell'uso di connessioni xDSL (come la banda larga), i computer sono diventati l'obiettivo privilegiato degli hackers, dei programmatori di virus, degli spammer e di ogni altro tipo di pirata informatico. Consci di questa tendenza, i pirati hanno persino iniziato a creare proprie associazioni. I backdoor possono venir usati per ricavare informazioni dai sistemi infetti, permettendo ai pirati di avere un quadro dettagliato dello stato di propagazione dell'infezione. In questo modo riescono anche ad ottenere le password, che possono usare per accedere alla rete aziendale.

Se un vostro computer così infettato venisse utilizzato per diffondere spam all'insaputa dell'utente, sarebbe un disastro, non solo perché in questo modo si impegnano le risorse del computer, il che ha un impatto sulla produttività, ma anche perché il vostro relay ISP potrebbe finire sulla lista nera di qualche server di posta elettronica o l'intera azienda potrebbe venir inserita sulla Realtime BlackHole List (RBL), e, a quel punto, i destinatari delle vostre mail potrebbero rifiutarle, anche se sono innocue.

Ma il fatto che desta più allarme è che i computer colpiti potrebbero venir usati per lanciare ulteriori attacchi, dando così vita ad un "network maligno" formato da sistemi infettati. In questo modo, il pirata può nascondersi dietro uno o più computer, facendo sembrare che l'attacco provenga da un utente, che, in realtà, non ha alcun collegamento con il pirata stesso. Ciò potrebbe dare adito a una quantità di controversie legali – è l'utente colpevole di essersi infettato o no?...

Per fortuna, gli sviluppatori di software per la sicurezza delle reti sono perfettamente consapevoli della natura dinamica dei virus informatici e hanno rapidamente adeguato la loro offerta di prodotti per far fronte alla crescente complessità dei codici maligni.

Alcuni dei più recenti strumenti di protezione fanno scattare dei meccanismi che prevengono lo scoppio dell'infezione, scoprono e bloccano i virus all'inter-

no del flusso di dati del network e assistono l'amministratore di sistema nel monitoraggio dell'attività di rete usando l'analisi euristica. Questa si basa su dei filtri che passano al vaglio grandi volumi di posta o di dati e identificano le caratteristiche distintive dei messaggi pericolosi. I risultati così raccolti sono quindi usati per costruire delle regole generali per motori euristici, che, grazie a ulteriori filtri, stabiliscono se un dato in entrata o in uscita è nocivo o meno.

Ne consegue che il filtraggio degli allegati e-mail e il software antivirus che scansisce il gateaway rimarranno fondamentali per eliminare i file infetti che passano attraverso il network aziendale. Altrettanto importante è forse il fatto che i programmi di nuova concezione sono in grado di riconoscere i diversi tipi di file e di archivi compressi che sono stati usati frequentemente per aggirare il software convenzionale di filtraggio degli allegati. Analogamente, i software di gestione che garantiscono un maggiore controllo e standard di sicurezza più elevati saranno sempre più importanti, come anche i servizi operanti a livello centrale per il controllo dei contenuti, che molti rivenditori ora offrono.

VII. GLOSSARIO DEI TERMINI TECNICI

Amministratore di rete
Persona che gestisce il network assicurandosi che tutto proceda nel migliore dei modi

Amministratore di Sistema
Persona che gestisce il modo in cui vengono usati i vari sistemi sul network. Spetta a lei assegnare i diritti d'accesso ai diversi utenti e assicurarsi che i sistemi funzionino correttamente.

Applicazione
Un software acquistato da un rivenditore o costruito su misura dagli sviluppatori di applicazioni o da un programmatore. Si basa sul sistema operativo ed è utilizzato dagli utenti finali per svolgere specifici compiti.

Applicazioni tipiche sono i word processor, come Microsoft Word per la scrittura di documenti, e i fogli di calcolo, come Microsoft Excel per svolgere operazioni matematiche.

Autenticazione
Processo che, previa immissione nel sistema dei dati personali, determina l'identità di un individuo, basandosi in genere sul suo nome in codice e sulla password,.

Back-up e recupero dei dati
Il back-up è la copia dei file su un supporto secondario, fatta precauzionalmente o direttamente dal computer o da un supporto primario, nell'eventualità che l'uno o l'altro abbiano qualche problema. Il recupero ("recovery") è il processo che ripristina i dati presenti su un computer o su un dispositivo di memoria che è già stato danneggiato, modificato, o comunque reso inoperativo.

Banda di network
E' la quantità di dati che può essere trasferita all'interno della rete in un tempo dato.

Bug
E' un errore di software o di hardware che causa il malfunzionamento di un'applicazione o di un programma

Certificati digitali
Sono dei file che forniscono informazioni per la codifica cifrata (chiavi). I dati personali cifrati devono essere convalidati dall'ente che rilascia il sistema di codifica (ad es. la Verisign) per essere "affidabili".

Comprimere/compressione
Procedimento di immagazzinamento dei dati effettuato in modo tale da occupare meno spazio del normale, ad esempio, su di un hard disk.

Configurazione
E' il modo in cui il sistema è predisposto a funzionare e il termine si applica sia al software che all'hardware.

Continuità Aziendale
E' un piano elaborato per minimizzare le conseguenze di un evento disastroso, come un incendio o un'alluvione. Comprende anche la messa in atto di processi e procedure volte ad affrontare i problemi che riguardano la struttura IT.

Controllo di versione
Software che permette agli sviluppatori di tenere sotto controllo le diverse versioni delle applicazioni da loro scritte e di rintracciare i vari cambiamenti fatti nel tempo. Ad esempio, se viene scoperto un bug in un'applicazione, i sistemi di controllo versione consentono allo sviluppatore di capire quali cambiamenti apportati al programma hanno originato il bug.

Disk Drive
Dispositivo per la lettura e la scrittura di dati su disco. Ce ne sono molti tipi, alcuni interni al computer, come gli hard drive, che leggono e scrivono dati sugli hard disk, altri esterni, come i floppy, che sono portatili.

Download
Processo consistente nella trasmissione di un file o di un documento da un computer ad un altro. In ambito internet, si riferisce al trasferimento di un file da un server web al computer dell'utente.

Eseguibile
Un codice software scritto in un formato che il computer è in grado di leggere e far partire.

Exploit
E' la configurazione difettosa di un sistema o un bug in un'applicazione o in un

sistema operativo tale da poter essere sfruttata da un intruso per ottenere l'accesso non autorizzato a un computer o al network a cui è collegato.

Gateaway
Dispositivo di network che funge da punto di entrata ad un altro network, come internet, e che smista il traffico in entrata e in uscita da esso.

Hard Disk
Un disco magnetico sul quale vengono immagazzinati i dati nel computer.

Instant Messaging
Servizio di comunicazione che permette di creare un'area privata in cui comunicare in tempo reale con altre persone tramite internet. Il sistema di instant messaging avvisa quando un vostro amico o collega è in linea, permettendovi così di iniziare una sessione di chat con lui o con lei.

Intranet
Sito web interno a cui ha accesso solo il personale autorizzato, manager o terze parti, usato per condividere le informazioni.

Memoria
Chip di silicio che immagazzina i dati nel computer. Ve ne sono molti tipi. La RAM o Random Access Memory (Memoria ad accesso casuale), conosciuta anche come memoria principale, permette di copiare i dati da un dispositivo di immagazzinamento, come un disco, ad un'area apposita in cui possono essere utilizzati da un programma. Consente anche di copiare i dati dalla memoria principale al dispositivo di immagazzinamento.

La ROM o Read-only Memory (Memoria di sola lettura), invece, contiene le informazioni necessarie ad avviare il computer.

Off-line
Computer o periferica, come una stampante, spenta o non collegata al network.

Programma
Un software che fornisce informazioni al computer su come comportarsi dopo aver eseguito una lista ordinata di operazioni. Include una lista di variabili, testuali, numeriche, grafiche, e una lista di comandi, che dicono al computer cosa fare con le variabili. Il termine è usato spesso come sinonimo di applicazione.

Registro
Database del sistema operativo Windows che immagazzina le informazioni condivise da più programmi, ad esempio i parametri di configurazione, ecc.

Repository
Archivio centrale in cui i dati sono immagazzinati e custoditi. E' simile ad un database.

Risorse di sistema
Qualsiasi risorsa presente sul computer, come la potenza di elaborazione, la memoria, l'hard disk e i dati.

Router
Dispositivo che stabilisce il percorso più efficiente per trasferire i dati all'interno del network. Sono collocati sul gateaway e di solito collegano almeno due network – quello interno aziendale e internet.

Script Kiddies
Termine spregiativo usato dagli Hacker e dai Cracker per indicare le persone meno capaci di loro a sfruttare le brecce nei sistemi di sicurezza. Si tratta spesso di adolescenti annoiati che usano vari espedienti e programmi (vale a dire "script") ben conosciuti e facilmente reperibili per sfruttare le debolezze di altri computer collegati ad internet. Mentre gli Hacker provano orgoglio per la qualità del loro lavoro, gli script kiddies puntano in genere più sulla quantità che sulla qualità, allo scopo di attirare l'attenzione e acquisire notorietà.

Security Patch
Una patch, ossia un aggiornamento, che rimedia ad una falla nella sicurezza, rilasciata dal produttore per fornire protezione contro un nuovo punto debole appena scoperto.

Server
Computer o dispositivo che gestisce le diversi risorse del network. Ad esempio: un file server immagazzina e gestisce i file, un print server controlla le stampanti e un database server gestisce il database e tutte le ricerche fatte sul database stesso.

Sistema operativo
Il software che risiede tra l'utente e l'hardware e stabilisce il modo in cui il software e l'hardware interagiscono fra loro. Permette il funzionamento delle applicazioni.

Switch
Dispositivo che filtra e inoltra i dati tra le diverse parti del network.

Test di penetrazione
Uso di strumenti software per valutare fino a che punto un computer o una rete è vulnerabile a intrusioni ostili.

Traffico
La quantità di dati che circolano nel network.

Upload
Processo di copiatura di un file o di un documento dal vostro computer a quello di un altro o ad un sito web.

URL
Acronimo di Uniform Research Locator, è l'indirizzo al quale è possibile trovare le varie pagine web su internet.

VIII. INDIRIZZI UTILI

Strategie per la sicurezza in imprese con meno di 250 utenti
http://it.trendmicro-europe.com/smb/products/strategy.php
HackerCheck: Scanner gratuito su internet
http://www.hackercheck.com/?mode=c
Housecall: Controllate se il vostro PC ha un Virus!
http://it.trendmicro-europe.com/consumer/products/housecall_launch.php
Sicurezza "fai da te"
http://it.trendmicro europe.com/smb/security_info/save_computing_guide.php
Servizio di avviso SMS in caso di allarme:
http://it.trendmicro-europe.com/enterprise/about_us/send.php?cat=sms
Eicar: European Institute for Computer Antivirus Research:
http://www.eicar.org/
Soluzioni per le PMI
http://it.trendmicro-europe.com/smb/
Soluzioni AntiSpyware
http://it.trendmicro-europe.com/enterprise/products/spyware_overview.php
Informazioni sulla sicurezza:
http://it.trendmicro-europe.com/smb/security_info/security_overview.php
Cos'è un Virus?
http://it.trendmicro-europe.com/smb/security_info/overview.php
Informazioni sui Virus:
http://it.trendmicro-europe.com/smb/security_info/glossar.php

La Trend Micro non fa alcuna istanza su qualsiasi altro sito web. Quando accedete ad un sito web non-Trend Micro, teniate presente che esso è indipendente dalla Trend Micro e che la Trend Micro non ha alcun controllo sui contenuti di un tale sito. Un collegamento ad un sito web non-Trend Micro non implica che la Trend Micro si assuma una qualsiasi responsabilità per il contenuto o l'uso di un tale sito web o che lo approvi.

Edizione 2006

TREND MICRO ITALY - Via Donat Cattin, 5 - 20063 Cernusco sul Naviglio (Mi)
Tel. +39 02 925931 - Fax +39 02 92593401 - www.trendmicro-europe.com