SICUREZZA INFORMATICA

MINACCE

REGOLE DI COMPORTAMENTO

Ver.1.0, 12 gennaio 2015

Pagina lasciata intenzionalmente bianca

1. SICUREZZA INFORMATICA

È molto complicato cercare di dare una definizione univoca di **sicurezza informatica**. Basta una semplice ricerca per trovare diverse definizioni ognuna delle quali mette in evidenza un aspetto piuttosto che un altro di ciò di cui la sicurezza informatica si occupa.

Quella che riportiamo di seguito è una delle tante che riassume molti dei concetti comuni a tutte:

"*la sicurezza informatica può essere definita come l'insieme delle misure, di carattere organizzativo e tecnologico, atte a garantire l'**autenticazione** dell'utente, la **disponibilità**, l'**integrità** e la **riservatezza** delle informazioni e dei servizi, **gestiti** o **erogati** in modo digitale*".

Da questa definizione si capisce come la sicurezza informatica sia applicabile, con le opportune differenze, sia a sistemi industriali, grandi, condivisi dinamici e distribuiti, sia a sistemi "micro", come il PC (*personal computer*) di ognuno di noi. È chiaro che in questo caso le misure "organizzative" e "tecnologiche" per proteggere i nostri dati siano a carico di noi stessi.

È quindi essenziale capire quali siano i rischi che corrono i nostri dati. Muoversi in questo mondo presuppone la conoscenza delle possibili minacce e delle relative, semplici azioni che possono essere fatte per prevenire e proteggerci da queste.

Con la presente guida si intende quindi fornire una veloce panoramica della terminologia, delle possibili minacce e delle regole base di comportamento da tenere per garantire un livello minimo di "sicurezza" per il nostro patrimonio informativo digitale.

2. MALWARE

Con il termine ***malware*** (dalla contrazione delle due parole inglesi "*mal*icious" e "soft*ware*", letteralmente "programma maligno" o "codice maligno") si indica genericamente un qualsiasi *software*, ovvero un qualsiasi programma, creato con lo scopo di causare danni più o meno gravi ad un computer o a un qualsiasi sistema informatico su cui viene eseguito ed ai dati degli utenti ivi contenuti.

All'interno della categoria dei *malware* esistono una serie di programmi ognuno dei quali agisce con modalità differenti e con obiettivi specifici particolari. Spesso viene fatta confusione tra queste tipologie (per esempio, spesso si parla di *virus* come generico *malware*, ma, come descritto in seguito, il *virus* è, propriamente, un ben preciso tipo di *malware*); scopo dei paragrafi seguenti è fornire una descrizione delle principali tipologie di *malware*: ogni computer, soprattutto se è collegato alla rete, è esposto a pericoli quali *virus*, *worm* ("vermi" informatici) o *trojan* ("cavalli di Troia") nonché a *spyware*, che possono causare la perdita di dati con gravi pregiudizi alla sfera privata. D'altra parte anche la tecnica del *phishing* può portare alla perdita di informazioni personali estremamente delicate, mentre *hoax* o *spam* sono spesso solo fastidiosi, qualora si adottino le appropriate contromisure comportamentali.

2.1 Virus

Un **virus** è un programma informatico composto da una serie di istruzioni elementari, come qualsiasi altro programma. È solitamente composto da un numero molto ridotto di istruzioni ed è specializzato per eseguire soltanto poche e semplici operazioni ed ottimizzato per impiegare il minor numero di risorse, in modo da rendersi il più possibile invisibile. Caratteristica principale di un virus è quella di riprodursi e quindi diffondersi nel computer ogni volta che viene aperto un file infetto.

In analogia con un virus biologico, un virus non è un programma eseguibile a sé stante, ma per essere attivato deve infettare un programma ospite, o una sequenza di codice che viene lanciata automaticamente, come ad esempio i virus che sfruttano il "boot sector" che viene eseguito ad ogni avvio della macchina. La tecnica solitamente usata dai virus è quella di infettare i file eseguibili: il virus inserisce una copia di se stesso nel file .exe che deve infettare, ponendo tra le prime istruzioni un'istruzione di salto alla prima linea della sua copia ed alla fine di essa un altro salto all'inizio dell'esecuzione del programma originario. In questo modo quando un utente lancia un programma infettato viene comunque assicurata l'esecuzione del programma stesso: l'utente in questo modo non si accorge che il virus è in esecuzione e sta svolgendo, a sua insaputa, le operazioni contenute nel suo codice e per il quale è stato progettato.

Il virus, oltre ad auto-replicarsi, può procedere ad una serie di operazioni estremamente dannose, che vanno dal semplice far apparire messaggi (per esempio *banner* o *popup* non richiesti), all'apertura di *backdoor* che possono consentire ad utenti esterni malintenzionati di accedere alla macchina, alla cattura di dati ed informazioni presenti sulla macchina, alla loro compromissione, fino ad arrivare alla loro distruzione.

2.2 Worm

Come i virus, i **worm** (dall'inglese: "vermi") sono dei programmi opportunamente progettati per danneggiare l'utente, ma, contrariamente ai virus, non necessitano di un programma ospite per funzionare, essendo essi stessi dei programmi completi. Essi sfruttano invece lacune di sicurezza (in gergo "**vulnerabilità**") o errori di configurazione del sistema operativo per propagarsi autonomamente da un computer all'altro. Obiettivo dei worm sono computer che presentano lacune di sicurezza o errori di configurazione e che sono collegati ad altri computer, tipicamente attraverso internet.

Anche in questo caso, il programma, una volta lanciato, può portare a conseguenze estremamente dannose per l'utente: dall'accesso non autorizzato alla macchina da parte di utenti malintenzionati, alla perdita di dati confidenziali, alla totale compromissione del computer.

2.3 Trojan

I **trojan** (letteralmente "cavalli di Troia") sono programmi che eseguono di nascosto operazioni nocive, nascondendosi all'interno di applicazioni e documenti utili per l'utente. Questi sfruttano lacune di sicurezza dei programmi utilizzati per aprire i file infetti per installarsi nel sistema ad insaputa dell'utente. Per esempio potrebbero trovarsi all'interno di brani musicali .mp3 e sfruttare una qualche vulnerabilità del programma di riproduzione, soprattutto qualora questo non fosse aggiornato all'ultima versione.

Spesso i trojan sono programmi scaricati da internet, altre volte vengono propagati per il tramite di allegati alle Email.

I pericoli sono gli stessi che si corrono con i classici virus: spionaggio di dati confidenziali (password, codici di accesso ai servizi bancari, pin ecc.) mediante registrazione e comunicazione inconsapevole al malintenzionato dei dati digitati sulla tastiera piuttosto che accesso non autorizzato al computer.

2.4 Spyware e Adware

Lo "**spyware**" (termine derivante dalla contrazione delle parole inglesi "*spy*" e "soft*ware*") è destinato a raccogliere all'insaputa dell'utente informazioni sulle sue abitudini di navigazione oppure sulle configurazioni di sistema per trasmetterle a un indirizzo predefinito. Il tipo di informazioni lette varia da uno spyware all'altro e può spaziare dalle abitudini di navigazione sino alle password.

Il termine di "**adware**" deriva invece dalla contrazione delle parole inglesi "*ad*vertising" (pubblicità) e "soft*ware*". In genere l'adware è utilizzato a scopi pubblicitari, nel senso che le abitudini di navigazione dell'utente vengono registrate e sfruttate per offrirgli prodotti corrispondenti (ad es. per il tramite di link personalizzati), pur senza che questi ne abbia fatto richiesta esplicita. Lo spyware e l'adware si installano solitamente sul computer quando si scaricano programmi.

In questo caso i pericoli vanno dallo spionaggio di dati confidenziali (dalle abitudini di navigazione fino alle password) con evidente pregiudizio della sfera privata alla pubblicità indesiderata, nel caso tipico degli adware.

2.5 Social Engineering

Gli attacchi di "**social engineering**" sfruttano la disponibilità, la buona fede e l'insicurezza delle persone per accedere per esempio a dati confidenziali o per indurre le vittime a effettuare determinate operazioni. Fra le tante possibilità di attacco, questa è ancora una delle più efficaci. Chi sfrutta il social engineering può per esempio accedere al nome di utente e alla password dei collaboratori di un'impresa facendosi per esempio passare al telefono come amministratore del sistema o come responsabile della sicurezza. Abbagliata dal pretesto di gravi problemi informatici e dallo scambio di informazioni sul sistema (ad es. nome del superiore, processi di lavoro, ecc.), la vittima è resa insicura fino al punto da comunicare le informazioni richieste. Per la propagazione di virus e di cavalli di Troia vengono sovente applicati metodi di social engineering; ne è il caso quando il nome dell'allegato a un Email contenente un virus promette contenuti particolarmente interessanti. Il "phishing" è una speciale forma di attacco di social engineering.

Le conseguenze di un attacco di social engineering andato a buon fine sono la rivelazione di informazioni confidenziali attraverso l'inganno e, in taluni casi, la propagazione di virus o trojan.

2.6 Phishing

La parola **phishing** deriva dalla contrazione delle parole inglesi "password", "*harvesting*" (raccolta) e "*fishing*" (pesca): i malintenzionati tentano di accedere ai dati confidenziali di ignari utenti. Si può trattare per esempio, caso tipico, di dati di accesso a servizi bancari on-line. I truffatori sfruttano la buona fede e la disponibilità delle loro vittime inviando loro Email nei quali l'indirizzo del mittente è falsificato ed in cui si annuncia che le informazioni sul suo conto devono essere modificati avvalendosi del link integrato nell'Email. Il link non indirizza però alla pagina del presunto mittente, ma su una abilmente falsificata allestita dal truffatore. Grazie ai dati ottenuti (principalmente le credenziali di accesso), il truffatore può effettuare transazioni bancarie a nome della vittima entrando in maniera abusiva nel suo conto on-line, con evidente enorme danno immediato.

2.7 Vulnerabilità

Un "**programma**" informatico (**software**) è costituito da una serie di "istruzioni" (o "codice") che assegnano al computer operazioni da eseguire. Il software installato sui nostri personal computer comprende decine di migliaia di righe di codice: non deve quindi sorprendere che vi possano essere contenuti alcuni errori. Ogni giorno vengono scoperti e pubblicati errori di progettazione e di realizzazione dei programmi che correntemente vengono fatti funzionare sulle nostre macchine. La maggior parte di questi errori non ha alcun impatto sulla sicurezza del sistema ma alcuni sono tali da poter rendere possibile un accesso non autorizzato ai dati e al sistema. Si parla in questo caso di "**vulnerabilità**" del sistema, in quanto tali errori possono consentire ad utenti malintenzionati di accedere in qualche modo ai dati contenuti nel nostro computer.

2.8 Hoax

Le Email contenenti informazioni su nuovi virus o presunti tali sono quasi sempre notizie false ("**hoax**", termine inglese per designare scherzi o notizie false). In genere si viene messi in guardia contro nuovi virus estremamente pericolosi, impossibili da combattere anche con i normali antivirus e si viene invitati a diffondere la notizia a tutti i conoscenti o a seguire delle istruzioni per evitare la minaccia. Talvolta si parla anche di "catene di sant'Antonio", quando l'obiettivo è quello di far circolare il messaggio con un contenuto spesso assurdo e che fa generalmente leva su aspetti scaramantici o emotivi.

2.9 Spam

Con “**spam**” si indicano generalmente tutte le Email indesiderate, con un contenuto di vario genere, da quello pubblicitario, a quello più o meno fantasioso ed assurdo tipico delle catene di sant'Antonio. Lo “spammer” è il mittente di queste comunicazioni, mentre il fenomeno del loro invio è denominato “spamming”.

Lo spammig porta ad una notevole perdita di tempo da parte di chi riceve il messaggio, anche per la sua sola cancellazione, oltre ad un inutile sovraccarico della infrastruttura tecnica (rete, server di posta ecc.).

2.10 Cookies

I **cookies** (dall’inglese, “biscotti”) sono piccoli file di testo creati sul computer dell'utente quando visita una pagina web e sono nati per facilitare l'utente stesso. Ad esempio, per l'accesso a taluni servizi online sono necessari un nome di utente e una password: per non dover ripetere ogni volta l'immissione, queste informazioni sono registrate in un cookie locale e inserite automaticamente nei campi corrispondenti ad ogni visita della pagina. Altro esempio è quello fatto dai servizi di commercio on-line per il salvataggio temporaneo del contenuto del carrello degli acquisti o per mostrare prodotti nuovi rispetto a quelli disponibili al momento dell’ultima visita. I cookies possono essere di “breve durata” (“**session** cookies”) o di “lunga durata” (“**persistent** cookies”). I primi sono cancellati alla chiusura del browser, mentre i “persistent cookies”, la data di scadenza viene stabilita dall'applicazione web, che utilizzerà il cookie sino a quella data.

Un utilizzo “improprio” dei cookies può portare pregiudizio alla riservatezza della propria sfera privata, rendendo possibile il tracciamento delle attività dell’utente ed un suo inconsapevole “tracciamento”.

2.11 Chat e Instant Messaging

Per **chat** si intende la possibilità di comunicazione offerta da Internet, grazie alla quale ci si può intrattenere in tempo reale con altri utenti. Diversamente dalle conversazioni telefoniche, la discussione non si svolge con la parola, bensì tramite digitazione delle informazioni. A seconda delle tematiche sono disponibili diversi spazi chat (“canali”). L'utente può comunicare contemporaneamente con tutti gli altri partecipanti oppure "ritirarsi" con un altro utente in uno spazio privato non accessibile agli altri. Per la loro apparente anonimità, i servizi chat (o di instant messaging) vengono spesso sfruttati per operazioni illegali (ed esempio adescamento) o possono essere utilizzati come vettori di infezione (virus, worm o

trojan) quando i partecipanti alla chat sono invitati a cliccare su link o a digitare comandi sconosciuti.

2.12 Wireless LAN

L'abbreviazione WLAN (“**Wireless Local Area Network**”) significa “rete locale senza fili” in cui un apparato (ad es. un personal computer) comunica senza fili con un cosiddetto WLAN Access Point (“router”), collegato a sua volta a internet o a una rete. Grazie all'assenza del cablaggio, gli utenti degli apparati finali sono più mobili e questo costituisce il vantaggio di una WLAN.

Una configurazione imprudente del WLAN Access Point può determinare l'accesso illimitato a persone non autorizzate rendendo possibile l'accesso al computer e ai dati e l'utilizzazione abusiva del collegamento a internet. Inoltre una cifratura insufficiente dei collegamenti WLAN consente la lettura dei dati scambiati tra gli apparati ed i router attraverso strumenti relativamente semplici.

3. PROTEZIONI

3.1 Personal Firewall *COMODO*

Un **firewall** (“muro tagliafuoco”) controlla i collegamenti entranti e uscenti dal proprio computer o dalla propria rete ed eventualmente rifiuta le connessioni non autorizzate. Il firewall può essere paragonato a un posto di guardia all'entrata di un castello: la decisione di accettazione o di rifiuto dei collegamenti si basa su regole semplici, verificate ad ogni nuovo collegamento. Grazie al firewall può essere ridotto il rischio di accesso non autorizzato da parte di malintenzionati e minimizzato il pericolo di infiltrazione da parte di worm, trojan o spyware. La maggior parte delle imprese proteggono le loro reti mediante un potente firewall installato su un apposito computer e situato tra internet e la propria rete. Il “personal” firewall (o “desktop” firewall) è concepito per la protezione di un singolo computer ed è installato direttamente sul sistema da proteggere, ossia sul singolo computer.

Un semplice regola di comportamento è:

Installare il personal firewall

Come gli antivirus, anche i personal firewall sono disponibili come software complementare e possono essere scaricati, talvolta gratuitamente, da internet. I principali sistemi operativi sono già dotati di un personal firewall che dovrebbe essere sempre utilizzato

Attivare il personal firewall

Se il computer dispone di un personal firewall, attivarlo sempre prima di collegarlo per la prima volta a internet. Lo scaricamento di aggiornamenti del software, o di qualsiasi programma, dovrebbe essere effettuato unicamente a personal firewall attivato

3.2 Software Updates

Particolarmente importanti ai fini della sicurezza sono gli **aggiornamenti del software** (software update, le cosiddette “patch”), perché consentono di colmare le falle di sicurezza che vengono scoperte quasi quotidianamente. La falle di sicurezza sono responsabili dell'accesso non autorizzato ai vostri dati e della propagazione di virus e worm e si verificano sia nel sistema operativo (ad es. Windows, Linux, ecc.), sia nelle applicazioni (ad es. Apache, Internet Explorer, Media Player, ecc.). Per accrescere la sicurezza dei

vostri dati assume pertanto grande importanza l'installazione degli aggiornamenti del software resi disponibili dai produttori.

Le semplici regole da seguire sono:

Aggiornamento regolare del sistema operativo e delle applicazioni

Alcuni prodotti dispongono di una funzione automatica di aggiornamento che dovrebbe essere sempre utilizzata. Verificarne regolarmente il funzionamento. Solitamente le informazioni sugli aggiornamenti del software sono disponibili sulle pagine web dei rispettivi produttori

Seguire le notizie relative agli aggiornamenti del software

Esistono servizi che informano regolarmente sulla scoperta di nuove falle di sicurezza (vulnerabilità) nonché sui corrispondenti aggiornamenti.

Anche nel caso in cui si proceda ad un aggiornamento tempestivo (possibilmente automatico) del software, esistono le cosiddette falle di sicurezza "**0-day**", ossia vulnerabilità note per le quali non esiste ancora alcun aggiornamento di sicurezza. Tali falle di sicurezza compaiono quasi quotidianamente nelle più svariate applicazioni, tra cui anche i browser (Internet Explorer, Firefox, Chrome ecc.). Poiché una gran parte di virus sono veicolati tramite internet e, quindi, i browser di navigazione, può rivelarsi opportuna una strategia cosiddetta a "doppio browser", ovvero avere sempre una coppia di browser installati sul proprio computer ed utilizzare, almeno temporaneamente, il secondo browser finché la falla di sicurezza del primo non sia stata risolta dal produttore.

3.3 Antivirus *COMODO*

I software "**antivirus**" proteggono il sistema ed i dati dai virus, dai worm e dai trojan.

Un software antivirus aggiornato è assolutamente **indispensabile** se si naviga in internet e si scaricano programmi. Dato che giornalmente nascono numerosi nuovi malware, è tassativamente indispensabile anche un **aggiornamento frequente** del software antivirus.

Le semplici regole da seguire:

Installare un software antivirus

È assolutamente necessario installare una versione aggiornata del software antivirus

Aggiornare regolarmente il software antivirus

Il software antivirus va aggiornato almeno due o tre volte alla settimana. La maggior parte dei prodotti dispongono di funzioni automatiche di aggiornamento che dove essere assolutamente attivata

Verificare la validità della licenza

Sincerarsi regolarmente che la licenza del software antivirus utilizzato sia ancora valida: il software potrebbe anche continuare a funzionare dopo la scadenza della durata di validità, ma a partire da allora non possono più essere installati gli aggiornamenti

3.4 Protezione dei Dati

Non può mai essere escluso che i propri dati vengano parzialmente o completamente persi a seguito di errori involontari o inconsapevoli (es. cancellazione del file sbagliato), di problemi tecnici (es. cadute dell'alimentazione elettrica durante il lavoro, anomalie dei programmi) o per colpa di malware presente sul proprio computer. Per ridurre al minimo il rischio di perdita irrimediabile dei dati, è necessario effettuarne regolarmente il salvataggio ("backup") su differenti supporti.

Alcune semplici regole.

Backup regolare dei dati

I dati che si vuole proteggere devono essere copiati **periodicamente** su supporti **esterni** (tipicamente CD-ROM, DVD, pennette USB o dischi fissi esterni)

Conservazione dei dati di backup

I supporti esterni devono essere conservati in luoghi al riparati e sicuri, teoricamente non nelle dirette adiacenze del computer in uso

Verifica delle copie di sicurezza

È sempre buona norma il controllo regolare dell'integrità e della leggibilità dei backup mediante verifica periodica dei file di ripristino contenuti nel backup stesso

4. REGOLE DI COMPORTAMENTO

Oltre agli accorgimenti tecnici descritti in precedenza (personal firewall, aggiornamenti del software, software antivirus), per aumentare la sicurezza del proprio computer è di importanza fondamentale il corretto e consapevole comportamento di ogni singolo utente.

Tra le regole di base che possiamo suggerire ci sono:

4.1 Scelta di buone password

Sono molti i servizi che richiedono l'uso di una password di accesso. La scelta poco avveduta di una password costituisce un notevole incremento dei rischi per la sicurezza. Nella scelta della password devono essere osservati i seguenti principi:

lunghezza minima

La lunghezza minima di una password dovrebbe essere di 8 caratteri, meglio se 12 o 16; essa dovrebbe essere composta sempre in parte di lettere dell'alfabeto, in parte di cifre ed in parte di caratteri speciali

facilità di memorizzazione

La password deve essere scelta in modo che possa essere memorizzata facilmente senza annotarla per scritto. Buone password sono frasi/parole compiute che contengono anche segni speciali; ad esempio : "m1_ch1am0%P1pp0!". Sono disponibili diversi programmi con l'ausilio dei quali potete collaudare la robustezza di una password (non effettuare mai questi test con password originali, ma con password similari)

un servizio, una password

Utilizzare password diverse per scopi diversi. Nel caso dell'utilizzazione di servizi online si raccomanda fortemente di utilizzare per ognuno di essi una password diversa

modifica regolare

La password dovrebbe essere modificata a intervalli regolari (ogni tre mesi circa), ed immediatamente quando si presume che possa essere conosciuta da terzi.

4.2 Prudenza nella gestione delle Email

La prudenza nella gestione delle Email ricevute contribuisce in grande misura alla sicurezza dei vostri dati e del vostro computer. Il rispetto delle semplici regole che seguono sono una ottima protezione contro gran parte delle attuali minacce.

prudenza nella apertura di Email con mittente ignoto

Diffidare delle Email di cui non si conosce l'indirizzo del mittente. In questo caso **non aprire mai gli allegati** o i programmi ivi contenuti, **né selezionare i link indicati**

verifica dell'affidabilità della fonte

Aprire unicamente i file o i programmi provenienti da fonti affidabili e solo previa verifica con un programma antivirus aggiornato

attenzione ai file con due estensioni

Non aprire mai gli allegati ad Email provvisti di due estensioni (ad es. picture.bmp.vbs) e non lasciarsi ingannare dall'icona di simili file. Disattivare nelle opzioni del browser, dove presente, l'opzione "nascondi le estensioni per i tipi di file conosciuti"

aggiornamento del software

Anche i programmi di gestione delle Email possono presentare vulnerabilità: sincerarsi regolarmente di aver installato l'ultima versione del software

comunicazione del proprio indirizzo Email

Per limitare lo spam, è sempre opportuno comunicare il proprio indirizzo Email alle **sole** persone necessarie

utilizzo di un secondo indirizzo Email

Per la compilazione di moduli web, l'abbonamenti a Newsletter, iscrizione a registri dei visitatori, ecc. si suggerisce di utilizzare un secondo indirizzo Email. Se questo secondo indirizzo dovesse essere oggetto di spam, è possibile cancellarlo o sostituirlo

non rispondere agli spam

Rispondere ad un messaggio di spam equivale ad informare lo spammer che l'indirizzo Email è valido e quindi questi invierà ulteriori spam oppure metterà il vostro indirizzo a disposizione di altri spammer. Particolare attenzione va portata agli spam con l'opzione di "cancellazione dall'elenco" in cui si promette la cancellazione dall'elenco di distribuzione tramite l'invio di un Email con un determinato contenuto. Da questo punto di vista va data particolare attenzione alle Email di risposta automatica in caso di

assenza per vacanze. Tali risposte automatiche dovrebbero essere attivate unicamente per gli indirizzi conosciuti

hoax

Nella maggior parte dei casi gli avvertimenti di pericolo di virus inviati tramite Email sono false informazioni (hoax): non eseguire mai, in nessun caso, le raccomandazioni ivi contenute. Questo con particolare riferimento a: cancellazione di file, installazione di un determinato programma, inoltro dell'informazione ai conoscenti. In caso di dubbio consultate le pagine web ufficiali dei produttori di programmi antivirus. Analoghe considerazioni sono valide nel caso delle catene di "sant'Antonio"

4.3 Prudenza nella navigazione in internet

Gran parte dei pericoli per la sicurezza del proprio computer vengono corsi durante la navigazione in internet. Molti di questi pericoli possono essere evitati adottando opportune misure comportamentali che vengono riportate di seguito.

non scaricare programmi sconosciuti

Non scaricare mai programmi sconosciuti da internet prima di averne accertato la provenienza

aggiornamento del software dai siti dei produttori

Scaricare gli aggiornamenti di software e driver **esclusivamente** dalla pagina web dei relativi produttori. È sempre buona norma anche verificarli successivamente con un programma antivirus aggiornato

prudenza nella trasmissione di informazioni

Non comunicare **mai** a nessuno le proprie credenziali di accesso (nome di utente e password). Nessun fornitore di servizi serio chiederà la vostra password (nemmeno telefonicamente). Questo vale anche quando la richiesta appare credibile. Nel caso di transazioni online, rivolgersi solo a fornitori seri: comunicare il numero della carta di credito unicamente per il tramite di pagine web che garantiscono la cifratura dei dati. Tale garanzia è riconoscibile da un lucchetto dorato che appare all'interno del browser oppure dal protocollo utilizzato (tipicamente "https" invece di "http")

chiudere le applicazioni

Utilizzare sempre l'apposita notifica di chiusura ("logout") quando si esce da un'applicazione web che abbia richiesto l'introduzione delle proprie credenziali di accesso

riservatezza nella divulgazione delle informazioni personali

Evitate di rivelare dati personali durante la compilazione di moduli Web o la fornitura di contributi a newsgroup, forum o registri di visitatori

attenzione alla configurazione del browser

Molte delle minacce che si incontrano durante la navigazione in internet sono legate all'utilizzo dei componenti "dinamici" delle pagine web tipicamente realizzati tramite controlli ActiveX o funzioni JavaScript. Tali funzionalità sono spesso indispensabili per il corretto funzionamento della pagina, ma spesso vengono utilizzate in maniera malevola da parte di malintenzionati per il lancio di malware sulla macchina ospite. Una possibile contromisura può essere la limitazione di JavaScript o dei ActiveX:

- provare a limitare o a disattivare l'esecuzione di JavaScript mediante la configurazione del browser. Va però osservato che in caso di disattivazione di JavaScript numerose pagine Web non funzionano più correttamente. In tal caso è possibile allentare gradualmente le limitazioni sino a un livello minimo di funzionalità

- provare a limitare nella misura del possibile l'esecuzione dei controlli ActiveX mediante la configurazione del navigatore.

Mantenere tendenzialmente le opzioni di sicurezza automatiche (per la configurazione delle quali si rimanda alla documentazione del browser che si utilizza) sul valore "alto".

4.4 Configurazione del sistema

Alcune semplici regole da seguire nella configurazione del proprio sistema:

Password robusta

Assegnate una password efficace a ogni conto di utente disponibile.

Nessun accesso libero

Verificate che non siano configurati accessi liberi (cosiddetti shares) sul vostro computer. Su un sistema Windows per esempio, gli accessi liberi consentono di mettere a disposizione degli altri utenti, tramite la rete, file o interi dischi fissi. Gli accessi liberi non costituiscono soltanto un punto d'attacco per i virus e i vermi informatici, ma possono rendere accessibili a una grande cerchia di utenti (nella peggiore ipotesi a tutti gli utenti di Internet) i vostri dati (confidenziali).

4.5 Prudenza nella navigazione sulle reti “peer-to-peer”

La comunicazione “peer-to-peer” (“P2P”)costituisce un'alternativa rispetto al classico modello client-server, nel quale un “server” offre prestazioni di servizi utilizzate dai “client”. Nel modello “peer-to-peer” (dall’inglese, “pari a pari”) ogni computer è contemporaneamente client e server, ossia offre e riceve prestazioni di servizi dagli altri computer della rete. Questa forma di comunicazione è in particolare utilizzata per lo scambio di file e, per tale scopo, è in genere necessario un software dedicato. Spesso questa modalità di scambio di file (anche molto grandi, come brani musicali o film interi) viola la legge del diritto di autore (“copyright”) e, pertanto, un uso improprio è spesso sinonimo di violazione di legge.

Ma oltre agli aspetti legislativi relativi ai diritti d'autore, l’uso di questa tipologia di comunicazione è fonte di ulteriori problemi: numerosi file offerti, infatti, sono infettati da virus o da trojans. Inoltre il software P2P può contenere spyware e adware e presentare diverse falle di sicurezza. Infine c’è il rischio non secondario che gli utenti rendano accessibili per errore dati confidenziali contenuti nel proprio sistema.

Per tutte queste ragioni il ricorso all’uso di tali metodologie deve essere fatto, oltre che nel rispetto delle leggi vigenti, anche con estrema attenzione e perizia nell’uso di tale tecnica.

4.6 Wireless LAN (reti “WiFi”)

L’utilizzo di tecnologie “senza fili”, ha il grande vantaggio di offrire maggiore “mobilità” agli utenti finali oltre che una maggiore semplicità di accesso alla rete.

Ma è essenziale seguire alcune semplici regole per evitare che il proprio sistema possa essere compromesso da utenti malintenzionati, poiché il tratto “aereo” deve essere opportunamente protetto da tentativi di intrusione.

Protezione della pagina di amministratore

La maggior parte degli “Access Point” (ovvero i cosiddetti “router WiFi”) consentono l'amministrazione tramite un'interfaccia utente, accessibile con un normale browser (tipicamente con un accesso http://192.168.0.0 o simile) dalla quale possono essere configurati, tra gli altri, i parametri riportati sotto. L'accesso alla pagina di amministratore è protetto da una password standard riportata nel manuale del router, che dovrebbe essere immediatamente modificata.

Identificazione di rete

Modificare l'identificazione di rete standard (“SSID”)

Occultamento dell'emissione dell'SSID

Si consiglia di impedire che il router emetta regolarmente la propria identificazione di rete (SSID). A tale scopo l'opzione "Broadcast SSID" dovrebbe essere impostata su "no"

Limitazione degli accessi

Limitare il collegamento all'Access Point in modo che solo le vostre apparecchiature finali possano comunicare con esso. Tale limitazione può essere realizzata registrando l'indirizzo MAC delle proprie apparecchiature

Attivazione della cifratura

Attivare sempre la cifratura WPA o, meglio, WPA2 scegliendo una password molto robusta. La cifratura WEP è ormai completamente superata e non garantisce la necessaria sicurezza nella trasmissione e non è più usata nei router più moderni

4.7 Reti Bluetooth

Le raccomandazioni fatte per le reti WiFi valgono, con gli opportuni aggiustamenti, anche per le reti che si basano su interfacce “radio”. Ad esempio, diversi apparati hanno interfacce Bluetooth; in questo caso i consigli sono quelli di:

- attivare Bluetooth solo quando necessario e disattivarlo dopo l’uso
- utilizzare Bluetooth soltanto in ambiente “sicuro” (possibilmente non in luogo pubblico) e se indispensabile
- attivare la visibilità Bluetooth dell'apparecchio solo se necessario
- utilizzare sempre le opzioni di sicurezza, attivando quando possibile le opzioni di autenticazione e cifratura

Browser consigliati:
Firefox, DuckDuckGo