La sicurezza delle reti

Il problema della sicurezza dei computer connessi alla rete è diventato molto importante con la crescita di Internet: si parla spesso di virus, attacchi informatici, sistemi violati e truffe informatiche.

Il problema risiede nel fatto che fisicamente i computer, per definizione, sono tutti collegati alla stessa rete. Questo è il grande vantaggio di Internet, che espone però a rischi che possono coinvolgere un numero considerevole di computer.

I protocolli e i servizi di Internet non sono la causa principale dei problemi di sicurezza: le tecnologie alla base di Internet si evolvono continuamente e rapidamente per risolvere i problemi che si presentano nel tempo, producendo nuovi servizi e software più sicuri.

La parte più importante di Internet non sono i computer e le connessioni che compongono la rete delle reti (parte hardware), ma i programmi che la gestiscono e ne permettono l'uso (parte software). I programmi sono sviluppati da programmatori, che sono soggetti a errori umani. L'errore presente in un programma (indicato nel gergo informatico con il termine *bug*) può essere sfruttato per far compiere al programma stesso operazioni non previste.

Per esempio molti virus, che si sono diffusi negli anni recenti, hanno utilizzato errori o imprecisioni presenti nel server Web o nei programmi di posta elettronica.

Le vulnerabilità software possono essere più o meno gravi, essere più frequenti in certi programmi invece che in altri, ma la responsabilità del computer è sempre a carico dell'utente. Quindi è necessario che gli utenti prendano tutte le precauzioni possibili per garantire la sicurezza del proprio computer, in particolar modo se connesso a Internet.

Alcuni aspetti di sicurezza possono essere gestiti a livello di rete aziendale, attraverso diverse tecniche:

- Il **firewall** (letteralmente, *muro taglia fuoco*) è un dispositivo o un insieme di dispositivi che hanno l'obiettivo di creare una separazione tra Internet, intesa come rete pubblica, e la rete aziendale, ritenuta vulnerabile, al fine di preservarla da intrusioni fraudolente o non autorizzate. Il firewall può essere un computer (hardware) specializzato in queste funzioni di controllo della rete, oppure un programma software installato sul server della rete.
- Il **tunneling** può essere definito come la via per trasferire dati tra due reti simili attraverso una rete intermedia. Il tunneling incapsula un tipo di pacchetto di un generico protocollo in un pacchetto di un altro protocollo trasportabile in Internet. Prima che l'incapsulamento abbia luogo, i pacchetti sono crittografati, in modo che i dati non siano leggibili da chiunque tenga costantemente monitorata la rete con scopi fraudolenti. Questi pacchetti incapsulati viaggiano attraverso Internet fino a raggiungere la loro destinazione. All'arrivo i pacchetti riprendono l'aspetto originario, perché sono i due punti di entrata e di uscita del tunnel che conoscono e utilizzano il protocollo di incapsulamento.
- La **VPN** (*Virtual Private Network*) è un'estensione di una Intranet privata attraverso una rete pubblica, come Internet, che stabilisce una connessione privata sicura, essenzialmente attraverso un tunnel privato. La VPN racchiude utenti remoti, sedi aziendali distaccate e reti di vendita, in una rete aziendale estesa.

Altri aspetti di sicurezza riguardano il controllo **antivirus** e l'aggiornamento delle definizioni dei virus, oltre all'applicazione di filtri sul server di posta per proteggere la rete dallo *spamming*. Il termine **spam** indica l'invio di posta indesiderata a un grande numero di caselle di posta. Spesso questi messaggi, oltre ad intasare inutilmente le caselle e-mail, contengono allegati portatori di virus.
È ovvio comunque che la sicurezza viene garantita anche dal comportamento degli utenti e da un efficace metodo di salvataggio periodico dei dati più importanti (*backup*).

Virus

I principali tipi di virus e di attacchi alla sicurezza del computer sono:

- Virus che provocano *infezione sui file*, in particolare sui file eseguibili .COM o .EXE e che vengono caricati nella memoria del computer ogni volta che il programma viene eseguito. Sono tipi di virus che di solito arrivano sul computer collegati ad altri programmi o come allegati a messaggi di posta elettronica.
- Virus di *avvio* che attaccano il sistema e in particolare il *boot-record* del disco, cioè il blocco del disco che contiene le informazioni sull'avvio del computer.
- Virus per le *macro*: le macro sono comandi simbolici costruiti dall'utente all'interno dei programmi Office (Word, Excel, Access) e che consentono di eseguire una sequenza di operazioni elementari frequentemente utilizzate. L'infezione di questo tipi di virus provoca malfunzionamenti nei programmi Office.
- Cavalli di Troia (*Trojan*): sono programmi all'apparenza normali che possono però distruggere i file sul disco oppure l'intero disco. A differenza dei virus precedenti, non replicano se stessi su altri computer.
- I virus *Worm* sono programmi autoreplicanti che hanno come caratteristica principale la capacità di diffondersi rapidamente sulla rete di computer e in Internet.
- Gli *spyware* sono programmi che vengono mandati in esecuzione durante la navigazione Web, all'insaputa dell'utente, e che trasmettono ad altri server informazioni sui siti visitati dall'utente, in modo che nei successivi accessi alla rete, sul video dell'utente compaiano messaggi pubblicitari o reindirizzamenti verso altri siti.
- I *malware* (software maligni), in analogia agli spyware, inviano pubblicità non richiesta, aprono finestre pop-up sullo schermo, modificano la pagina iniziale del browser oppure attivano chiamate telefoniche su numeri a pagamento (*dialer*).

Regole pratiche per prevenire l'infezione dei virus per computer

1. Installare e usare un buon programma antivirus.
2. Assicurarsi che la protezione del programma antivirus sia sempre attivata soprattutto nelle sessioni di lavoro con collegamenti in rete o in Internet.
3. Aggiornare frequentemente le definizioni dei virus, scaricando gli aggiornamenti dal sito Internet del fornitore del software antivirus.
4. Non aprire messaggi di posta elettronica di dubbia provenienza.
5. Non aprire allegati contenuti all'interno di messaggi di posta elettronica con mittente sconosciuto o non sicuro e non impostare il programma di posta elettronica per l'esecuzione automatica degli allegati.
6. Utilizzare un client di posta con filtri antispam.
7. Fare la scansione dei supporti di memorizzazione (chiavi USB, ecc.) provenienti da fonte insicura, prima di usare i file e i programmi in essi contenuti.
8. Non scaricare musica, file multimediali o filmati da un sito Internet che non offra garanzie di sicurezza.
9. Dopo aver scaricato un programma da Internet, effettuare il controllo antivirus prima di installarlo ed eseguirlo.
10. Operare con cautela la condivisione di file e musiche con altri utenti della rete; durante la connessione con condivisione di cartelle sul disco, il computer è aperto all'ingresso non autorizzato e all'attacco da parte di utenti esterni.
11. Effettuare frequentemente copie di sicurezza (su dischi remoti o supporti di backup) dei documenti e file che riteniamo importanti per il nostro lavoro.
12. Eseguire una scansione manuale settimanale (o automatica) dei dischi rigidi.
13. Proteggere con una password le unità di rete condivise.

Phishing

Una tecnica che viene utilizzata da truffatori, ma che non può essere classificata come virus, è il *phishing*. Il **phishing** è una frode informatica che consiste nel creare una copia identica di un sito Internet (per esempio la *home page* di una banca) e indurre l'utente ad inserire i propri dati personali. Il truffatore può successivamente utilizzare i dati ottenuti per i propri scopi.

La truffa tramite *phishing* utilizza di solito la posta elettronica per cui spesso si parla di *phishing mail*.

Le **phishing mail** hanno lo stesso aspetto dei normali messaggi di e-mail. Il destinatario ha l'impressione di aver ricevuto una regolare comunicazione ufficiale da una banca, una società o dalle Poste italiane. Di solito il messaggio contiene un link che porta l'utente ad una pagina del tutto identica alla *home page* del sito istituzionale, ma in realtà residente su un server esterno gestito dai truffatori. Indicando erroneamente i dati del proprio account, come indirizzo mail, username e password, oppure dati e riferimenti bancari (numero conto corrente, codice segreto del Bancomat, numero di carta di credito) avviene il cosiddetto *phishing* dei dati personali. Gli autori della truffa possono quindi abusare di questi dati, comportando danni economici, ma anche conseguenze penali.

Regole pratiche per prevenire frodi da phishing

1. Normalmente le comunicazioni tramite e-mail hanno:
   - un oggetto significativo,
   - non sono generiche,
   - contengono i nostri dati personali
   - non richiedono mai la password a utenti o clienti.

   Una mail che non rispetta tutti questi requisiti è da considerarsi sospetta.
2. Se si ha ancora qualche dubbio e si vuole comunque visitare il sito istituzionale non fare clic sul link presente nella mail (che potrebbe essere contraffatto), ma digitarlo manualmente nella barra degli indirizzi.
3. Spesso i messaggi di phishing sono generati con traduttori automatici dei testi e quindi contengono molti errori grammaticali o utilizzano termini della lingua italiana in modo non appropriato.
4. L'indirizzo del sito malevolo è diverso da quello originale per cui, prima di inserire qualsiasi dato, controllare sempre che nella casella *Indirizzo* del browser (URL) sia indicato l'indirizzo esatto della Banca o dell'Ente. In caso di dubbio contattare la propria Filiale o il servizio ICT dell'Ente.
5. Solitamente banche, aziende e poste utilizzano sempre protocolli crittografati, per cui è opportuno controllare che il protocollo utilizzato sia *https* e non il semplice *http*.

Continuità operativa

La **continuità operativa** (o *business continuity*) indica l'insieme di attività volte a ripristinare lo stato del sistema informatico o parte di esso, compresi gli aspetti fisici e organizzativi e le persone necessarie per il suo funzionamento, con l'obiettivo di riportarlo alle condizioni antecedenti a un evento disastroso, che ha colpito un'organizzazione o parte di essa, garantendo la continuità delle attività in generale.

Quindi queste attività non sono riferite solo alla parte informatica di un'azienda o di una pubblica amministrazione, ma all'intera organizzazione.

La continuità operativa riguarda gli aspetti organizzativi, logistici e comunicativi che permettano la prosecuzione delle attività di un'organizzazione, oltre alla continuità tecnologica, cioè l'infrastruttura informatica e di telecomunicazioni.

Disaster Recovery

Per gli aspetti specifici che riguardano la continuità operativa della parte informatica di un'organizzazione, le misure da adottare vengono indicate con il termine **disaster recovery**, cioè le procedure e le soluzioni da attivare in caso di evento disastroso, per ripristinare il normale funzionamento dei servizi alle condizioni di operatività precedente all'evento e ridurre al minimo l'indisponibilità dei sistemi informativi.

Nelle politiche di sicurezza occorre considerare anche gli aspetti non tecnologici, quali l'indisponibilità di risorse umane (casi di epidemia che causano assenze di personale), problemi di logistica (collegamenti e trasporti), mancanza di energia elettrica (riscaldamento e condizionamento degli ambienti), che potrebbero anche verificarsi contemporaneamente.

Le attività necessarie a gestire l'evento negativo sono riassunte in un documento operativo, chiamato *Piano di disaster recovery*.