La sicurezza informatica

Borgogno Monica

Introduzione

Il problema della sicurezza informatica è strettamente legato all'utilizzo di internet e della posta elettronica. Avere una connessione a internet predispone quindi l'utente a diversi rischi che se vengono sottovalutati possono creare problemi seri.
Le motivazioni per cui avvengono queste violazioni di sicurezza possono essere diversi come ad esempio il sottrarre informazioni riservate, lo spionaggio industriale oppure motivazioni più subdole come una vendetta o un desiderio di diffamazione. Quindi adottare misure di sicurezza per impedire a estranei di introdursi nel sistema informatico è necessario per impedire la perdita o la distruzione di dati importanti, ridurre il rischio di furto di dati e impedire accessi non consentiti.
Quando viene utilizzato internet alcune informazioni quali il browser utilizzato, la risoluzione dello schermo, l'indirizzo IP e altri dati di tipo tecnico sono resi disponibili al sito con cui ci si connette. Spesso se i beni informatici non sono protetti è perché non si ha l'esatta percezione del rischio reale che si corre.
Occorre individuare principalmente quali componenti del sistema devono essere protette tra:

1) hardware: il computer, la stampante, lo scanner sono vulnerabili ai danni fisici come urti, umidità e cadute, ai furti o ai danni provocati da interruzioni elettriche. Dobbiamo quindi proteggerlo con le opportune misure di salvaguardia fisica o elettrica (ad esempio un gruppo di continuità);
2) software: il sistema operativo e tutti i programmi istallati sul nostro computer possono essere danneggiati o per attacchi dall'esterno o per malfunzionamenti del computer. In questo caso è possibile istallarli nuovamente e per questo dobbiamo avere a disposizione i dischi e i CD di istallazione di tutti i programmi;
3) dati informatici: sul computer sono memorizzati tutti i nostri dati personali (lettere, documenti contabili, posta elettronica, informazioni private, filmati, fotografie, musica, ecc) che in caso di perdita difficilmente potrebbero essere ricostruiti. Inoltre tutti questi dati devono essere protetti da persone non autorizzate a venirne in possesso;
4) dati critici: questi dati non sono necessariamente memorizzati sul computer ma sono fondamentali per il suo funzionamento o per l'avvio di applicazioni o servizi finanziari. Se venissero scoperti da un malintenzionato, potrebbero essere usati per svolgere attività illecite e truffaldine. Tra i dati critici più significativi abbiamo: le password, il codice pin, le liste di stralcio (i numeri usati a complemento delle password nei servizi finanziari e bancari), i numeri di carta di credito e il crediti card validation code (il numero timbrato sul retro della carta di credito che viene sempre richiesto nelle transazioni di commercio elettronico), i dati anagrafici, i dati finanziari e gli indirizzi di posta elettronica.

Successivamente occorre conoscere bene da cosa ci si deve proteggere.
Le principali minacce sono rappresentate da:

- malware: sono software indesiderati che compiono azioni dannose. I virus infettano un programma o un documento esistente e lo usano come vettore per riprodursi oppure per danneggiare dati e/o programmi presenti su supporti registrabili, vi sono diversi tipi di virus, come i virus di file che si sostituiscono in parte o

completamente a un programma e quando viene eseguito il programma verrà eseguito il virus, i virus di boot che sfruttano il settore di boot o MBR del disco per essere eseguiti a ogni avvio e risiedono in memoria, i virus multi partiti che sono i più pericolosi in quanto possono infettare sia il settore di avvio che i programmi, i virus di macro che infettano solo file di dati macro e non i programmi; i worms sono frammenti di codice indipendenti e autonomi che agiscono principalmente in memoria e non hanno bisogno di legarsi ad altri programmi per diffondersi, usano una rete per poter infettare altre componenti, ad esempio viene inviato con una e-mail, questo tipo di malware non mira a danneggiare i dati ma crea malfunzionamenti tipo rallentamento o blocco del sistema oppure servono a carpire informazioni personali; i trojan sono programmi dannosi mascherati però da programmi innocui che consentono il controllo remoto del PC e la perdita o furto di dati; backdoor (porta posteriore) è un metodo che serve per aggirare le normali procedure di autenticazione nei sistemi, per ovviare a questo tipo di malware sarebbe opportuno utilizzare software open source; spyware: sono software che raccolgono informazioni personali riguardanti l'attività on-line degli utenti senza alcun consenso, non si replica ma ne richiede l'esecuzione inconsapevole da parte dall'utente, le conseguenze possono riguardare l'invio di pubblicità non richiesta (spam), la modifica della pagina iniziale del browser, la redirezione su falsi siti di e-commerce (phishing); dialer sono software che prendono il controllo del modem per poter chiamare numeri a pagamento, ma la connessione ADSL è immune da questo pericolo;

- Intercettazioni: sono intromissioni esterne che possono essere effettuate su una comunicazione telefonica, su e-mail o su comunicazioni http, con lo scopo di ottenere informazioni. Classico esempio sono i "man in the middle" cioè le intercettazioni di messaggi che producono modifiche ai messaggi stessi senza che gli utenti se ne accorgano. Si ovvia a questo pericolo attraverso l'autenticazione oppure la cifratura.
- Social engineering: sono tecniche per influenzare persone ad effettuare procedure che consentono di carpire informazioni sensibili.
- Denial on service: hanno lo scopo di rendere inutilizzabile un intero sistema cioè viene intasato il server. Questo tipo di minaccia è difficile da combattere.

I crimini su internet sono sempre più frequenti, si manifestano come varianti dei crimini già presenti nella vita reale come la pedofilia, la pornografia dura, l'incitamento al razzismo, le truffe, le frodi, l'abuso delle carte di credito o la violazione dei diritti d'autore. Esistono crimini più specifici dell'ambiente informatico come l'accesso illecito a sistemi, il cybercrime, il danneggiamento dei dati informatici, il danneggiamento o il blocco dei siti internet, la diffusione di virus informatici, il sabotaggio delle infrastrutture. Esistono anche altri tipi di crimini commessi da vere e proprie organizzazioni attive nel mondo reale che hanno individuato le possibilità di guadagno della rete e che si muovono ormai a livello planetario con decisione, professionalità e disponibilità di mezzi. Attività apparentemente innocue, come lo spamming e la diffusione di virus, vengono usate come mezzo per portare successive truffe, ma anche frodi, ricatti e attacchi nei confronti di siti internet con la minaccia di farli cadere fino ai possibili attentati alle infrastrutture critiche. Per impedire al crimine organizzato di invadere il cyberspazio sono importanti due cose:
- mostrare l'alta intolleranza verso le attività criminali su internet e perseguirle legalmente;

- diffondere l'informazione sui diversi tipi di crimine e sulle possibili vittime per fare in modo che la conoscenza dei rischi informatici cominci a far parte della consapevolezza che abbiamo dei rischi quotidiani.

Per la sicurezza in rete è necessario osservare alcune regole fondamentali prima fra tutte l'utilizzo di password, cioè di una sequenza di caratteri segreta che da accesso a servizi internet alla persona autorizzata solo con l'autenticazione; inoltre sarebbe opportuno non creare password basate su informazioni personali come la data di nascita, è sempre preferibile usare combinazioni di lettere maiuscole e minuscole, numeri e simboli.
Inoltre occorre utilizzare dei programmi chiamati antivirus che hanno la funzione di proteggere l'utente dalle principali minacce.