Consiglio Nazionale delle Ricerche

Computer virus e posta elettronica: una guida per l'utente

F. Gennai, M. Buzzi

IIT B4-06/2002

Nota Interna

Dicembre 2002

Istituto di Informatica e Telematica

Indice

Abstract

Oggi Internet è una preziosa fonte di informazioni così come un semplice ma potente mezzo di comunicazione e per questo, è ormai diventato uno strumento di studio e di lavoro indispensabile. Il suo utilizzo, comunque, espone a qualche rischio: le reti di computer infatti sono il principale veicolo di diffusione dei virus elettronici. Gli utenti Internet sono costantemente minacciati dal contagio di nuovi virus nascosti in messaggi di Posta Elettronica o in applicazioni apparentemente innocenti scaricate dalla rete.

Il danno provocato da una infezione elettronica può essere veramente alto in termini di perdita di lavoro e di risorse utilizzate per ripristinare la situazione preesistente, e può diventare critico se investe dati sensibili o riservati.

La regola fondamentale per evitare la perdita di dati è effettuarne frequenti salvataggi (backup) in modo da poterli recuperare velocemente all'occorrenza. Un altro importante fattore per la prevenzione delle infezioni è investire nella educazione degli utenti, per renderli consapevoli dei rischi di certe azioni e delle tecniche di difesa elementari.

In questa presentazione saranno descritte le nozioni di base del funzionamento dei virus: tipi, modalità di propagazione, tecniche di disinfezione. Saranno quindi delineate alcune "norme di buon comportamento" che l'utente dovrebbe adottare per cercare di limitare la possibilità di contrarre infezioni.

Introduzione

Il problema dei virus elettronici o "computer virus" rientra nel più ampio problema della sicurezza informatica che a sua volta abbraccia due grandi aree: la sicurezza dei dati e la sicurezza dei sistemi. E' chiaro che le due aree non sono disgiunte, un attacco ad un sistema ad esempio può essere effettuato per danneggiare o carpire dati in esso contenuti, però una loro distinzione è utile perchè vengono applicate tecniche di protezione differenti.

La sicurezza dei dati, come suggerisce il nome, studia, definisce e applica regole di comportamento, strumenti e tecnologie per la protezione delle informazioni. Essa contempla un'ampia gamma di possibili danni: dal guasto di singole apparecchiature, a danni più generali quali incendi o catastrofi naturali, al furto, manomissione, uso improprio o non autorizzato dell'informazione. Le strategie di protezione spaziano quindi da sistemi, più o meno sofisticati, di salvataggio e ripristino (backup restore) a interventi di cifratura tramite crittografia. A titolo di esempio ricordiamo che l'utilizzo della firma elettronica applicata ad un messaggio di Posta Elettronica, garantisce l'autenticazione del mittente, l'integrità del contenuto e il non ripudio della destinazione, mentre la cifratura del messaggio ne assicura la confidenzialità.

La sicurezza dei sistemi fa invece riferimento alla capacità di non subire intrusioni provenienti sia dall'esterno sia dall'interno, in computer o altri dispositivi di gestione della connettività (ad es. router[1]) che possano sfruttare risorse dell'organizzazione (ad es. per effettuare elaborazioni, inviare messaggi commerciali a migliaia di utenti, etc.), danneggiare dati o sistemi, carpire informazioni riservate, o svolgere altre azioni illecite anche su sistemi informatici di altre organizzazioni.

Le tecniche di protezione dei sistemi includono la protezione del perimetro di rete mediante dispositivi preposti per il controllo del traffico entrante ed uscente dalla rete (i cosiddetti firewall), la configurazione dei router per bloccare tutto il traffico non autorizzato, la creazione di reti private virtuali sicure attraverso le quali i dati passano su canali cifrati (Virtual Private Network), l'utilizzo di programmi anti-virus o di sistemi che rilevano intrusioni (Intrusion Detection System) e tante altre.

Nel mondo della rete vengono comunemente chiamati hacker persone appassionate di informatica che pur cercando vulnerabilità in reti o sistemi non hanno comportamenti distruttivi mentre i cracker sono i veri cyber-criminali che intenzionalmente cercano di effettuare intrusioni e provocare danni all'organizzazione che subisce l'attacco. Anche se in alcuni Paesi questi comportamenti distruttivi sono perseguibili, in molti altri ancora non esiste legislazione a riguardo, impedendo di fatto di avere un controllo efficace su tali fenomeni.

In questo seminario trattiamo un aspetto della sicurezza dei sistemi: la protezione da virus, focalizzandoci principalmente sugli aspetti di interesse per l'utente.

[1] Un router è un dispositivo che si occupa dell'instradamento dei dati da/a rete locale a/da rete Internet.

I virus elettronici

Un virus elettronico è un programma che viene installato all'insaputa dell'utente e tenta di installare se stesso su altri sistemi. Da questa sua capacità di auto-replicazione nasce l'analogia con i virus biologici. Nell'informatica il termine "virus" è molto generico ed indica varie categorie di programmi capaci di moltiplicarsi infettando altri programmi (file eseguibili), documenti, o parti del sistema quali il disco rigido (hard disk) o quello estraibile (floppy disk). In aggiunta all'attività di replicazione, i virus possono effettuare altre azioni dannose (payload) che possono variare da lievi azioni di disturbo fino al danneggiamento irreversibile di documenti e programmi, o addirittura ad utilizzare il computer infetto per attaccare una organizzazione esterna.
Un computer diventa infetto quando una copia del virus si insedia nella macchina. Una volta che il virus è caricato in memoria comincia a replicarsi e, se il sistema è connesso alla rete, l'infezione si può propagare molto velocemente ad altre macchine. Questo processo si può fermare solo con la individuazione e l'eliminazione del virus stesso.

Esistono molti tipi di virus ma i più comuni possono essere raggruppati nelle seguenti categorie:

- **Parassiti, eseguibili (parasitic, executable)**. Questi tipi di virus non sono programmi veri e propri, non hanno vita propria ma, come dice il nome, sono frammenti di programma che, per attivarsi, hanno bisogno di attaccarsi ad un programma eseguibile esistente. Quando l'utente lancia il programma infettato, viene attivato il virus che, una volta in esecuzione, acquisisce tutti i diritti del programma originario ed è quindi in grado di cominciare il processo di replicazione e di effettuare le azioni dannose.
- **Internet Worm**. Un Internet worm non infetta altri file ma si diffonde via rete sfruttando gli errori presenti in programmi molto diffusi (come il software di Posta Elettronica in esecuzione su un personal computer o il programma di gestione di un server web[2]). Tipicamente il worm scandisce gli indirizzi di rete in cerca di sistemi non protetti in cui insediarsi e da cui avviare un nuovo processo di replicazione. Questo meccanismo gli consente di propagarsi molto velocemente (il suo potere infettante è molto alto) e per questo può saturare le risorse della rete. In aggiunta a ciò, il worm può compiere azioni veramente dannose, come predisporre un attacco di tutti i sistemi infetti verso un sistema o una rete esterna (di tipo Distributed Denial of Service[3]).
- **Cavalli di Troia (Trojan Horse)**. Come dice il nome, il cavallo di Troia è un programma in apparenza utile, interessante e attraente, che in realtà nasconde un codice malizioso che, una volta in esecuzione, provoca danni. Una caratteristica che lo differenzia dagli altri tipi di virus è che non si auto-replica, quindi i danni sono limitati al sistema infettato.
- **Macro Virus**. Una macro è un insieme di comandi che possono essere inseriti all'interno di un documento. I Macro virus sono macro contenenti codice malizioso che può danneggiare il sistema. Quando il documento viene aperto, la macro viene eseguita in modo automatico e all'insaputa dell'utente. Il macro virus è stato uno dei più famosi tipi di virus degli ultimi anni per varie ragioni: è abbastanza semplice da scrivere (non richiede grandi conoscenze tecniche); molte applicazioni fanno uso di macro (elaboratori di testo, fogli elettronici, presentazioni); e infine i documenti sono un tipo di file frequentemente scambiato tra gli utenti. Per ridurre il rischio di infezioni di questo tipo, le versioni più recenti delle applicazioni che utilizzano macro, non ne abilitano più l'esecuzione in modo automatico, e visualizzano messaggi di avvertimento sul rischio di questi virus.

[2] Il server web è un ambiente software che consente di "pubblicare" (ciò rendere visibile) un insieme di informazioni e/o servizi in Internet. L'utente accede queste informazioni e/o servizi attraverso un programma in esecuzione sul proprio personal computer (il cosiddetto browser o software di navigazione).

[3] Questo tipo di attacco cerca di saturare tutte le risorse di un sistema o di una rete (ad es. saturando le connessioni), in modo da collassare un servizio (sia esso posta elettronica, web, etc).

- **Virus del settore di boot (Boot sector)**. Questo tipo di virus infetta il computer rimpiazzando il contenuto del programma di caricamento del Sistema Operativo (boot sector program che va automaticamente in esecuzione all'accensione della macchina), con la sua versione infetta. Questi virus non rappresentano più una grave minaccia perché la macchina può essere configurata per impedire la scrittura del settore di boot ed inoltre virus può infettare la macchina solo se il caricamento del sistema operativo avviene da un floppy disk infetto ed oggi i floppy sono utilizzati molto meno che in passato perchè non sono adatti a contenere applicazioni di grosse dimensioni.
- **Bufale (Hoax)**. Da ultimo menzioniamo anche le cosiddette "Bufale" o "Beffe" che non sono virus, ma semplici messaggi contenenti false informazioni (di solito allarmanti!) e istruzioni in linguaggio pseudo-tecnico per indurre persone di formazione non tecnica ad effettuare azioni dannose. Spesso l'utente è istigato a inviare il messaggio a tutte le persone che conosce creando una vera e propria catena di San Antonio elettronica che, come minimo, provoca un'inondazione di messaggi non necessari impegnando inutilmente (e potendo saturare) le risorse della rete.

Sebbene oggi la principale piattaforma per la diffusione dei virus, anche a causa della sua ampia diffusione in ambienti privi di competenze informatiche, sia rappresentata dai sistemi Windows, infezioni e vulnerabilità sono presenti anche negli altri sistemi operativi (Unix, Macintosh, OpenVMS, ...).

La tendenza dei virus negli ultimi anni mostra come macro e boot virus stiano ormai scomparendo mentre, riflettendo le mutate condizioni ambientali (crescita e diffusioni delle reti di computer), eseguibili e worm rappresentino la nuova minaccia. Il rapporto annuale del centro di esperti di sicurezza in Internet (CERT) in cui vengono registrati gli incidenti a livello mondiale, per l'anno 2001 include i worm tra le più comuni attività di intrusione [1], [2].

Esempi

Iloveyou (Love Bug)

Il worm Iloveyou (anche conosciuto come LoveLetter o Love Bug), ha fatto la sua apparizione nel 2000. Questo worm prova a replicarsi in vari modi, anche se in generale si auto-invia come allegato di un messaggio di Posta Elettronica. La e-mail infetta ha come soggetto: Iloveyou e contiene il testo inglese corrispondente a: "gentilmente apri la lettera d'amore allegata che ti sto inviando". L'allegato LOVE-LETTER-FOR-YOU.TXT.vbs ha doppia estensione, e nel caso in cui Windows sia configurato per nascondere le estensioni, appare come un innocente file di testo.

Dato che l'allegato infetto è scritto in Visual Basic, per essere eseguito richiede che sulla macchina dell'utente sia attivata l'esecuzione di questo tipo di programmi (Windows Scripting Host). Per disabilitare questa configurazione nei vari ambienti Windows seguire le istruzioni contenute in [3].

Se l'utente utilizza il programma di Posta MS Outlook, il worm si attiva e prova ad inviare il messaggio ad ogni indirizzo e-mail contenuto nella rubrica. Esso inoltre può può distribuirsi anche via chat, se l'utente utilizza IRC[4] (Internet Relay Chat), e addirittura può cambiare l'impostazione della pagina di partenza di Internet Explorer perchè punti ad un sito dove risiede un file eseguibile (WIN-BUGSFIX.exe) che, una volta scaricato, modifica i registri di Windows per essere eseguito al successivo riavvio del sistema.

[4] In aggiunta ai classici sistemi di comunicazione quali la Posta Elettronica e le News nei quali, un messaggio inviato rimane memorizzato fino a che non viene scaricato e letto dall'utente, in Internet sono presenti una varietà di sistemi per la messaggistica interattiva (instant message system), che possono essere utilizzati per "chat" cioè chiacchierate elettroniche. IRC, è uno di questi sistemi software che consente a un grande numero di persone di comunicare simultaneamente. Un altro sistema di chat molto famoso è ICQ.

Infine il worm cerca tutti i dischi locali o di rete, e sovrascrive tutti i file VBS, VBE, JS, JSE, CSS, WSH, SCT o HTA con se stesso, e rinomina le loro estensioni in VBS. Tutti i file JPG o JPEG sono ugualmente sovrascritti con il worm e viene aggiunta estensione .VBS al nome del file. Tutti i file MP2 e MP3 sono sovrascritti con il worm ma sono anche copiati in un nuovo file con estensione.VBS aggiunta al nome del file. I file originari vengono "nascosti".

Nimda

Nimda è uno dei virus più noti del 2001. E' un virus di tipo eseguibile che si diffonde via posta elettronica, condivisioni di rete e siti web e può infettare tutte le versioni dei sistemi Windows (95/98/ME/NT/2000).

Le e-mail affette dal virus hanno un allegato README.EXE. Il virus tenta di sfruttare una vulnerabilità di alcune versioni di MS Outlook, Outlook Express, ed Internet Explorer per permettere l'esecuzione automatica dell'eseguibile, senza che l'utente apra l'allegato.

Una volta attivato, il virus copia se stesso nella directory Windows con i nomi load.exe e riched20.dll (entrambi con attibuti del file "nascosto") e modifica il file System.ini per permettere la sua esecuzione alla partenza di Windows. Il virus si invia a tutti gli indirizzi e-mail contenuti sul computer infettato e tenta di diffondersi ad altri sistemi attraverso le condivisioni di rete.

Inoltre cerca una vulnerabilità dei server web operanti con il sistema Microsoft Internet Information Server (IIS) che consente di alterare il contenuto di pagine pubblicate su tali server (con nomi standard tipo index.htm index.html, index.asp, etc.), aggiungendo alla fine del file una parte codice Javascript malizioso. A questo punto, se questi siti vengono visitati da utenti che utilizzano una versione insicura di Internet Explorer, il codice malizioso scarica automaticamente sul computer del malcapitato il file readme.elm che viene quindi eseguito infettando il computer dell'utente. Gli amministratori di questi server devono applicare le opportune misure (applicare le correzioni rilasciate da Microsoft) per ripristinare il server web in una condizione sicura.

Per infettare questi server web, Nimda sfrutta delle vulnerabilità lasciate dall'attacco del Cavallo di Troia CodRed-II, un virus diffusosi in precedenza che compromette il web server IIS, ed esso stesso prova ad aprire varchi addizionali, per esempio fornendo poteri di amministratore all'utente "guest" (ospite) che non dovrebbe avere alcun privilegio per operare sul sistema. E' buona norma cancellare l'utente "guest" (in sistemi Window NT/2000).

Quando si diffonde attraverso le condivisioni di rete, Nimda rilascia un numero di file con nomi casuali ed estensioni .ELM e NWS e con lo stesso contenuto del file readme.elm.

Klez

Klez è un worm insidioso che a partire dall'Ottobre del 2001 si è diffuso in molte varianti (Klez-A, Klez-B, ... Klez-H). Esso si propaga via e-mail e condivisioni di rete, trasportando una copia compressa del virus Elkern, che una volta attivato, rilascia ed esegue. Klez sfrutta delle vulnerabilità di alcune versioni di MS Outlook, Outlook Express, ed Internet Explorer, in modo analogo a quanto visto in precedenza. In questo caso però, il worm è molto "furbo" ed è in grado di neutralizzare i più noti anti-virus cancellandoli o corrompendoli.

Per l'invio dei messaggi non utilizza i programmi di Posta dell'utente, ma un software proprio, quindi falsifica il campo From (mittente) del messaggio per fare credere che provenga da alcuni tra i più noti produttori di anti-virus. Il messaggio può contenere vari testi, tra cui uno in cui il worm stesso si spaccia per uno strumento per proteggersi dal pericoloso virus Klez-E e istiga l'utente ad attivarlo e a

continuare la sua esecuzione, anche in caso di warning (avviso di pericolo) da parte di un eventuale anti-virus.

Tra le azioni distruttive sul computer dell'utente Klez sovrascrive alcuni file (il giorno 6 dei mesi dispari) o tutti i file su tutti i dischi (a Gennaio e Luglio) e, in alcune varianti, estrae ed invia parti di documenti dell'utente, con possibili violazioni della loro confidenzialità.

BugBear

BugBear è un worm apparso di recente che sfrutta due vulnerabilità di alcune versioni di MS Outlook (già note da circa un anno). Esso si diffonde via e-mail e attraverso condivisioni di rete. Il suo potere infettante non è molto alto perchè molti utenti hanno già aggiornato i loro programmi di Posta in seguito a precedenti infezioni di questo tipo.

Infezioni

Il principale veicolo per la diffusione di virus è Internet: milioni di reti e sistemi interconnessi rappresentano un fertile terreno per la diffusione di infezioni elettroniche! Una volta che un computer diventa infetto, il virus, per propagarsi, cerca di sfruttare i protocolli di comunicazione, le condivisioni di risorse e le vulnerabilità dei sistemi. Sebbene i sistemi operativi e le applicazioni continuino ad aggiungere protezioni, i virus continuano a diffondersi più numerosi e con potere infettivo maggiore che in passato. Molti fattori contribuiscono a facilitare tale diffusione come [2]:

- Internet è stato progettato per favorire semplicità, affidabilità e interoperabilità quando i mezzi di comunicazione non erano stabili e i protocolli di base non includevano meccanismi di sicurezza. Inoltre, in Internet la possibilità di attaccare un sistema dipende dallo stato di sicurezza globale della rete: per quanto cerchiamo di difendere la nostra rete, un attacco verso la nostra organizzazione può sfruttare le debolezze di altre reti e altri sistemi.
- Importantissimo è il problema degli errori nei programmi di uso comune che rappresentano potenziali buchi nella sicurezza utilizzabili da malitenzionati (cracker) per penetrare in reti e sistemi. La crescente richiesta di nuove applicazioni e gli stringenti requisiti del tempo di immissione di un nuovo prodotto nel mercato (time-to-market) impongono scadenze veramente strette agli sviluppatori, che si traducono in minore qualità e affidabilità dei prodotti software. Il numero di vulnerabilità nei prodotti riportate dal CERT è in costante aumento (nel 2001 sono raddoppiate rispetto all'anno precedente).
- I virus, e in generale gli strumenti per intrusioni e attacchi, diventano sempre più sofisticati: cresce il livello di automazione, modularità e velocità di replicazione (l'infezione diventa veramente attiva). Esistono virus polimorfici che cambiano dinamicamente, creando differenti varianti per rendere più difficile la loro identificazione. Possono utilizzare differenti funzioni di cifratura, variare la sequenza dei comandi, etc. In aggiunta a ciò, dato che oggi i virus per replicarsi utilizzano svariati protocolli di comunicazione (web, posta elettronica, chat, condivisione di risorse, ...) l'ispezione del traffico di rete allo scopo di discernere tra traffico autorizzato e fraudolento, richiede sistemi con adeguate risorse, altrimenti le prestazioni della rete possono degradare. Di conseguenza diventa più difficile prevenire o evitare attacchi.
- Contenuti attivi (active content). Questo termine si riferisce a tecnologie (come Java, ActiveX, Javascript, etc.) che possono attivare l'esecuzione automatica di programmi disponibili su server di rete, sul computer dell'utente. Queste tecnologie offrono molti vantaggi, che spaziano dalla riduzione del carico di lavoro del server alla semplificazione delle interfacce utenti, e sono quindi sempre più utilizzati dagli sviluppatori di prodotti software. Di fatto il loro uso sposta i problemi di sicurezza dal server verso il computer dell'utente, infatti il software scaricato potrebbe contenere codice malizioso. L'uso della firma digitale associata a un contenuto attivo assicura l'integrità del

contenuto e autentica l'origine (per es. il sito web da cui viene scaricata), ma non offre nessuna garanzia che il software non possa provocare danni [4].

- L'ignoranza dei rischi insiti in certi comportamenti e dei meccanismi di base della sicurezza, insieme con la cresciuta automazione delle applicazioni (progettate per facilitare l'interazione con l'utente) giocano un ruolo fondamentale nella propagazione dei virus. Per esempio, un grande numero di infezioni è propagato via e-mail: il virus si replica spedendosi via e-mail a tutti gli indirizzi trovati nella rubrica dell'utente infetto. Se un utente, ignaro del rischio, clicca sull'allegato attiva l'applicazione ad esso associata, abilitando in questo modo il virus ad infettare. Peggio, alcune vecchie versioni di programmi di Posta Elettronica, per rendere il processo più semplice per l'utente, aprono automaticamente l'allegato appena l'utente scarica il messaggio, accrescendo il potere infettante del virus stesso.

Prevenzione

Poche norme di base possono contribuire a ridurre i rischi di infezione o a limitarne i danni, infatti spesso i virus agiscono con l'inconsapevole aiuto dell'utente: aprire un allegato di un messaggio di posta elettronica, scaricare un file da Internet comportano un rischio di infezione. Per questo è importante avere una conoscenza di base del problema ed avere coscienza dei rischi insiti nei nostri comportamenti.

Il rispetto di poche norme di base nell'intera organizzazione offre contributi fondamentali ad una efficace strategia anti-virus:

- Prima di tutto è necessario investire nella formazione, rendendo gli utenti coscienti dei problemi di sicurezza. L'educazione degli utenti gioca un ruolo fondamentale nel prevenire le infezioni, perchè le persone sono curiose e quindi sono fortemente tentate a provare nuovi strumenti ed applicazioni.
- In secondo luogo è necessario disporre di procedure efficaci per il salvataggio di sistemi, applicazioni e dati, in modo da poter facilmente ripristinare la situazione nel caso di attacco di virus. In generale, la sicurezza dei dati residenti su personal computer è affidata all'utente che, in funzione delle proprie esigenze (variabilità dei dati nel tempo, loro importanza, ...), deve provvedere ad eseguire copie periodiche di salvataggio.
- E' importante definire una politica di sicurezza specifica per l'organizzazione che preveda il monitoraggio della rete ed il controllo del traffico [5], [6]. L'uso di un anti-virus è solo una delle molteplici componenti che rendono efficace una politica di sicurezza, che in grandi organizzazioni il cui lavoro è basato sulla rete (per es. società di commercio elettronico) richiede una profonda ed accurata analisi e valutazione.

Le principali linee guida che un utente può seguire includono:

1. Configurare Windows in modo da rendere visibili le estensioni dei file (ad es. in W2000 da pannello di controllo selezionare Opzioni Cartelle).
2. Sospettare se si ricevono file con doppie estensioni come ad es. XXX.TXT.VBS o YYY.DOC.EXE. In questi casi, se le estensioni dei file non sono visibili, la parte a destra (.VBS o .EXE) non appare e l'utente pensa di aprire file innocui.
3. Non fidarsi delle estensioni dei file che possono essere facilmente modificate: una falsa estensione può essere inserita in file eseguibili per ingannare gli utenti.
4. Non aprire mai file allegati con estensioni EXE, COM, VBS, SCR, BAT, o PIF perchè sono file eseguibili e, come tali, possono attivare virus, sempreché non provengano da ambienti "sicuri". Nei casi sospetti conviene cancellare i messaggi e vuotare il cestino per non rischiare di rimanere inavvertitamente contagiati.
5. Anche se i file video e audio (ad es. JPG, GIF, MP3, MPG) non possono essere infettati da virus, i virus possono camuffarsi sotto le sembianze di tali file (utilizzando delle false estensioni). Immagini, grafici, salva-schermi e filmati dovrebbero essere trattati con la stessa attenzione di tutti gli altri tipi di file.

6. Non aprire allegati con nomi sospetti (sesso, soldi, etc.) e messaggi pubblicitari o comunque non richiesti[5] e non seguire i link in essi contenuti. Bisogna essere coscienti del fatto che seguire un link può corrispondere all'azione di scaricare un file sul proprio computer. Attenzione perchè esistono programmi che una volta scaricati "spiano" le azioni dell'utente, ad esempio i siti visitati a scopo di informazione commerciale. Altri programmi possono istruire il modem per chiamare un numero diverso da quello del vostro provider (tenere sempre il volume alto), con spiacevoli sorprese al ricevimento della bolletta.
7. Anche se i messaggi sono inviati da conoscenti, in caso di contenuto sospetto (lingua straniera, contenuto non comprensibile), prima di aprire gli allegati chiedere una conferma al mittente (il virus può spedire messaggi a nome dell'utente).
8. Non attivare la condivisione di una cartella di lavoro se non è necessario. In tal caso condividere solo la cartella contenente i dati (non tutto il disco) e rimuovere la condivisione quando non è più necessaria. I virus si possono diffondere attraverso queste condivisioni, copiandosi da un computer ad un altro.
9. Se possibile, disabilitare tutte le forme di avvio automatico di script o programmi come ActiveX e Java;
10. Inviare i documenti in formati di stampa in formato PDF (Adobe Acrobat Writer) se non devono essere modificati, oppure in formati che non contengono macro, come Rich Text Format (RTF) invece di usare il DOC di MS Word;
11. Non utilizzare file compressi che si auto-scompattano perchè non mostrano il loro contenuto;
12. Tenere aggiornati il programma di Posta Elettronica ed il Sistema Operativo, e in caso di vulnerabilità, applicare subito gli aggiornamenti (patch). In caso di utilizzo di ambiente Windows sarebbe opportuno che l'amministratore dei servizi di rete si iscrivesse alla apposita lista di distribuzione della Microsoft (Microsoft Security Notification Service) e comunicasse agli utenti gli avvisi di loro interesse.
13. Porre attenzione nello scaricamento di file da Internet (via web, ftp, chat, newsgroup, etc.). Se si utilizza una casella di Posta Elettronica su server esterni a cui si accede via web, prima di scaricare qualsiasi allegato (cliccando il link), porre la stessa attenzione utilizzata per gli allegati ricevuti mediante i programmi di Posta Elettronica (Outlook, Netscape).
14. Riportare ogni allarme relativo a nuovi virus al responsabile della sicurezza informatica che può discernere tra vere e false comunicazioni ("bufale");
15. Configurare il PC per impedire il caricamento del Sistema Operativo da floppy disk per eliminare la possibilità di contagi da parte dei virus del settore di boot.
16. Ovviamente è fondamentale evitare di cancellare il programma anti-virus del proprio computer ed è altrettanto importante curare l'aggiornamento di tale programma, che avviene solitamente in modo automatico.
17. Infine, come già ricordato in precedenza, è veramente fondamentale effettuare il salvataggio periodico di dati e di documenti importanti (back-up).

Se si viene infettati dal virus interrompere immediatamente la connessione ad Internet (staccare il cavo di rete o spegnere il modem) per evitare la diffusione del contagio, disinfettare il computer con un anti-virus aggiornato ed in caso di difficoltà chiamare il proprio amministratore di rete. E' buona norma disconnettere la rete o il modem quando non si utilizza il computer.

[5] I messaggi non richiesti di solito di origine commerciale (Unsolicited Commercial E-mail o Unsolicited Bulk E-mail) stanno diventando uno spiacevole fenomeno che, come minimo, fa perdere tempo all'utente. L'invio di massicce quantità di messaggi non richiesti viene comunemente detta spamming.

Danni provocati da virus

Deve essere chiaro che la presenza di programmi anti-virus sui personal computer degli utenti e su alcuni server, quale quello della posta elettronica, non garantisce in modo assoluto la sicurezza. Infatti può succedere che l'antivirus non riesca a riconoscere un nuovo virus. I programmi anti-virus sono istruiti per intercettare i virus esistenti; quando viene realizzato un nuovo virus, esiste sempre un intervallo di tempo in cui il virus si diffonde senza ostacoli perché gli anti-virus non lo conoscono e, quindi, non sono in grado di intercettarlo.

La valutazione dei costi che una organizzazione deve sostenere per ripristinare una situazione pre-esistente all'attacco di un virus è un'operazione difficile, talvolta impossibile perchè il danno dipende da molti fattori come la capacità di penetrazione del virus, il valore dei dati corrotti, la disponibilità di copie salvate, etc. Nella valutazione dei danni dobbiamo comunque includere:

- tempo dei tecnici informatici e risorse necessarie per disinfettare i sistemi e ripristinare dati e applicazioni;
- tempo di lavoro perso dagli utenti finali finchè i sistemi non sono ripristinati;
- eventuali interruzioni della connettività di rete e quindi possibili perdite di introiti;
- diminuita credibilità interna ed esterna;
- violazione della confidenzialità (eventuali informazioni carpite).

A queste conseguenze devono essere aggiunti il fattore psicologico, che induce persone spaventate dalla possibilità di essere contagiate da virus a rimuoversi da newsgroup e mailing list.

Per avere un idea dell'impatto economico globale di una infezione virale, citiamo due dati da Computer Economics, che ha stimato l'impatto totale (a livello mondiale) del virus Nimda (2001) e del worm Love Bug (2000) rispettivamente in 635 Milioni e 8.75 Miliardi di dollari [10]. Per limitare i danni dovuti ad un attacco virale, è veramente importante cercare di individuare e debellare l'infezione elettronica il più presto possibile.

Anti-virus

Oggi il mercato offre una grande scelta di sistemi anti-virus [11], è quindi importante riuscire a valutare quello più idoneo alle esigenze specifiche dell'organizzazione. Le tecniche base degli anti-virus sono suddivisibili in [12]:

- **Scanner** che individuano e disinfettano tutti i tipi conosciuti di virus (sistemi basati sulla impronta del virus). Facili da utilizzare, questi tipi di anti-virus forniscono informazioni sul virus individuato, sul file infettato e se è stato o no disinfettato. Il principale problema di questo anti-virus è che per rimanere efficace deve essere costantemente mantenuto aggiornato.
- **Checksummer** si basano sulla individuazione di cambiamenti: se un virus infetta un oggetto, allora esso cambia. Il principale svantaggio di questi tipi di anti-virus è che non sono capaci di prevenire le infezioni, ma possono solo individuarle una volta contratte. In più le risposte dei checksummer devono essere interpretate da una persona capace di distinguere tra i cambiamenti leciti e quelli virali. Il vantaggio è che richiede meno risorse degli scanner, e quindi se utilizzato su PC, non rallenta la macchina.
- **Euristici** applicano regole per individuazione di virus. L'analisi euristica rimane valida solo se i nuovi virus sono dei rifacimenti dei vecchi, per es. se utilizzano lo stesso metodo di replicazione, altrimenti le regole devono cambiare e quindi il programma anti-virus deve essere aggiornato. Gli anti-virus di questo tipo possono creare falsi allarmi etichettando erroneamente come virus degli oggetti leciti.

I programmi anti-virus dovrebbero essere collocati nelle posizioni strategiche dove fluisce il traffico Internet come i punti di accesso sul perimetro della rete, in modo da eseguire funzioni quali l'ispezione e filtraggio dei dati in transito. Sono quindi candidati ad ospitare programmi anti-virus.

- I punti di connessione tra la rete interna e Internet (**Internet/intranet gateway** o **router** o **firewall** o **proxy)**. Su questi sistemi è possibile ispezionare tutto il traffico in ingresso ed in uscita, intercettando e fermando i virus in ingresso/uscita. L'uso dell'anti-virus e/o l'applicazione di regole

di filtro (per scartare traffico non autorizzato) sono provvedimenti particolarmente efficaci perché consentono di prevenire le infezioni. Il principale problema a questo livello è che non tutti i messaggi in transito possono essere controllati, ad esempio i file cifrati non sono interpretabili durante il transito, ma solo al loro arrivo nella destinazione finale (per es. quando vengono letti dall'utente). Inoltre l'ispezione del traffico consuma risorse e carica i sistemi di connessione che, nel caso di traffico intenso, possono rallentare il transito dei dati.

- **Server di Posta Elettronica**. L'anti-virus sul server di Posta Elettronica permette la scansione di tutto il traffico in ingresso e in uscita e la rimozione delle parti infette. Anche in questo caso la posta cifrata non è interpretabile durante il transito ma solo quando raggiunge il destinatario finale.
- **Server**. Se l'organizzazione utilizza server centralizzati su cui mantiene le informazioni (per esempio server di gruppo), l'anti-virus può essere installato su tale server, a protezione dei dati di più utenti.
- **Sistemi utente**. Se il virus attraversa le difese di frontiera (router e/o firewall, server e-mail, web, etc.) può essere intercettato sul sistema dell'utente. In aggiunta a ciò i virus possono entrare nel computer dell'utente via Compact Disk e floppy disk. D'altra parte l'anti-virus può ritardare le attività dell'utente quando è attiva la scansione. Un altro svantaggio è che, in organizzazioni con molti posti di lavoro è oneroso mantenere aggiornate tutte le installazioni.

Spesso in reti estese e molto complesse viene utilizzato un approccio di anti-virus a più livelli (per es. in tutti i punti di accesso) allo scopo di compensare i punti deboli di un livello con la forza di un altro. Per evitare che tutti i livelli mantengano le stesse debolezze, è importante diversificare le tecniche di protezione dei diversi livelli [13].

Conclusioni

In base alla legislazione nazionale e internazionale hacker, cracker e cyber-criminali, che causano infezioni virali, possono essere perseguiti per i loro comportamenti distruttivi [16]. A dispetto di ciò, la creazione e la diffusione di virus cresce ad un ritmo allarmante, così come cresce il loro grado di automazione e di sofisticatezza. Man mano che la tecnologia evolve, aumentano le protezioni verso certi attacchi ma sorgono nuove vulnerabilità, come problemi di sicurezza per telefoni cellulari e palmari.

Oggi, non c'è alcun modo per implementare una politica di sicurezza totale, ma è necessario creare una strategia diversificata per contrastare intrusioni e combattere la piaga dei virus.

I costi sostenuti da una organizzazione per definire ed implementare una politica di sicurezza rappresentano un buon investimento per il futuro.

Bibliografia

1. CERT Coordination Center. 2001 Annual Report. http://www.cert.org/annual_rpts/cert_rpt_01.html
2. CERT Coordination Center. Overview of attack trends. http://www.cert.org/archive/pdf/attack_trends.pdf
3. How to disabling Windows Scripting Host - http://www.sophos.com/support/faqs/wsh.html
4. Carr, K.: Active content: friend or foe. http://www.sophos.com/virusinfo/whitepapers/activecontent.html (2002)
5. Fraser, B.: RFC2196: Site Security Handbook. (1997)
6. CERT Security Improvement Module - http://www.cert.org/security-improvement/
7. Kandula, S, Singh, S. and Sanghi, D.: Argus: A Distributed Network Intrusion Detection System. Proceeding of SANE 2002, 27-31 May, Maastricht, pp.333-350. http://www.nluug.nl/events/sane2002/papers.html (2002)
8. The honeynet project. http://www.project.honeynet.org/
9. Donkers, A: Honey, I caught a worm. Building yourself a honeypot, some pratical issue. Proceeding of SANE 2002, 27-31 May, Maastricht, pp.304-318. http://www.nluug.nl/events/sane2002/papers.html (2002)
10. Press Releases - Malicious Code Attacks Had $13.2 Billion Economic Impact in 2001 http://www.computereconomics.com/
11. CERT Coordination Center. Computer Virus Resources http://www.cert.org/other_sources/viruses.html
12. Hruska, J.: Computer virus prevention: a primer. http://www.sophos.com/virusinfo/whitepapers/prevention.html (2000)
13. FitzGerald, N.: Free Anti-Virus Techniques. VB2002 Conference, 26-27 Sept, New Orleans (USA). http://www.virusbtn.com/VB2002/abstracts/free_techniques.html (2002)
14. CERT. Survivable network systems: an emerging Discipline. http://www.cert.org/research/97tr013.pdf
15. MS Security Bulletins. http://www.microsoft.com/security/
16. De Villiers, M.: Computer Viruses and The Law. VB2002 Conference, 26-27 Sept, New Orleans. http://www.virusbtn.com/VB2002/abstracts/the_law.html (2002)