Capitolo 4 – Come possiamo difenderci

Riferimento Syllabus 1.4.1	***Comprendere l'effetto di attivare/disattivare le impostazioni di sicurezza delle macro.***
Riferimento Syllabus 1.4.2	***Impostare una password per file quali documenti, file compressi, fogli di calcolo.***
Riferimento Syllabus 2.3.1	***Comprendere come funziona il software anti-virus e quali limitazioni presenta.***
Riferimento Syllabus 2.3.2	***Eseguire scansioni di specifiche unità, cartelle, file usando un software anti-virus. Pianificare scansioni usando un software anti-virus.***
Riferimento Syllabus 2.3.3	***Comprendere il termine quarantena e l'operazione di mettere in quarantena file infetti/sospetti.***
Riferimento Syllabus 2.3.4	***Comprendere l'importanza di scaricare e installare aggiornamenti di software, file di definizione di antivirus.***
Riferimento Syllabus 3.4.2	***Riconoscere buone politiche per la password, quali evitare di condividere le password, modificarle con regolarità, sceglierle di lunghezza adeguata e contenenti un numero accettabile di lettere, numeri e caratteri speciali.***
Riferimento Syllabus 4.1.1	***Essere consapevoli che alcune attività in rete (acquisti, transazioni finanziarie) dovrebbero essere eseguite solo su pagine web sicure.***
Riferimento Syllabus 4.1.2	***Identificare un sito web sicuro, ad esempio associato ad https, simbolo del lucchetto.***
Riferimento Syllabus 4.1.4	***Comprendere il termine "certificato digitale". Convalidare un certificato digitale.***
Riferimento Syllabus 4.1.6	***Selezionare impostazioni adeguate per attivare, disattivare il completamento automatico, il salvataggio automatico quando si compila un modulo.***
Riferimento Syllabus 4.1.7	***Comprendere il termine "cookie".***
Riferimento Syllabus 4.1.8	***Selezionare impostazioni adeguate per consentire, bloccare i cookie.***

Riferimento Syllabus 4.1.9	***Eliminare dati privati da un browser, quali cronologia di navigazione, file temporanei di internet, password, cookie, dati per il completamento automatico.***
Riferimento Syllabus 4.1.10	***Comprendere lo scopo, la funzione e i tipi di software per il controllo del contenuto, quali software per il filtraggio di internet, software di controllo genitori.***
Riferimento Syllabus 4.2.2	***Essere consapevoli della necessità di applicare impostazioni adeguate per la privacy del proprio account su una rete sociale.***
Riferimento Syllabus 5.1.1	***Comprendere lo scopo di cifrare, decifrare un messaggio di posta elettronica.***
Riferimento Syllabus 5.1.2	***Comprendere il termine firma digitale.***
Riferimento Syllabus 5.1.3	***Creare e aggiungere una firma digitale.***
Riferimento Syllabus 5.2.3	***Riconoscere metodi per assicurare la confidenzialità durante l'uso della messaggistica istantanea, quali cifratura, non divulgazione di informazioni importanti, limitazione di condivisione di file.***
Riferimento Syllabus 6.1.2	***Riconoscere l'importanza di avere una procedura di copie di sicurezza per ovviare alla perdita di dati, di informazioni finanziarie, di segnalibri/cronologia web.***
Riferimento Syllabus 6.1.4	***Effettuare la copia di sicurezza di dati.***
Riferimento Syllabus 6.1.5	***Ripristinare e validare i dati sottoposti a copia di sicurezza.***
Riferimento Syllabus 6.2.3	***Identificare i metodi più comuni per distruggere i dati in modo permanente, quali uso di trita documenti, distruzione di memorie di massa/dispositivi, smagnetizzazione, uso di utilità per la cancellazione definitiva dei dati.***
Contenuti della lezione	***In questa lezione vedremo: come gestire le nostre password, come utilizzare i programmi anti-malware, come correre meno rischi nelle attività in rete, come adoperare le funzioni del browser per assicurare un elevato livello di privacy, come organizzare ed effettuare copie di sicurezza e ripristinare i dati in caso di necessità.***

Riconoscere buone politiche per la password, quali evitare di condividere le password, modificarle con regolarità, sceglierle di lunghezza adeguata e contenenti un numero accettabile di lettere, numeri e caratteri speciali

L'utente viene riconosciuto da un sistema informatico quando presenta le proprie credenziali, costituite dal nome o identificativo dell'utente (ID) e dalla password. All'interno di un'organizzazione, come ad esempio un'azienda, le credenziali abiliteranno l'utente alle operazioni che gli sono consentite in base al suo ruolo, come accedere a procedure e informazioni tratte dagli archivi aziendali. Quando l'utente fornisce le proprie credenziali al sistema, avvia un processo di riconoscimento che viene definito come autenticazione ed è alla base della sicurezza informatica. Il processo di autenticazione dovrebbe garantire l'identificazione di chi L'utente viene riconosciuto da un sistema informatico quando presenta le proprie credenziali, costituite dal nome o identificativo dell'utente (ID) e dalla password. All'interno di un'organizzazione, come ad esempio un'azienda, le credenziali abiliteranno l'utente alle operazioni che gli sono consentite in base al suo ruolo, come accedere a procedure e informazioni tratte dagli archivi aziendali. Quando l'utente fornisce le proprie credenziali al sistema, avvia un processo di riconoscimento che viene definito come autenticazione ed è alla base della sicurezza informatica. Il processo di autenticazione dovrebbe garantire l'identificazione di chi

$@9x&%Yhò#_^uwq!!

Figura 12: Una buona password

L'identificativo dell'utente è generalmente pubblico. Pertanto la password costituisce l'unico elemento veramente critico del processo di autenticazione. L'assegnazione di identificativo e password segue regole diverse a seconda che si tratti della propria organizzazione, che ha la possibilità di verificare l'identità dell'utente “de visu” o di servizi Internet. Generalmente nell'ambito di un'organizzazione l'ID è imposto, mentre l'utente sceglie la propria password e ha la possibilità di cambiarla.

I servizi offerti via Internet possono lasciare libera la scelta dell'ID (sempre che non sia già stato scelto da un altro utente del servizio) ma imporre vincoli alla password. Se è il sistema ad assegnare la password, questa viene spedita all'utente per posta elettronica o sul cellulare. L'utente ha sempre la possibilità di cambiarla successivamente.

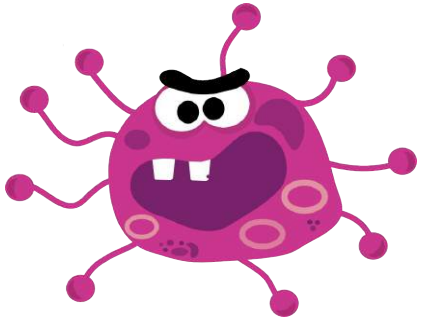
Esistono numerosi programmi destinati ad individuare le password e sono molto frequenti i tentativi fatti da

malintenzionati per accedere ai sistemi informatici violandone la sicurezza. E' quindi fondamentale seguire alcune politiche per scegliere e gestire la propria password. Una buona password (Figura 12) di norma:

- è lunga almeno 8 caratteri
- è composta da lettere, numeri e segni di interpunzione
- non è una parola di senso compiuto
- non contiene elementi comuni con l'ID
- non contiene nomi di familiari o date importanti per il proprietario
- non va scritta su un foglietto incollato sul video per ricordarsela
- va cambiata periodicamente. Si ricordi che può essere intercettata, senza che l'utente se ne accorga.

Comprendere come funziona il software anti-virus e quali limitazioni presenta

Per proteggere i propri dati da danni causati dai virus, è consigliabile avere sempre un anti-virus aggiornato e in esecuzione sul proprio computer in grado di intercettare ospiti sgraditi e impedire che possano infettare il computer oppure, se già presenti, in grado di individuarli e rimuoverli.



Non è vero che esistono soltanto virus per i sistemi operativi Windows ma è indubbio che questi sono più vulnerabili dal punto di vista della sicurezza e quindi maggiormente bersagliati da virus, anche per la loro maggior diffusione. Mentre è concepibile un computer con Linux o OS X senza anti-virus, non lo è uno con Windows.

Il programma anti-virus viene attivato al momento dell'accensione del computer e rimane attivo fino al suo spegnimento. Le sue funzioni principali sono di:

- eseguire costantemente una scansione della memoria centrale del computer (RAM) per individuare eventuali malware residenti, magari anch'essi attivati all'accensione
- eseguire periodicamente un controllo delle cartelle e dei file delle unità di memorizzazione fisse per identificare file contenenti malware, isolarli e impedire che compiano la loro azione

- effettuare il controllo delle unità mobili (chiavette USB per esempio), automaticamente quando inserite o a richiesta dell'utente. Questa azione è particolarmente importante visto l'uso che si fa delle chiavette USB per trasferire dati da un computer ad un altro.
- controllare i dati che vengono spediti o ricevuti tramite posta elettronica, con particolare attenzione al controllo degli allegati.

Le limitazioni degli anti-virus sono riconducibili ai metodi che adoperano per riconoscere la presenza di un virus in un file o in memoria, oltre che alla rincorsa permanente tra virus e anti-virus. Gli anti-virus infatti gestiscono un catalogo di tutti i virus censiti (detto file di definizione dei virus) e dei metodi per riconoscerli (detti pattern oppure firme) al quale confrontano il contenuto dei file o della memoria centrale. Possono così commettere due tipi di errore: non individuare un virus (perché troppo recente, per esempio) oppure segnalare la presenza di un virus in un programma che invece non lo contiene. Come vedremo fra poco, il primo errore si riduce tenendo costantemente aggiornato il programma anti-virus.

Eseguire scansioni di specifiche unità, cartelle, file usando un software anti-virus. Pianificare scansioni usando un software anti-virus

Per il sistema operativo Windows, esistono diversi tipi di programmi anti-virus: programmi gratuiti, programmi commerciali e addirittura un anti-virus fornito gratuitamente da Microsoft: Microsoft Security Essentials.

Per illustrare come eseguire scansioni e controlli, utilizzeremo questo programma. Potete scaricarlo liberamente dall'area Download (Download Center) del sito Microsoft e poi installarlo sul vostro computer, seguendo le indicazioni che avrete senz'altro letto nell'IBUQ *ECDL Computer Essentials*. Dopo l'installazione, il programma, è eseguito automaticamente all'avvio del PC e aggiorna costantemente il file di definizione dei malware.

Se disponete di un diverso software anti-virus, non installate quello Microsoft ma adoperate quello presente sul vostro computer. I comandi possono differire leggermente ma le funzioni sono sostanzialmente le stesse.

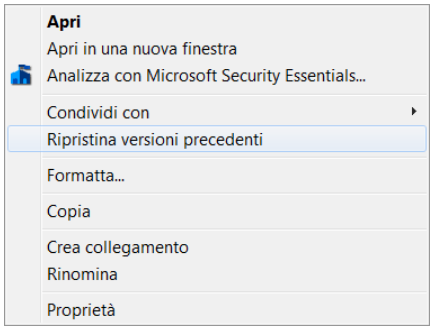


Figura 13: Scansione di un'unità

Oltre alle scansioni e controlli che il programma effettua automaticamente, potete richiedere l'esecuzione di scansioni a vari livelli: intera unità, cartella o singolo file.

Per richiedere la scansione di una specifica unità (per esempio un disco fisso, una chiavetta o unità esterna USB), è sufficiente:

- eventualmente collegare il dispositivo esterno (inserendo la chiavetta o l'unità a disco USB)
- aprire la finestra *Computer*
- fare click destro sull'unità desiderata
- nel menu che compare (Figura 13), scegliere la voce ***Analizza con Microsoft Security Essentials***
- compare una finestra (Figura 14) che presenta lo stato di avanzamento della scansione
- al termine, vengono visualizzati gli eventuali virus trovati.

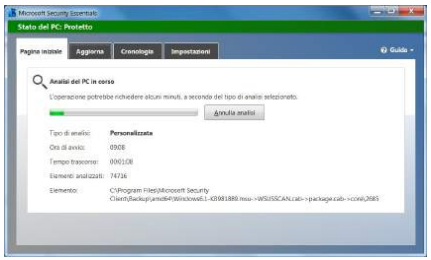


Figura 14: Avanzamento della scansione

Per richiedere la scansione di un'intera cartella, occorre:

- visualizzare la cartella di livello superiore che contiene la cartella da controllare
- fare click destro sull'icona della cartella
- procedere come prima.

Nello stesso modo, per effettuare la scansione di un singolo file si apre la cartella che contiene il file, si fa click destro sull'icona del file e si prosegue come prima.

E' possibile pianificare scansioni in modo che venga fatto periodicamente un controllo del PC scegliendo l'orario. Per questo, occorre:

- aprire il programma tramite l'icona Stato del PC presente nell'Area di notifica (in basso a destra dello schermo)
- nella finestra che compare, scegliere la scheda *Impostazioni* e la voce *Analisi pianificata* nella colonna di sinistra
- scegliere quindi il tipo di analisi (veloce o completa), il giorno e l'ora ed eventualmente il valore degli altri parametri
- al termine, cliccare sul pulsante *Salva modifiche*.

In questo modo, se il computer sarà accesso, verrà fatta un analisi delle unità per cercare eventuali malware nel giorno e ora specificati.

Comprendere il termine quarantena e l'operazione di mettere in quarantena file infetti/sospetti

Un malware può infettare diversi tipi di file: file contenenti dati dell'utente (per esempio inserendo una macro in un documento di testo), programmi applicativi, programmi di sistema, ... In tutti i casi, la cancellazione immediata del file da parte del programma antivirus al momento della sua individuazione potrebbe arrecare danni all'utente: perdita di dati, arresto del funzionamento del sistema operativo, ... Nella maggior parte dei casi invece, il programma antivirus pone il file infetto in quarantena ossia lo trasferisce in una cartella particolare, gestita dall'antivirus stesso e avvisa l'utente che può scegliere l'azione da compiere.

Si può così decidere se effettuare una pulizia del file, rimuovendo quando possibile il codice pericoloso e facendo uscire il file dalla quarantena, oppure ripristinare una copia non infetta del file e cancellare quello infetto.

Comprendere l'importanza di scaricare e installare aggiornamenti di software, file di definizione di antivirus

Va sottolineato che i virus alimentano una parte del mercato del software e sono sempre più evoluti: scrivere virus non è particolarmente difficile e in rete sono disponibili programmi per lo scopo. Ogni giorno nuovi virus vedono la luce e per questa ragione è importante che l'antivirus sia sempre aggiornato all'ultima versione. Come detto, la maggior parte dei virus sono concepiti per far danni al sistema operativo Windows: usare un sistema operativo basato su Linux o su Mac OS X riduce quasi a zero la possibilità di infezioni.

Riepilogando, le principali misure per proteggersi dai virus sono:

- avere sempre un programma antivirus aggiornato ed attivo mentre si lavora
- effettuare periodicamente un controllo completo del sistema inclusi allegati di posta, chiavette USB, ...
- in caso di dubbi utilizzare antivirus diversi e specializzati per tipologie di infezione (adware, worm)
- non eseguire nessun programma di cui non si è certi della provenienza

- quando si scaricano programmi dalla rete, fare verifiche sul sito di provenienza
- disattivare la possibilità di eseguire macro in pacchetti applicativi
- non cliccare su link consigliati da amici in strani messaggi via mail o via messaggeria istantanea.

Le password sono tipicamente adoperate per proteggere l'accesso a siti o servizi di rete. Possono anche essere adoperate per singoli file.

Impostare una password per file quali documenti, file compressi, fogli di calcolo

I documenti di testo e i fogli di calcolo possono essere protetti tramite una password. In questo caso vengono cifrati al momento della registrazione e possono essere aperti soltanto da chi conosce la password. Anche se questo non costituisce un livello di sicurezza molto alto, impedisce a chi dovesse entrare in possesso del documento di accedere immediatamente ai contenuti.

Per impostare una password ad un documento di testo di LibreOffice, creato con Writer, è sufficiente:

- aprire il documento con Writer
- selezionare il menu ***File / Salva con nome*** (oppure ***File / Salva*** nel caso di un documento nuovo)
- nella finestra *Salva con nome* che compare, selezionare l'opzione *Salva con password* (Figura 15) e confermare con *Salva*
- viene richiesta la password, ripetuta per conferma (Figura 16)
- al termine, confermare con *OK*.

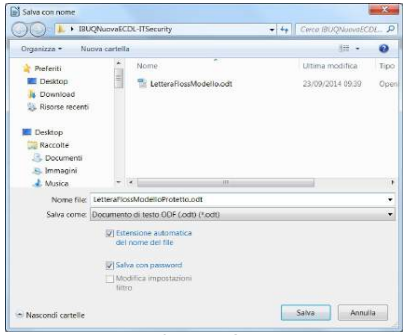


Figura 15: La finestra Salva con nome

Al momento della riapertura del documento, Writer chiederà di inserire la password segnalando l'eventuale password errata.

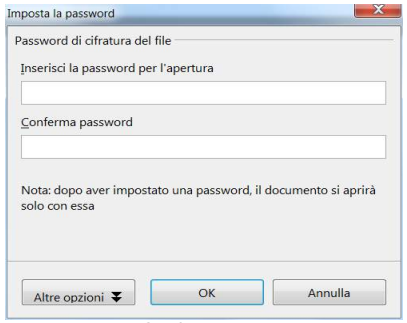


Figura 16: Conferma della password

Per impostare una password ad un foglio elettronico di LibreOffice,creato con Calc, oppure ad una presentazione creata con Impress, si procede nello stesso modo.

Come si può eliminare una password precedentemente inserita in un documento? Per questo è sufficiente salvare il file deselezionando l'opzione *Salva con password*.

Una procedura simile può essere applicata per proteggere un file compresso. Spesso i file compressi sono adoperati per raggruppare in un unico file intere cartelle: in questo modo con una sola password si protegge l'insieme dei file contenuti nel file compresso. La procedura dipende dal programma utilizzato. Contrariamente a Windows XP, Windows 7 non dispone di una funzionalità semplice per proteggere le cartelle compresse con una password ma esistono diversi programmi Open Source o commerciali che possono essere utilizzati. Uno dei più diffusi programmi di compressione/decompressione Open Source è 7-Zip (www.7-zip.org)

Con questo programma, per creare un file compresso ed assegnargli una password occorre:

- selezionare gli elementi da comprimere (cartella, singolo file o gruppo di file)
- fare click destro sulla selezione e scegliere la voce di menu ***7-Zip / Add to archive***
- compare la finestra nella quale si possono scegliere le diverse opzioni per la compressione (Figura 17). Nella sezione *Cifratura* si trovano le opzioni utili per la gestione della sicurezza:
  - *Inserisci password* e *Reinserisci password*, per assegnare una password al file compresso e cifrarlo
  - *Cifra anche il nome dei file* (per una maggior sicurezza, se si usa 7-Zip anche per decomprimerlo)
- confermare con il pulsante *OK*
- al termine viene creato il file compresso.

Comprendere l'effetto di attivare/disattivare le impostazioni di sicurezza delle macro

I programmi di produttività individuale (trattamento testi, fogli elettronici, presentazioni) hanno ormai raggiunto un livello tale di sofisticazione e una ricchezza tale di funzionalità che dispongono di centinaia di comandi, voci di menu, tasti funzione e icone. Per agevolare il lavoro dell'utente possono registrare sequenze di comandi (tasti, funzioni, voci di menu, ...) e rieseguirle su semplice richiesta dell'utente, evitandogli così di eseguire manualmente sequenze lunghe, complesse e ripetitive. Queste sequenze, denominate *macro*, sono memorizzate come una vera e propria sequenza di istruzioni. Tant'è che le diverse applicazioni sono dotate di un vero e proprio linguaggio di programmazione, utilizzabile dall'utente evoluto per arricchire le funzionalità delle macro e automatizzare, anche in modo spinto, le elaborazioni da svolgere. Mentre alcune macro vengono eseguite solo su esplicita richiesta dell'utente, altre possono essere state create da qualche autore malevolo in modo da attivarsi all'insaputa dell'utente se compie qualche azione o semplicemente al momento in cui esso apre il documento.

Se da un lato facilitano l'attività dell'utente, dall'altro possono rappresentare un pericolo: potenzialmente si potrebbe ricevere un file con una macro contenente istruzioni pericolose in grado di danneggiare dati presenti nel computer. Per questo, i programmi di produttività dispongono di funzionalità che permettono all'utente di scegliere il livello di sicurezza delle macro e di allerta in caso di presenza di macro nel file. Al momento dell'apertura del file, può decidere inoltre se abilitare o disabilitare le macro presenti nel file.

In LibreOffice, si può scegliere il livello di sicurezza delle macro presenti nei documenti. Per questo occorre:

- selezionare il menu ***Strumenti / Opzioni***
- nella finestra che compare, scegliere nella colonna di sinistra la voce *LibreOffice / Sicurezza*
- cliccare sul pulsante *Sicurezza delle macro*
- si può così impostare il livello di sicurezza delle macro (Figura 18).

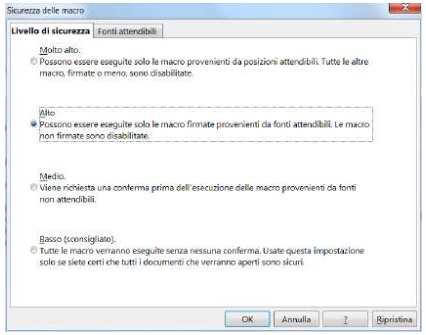


Figura 18: I livelli di sicurezza delle macro

Si consiglia di mantenere il più alto livello di sicurezza possibile, compatibilmente con l'uso abituale che si fa di LibreOffice. Aprendo un documento che contiene macro, a seconda del livello di sicurezza possono comparire messaggi di avviso relativi alle macro (Figura 19).

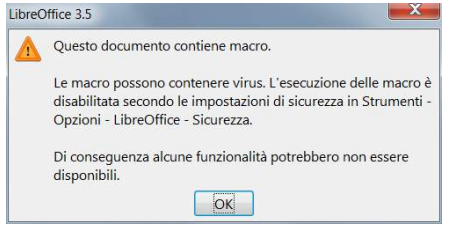


Figura 19: Attenzione. Possibile pericolo!

E' vero che "Il pericolo viene dalla rete"?

Con l'aumento della diffusione di Internet, diventa sempre più facile entrare in contatto con persone con le quali altrimenti non si sarebbe mai comunicato. Aumenta naturalmente il rischio che tali persone siano malintenzionate e approfittino dell'immediatezza offerta dallo strumento informatico per commettere qualche reato a danno dell'utente sprovveduto. E' importante d'altro canto non demonizzare Internet né pensare che sia la causa dei reati che vengono perpetrati per il suo tramite. Internet è solo uno strumento di comunicazione, Così come altri strumenti tecnologici sono stati utilizzati per delinquere quando sono nati (telefono, cassette video, ...) anche Internet viene adoperato agli stessi fini. Truffe e raggiri esistevano ben prima di Internet, così come le prepotenze, le molestie e la diffusione di contenuti proibiti dalla legge.

Senza voler esagerare, è indubbio che alcune delle attività che svolgiamo in rete sono più sensibili di altre e richiedono maggiori cautele. Sono soprattutto quelle che hanno risvolti finanziari: gli acquisti (e-commerce) e le operazioni bancarie (e-banking).

Essere consapevoli che alcune attività in rete (acquisti, transazioni finanziarie) dovrebbero essere eseguite solo su pagine web sicure

Queste operazioni più delicate devono essere eseguite soltanto su pagine web sicure. La sicurezza dei siti e delle loro pagine è legata a due fattori:

- *la notorietà e l'autorevolezza del sito*. Senza voler fare pubblicità, fare acquisti sul sito *www.amazon.it* è meno rischioso che sul sito *www.vienniquikessicompramelio.ng*.
- *le misure di sicurezza che il gestore del sito ha messo in opera*. Le misure di sicurezza tecniche verranno esaminate nei punti successivi e riguardano principalmente la cifratura dei dati trasmessi e l'identificazione del proprietario del sito.

Per quanto riguarda la notorietà del sito al quale ci si collega, va sempre prestata molta attenzione a collegarsi effettivamente al sito reale e non a qualche sito *fake* (fasullo) che ha lo scopo di carpire codice utente e password, magari con qualche tentativo di pharming (vedere punto 4.1.3). Nell'e-banking e le transazioni finanziarie, i rischi sono ridotti grazie al basso numero di banche alle quali ci colleghiamo e alle misure di sicurezza aggiuntive poste in opera dalle banche stesse.

Alcune osservazioni vanno fatte invece sugli acquisti online (e-commerce), anche perché il settore non è regolamentato come quello delle banche e il numero di negozi online è in costante crescita. Anche se l'Italia non è fra i primi paesi per diffusione, è indubbio che il commercio elettronico ha raggiunto dei livelli significativi e che tutte le stime lo danno in costante crescita nei prossimi anni. Crescita rallentata nel nostro paese dalla diffidenza da parte dei privati e dai timori legati proprio al pagamento online. Quali sono i rischi degli acquisti fatti tramite e-commerce? Si pensa prevalentemente a quelli legati al pagamento online con carta di credito: "non mi fido a comunicare i dati della mia carta di credito" è un motivo ricorrente. Va sottolineata l'importanza di rivolgersi a siti noti e di elevata reputazione che dispongono di sistemi di sicurezza molto sofisticati che rendono il furto di dati personali e finanziari molto difficili. Non altrettanto si può dire di tutti i siti di vendita online: quelli più "artigianali" investono probabilmente meno nella sicurezza.

In realtà esistono altri rischi, spesso sottovalutati che non sono legati ai pagamenti online. Per esempio quello di mancata consegna della merce o di consegna di merce di qualità più bassa di quella attesa o pubblicizzata. Immaginate, allettati da prezzi particolarmente bassi, di ordinare un bene, effettuare il

pagamento e non ricevere la merce. Se il bene è di moderato valore, l'azienda è all'estero e non risponde alle mail o vi assicura che si tratta solo di un piccolo ritardo, le vostre possibilità di ricorso sono pressoché nulle. Diffidate quindi da prezzi troppo bassi per essere veri, da siti in cui non si capisce bene dove è la sede del beneficiario del pagamento, di quelli che effettuano l'addebito al momento dell'ordine e non della spedizione.

Siete spaesati e rimanete timorosi?

Se volete essere più tranquilli, prima di effettuare un acquisto, cercate con un motore di ricerca informazioni sull'azienda alla quale vorreste rivolgervi, in particolare forum dove potete trovare pareri scritti da utenti. Se questi sono tutti positivi, cercate di capire se sono reali ma se sono proprio negativi, cercate un altro negozio.

Un ultimo consiglio operativo: se vi autenticate con nome utente e password ad un sito per effettuare operazioni (per esempio alla vostra banca o a un sito di e-commerce dove avete registrato la vostra carta di credito per velocizzare gli acquisti) ricordatevi sempre di disconnettervi dal sito in modo che non rimanga la sessione aperta. Impedirete così a chi dovesse usare il personal computer dopo di voi di effettuare delle operazioni a voi non gradite!

Veniamo alle vere e proprie misure di sicurezza tecniche, messe in opera dal gestore del sito.

Identificare un sito web sicuro, ad esempio associato ad https, simbolo del lucchetto

Il tema della sicurezza su Internet costituisce uno dei problemi più sentiti e presenta numerose sfaccettature. Una di queste è la riservatezza delle informazioni. Nella maggior parte dei casi le informazioni che otteniamo da Internet sono pubbliche. In compenso sono sempre più numerosi i servizi e le applicazioni che richiedono che le informazioni che trasmettiamo o riceviamo tramite browser non siano leggibili da altri. Ed è proprio il caso delle applicazioni che hanno risvolti finanziari: applicazioni di commercio elettronico in cui inviamo i dati della nostra carta di credito oppure e-banking, anche solo per consultare la posizione del nostro conto corrente.

Figura 20: Protocollo sicuro

Fra i numerosi sistemi di protezione che coprono i diversi aspetti della sicurezza, è basilare quello della criptazione dei dati scambiati dal sito web al proprio browser. Se le informazioni viaggiassero "in chiaro", chi dovesse sbirciare quanto passa sulla nostra linea di collegamento ad Internet potrebbe vedere molto facilmente tutte le informazioni. Se vengono criptate, sono molto più difficilmente riconoscibili e decifrabili.

Per questo, i siti che vogliono garantire questo livello di sicurezza adoperano per lo scambio di informazioni il protocollo https (HyperText Transfer Protocol over Secure Socket Layer) al posto del protocollo http abituale, garantendo così che le informazioni scambiate siano criptate, con un elevato livello di sicurezza.

L'attivazione, da parte del sito web, di questa protezione è riconoscibile da due elementi:

- la presenza di https:// nell'indirizzo della pagina (Figura 20)
- la visualizzazione di un lucchetto, nella Barra di navigazione di Firefox a sinistra dell'indirizzo della pagina (Figura 21).

Figura 21: Il lucchetto

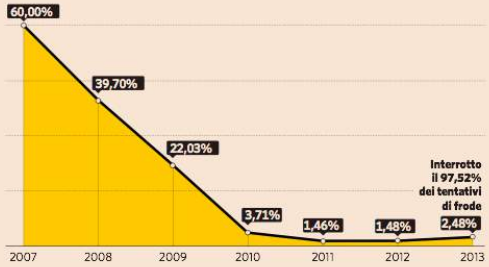
Più precisamente, in Mozilla Firefox il simbolo che compare a sinistra dell'indirizzo del sito nella Barra di navigazione può essere di tre tipi, a seconda del livello di sicurezza (Figura 22):

- il *mappamondo grigio*: indica una connessione non cifrata, non sicura ad un sito che non fornisce informazioni di identificazione
- il *lucchetto grigio*: indica una connessione cifrata, considerata sicura, e un sito che è stato verificato, anche se non c'è la certezza di chi ne sia il titolare
- il *lucchetto verde*: indica una connessione cifrata, considerata sicura, e un sito che è stato verificato, così come l'identità del titolare al quale risulta appartenere il sito.

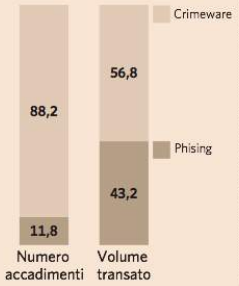
Figura 22: I vari livelli di sicurezza

Anche se questo è lontano dal risolvere tutti i problemi di sicurezza, lo si può considerare come un requisito basilare e di conseguenza aver l'accortezza di non trasmettere o ricevere informazioni riservate se non vi è almeno questo livello di protezione. In assenza di lucchetto, grigio o verde, è preferibile non effettuare operazioni che prevedono l'invio di dati personali e/o finanziari.

CLIENTI RETAIL ATTIVI CHE HANNO PERSO DENARO PER LA PERDITA DI CREDENZIALI
Trend 2007-2013. *Valori in %*

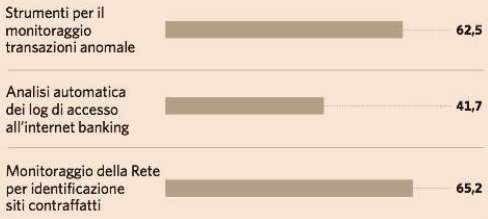


MODALITÀ DI ATTACCO
Tentativi e volume per tipologia. *In %*



COSÌ LE BANCHE INFORMANO I CLIENTI
Strumenti utilizzati, risp. multiple. *In %*

IL MONITORAGGIO DELLE TRANSAZIONI: LE DOTAZIONI TECNOLOGICHE UTILIZZATE
Strumenti messi in campo delle banche. *Risposte in % sul campione*



Fonte: ABI Lab, 2014

Serve buon senso per tutelarsi da sé

Aggiornare l'antivirus, evitare di cliccare su siti, codici e link ignoti, usare password diverse Occhio ai social network

Gabriele Petrucciani

■ Dal *phishing* al *malware*, fino ad arrivare al *crimeware*. Gli attacchi degli *hacker* ai nostri dati personali sono molteplici. Oggi ci sono talmente tanti virus che l'attenzione deve rimanere sempre alta. Certo, le nuove generazioni sono più preparate, soprattutto da un punto di vista informatico. Ma non basta per sentirsi protetti al 100 per cento. A volte anche i più esperti, per fare un esempio, disabilitano, seppure per un attimo, l'antivirus sul proprio computer per accelerarne le prestazioni e concludere più velocemente una transazione. In questo modo, però, ci si espone all'attacco dei pirati informatici, che può avvenire nei modi più disparati.

«Con una mail – fa notare Domenico Raguseo, manager delle vendite tecniche per l'Europa dei sistemi di sicurezza di Ibm – ma anche attraverso gli *short link*, nati per facilitare l'utilizzo dei dispositivi mobili, o ancora attraverso i *QR code* (i codice a barre bidimensionali, spesso a forma di quadrato, *ndr*)», che potrebbero ricondurre a siti malevoli in grado di infettare il proprio dispositivo, mobile o fisso.

Per tutelarsi al meglio occorre in primis buon senso. «Parlando di *fishing* – sottolinea Paolo Frizzi, amministratore delegato di Libraesva, società attiva nell'ambito delle soluzioni avanzate di *email security* – bisogna sempre ricordarsi che le società con cui siamo legati, tipo le banche per il conto corrente o le compagnie telefoniche, hanno già i nostri dati. Quindi dobbiamo sempre diffidare dalle email che per esempio riceviamo dal nostro istituto di credito e in cui ci viene chiesto di inserire nuovamente i dati personali». Inoltre, quando si naviga sul web, o si fanno delle transazioni nel mondo virtuale, è fondamentale accertarsi dell'esistenza di un protocollo di sicurezza, «che può essere verificato controllando che all'inizio dell'indirizzo internet ci sia la sigla https:// o il simbolo del lucchetto», aggiunge ancora Frizzi.

In linea generale, comunque, per evitare di incappare in *malware* o *crimeware* è consigliabile dotare il proprio pc di un buon antivirus, mantenendolo sempre aggiornato. «Una pratica da seguire anche sui dispositivi mobili – puntualizza il ceo di Libraesva – soprattutto su quelli Android. Sui device Apple, che adottano un sistema operativo chiuso, prendere un virus è quasi impossibile. Android, invece, è un sistema aperto, e il processo di approvazione delle applicazioni è meno severo. Quindi è più facile imbattersi in App malevole».

Al di là degli aspetti più tecnologici, ci sono anche una serie di buone pratiche che è consigliabile seguire, «evitando, per esempio, di utilizzare la stessa password per social network e applicazioni, anche bancarie – continua Raguseo di Ibm –. Ancora, le *password* non dovrebbero mai richiamare i propri dati, come la propria data di nascita o quella dei figli. Inoltre, bisogna prestare molta attenzione a cliccare *short link* o a fotografare *QR code* provenienti da sconosciti». Potrebbero contenere un virus capace di catturare, attraverso *screenshot* o la registrazione delle sequenze dei tasti digitate, i dati di accesso all'*home banking*. Occhio, infine, a collegarsi a reti wi-fi aperte; dietro potrebbe nascondersi uno dei tanti hacker spia.

Comprendere il termine "certificato digitale". Convalidare un certificato digitale

Oltre alla necessità della riservatezza delle informazioni scambiate, assicurata dalla loro criptazione, sussiste un altro requisito: quello della identificazione del sito. L'identificazione sicura del sito al quale ci si collega è di fondamentale importanza per evitare di cadere in truffe varie e tentativi di frode informatica quale il *phishing*, basato su imitazioni di siti web, prevalentemente bancari, per carpire codice utente e password di accesso.

Il tema dell'identificazione è una problematica generale nelle comunicazioni informatiche nella quale ricade l'identificazione dei siti web. Lo strumento adoperato è lo stesso e si basa sul concetto di certificato digitale.

Un certificato digitale è un documento elettronico, rilasciato da un ente certificatore, che identifica il titolare e contiene diverse informazioni, fra le quali una chiave usata per crittografare le informazioni. Al momento del collegamento ad un sito con modalità https, viene inviato il certificato al browser, rendendo così disponibili all'utente le informazioni certificate sul sito web. Viene inoltre utilizzata la chiave per criptare la trasmissione delle informazioni scambiate.

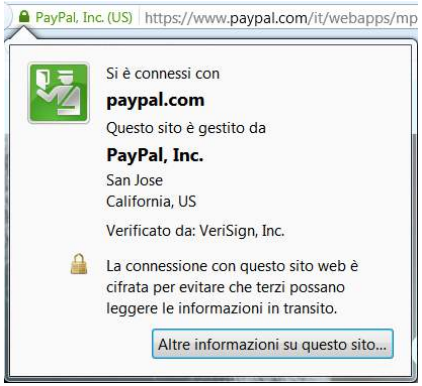


Figura 23: Il certificato digitale

L'utente può verificare manualmente il certificato. Per questo deve:

- fare click sul lucchetto che compare nella Barra di navigazione del browser
- compare una finestra con le informazioni più importanti (Figura 23)
- cliccare sul pulsante *Altre informazioni su questo sito...*
- nella finestra successiva compaiono altre informazioni (Figura 24)
- cliccando sul pulsante *Visualizza certificato*, si accede ai dati di dettaglio del certificato digitale (Figura 25).

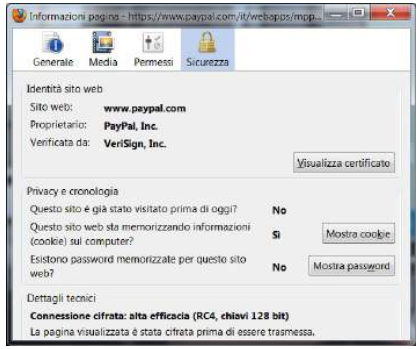


Figura 24: Altre informazioni sul sito

L'insieme di queste informazioni presenti nel certificato digitale permette di convalidare l'identità del proprietario del sito.

Ricordiamo che, in assenza di protezioni particolari attivate sul server che ospita il sito web, collegandoci ad un sito le informazioni che inviamo vengono trasmesse così come le digitiamo e le informazioni che riceviamo (e visualizziamo nel browser) vengono trasmesse così come visibili nella pagina web. Questo significa che chi si intromettesse sulla linea di collegamento potrebbe leggere abbastanza facilmente le informazioni scambiate tra browser e sito.

La responsabilità della sicurezza non ricade solo sul proprietario del sito ed anche l'utente deve assumersene l'onere. L'utente interagisce con i siti web con il browser ed è tramite il browser che può tutelarsi ad aumentare il livello di sicurezza della sua navigazione.

Il nome *personal computer* evoca un computer adoperato da una sola persona. In realtà, sono sempre più numerosi i PC pubblici, condivisi da un numero non ben definito di persone: si pensi a quelli di una biblioteca o di un'aula informatica in una Scuola. L'uso da parte di più persone aumenta i requisiti di sicurezza, senza i quali chi usa PC può accedere alle "tracce informatiche" lasciate dall'utilizzatore precedente. E queste tracce informatiche potrebbero contenere dati riservati: un caso è quello dei dati che si inseriscono nei moduli presenti nelle pagine web per permettere l'interazione dell'utente.

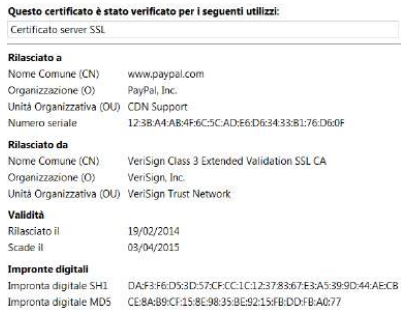


Figura 25: Informazioni di dettaglio sul certificato

Selezionare impostazioni adeguate per attivare, disattivare il completamento automatico, il salvataggio automatico quando si compila un modulo

Mozilla Firefox è un browser che permette una gestione piuttosto articolata della sicurezza e della propria privacy. Consente infatti sia di scegliere quali informazioni memorizzare per la comodità dell'utente, sia di cancellare selettivamente i dati mantenuti in memoria. Per quanto riguarda i moduli, la memorizzazione delle informazioni ha il vantaggio che possono essere reinseriti in un nuovo modulo senza doverli ridigitare (si ha così il completamento automatico del campo che accoglie il dato) ma presenta l'inconveniente che chi utilizza successivamente il computer potrebbe vedere le informazioni che sono state inserite in precedenza.

Per gestire il livello di memorizzazione delle informazioni relative ai moduli, occorre:

- selezionare il menu ***Strumenti / Opzioni*** (in Linux si usa invece ***Modifica / Preferenze***)
- nella finestra che compare, scegliere la scheda *Privacy* (Figura 26)
- nella sezione *Cronologia*, alla voce *Impostazioni cronologia*, scegliere *Utilizza impostazioni personalizzate*
- nella sezione che compare, mettere o togliere un segno di spunta alla voce *Conserva la cronologia delle ricerche e dei moduli* per attivare o disattivare la memorizzazione delle informazioni
- confermare premendo il pulsante *OK*.

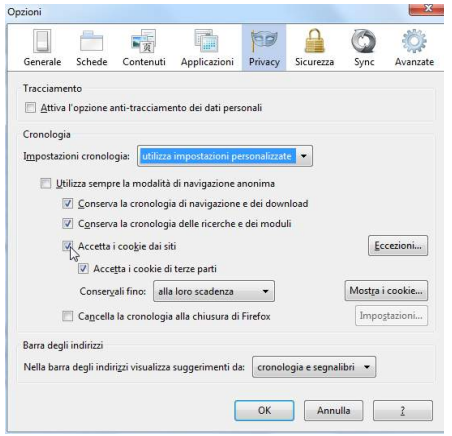


Figura 26: Strumenti / Opzioni / Privacy

Comprendere il termine "cookie"

I siti ai quali si accede durante la consultazione delle pagine web possono registrare informazioni sul personal computer dell'utilizzatore e sempre di più lo fanno. Queste informazioni sono memorizzate, tramite il browser, in piccoli file chiamati cookie, come i dolci con briciole di cioccolato (Figura 27). Sono spesso utilizzati per evitare di richiedere più volte le stesse informazioni all'utilizzatore memorizzandole per un certo periodo di tempo.

Alcuni esempi possono illustrarne gli usi principali:

- una volta inseriti il codice utente e la password, le informazioni di riconoscimento vengono memorizzate e non vengono più richieste per un certo periodo
- in un sito di commercio elettronico, la lista dei prodotti che si stanno comprando può essere memorizzata sotto forma di cookie nel cosiddetto "carrello"
- la prima volta che si accede ad un sito vengono chieste all'utilizzatore - e memorizzate - informazioni che ne consentono il riconoscimento da parte del sito le volte successive e permettono per esempio al sito di scrivere Ben tornato anziché Benvenuto.

A fianco degli usi legittimi, i cookie si prestano ad usi meno corretti da parte di siti che possono registrare informazioni a carattere personale, spesso all'insaputa dell'utente. L'utente deve quindi essere in grado di gestire i cookie in base al livello di sicurezza che desidera, con la possibilità di accettare o rifiutare i cookie, globalmente o selettivamente per alcuni siti. Inoltre deve essere in grado di cancellarli quando lo ritiene opportuno.

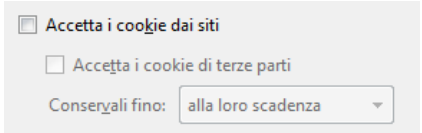


Figura 28: Non accettare i cookie dai siti

Come impostazione standard, Firefox accetta i cookie da tutti i siti.

Selezionare impostazioni adeguate per consentire, bloccare i cookie

Per bloccare i cookie provenienti da tutti i siti, occorre:

- selezionare il menu ***Strumenti / Opzioni*** (in Linux si usa invece ***Modifica / Preferenze***)
- nella finestra che compare, scegliere la scheda *Privacy* (Figura 26)
- nella sezione *Cronologia*, alla voce *Impostazioni cronologia*, scegliere *Utilizza impostazioni personalizzate*
- nella sezione che compare, togliere il segno di spunta dalla voce *Accetta i cookie dai siti* (Figura 28)
- confermare premendo il pulsante *OK*.

Da questo momento, i cookie non vengono più accettati dai siti né registrati sul personal computer dell'utilizzatore. Per accettare o bloccare i cookie provenienti solo da alcuni siti scelti, occorre procedere come prima e nella sezione dedicata ai cookie scegliere le opzioni desiderate, per esempio inserendo alcuni siti come eccezioni alla regola del blocco totale. Da questo momento, i cookie vengono accettati o bloccati a seconda delle regole inserite.

Per consentire la memorizzazione di tutti i cookie, si riattiva l'opzione *Accetta i cookie dai siti*.

Vedremo al successivo punto 4.1.9 come si possono cancellare i dati dei moduli precedentemente memorizzati.

Firefox è un browser molto attento alla sicurezza ma ha la memoria lunga. Registra infatti molte informazioni su quanto avviene durante la navigazione che sono accessibili a chi dovesse utilizzare il computer dopo di noi se non vengono rimosse. Per esempio la cronologia delle pagine visitate, alcuni contenuti delle pagine stesse. Addirittura, come vedremo, delle password di siti ...

Eliminare dati privati da un browser, quali cronologia di navigazione, file temporanei di internet, password, cookie, dati per il completamento automatico

Ogni volta che si visualizza una pagina web, il browser ne memorizza l'URL e il titolo. La Cronologia non è nient'altro che l'elenco delle pagine visitate di recente e permette all'utente di ripercorrere la navigazione fatta e di tornare a pagine precedentemente visualizzate. Mentre questa funzionalità risulta particolarmente utile, può creare problemi in termini di riservatezza dei dati personali. Chiunque acceda al personal computer, aprendo il browser, può vedere quali siti e pagine sono stati consultati. Cancellare dati dalla Cronologia serve pertanto a eliminare una o più pagine dall'elenco delle pagine visualizzate e impedire che si possa risalire a tali informazioni.

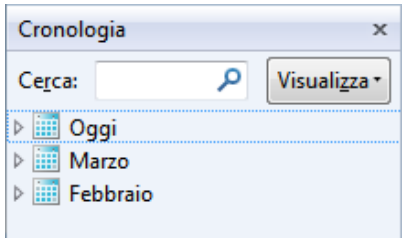


Figura 29: La Cronologia

Per cancellare parte della Cronologia, occorre:

- selezionare il menu ***Visualizza / Barra laterale / Cronologia*** (oppure premere **Ctrl + H**)
- compare sul lato sinistro la Cronologia (Figura 29)
- fare click destro sulla pagina che si desidera rimuovere dalla Cronologia
- dal menu contestuale che compare (Figura 30), scegliere la voce *Elimina*
- viene cancellato il riferimento dalla Cronologia.

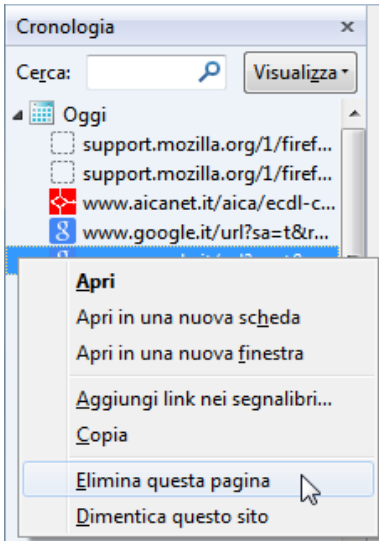


Figura 30: Elimina dalla Cronologia

La Barra di navigazione di Firefox memorizza le pagine più frequentemente consultate. Per accedervi, occorre:

- cliccare sull'icona con il triangolino nero rivolto verso il basso, presente all'estremità destra della Barra di navigazione
- compare un menu a discesa delle pagine più consultate
- posizionare il cursore del mouse sulla voce da cancellare (Figura 31)
- premere il tasto **Canc**
- viene cancellato il riferimento alla pagina.

Volendo invece cancellare tutta la cronologia, occorre:

- selezionare il menu ***Strumenti / Cancella la cronologia recente*** (oppure premere **Ctrl + Maiusc + Canc**)
- dalla finestra che compare (Figura 32), scegliere il periodo di tempo che si vuole cancellare

- premere il pulsante *Cancella adesso*
- vengono eliminate tutte le pagine dalla Cronologia.

Cancellare i dati dei moduli precedentemente memorizzati ci impedisce di usufruire del completamento automatica ma impedisce a chi dovesse accedere al computer di vedere i dati inseriti. Per cancellare tali dati, è sufficiente:

- selezionare il menu ***Strumenti / Cancella la cronologia recente*** (oppure premere **Ctrl + Maiusc + Canc**)
- dalla finestra che compare (Figura 32), scegliere il periodo di tempo che si vuole cancellare
- selezionare la sola voce *Moduli e ricerche*
- premere il pulsante *Cancella adesso*
- vengono eliminate tutte le informazioni relative ai moduli (e alle ricerche effettuate).

Nella stessa finestra compaiono diverse voci (Figura 33) che possono essere utilizzate per eliminare diversi elementi della cronologia, sempre scegliendo il periodo temporale desiderato.

Di conseguenza per eliminare i file temporanei di Internet (la cosiddetta cache), i cookie o i dati dei moduli, si seleziona rispettivamente in questa finestra le voci Cache, Cookie e Moduli e ricerche. In questo stesso modo, si sarebbe potuto anche cancellare la Cronologia delle pagine consultate.

Cosa ne è delle password?

Per molti sono un incubo: ricordarsi tutte le password - soprattutto adesso che si applicano le regole viste al punto 3.4.2 - è un'impresa! Dover digitare queste sequenze interminabili di segni! Allora quando Firefox ci viene in aiuto proponendo di salvare le password di accesso ai siti, come resistere?

Riconoscendo che stiamo inserendo un codice utente e una password in una pagina web, ci propone una scorciatoia per le volte successive munita di un bel pulsante *Ricorda la password* (Figura 34). Come dire di no? Peccato che pochi sappiano che:

- non solo viene memorizzata la password, ma anche il codice utente
- la password viene memorizzata in chiaro
- se il proprietario del computer non adotta opportuni accorgimenti, chi usa il computer successivamente può vedere tutte le password salvate.

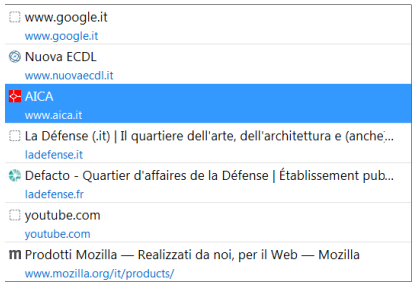


Figura 31: Pagine più frequenti

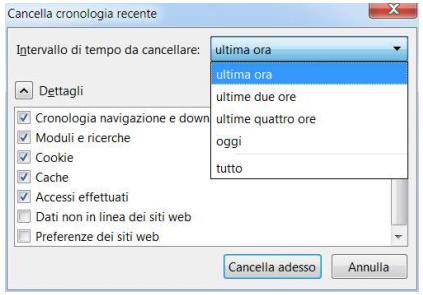


Figura 32: Elimina i file Internet temporanei

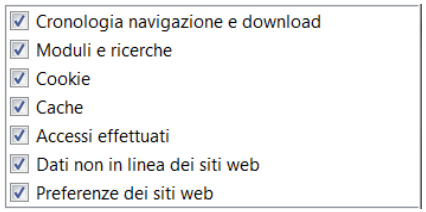


Figura 33: Opzioni per la cancellazione

Per questo, è sufficiente:

- selezionare il menu ***Strumenti / Opzioni***
- scegliere la scheda *Sicurezza*
- cliccare sul pulsante *Password salvate*
- nella finestra che compare, vengono visualizzati i siti per i quali è stata salvata la password (Figura 35) e relativo codice utente
- cliccare sul pulsante *Mostra password* per visualizzare le password.

Figura 34: Vogliamo salvare la password?

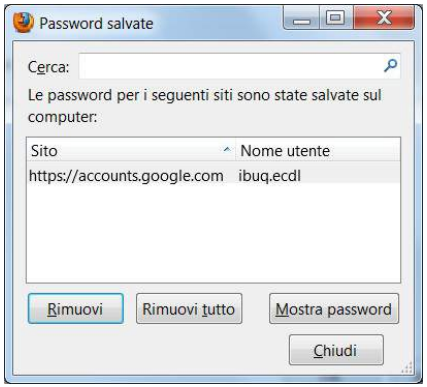


Figura 35: Password salvate

Nella stessa finestra, sono presenti i pulsanti di cancellazione di singoli siti e di cancellazione generale.

Due notizie di conforto:

- si può proteggere con una password l'accesso alla lista delle password (tramite l'opzione *Utilizza una password principale* nella scheda *Sicurezza* vista prima)
- in generale i siti sensibili (banche, ...) usano degli accorgimenti per l'accesso che impedisce la memorizzazione delle credenziali di autenticazione o il loro uso.

Comprendere lo scopo, la funzione e i tipi di software per il controllo del contenuto, quali software per il filtraggio di internet, software di controllo genitori

Tutti i computer aziendali sono collegati ad Internet ma molte aziende adottano sistemi per impedirne un uso ricreativo o non aziendale. Sotto certe condizioni, possono essere registrati gli indirizzi dei siti consultati e molto spesso è proprio inserito un sistema che impedisce la navigazione in particolari siti; siti di giochi online o siti contenenti materiale illegale (pornografia, pedofilia, opere soggetti a diritto d'autore, ...). Spesso sono bloccate le reti sociali, anche per vari abusi che sono stati raccontati da numerosi giornali. Oltre a limitazioni alla navigazione, sono frequenti le limitazioni allo scaricamento di file. L'elevata velocità dei collegamenti adoperati dalle imprese può indurre qualcuno a installare programmi di scaricamento peer-to-peer e approfittarne per scaricare filmati o brani musicali, non solo violando le leggi sul copyright ma anche peggiorando le prestazioni della linea. Queste limitazioni possono essere qualitative (non si scaricano certi tipi di file) o quantitative (non si scaricano file oltre ad un certa dimensione).

Una considerazione a parte meritano i sistemi di protezione destinati alla tutela dei bambini. L'uso da parte dei bambini e dei ragazzi, del computer, di Internet, dei videogiochi nonché degli strumenti elettronici e informatici in generale non può sempre essere lasciato alla loro libera scelta. Le limitazioni eventualmente introdotte dai genitori dipendono ovviamente dall'età dei figli. Si pensi alla televisione o ai videogiochi e al loro potere di coinvolgimento che rende impossibile per molti bambini e ragazzi autolimitarsi.

La necessità per bambini e ragazzi di diversificare le attività, di recepire gli stimoli educativi e formativi adatti alla propria età, di partecipare ad interazioni sociali "dal vivo" e non solo virtuali, induce i genitori ad esercitare una limitazione ed un controllo nel ricorso agli strumenti più "coinvolgenti". Non solo ma alcuni di questi strumenti non sono originariamente differenziati a seconda dell'età del fruitore. Basti pensare ai contenuti di Internet che sono tutti accessibili indiscriminatamente, senza distinzione di età, con forte possibilità di esposizione dei bambini e dei ragazzi a contenuti non adatti alla loro età. Per questo sono disponibili appositi software per regolarne le modalità di utilizzo, limitando il tempo di utilizzo o l'accesso a siti presenti in un apposito elenco. Per tutti però, è decisamente preferibile ricorrere a regole e interventi "umani" mirati piuttosto che a strumenti informatici automatizzati. Gli interventi di controllo e regolamentazione dipenderanno, come accennato, dall'età del bambino o del ragazzo ma saranno improntate a:

- evitare l'isolamento del bambino nell'uso degli strumenti, affiancandolo il più possibile durante l'utilizzo per indirizzarlo e per controllare l'aderenza dei contenuti alla sua età
- prevedere delle modalità di uso di questi strumenti "accompagnate" da un adulto
- definire delle limitazioni temporali nell'uso del computer, del collegamento a Internet, dei videogiochi a favore delle altre attività che devono svolgere bambini e ragazzi (attività sportive e scolastiche, ...)
- sensibilizzare bambini e ragazzi, in modo differenziato a seconda dell'età, sui contenuti e le possibilità di utilizzo della rete oltreché sui rischi e sugli accorgimenti da rispettare.

Saranno infatti più efficaci le limitazioni di uso se accompagnate da un affiancamento e da interventi di sensibilizzazione da parte dei genitori, piuttosto che la sola introduzione di sistemi automatici di filtro.

IL DECALOGO PER LA SICUREZZA ONLINE

1 **Attivare gli sms alert**
Si riceve un sms quando si accede al conto Internet, quando si fa un bonifico o quando si usa la carta.

2 **Proteggere i dati personali**
I dati come il pin delle carte o le password di accesso al proprio conto online vanno sempre protetti.

3 **Affidarsi a un antivirus**
Per proteggere i propri device, mobili e fissi, dai malware è consiglibile dotarsi di un buon antivirus.

4 **Selettivi sui social**
Numerosi social network, inclusi i più recenti, sono tra i principali bersagli per i tentativi di phishing.

5 **Verificare se il sito è sicuro**
Controllare che l'indirizzo web sia preceduto dalla sigla di sicurezza https:// e non da http://.

Comprendere lo scopo di cifrare, decifrare un messaggio di posta elettronica

Molti sistemi di posta elettronica inviano i messaggi in chiaro, ossia senza applicare tecniche crittografiche per cifrali. Questo significa che il messaggio è facilmente leggibile da chi dovesse intercettarlo, inserendosi per esempio nella rete del mittente o del destinatario e adoperando appositi programmi. Lo stesso dicasi per eventuali documenti allegati al messaggio.

Uno dei modi per rendere la posta elettronica uno strumento più sicuro è quello di cifrare il messaggio di posta al momento dell'invio. In questo modo il messaggio trasmesso verrà reso illeggibile a chi dovesse intercettarlo. Ovviamente l'operazione opposta, consistente nel decifrare il messaggio, dovrà essere fatta quando il messaggio verrà recapitato per consentirne la lettura al destinatario.

Per cifrare (e decifrare) messaggi di posta elettronica in modo trasparente per l'utente, esistono diversi programmi, liberi o commerciali, nonché servizi online.

Per quanto riguarda la sicurezza dei soli allegati, spesso si ricorre a metodi più semplici (anche se meno efficaci) consistenti nel proteggerli con una password e inviare la password al destinatario. L'invio della password, per motivi facilmente intuibili, va fatta con mail separata o con altri sistemi distinti dalla mail.

Si sta sempre di più diffondendo l'uso di protocolli di trasmissione più sicuri (cosiddetti SMTPS) che richiedono l'autenticazione dell'utente per l'invio di messaggi e cifrano la trasmissione dal client dell'utente al server che spedisce così come protocolli di ricezione (POPS, IMAPS) che rendono più sicura la lettura del messaggio dal server del destinatario al suo client di posta.

6 **Evitare link sospetti**
Diffidare delle email in cui la banca chiede di cambiare i propri dati personali cliccando su un link.

7 **Utilizzare reti wi-fi protette**
Dietro agli hotspot aperti si possono nascondere hacker che spiano le attività per rubare dati.

8 **Affidarsi a più password**
Utilizzare un'unica password per siti di e-commerce, conto online e social è altamente rischioso.

9 **Prudenza nell'uso del cloud**
È consigliabile agire con prudenza prima di mischiare documenti personali e di lavoro nel cloud.

10 **Controllare l'estratto conto**
Con un controllo regolare è possibile verificare che le transazioni riportate siano quelle effettuate.

Comprendere il termine firma digitale

Oltre al problema della scarsa riservatezza appena visto, la posta elettronica presenta anche il problema dell'identificazione del mittente. E' molto facile creare un messaggio di posta e spedirlo facendolo risultare come se fosse stato spedito da qualcun altro. La firma digitale sopperisce a questa carenza e permette di garantire l'identificazione del mittente. Non solo ma può essere applicata a documenti in formato elettronico, con tre benefici:

- *autenticità*. Il destinatario è sicuro dell'identità del mittente del documento
- *non ripudiabilità.* Il mittente non può negare di aver inviato il documento da lui firmato
- *integrità*. Il destinatario non può alterare un documento né crearne uno facendolo risultare firmato da qualcun altro.

Un sistema oggi largamente utilizzato è quello della Crittografia asimmetrica (o crittografia a chiave pubblica) accennato nel precedente punto 1.4.3.

Chi volesse saperne di più sulla firma digitale può far riferimento alle *Linee guida per l'utilizzo della Firma Digitale*, testo disponibile all'indirizzo https://ca.notariato.it//approfondimenti/LineeGuidaFD_200405181.pdf

Creare e aggiungere una firma digitale

Prima di poter apporre una firma digitale su un documento informatico, occorre disporre di una firma digitale. Per questo è necessario rivolgersi ad uno degli enti certificatori abilitati (l'elenco è disponibile sul sito dell'Agenzia per l'Italia Digitale, all'indirizzo http://www.agid.gov.it/).

Una volta ultimata la pratica, si dispone, fra l'altro, di un file contenente le informazioni che definiscono l'identità del titolare, la propria chiave pubblica e il periodo di validità del certificato stesso, oltre ai dati dell'ente certificatore che lo ha rilasciato. Questo file verrà utilizzato per firmare digitalmente i documenti tramite il software fornito in generale insieme al certificato.

In alternativa, una volta installato il certificato sul computer, si possono usare i software usuali per aggiungere la firma elettronica ad un documento.

In LibreOffice, per aggiungere una firma digitale ad un documento (creato con Writer, Calc o Impress), è necessario:

- aprire il documento
- selezionare il menu ***File / Firme digitali***
- nella finestra *Firme digitali* che appare cliccare sul pulsante *Firma documento*
- nella finestra, selezionare il certificato e premere sul pulsante *OK*
- di ritorno alla finestra *Firme digitali*, premere il pulsante *Chiudi*
- la firma viene aggiunta al documento e nella Barra di stato compare l'icona Firma digitale ad indicare lo stato della firma.

Analoga operazione si può svolgere con Thunderbird per apporre una firma digitale ai messaggi. Per questo occorre:

- installare il certificato nel programma di posta:
  - selezionando il menu ***Strumenti / Impostazioni account***
  - nella finestra *Impostazioni account*, scegliere la voce *Sicurezza* nella colonna di sinistra
  - nella sezione *Certificati* cliccare sul pulsante *Mostra certificati*
  - cliccare sul pulsante *Importa* per scegliere il file del certificato
- attivare l'uso del certificato:
  - di ritorno nella finestra *Impostazioni account*, nella sezione *Firma digitale*:
    - cliccare sul pulsante *Seleziona* e scegliere il certificato installato
    - attivare l'opzione *Apponi una firma digitale ai messaggi*.

Riconoscere metodi per assicurare la confidenzialità durante l'uso della messaggistica istantanea, quali cifratura, non divulgazione di informazioni importanti, limitazione di condivisione di file

Anche se non tutti su Internet sono sensibili e attenti alla riservatezza e alla protezione delle proprie informazioni, molti stanno prestando una crescente attenzione alla propria privacy. Un esempio fra tutti: ad inizio 2014, Facebook - noto per le sua attività di raccolta di informazioni personali e di profilazione degli utenti - ha acquistato il sistema gratuito di messaggistica istantanea WhatsApp. In seguito a questa operazione, molti utenti hanno abbandonato WhatsApp per passare ad altri sistemi come Telegram (https://telegram.org), emergente sistema di messaggistica, anch'esso gratuito, che assicura un elevato livello di sicurezza e riservatezza grazie alla cifratura dei messaggi.

Ricorrere ad un sistema che trasmette i messaggi in forma crittografata garantisce senz'altro un livello di sicurezza e di confidenzialità maggiore mettendo al riparo l'utente dalle intercettazioni. Ma questo è un aspetto esclusivamente tecnico che non esaurisce le misure di sicurezza.

La stessa condivisione di file, se non correttamente configurata, può mettere a disposizione di terzi delle informazioni che pensavamo essere al riparo da occhi indiscreti.

E' fondamentale infatti che chi utilizza Internet acquisisca una sensibilità alla protezione dei propri dati e alla non divulgazione delle informazioni personali. Come si può constatare dalla crescente diffusione degli attacchi di ingegneria sociale (si veda il punto 1.3.1) è spesso lo stesso utente che aiuta il malintenzionato a compiere frodi e altri illeciti, fornendogli informazioni riservate o sensibili. Involontariamente in un attacco di ingegneria sociale, volontariamente in caso di uso poco attento delle reti sociali. E' importante che la divulgazione di informazioni personali sia limitata allo stretto indispensabile e ai soli destinatari interessati.

Bisogna inoltre valutare attentamente:

- *il grado di importanza delle proprie informazioni*. Spesso si tende a pensare che certe informazioni siano poco rilevanti e possano essere divulgate senza cautele. Invece possono servire a creare un attacco di ingegneria sociale, sostituendosi più facilmente ad una persona

- *gli strumenti con i quali si scambiano informazioni*. Gli strumenti di condivisione di file (per esempio Drpbox) sono ritenuti tipicamente sicuri. Depositate un file troppo voluminoso per essere inviato per posta elettronica e mandate invece per posta elettronica o per messaggistica istantanea al vostro destinatario un link che gli permetterà di scarica il file. Il link, generato al momento in modo dinamico, è noto solo a lui e a chi ha compromesso la sua casella di mail o a chi ha intercettato il vostro messaggio istantaneo o a chi ...

Si raccomanda quindi di analizzare e valutare sempre bene il livello di sicurezza e di riservatezza nonché i rischi che dati personali possono correre.

Essere consapevoli della necessità di applicare impostazioni adeguate per la privacy del proprio account su una rete sociale

La partecipazione a una comunità virtuale e/o a una rete sociale spesso fornisce l'impressione di essere all'interno di un circuito protetto a cui possono accedere solo i nostri amici: questo può spingere le persone a rivelare molte informazioni, anche private, su di sé. Così come nella vita reale, anche in rete gli individui possono intendere le amicizie a diversi livelli, e così come possono nascere possono concludersi. Non va inoltre dimenticato che qualsiasi cosa scritta o pubblicata in rete non potrà mai essere cancellata: infatti anche se si cancella quella frase scritta in un momento di rabbia o quella foto imbarazzante, qualcuno potrebbe averla copiata su un altro server, rendendone difficile il reperimento o il controllo della diffusione.

Le reti sociali offrono un accesso gratuito ai propri servizi perché utilizzano le informazioni che ognuno fornisce a scopo di marketing: dichiarare le proprie preferenze o quali acquisti sono stati fatti serve per favorire la diffusione del passaparola che è considerato oggi il modo più efficiente di fare marketing in rete. Alcuni ricercatori hanno inoltre effettuato degli studi per cui l'esplicitazione delle proprie amicizie favorisce lo svelamento automatico e incontrollato anche di informazioni sui nostri amici. Oggi si tende a partecipare a molte reti, e a volte si ha l'impressione di non riuscire a gestirle: dopo il sovraccarico cognitivo (troppe informazioni equivalgono a nessuna informazione), siamo giunti al sovraccarico da social network.

Possono quindi essere utili alcuni suggerimenti per utilizzare le reti sociali e non esserne travolti:

- chiaritevi le idee sul perché iscrivervi e a cosa vi serve
- una volta scelto i network considerati interessanti, cercate di usarli per lo scopo con cui vi siete iscritti, onde evitare di duplicare le informazioni
- definite i vostri confini di utilizzo: se usate Facebook per il tempo libero e Linkedin per i contatti professionali, gestite le richieste di contatto in modo opportuno
- leggete bene le clausole relative alla privacy e al copyright, è sempre meglio essere informati in anticipo.

E' opportuno adoperare le funzionalità offerte dalle reti sociali per gestire la privacy dei propri dati. E' vero che lo scopo della rete sociale è "socializzare" e che la socializzazione passa proprio dalla condivisione dei propri dati ma è fondamentale sfruttare le possibilità di gestione delle autorizzazioni per controllare chi può accedere alla vostra pagina e con quali diritti: si impostano così per esempio, la visibilità dei dati, si inseriscono limitazioni, si definiscono eventuali liste di blocco, ...

L'attenzione alla propria privacy è un fenomeno in espansione e sono sempre più numerosi gli utilizzatori di reti sociali o di sistemi di messaggistica istantanea che si rivolgono a siti o app che garantiscono un elevato livello di riservatezza. La prova ne è lo sviluppo di sistemi dove conversazioni e informazioni pubblicate hanno un tempo limitato di permanenza sul sito, oltre al quale sono automaticamente cancellate.

Ricordiamo i tre approcci complementari che abbiamo presentato all'inizio della parte 2 di questo IBUQ in tema di sicurezza dei dati:

1. mettere in pratica tutte le misure per impedire il furto
2. fare in modo che in caso di furto il ladro non possa utilizzare i dati rubati
3. fare in modo che in caso di furto torniamo a disporre dei nostri dati in tempi molto brevi.

Il primo punto ha dei risvolti di sicurezza logica (riservatezza della password, ...), che abbiamo già esaminato; ma anche dei risvolti legati alla sicurezza fisica dei dispositivi per evitarne il furto o la distruzione che verranno considerati al successivo punto 6.1.1. Il terzo punto è molto importante in caso di furto, di distruzione o di perdita dei dati. La caratteristica "D" del modello CID, la disponibilità, deve essere interrotta il minor tempo possibile e ripristinata in tempi molto brevi. Qui entrano in gioco le copie di sicurezza dei dati.

Riconoscere l'importanza di avere una procedura di copie di sicurezza per ovviare alla perdita di dati, di informazioni finanziarie, di segnalibri/cronologia web

Nell'uso corrente del personal computer, i dati che creiamo o inseriamo vengono memorizzati sul disco fisso. Che siano legati ad un'attività lavorativa (relazioni, tabelle, ...) o al tempo libero (le foto delle vacanze) rivestono una notevole importanza. I file che li contengono corrono alcuni rischi, non sempre valutati. Il computer può infatti:

- subire un guasto, rendendo i file illeggibili e i dati inutilizzabili (ad esempio, danneggiamento dell'hard disk)
- essere distrutto in un incendio, un'inondazione, ...
- essere compromesso da virus o altri tipi di malware che intaccano l'integrità e la disponibilità dei file
- essere manovrato "distrattamente" e i dati che contiene essere cancellati inavvertitamente
- essere rubato, in particolare se si tratta di un computer portatile.

E' quindi molto importante, per ridurre i danni in caso di evento infausto, disporre di una o più copie di sicurezza (backup) dei file di dati presenti sul disco fisso. In questo modo, se i file originali non sono più disponibili si è immediatamente in grado - una volta ripristinata la funzionalità del personal computer - di reinserire i file dal backup e di disporre di tutti i dati precedentemente registrati.

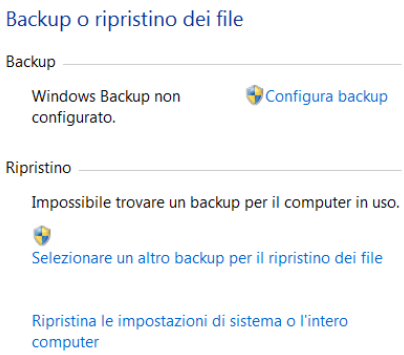


Figura 36: Backup o ripristino dei file

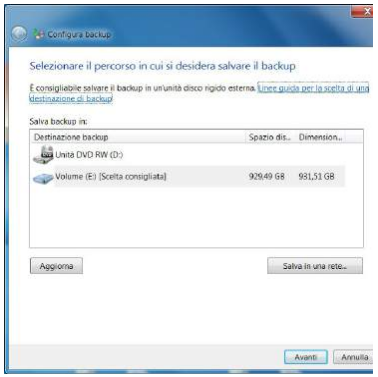


Figura 37: Unità di destinazione delle copie

Di conseguenza è buona norma:

- effettuare regolarmente una copia di backup dei dati su un supporto rimovibile (CD-RW, DVD-RW, chiave USB, disco esterno, ...). Farla su un'unità interna fissa serve solo a evitare il rischio di cancellazione accidentale dell'originale ma non quello di un guasto o di un furto
- rimuovere il supporto dal computer ed archiviarlo in luogo separato, sufficientemente lontano da non correre gli stessi rischi del computer.

E' quindi opportuno che ognuno definisca un metodo e una strategia personale per effettuare le copie dei propri documenti, stabilendo modalità e frequenza di esecuzione. Oltre ai sistemi di backup locali esaminati, vi è anche la possibilità di effettuare backup remoto, se il computer è collegato in rete. Verranno esaminate nella parte finale di questo IBUQ, a proposito delle imprese per le quali è un aspetto essenziale..

Effettuare la copia di sicurezza di dati

Quando si parla di copia di sicurezza dei dati, non si ha in mente l'azione estemporanea di copia-incolla di qualche file su una chiavetta USB bensì una procedura sistematica e periodica di duplicazione di un insieme strutturato di file, avente lo scopo di assicurare il ripristino dei dati allo loro stato prima di un evento dannoso che ne ha causato il danneggiamento parziale o la perdita totale. Spesso si tratterà, soprattutto in ambito aziendale, di una procedura automatica, eseguita per esempio di notte, di salvataggio dei dati dei server.

Esistono numerosi programmi Open Source e commerciali in grado di svolgere questa funzione sui supporti i più diversi. L'importanza delle copie di sicurezza ha portato a dotare Windows di una funzionalità di backup che può essere utilizzata allo scopo.

Questa funzionalità permette di creare la procedura di backup, definendo i file da copiare, l'unità sulla quale effettuare la copia e la pianificazione temporale del backup. Per creare la procedura di backup, occorre:

- selezionare ***Start / Pannello di controllo / Backup e ripristino*** (nella visualizzazione a icone)
- nella finestra *Backup o ripristino dei file* (Figura 36), cliccare sul pulsante *Configura backup*
- nelle finestre successive che vengono proposte, si scelgono:
  - l'unità, locale o di rete, di destinazione delle copie (Figura 37)
  - gli elementi (cartelle e file) che si vogliono copiare, scegliendo manualmente oppure accettando le impostazioni di default (Figura 38)
  - la pianificazione temporale del backup, frequenza, giorno e ora (Figura 39)
  - al termine, cliccando sul pulsante *OK* si avvia il backup (Figura 40).

Nella finestra *Backup o ripristino dei file*, una volta configurato il backup (Figura 36), sono visualizzate le informazioni relative al backup pianificato, modificabile tramite il pulsante *Cambia impostazioni* ed è possibile avviare un backup indipendentemente dalla pianificazione tramite il pulsante *Esegui backup*.

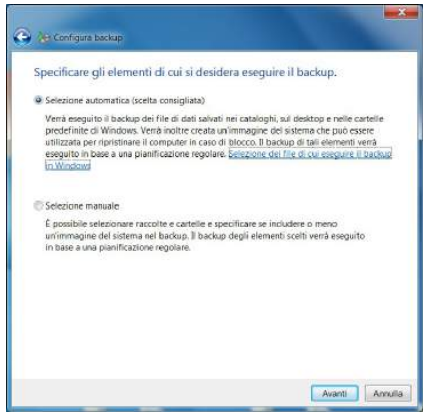


Figura 38: Elementi da copiare

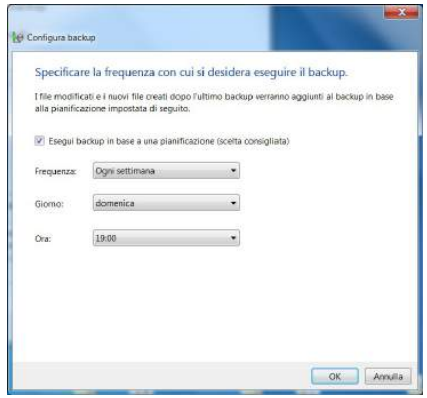


Figura 39: Pianificazione del backup

Come già ampiamente sottolineato, lo scopo delle copie di sicurezza (backup) è di poter ripristinare i dati (restore) in caso di furto o perdita degli stessi. Il backup di per sé è utile solo al momento in cui è necessario eseguire il restore. Come dice qualcuno con una lunga esperienza informatica:

"Il backup funziona sempre, è il restore che spesso non funziona."

Fortunatamente l'affidabilità attuale dell'hardware - in particolare le unità di memorizzazione - è molto elevata, soprattutto rispetto a quella che era anni addietro. Sfortunatamente, questo significa che fate scrupolosamente e fiduciosamente il backup dei dati per anni, fino al momento in cui capita la necessità di ripristinare i dati. Allora vi accorgete che il supporto è rovinato, oppure che i dati, in parte o tutti, non sono più leggibili, oppure che la procedura ne copiava solo una parte e non tutti quelli che pensavate oppure che nuovi dati si sono aggiunti negli anni ma non sono mai stati copiati oppure ...

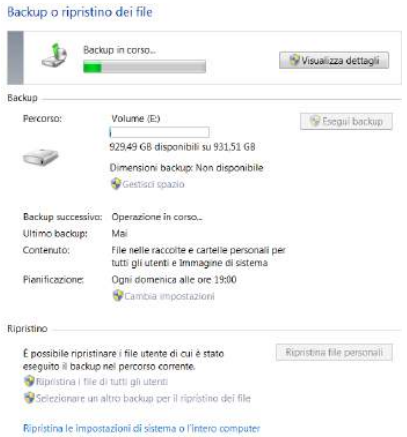


Figura 40: Avanzamento del backup

Ripristinare e validare i dati sottoposti a copia di sicurezza

Di conseguenza se è importante eseguire il backup, è fondamentale verificare periodicamente che l'operazione di restore sia in grado di ripristinare correttamente tutti i dati.

L'operazione di ripristino essendo strettamente collegata a quella di backup, la si attiva in modo simile al backup:

- selezionare ***Start / Pannello di controllo / Backup e ripristino*** (nella visualizzazione a icone)
- nella finestra *Backup o ripristino dei file* (Figura 41), nella sezione *Ripristino*, cliccare sul pulsante *Ripristina file personali*
- nelle finestre successive che vengono proposte, si scelgono:
  - gli elementi (cartelle e file) che si vogliono ripristinare, cercandoli nel backup più recente (Figura 42)
  - dove li si vuole ripristinare. Per un ripristino vero e proprio, li si può ripristinare nella loro posizione originale mentre per una verifica, li si ripristina su un'unità o in una cartella diversa
  - al termine, cliccando sul pulsante *Rispristina* si avvia il restore.

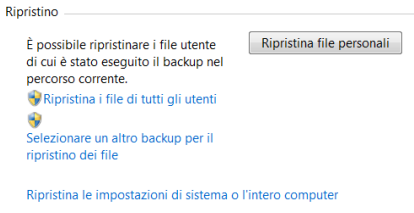


Figura 41: Ripristino dei file

Un link nella pagina *Backup o ripristino dei file* permette il ripristino da backup più vecchi anziché dall'ultimo.

Con il passare degli anni, si accumulano supporti magnetici, ottici o elettronici contenenti dati che possono essere diventati inutili. Fra questi vi sono sicuramente dati personali o dati sensibili che non ci sono più utili ma che potrebbero essere interessanti per un ladro di informazioni. In questo caso, è opportuno provvedere alla cancellazione di questi dati. Ma come abbiamo accennato al precedente punto 6.2.2, vi è una differenza fra cancellare e distruggere.

Identificare i metodi più comuni per distruggere i dati in modo permanente, quali uso di trita documenti, distruzione di memorie di massa/dispositivi, smagnetizzazione, uso di utilità per la cancellazione definitiva dei dati

I metodi da adoperare per distruggere in modo permanente i dati dipendono dal supporto sul quale sono registrati e dall'uso futuro che si vuol fare (o non fare più) del supporto.

Per distruggere i dati da un supporto ottico non riscrivibile (CR-ROM, DVD-ROM), occorre distruggere fisicamente il supporto (Figura 43). Oltre all'uso di strumenti quali pinze e martello, sconsigliati per i rischi che corre l'utilizzatore, esistono diversi modelli di trita documenti previsti per sminuzzare CD e DVD oltre ai soliti fogli di carta.

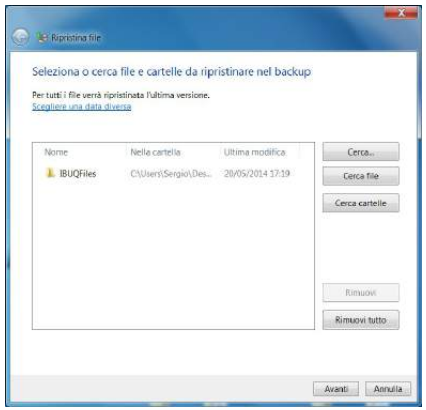


Figura 42: Seleziona i dati da rispristina

Per distruggere l'intero contenuto di un dispositivo (CD-ROM riscrivibile o chiavetta USB per esempio), non è sufficiente procedere alla formattazione del dispositivo in quanto spesso questa operazione non distrugge tutte le informazioni contenute nei file. Si può ricorrere alla cosiddetta "formattazione di basso livello" che esula dai temi di questo e-book e che sconsigliamo all'utente non esperto. Per maggiore sicurezza conviene adoperare appositi programmi di cancellazione sicura, già inseriti nel sistema operativo o aggiuntivi, gli stessi che permettono di distruggere cartelle e file. Va detto inoltre che esistono dispositivi hardware destinati a smagnetizzate i supporti magnetici. Chiamati degausser, sono generalmente in dotazione ai centri specializzati e permettono di eliminare i dati e rendere il dispositivo inutilizzabile, tramite l'applicazione di un campo magnetico di forte intensità.

Per distruggere in modo permanente una cartella o un file (e quindi anche l'intero contenuto di un'unità), è possibile - ed è il metodo maggiormente utilizzato - adoperare un apposito programma che oltre a cancellare i riferimenti ai file ne sovrascriva anche il contenuto. Sono disponibili numerosi programmi di questo tipo, per i diversi sitemi operativi, quali per esempio Wipe o Shred per Linux; SDelete, File Shredder o CBL Data Shredder per Windows, Disk Utility o srm in Mac OSX.

Figura 43: Supporti ottici distrutti

La cancellazione di un singolo elemento tramite l'applicazione che lo ha creato offre un minore livello di controllo sull'effettiva distruzione permanente dei dati. A titolo di esempio, il modo più sicuro offerto da Thunderbird (si veda l'IBUQ *ECDL Online Essentials*) per cancellare un messaggio di posta elettronica consiste nel:

- eliminare il messaggio, che viene così spostato nel Cestino di Thunderbird
- cancellare il messaggio dal Cestino, che viene nascosto e segnato come cancellato ma rimane nel Cestino
- compattare il Cestino o le cartelle di posta, eliminando così il messaggio dai file di Thunderbird.

Questo non garantisce che i dati del messaggio non siano rimasti sul disco del vostro personal computer, fuori dai file gestiti da Thunderbird, oppure che ne sia rimasta una copia sul server di posta del vostro Internet Service Provider oppure ...

Lo stesso legislatore ha prestato attenzione al problema emanando indicazioni specifiche per la distruzione permanente dei dati in caso di reimpiego o di smaltimento delle apparecchiature elettroniche. Riportiamo una parte del Provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008 "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali", pubblicato sulla Gazzetta Ufficiale n. 287 del 9 dicembre 2008.

Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008 *G.U. n. 287 del 9 dicembre 2008*

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

--- OMISSIS ---

TUTTO CIÒ PREMESSO IL GARANTE

1. ai sensi dell'art. 154, comma 1, lett. h) del Codice, richiama l'attenzione di persone giuridiche, pubbliche amministrazioni, altri enti e persone fisiche che, avendone fatto uso nello svolgimento delle proprie attività, in particolare quelle industriali, commerciali, professionali o istituzionali, non distruggono, ma dismettono supporti che contengono dati personali, sulla necessità di adottare idonei accorgimenti e misure, anche con l'ausilio di terzi tecnicamente qualificati, volti a prevenire accessi non consentiti ai dati personali memorizzati nelle apparecchiature elettriche ed elettroniche destinate a essere:

a. reimpiegate o riciclate, anche seguendo le procedure di cui all'allegato A);
b. smaltite, anche seguendo le procedure di cui all'allegato B).

Tali misure e accorgimenti possono essere attuate anche con l'ausilio o conferendo incarico a terzi tecnicamente qualificati, quali centri di assistenza, produttori e distributori di apparecchiature che attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle.

Chi procede al reimpiego o al riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche o di loro componenti è comunque tenuto ad assicurarsi dell'inesistenza o della non intelligibilità di dati personali sui supporti, acquisendo, ove possibile, l'autorizzazione a cancellarli o a renderli non intelligibili;

2. dispone che copia del presente provvedimento sia trasmesso al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica Italiana.

Roma, 13 ottobre 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Fortunato

IL SEGRETARIO GENERALE
Buttarelli

Allegato A) al provvedimento del Garante del 13 ottobre 2008

Reimpiego e riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche

In caso di reimpiego e riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche le misure e gli accorgimenti volti a prevenire accessi non consentiti ai dati personali in esse contenuti, adottati nel rispetto delle normative di settore, devono consentire l'effettiva cancellazione dei dati o garantire la loro non intelligibilità. Tali misure, anche in combinazione tra loro, devono tenere conto degli standard tecnici esistenti e possono consistere, tra l'altro, in:

Misure tecniche preventive per la memorizzazione sicura dei dati, applicabili a dispositivi elettronici o informatici:

1. Cifratura di singoli file o gruppi di file, di volta in volta protetti con parole-chiave riservate, note al solo utente proprietario dei dati, che può con queste procedere alla successiva decifratura. Questa modalità richiede l'applicazione della procedura di cifratura ogni volta che sia necessario proteggere un dato o una porzione di dati (file o collezioni di file), e comporta la necessità per l'utente di tenere traccia separatamente delle parole-chiave utilizzate.

2. Memorizzazione dei dati sui dischi rigidi (hard-disk) dei personal computer o su altro genere di supporto magnetico od ottico (cd-rom, dvd-r) in forma automaticamente cifrata al momento della loro scrittura, tramite l'uso di parole-chiave riservate note al solo utente. Può effettuarsi su interi volumi di dati registrati su uno o più dispositivi di tipo disco rigido o su porzioni di essi (partizioni, drive logici, file-system) realizzando le funzionalità di un c.d. file-system crittografico (disponibili sui principali sistemi operativi per elaboratori elettronici, anche di tipo personal computer, e dispositivi elettronici) in grado di proteggere, con un'unica parola-chiave riservata, contro i rischi di acquisizione indebita delle informazioni registrate. L'unica parola-chiave di volume verrà automaticamente utilizzata per le

operazioni di cifratura e decifratura, senza modificare in alcun modo il comportamento e l'uso dei programmi software con cui i dati vengono trattati.

Misure tecniche per la cancellazione sicura dei dati, applicabili a dispositivi elettronici o informatici:

3. Cancellazione sicura delle informazioni, ottenibile con programmi informatici (quali wiping program o file shredder) che provvedono, una volta che l'utente abbia eliminato dei file da un'unità disco o da analoghi supporti di memorizzazione con i normali strumenti previsti dai diversi sistemi operativi, a scrivere ripetutamente nelle aree vuote del disco (precedentemente occupate dalle informazioni eliminate) sequenze casuali di cifre "binarie" (zero e uno) in modo da ridurre al minimo le probabilità di recupero di informazioni anche tramite strumenti elettronici di analisi e recupero di dati.

Il numero di ripetizioni del procedimento considerato sufficiente a raggiungere una ragionevole sicurezza (da rapportarsi alla delicatezza o all'importanza delle informazioni di cui si vuole impedire l'indebita acquisizione) varia da sette a trentacinque e incide proporzionalmente sui tempi di applicazione delle procedure, che su dischi rigidi ad alta capacità (oltre i 100 gigabyte) possono impiegare diverse ore o alcuni giorni), a secondo della velocità del computer utilizzato.

4. Formattazione "a basso livello" dei dispositivi di tipo hard disk (low-level formatting–LLF), laddove effettuabile, attenendosi alle istruzioni fornite dal produttore del dispositivo e tenendo conto delle possibili conseguenze tecniche su di esso, fino alla possibile sua successiva inutilizzabilità;

5. Demagnetizzazione (degaussing) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici (dischi rigidi, floppy-disk, nastri magnetici su bobine aperte o in cassette), in grado di garantire la cancellazione rapida delle informazioni anche su dispositivi non più funzionanti ai quali potrebbero non essere applicabili le procedure di cancellazione software (che richiedono l'accessibilità del dispositivo da parte del sistema a cui è interconnesso).

Allegato B) al provvedimento del Garante del 13 ottobre 2008

Smaltimento di rifiuti elettrici ed elettronici

In caso di smaltimento di rifiuti elettrici ed elettronici, l'effettiva cancellazione dei dati personali dai supporti contenuti nelle apparecchiature elettriche ed elettroniche può anche risultare da procedure che, nel rispetto delle normative di settore, comportino la distruzione dei supporti di memorizzazione di tipo ottico o magneto-ottico in modo da impedire l'acquisizione indebita di dati personali.

La distruzione dei supporti prevede il ricorso a procedure o strumenti diversi a secondo del loro tipo, quali:

- *sistemi di punzonatura o deformazione meccanica;*
- *distruzione fisica o di disintegrazione (usata per i supporti ottici come i cd-rom e i dvd);*
- *demagnetizzazione ad alta intensità.*

Il testo completo è disponibile all'indirizzo http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1571514. A questo ha fatto seguito una scheda informativa tecnica "Istruzioni pratiche per una cancellazione sicura dei dati: le raccomandazioni degli operatori", disponibile all'indirizzo http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1574080 alla quale rinviamo il lettore interessato.

Capitolo 5 – I rischi per le aziende

Riferimento Syllabus 1.1.4	*Riconoscere le minacce ai dati provocate da forza maggiore, quali fuoco, inondazione, guerra, terremoto.*
Riferimento Syllabus 1.1.5	*Riconoscere le minacce ai dati provocate da impiegati, fornitori di servizi e persone esterne.*
Riferimento Syllabus 1.2.2	*Comprendere i motivi per proteggere informazioni commercialmente sensibili, quali prevenzione di furti, di uso improprio dei dati dei clienti o di informazioni finanziarie.*
Riferimento Syllabus 1.2.6	*Comprendere l'importanza di creare e attenersi a linee guida e politiche per l'uso dell'ICT.*
Riferimento Syllabus 1.3.1	*Comprendere il termine "ingegneria sociale" e le sue implicazioni, quali raccolta di informazioni, frodi e accesso a sistemi informatici.*
Riferimento Syllabus 1.3.2	*Identificare i metodi applicati dall'ingegneria sociale, quali chiamate telefoniche, phishing, shoulder surfing al fine di carpire informazioni personali.*
Riferimento Syllabus 3.1.1	*Comprendere il termine rete e riconoscere i più comuni tipi di rete, quali LAN (rete locale), WAN (rete geografica), VPN (rete privata virtuale).*
Riferimento Syllabus 3.1.2	*Comprendere il ruolo dell'amministratore di rete nella gestione delle operazioni di autenticazione, autorizzazione e assegnazione degli account all'interno di una rete.*
Riferimento Syllabus 3.1.3	*Comprendere la funzione e i limiti di un firewall.*
Riferimento Syllabus 3.4.1	*Comprendere lo scopo di un account di rete e come accedere alla rete usando un nome utente e una password.*
Riferimento Syllabus 3.4.3	*Identificare le comuni tecniche di sicurezza biometriche usate per il controllo degli accessi, quali impronte digitali, scansione dell'occhio.*

Riferimento Syllabus 4.1.5	***Comprendere il termine "one-time password".***
Riferimento Syllabus 6.1.1	***Riconoscere modi per assicurare la sicurezza fisica di dispositivi, quali registrare la collocazione e i dettagli degli apparati, usare cavi di sicurezza, controllare gli accessi.***
Riferimento Syllabus 6.1.2	***Riconoscere l'importanza di avere una procedura di copie di sicurezza per ovviare alla perdita di dati, di informazioni finanziarie, di segnalibri/cronologia web.***
Riferimento Syllabus 6.1.3	***Identificare le caratteristiche di una procedura di copie di sicurezza, quali regolarità/frequenza, pianificazione, collocazione della memoria di massa***
Contenuti della lezione	***In questa lezione vedremo: l'estrema importanza che rivestono le linee guida e politiche per l'uso delle ICT, l'importanza della protezione delle informazioni commerciali e finanziarie, le minacce ai dati, interne e esterne, l'ingegneria sociale e i suoi metodi, le reti, la loro gestione e messa in sicurezza e il ruolo dell'amministratore, alcuni strumenti tecnici di protezione e le procedure di salvataggio e ripristino dei dati.***

Comprendere l'importanza di creare e attenersi a linee guida e politiche per l'uso dell'ICT

Mentre nell'uso *personale* di un computer un buon livello di sicurezza può essere raggiunto senza necessità di formalizzazione particolare, con la sola conoscenza dei pericoli e delle precauzioni da prendere (per esempio tramite la lettura di questo IBUQ), diversa è la realtà inell'uso *professionale* di un computer in ambito lavorativo. Non solo il livello di articolazione dell'hardware è decisamente superiore (spesso si ha a che fare con reti interconnesse di personal computer nelle quali sono presenti numerosi server), non solo il livello di complessità del software è maggiore (procedure integrate fra di loro, basi di dati complesse) ma si aggiunge anche il peso degli aspetti organizzativi per i numerosi addetti che devono poter accedere al sistema informatico.

In questo caso, diventa fondamentale che l'impresa o l'organizzazione analizzi i risvolti legati all'uso, interno e esterno, delle Tecnologie dell'Informazione e della Comunicazione (TIC o ICT in inglese), con particolare riferimento ai rischi relativi e alle misure di sicurezza da attuare. Il risultato di questa analisi deve portare a formalizzare una politica per l'uso delle ICT contenenti le linee guida per una corretta gestione delle risorse informatiche, le procedure e regolamentazioni interne anche in termini di sicurezza.

Il documento che formalizza tali politiche e linee guida deve essere comunicato al personale in modo che tutti gli addetti conoscano la posizione dell'azienda sui vari aspetti legati all'uso del sistema informativo e delle risorse informatiche e possano attenersi alle regole aziendale destinate ad assicurare una corretta gestione delle ICT.

Comprendere i motivi per proteggere informazioni commercialmente sensibili, quali prevenzione di furti, di uso improprio dei dati dei clienti o di informazioni finanziarie

Le imprese, come le persone, possono essere oggetto di furti e di frodi. Se il furto di dati personali può avere conseguenze gravi, il furto di dati aziendali può avere conseguenze drammatiche. Un'azienda che detiene dati relativi a persone, fornitori, clienti può essere tenuta responsabile in caso di furto e/o uso improprio di tali dati. Ma questo è per così dire il danno minore rispetto a quelli che possono nascere, per esempio, dalla

vendita dei dati dei clienti ad un'azienda della concorrenza o alla diffusione di informazioni finanziarie sui clienti di una banca o al furto dei numeri di carta di credito dei clienti di un'istituzione finanziaria- Per non parlare dello spionaggio industriale che vede il furto di informazioni tecniche o commerciali su nuovi prodotti o progetti.

Ad un certo livello, oltre ad un rischio di reputazione, tali crimini informatici possono portare alla perdita di tutti o parte dei clienti e alla chiusura dell'azienda.

Riconoscere le minacce ai dati provocate da impiegati, fornitori di servizi e persone esterne.

Non sempre la percezione che si ha della sicurezza - o insicurezza - informatica corrisponde alla realtà. Spesso si pensa alle frodi realizzate su Internet mentre la maggior parte è fuori dalla rete, al furto di dati delle carte di credito in rete mentre ce ne sono di più nei canali tradizionali, all'uso di strumenti di attacco altamente sofisticati mentre si dimentica l'ingegneria sociale (come si vedrà più avanti). Non ultimo, nel mondo delle imprese spesso ci si protegge da attacchi esterni mentre si ignorano o dimenticano i rischi provenienti dall'interno. In sintesi si associano i crimini informatici o le minacce ai dati a malware penetrati nel sistema e ad attacchi di tipo informatico, magari compiuti in modo remote via Internet.

Si tende invece a sottovalutare il rischio di attacchi tecnologicamente più modesti, che possono essere compiuti da persone che per motivi fra i più leciti hanno occasione di entrare in azienda e di accedere a dati riservato o al sistema informativo aziendale.

Pensiamo per esempio a fornitori di servizi informatici che per ragioni tecniche devono poter intervenire sui personal computer degli utenti o sui server aziendali per installare o aggiornare i programmi. I tecnici operano in genere con il massimo dei permessi di accesso, proprio per esigenze tecniche, e così come hanno accesso ai programmi hanno anche accesso ai dati. Con il rischio di distruzione o modifica accidentali piuttosto che di sottrazione o distruzione volontaria.

Più semplicemente, pensiamo a persone esterne anche non tecniche che possono accedere, perché presenti in azienda, al sistema informativo: un personal computer lasciato momentaneamente incustodito e non protetto da password è un facile punto di accesso al sistema informativo. Così come una rete Wi-Fi lasciata aperta o non correttamente protetta è facilmente utilizzabile tramite un portatile, un tablet o addirittura uno smartphone per carpire o danneggiare dati presenti nel sistema informativo.

In tutti questi casi abbiamo fatto riferimento a personale esterno all'azienda, alla scuola o all'ente proprietario del sistema informativo. Ancora più importanti perché spesso inaspettato sono le minacce che provengono dall'interno. Chi più di un dipendente accede al sistema informativo? Per la sua stessa attività deve poter accedere ai dati e involontariamente, in caso di disattenzione, può provocare una perdita dei dati. Oppure volontariamente, in caso di comportamento fraudolento, impossessarsi dei dati, portarli all'esterno dell'azienda all'insaputa del datore di lavoro e farne un uso non corretto. O ancora distruggere dati o danneggiare il sistema informatico per ripicca o vendetta. In questo caso, la tutela è molto più complessa e richiede un'attenta politica di sicurezza che oltre a un sistema di autenticazione che consenta l'accesso al sistema solo agli utenti registrati, preveda anche un sistema di autorizzazioni che permetta agli utenti registrati di accedere soltanto ai dati per i quali sono stati specificatamente autorizzati. Oltre a un efficace sistema di salvataggio dei dati.

Riconoscere le minacce ai dati provocate da forza maggiore, quali fuoco, inondazione, guerra, terremoto

Anche se gli eventi straordinari che possono minacciare un sistema informatica sono rari, i danni che ne derivano possono essere particolarmente gravi per le imprese. Molte imprese, soprattutto quelle di una certa dimensione o quelle che trattano dati dei clienti di particolare importanza (si pensi alle banche e alle assicurazioni, ai grandi ISP), mettono in atto delle vere e proprie politiche di *disaster recovery* che garatiscono una ripartenza del sistema informatico in tempi ridotti, anche in caso di distruzione totale provocate da cause di forza maggiore (catastrofi naturali, eventi straordinari, ...), magari in luoghi diversi rispetto alla loro sede originaria. Si ricorda per esempio la notizia relativa a Aruba vista prima.

In questi casi, a politiche di protezione fisica degli edifici che ospitano le infrastrutture informatiche, si affiancano politiche di ripristino che prevedono la duplicazione (spesso presso centri esterni) delle apparecchiature e test periodici dell'efficienza della continuità dei servizi con simulazione delle interruzioni.

Queste misure, per i loro costi e oneri di gestione molti elevati, sono messe in pratica da poche aziende per le quali il sistema informatico è realmente strategico e nulla hanno a che fare con le "semplici" procedure di backup e restore che l'utente di personal computer può mettere in atto. Non si tratta infatti di un banale backup dei dati ma di una duplicazione dell'intera struttura elaborativa (hardware, software, reti, dati).

Riconoscere modi per assicurare la sicurezza fisica di dispositivi, quali registrare la collocazione e i dettagli degli apparati, usare cavi di sicurezza, controllare gli accessi

Il tema delle sicurezza fisica riguarda da vicino tutte le imprese, più degli utenti singoli di PC. Il furto di portatili, tablet o smartphone è un fenomeno in aumento che tocca tutti. Nel caso però delle imprese, il fenomeno è acuito dal maggior numero di dispositivi che possono trovarsi nei locali di un'impresa e dal maggior flusso di persone esterne che, per un motivo o un altro, hanno occasione di entrare in azienda.

Figura 44: Un dispositivo antifurto

Per ridurre i rischi di furto o di danneggiamento delle apparecchiature, con conseguente furto o perdita di dati, le imprese intervengono su più aspetti:

- *controllo degli accessi*. Si regolamenta l'accesso agli edifici e ai locali in cui si svolge l'attività dell'impresa, con un livello di protezione variabile a seconda dei rischi che si possono incorrere in ogni zona: l'accesso a locali più "sensibili" sarà soggetto a regole più restrittive, fra le quali per esempio l'identificazione delle persone che hanno accesso.
- *protezione fisica dei computer*. Mentre i server saranno in locali ad accesso controllato e limitato, i computer periferici potranno essere protetti contro il furto da cavi di sicurezza, in particolare i personal computer e ancora di più i portatili (Figura 44).

- *censimento e localizzazione delle apparecchiature*. Tenere un registro - costantemente aggiornato - delle apparecchiature informatiche con per ognuno marca, modello, configurazione, dispositivi collegati e collocazione aiuta nella gestione tecnica del parco macchine e facilita la rapida individuazione di manomissioni o furti.

Comprendere il termine "ingegneria sociale" e le sue implicazioni, quali raccolta di informazioni, frodi e accesso a sistemi informatici

Come si fa a carpire una password per accedere a dati riservati?

Esistono diversi metodi che richiedono conoscenze tecniche e disponibilità di strumenti per attaccare il sistema cercando scoprire la password, come per esempio i tentativi di *brute force attack* (attacco di forza bruta) in cui si generano molteplici password combinando caratteri e si provano in sequenza, oppure l'uso di dizionari di password, che sfruttano le parole e le combinazioni di caratteri più usate dagli utenti come password.

Ma esiste un metodo molto più semplice, che non richiede nessuna conoscenza tecnica né strumento informatico: farsi dire la password da chi la conosce.

Questo è il modo di procedere e l'obiettivo dell'ingegneria sociale (o *social engineering*). Per usare i termini dell'ex hacker Kevin Mitnick, ora hacker etico (vedere punto 1.1.3), uno dei massimi esperti in materia:

> *Social Engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology.*

ossia

> *L'ingegneria sociale usa ascendente e potere di persuasione per ingannare le persone convincendole che l'ingegnere sociale è qualcuno che non è, o manipolandole. Come tale, l'ingegnere sociale è capace di usare le persone per ottenere informazioni con o senza l'uso della tecnologia.*

L'ingegneria sociale si basa sui rapporti umani, più che sulla conoscenza di tecniche avanzate, e sulla psicologia delle persone, più che su strumenti tecnologici, con scopi fraudolenti quali carpire informazioni personali o riservate, ottenere credenziali di autenticazione per accedere a sistemi informatici. compiere furti di dati o di identità per sostituirsi ad altri per compiere frodi, malversazioni o reati.

Come ti assicuro dalle insidie del cyber crime

Dopo gli attacchi ai siti dei colossi eBay e Target, gli hacker fanno più paura anche in Italia

Federica Pezzatti

Il pericolo hacker comincia a turbare seriamente i sonni degli italiani. Lo ha rilevato anche l'«Allianz Risk Barometer 2014», ricerca condotta dal colosso assicurativo tedesco, intervistando oltre 400 esperti di insurance corporate provenienti da 33 Paesi inclusa l'Italia. Se infatti il cyber crime si colloca all'ottavo posto nella graduatoria mondiale dei principali rischi di business – segnando maggior allarme rispetto dal quindicesimo posto del precedente report –, in Italia il crimine informatico è arrivato addirittura fino al sesto posto della classifica dei principali minacce, superando persino il rischio di rottura dell'eurozona, piuttosto che il timore di incendio o dell'inasprirsi della competizione. Anche nel Belpaese dunque aumenta la percezione del pericolo del cyber crime che, oltre agli hacker "attivisti" coinvolge sempre più anche la criminalità organizzata che ha trovato in internet un terreno fertile per impiantare nuovi business (dalle frodi al furto di dati).

Il tema è talmente "caldo" anche a livello internazionale che il "Financial Times" del 6 giugno 2014 gli ha dedicato un report speciale di quattro pagine intitolato «cyber security», con l'articolo di apertura che spiegava come la maggiore invasività degli hacker, che nel 2014 hanno alzato il tiro, portato a termine attacchi devastanti anche a colossi come eBay e Target, provochi l'aumento della paura collettiva.

«A essere più vulnerabili, purtroppo, sono le strutture medio piccole che non investono particolarmente in sicurezza informatica - spiega anche Giorgio Bidoli, ceo di Allianz Global Corporate & Specialty (Agcs) Italia -. Tra l'altro, proprio le Pmi sono spesso i target preferiti dei cyber criminali. I pirati informatici puntano a queste aziende che possono avere politiche e procedure di sicurezza dei dati meno sofisticate, e questo non solo per colpire loro, ma per utilizzarne i sistemi come porte di ingresso agli ambienti più sicuri delle grandi aziende con le quali sono in rapporti di affari», conclude il manager di Agcs, gruppo che, proprio tenuto conto dell'aumento della sensibilità al tema , ha studiato una soluzione assicurativa ad hoc anche per l'Italia. Si chiama "Cyber Protect" ed è una polizza declinata in tre formulazioni (la versione base, la versione Premium, con rafforzamento in caso di interruzione delle attività e la versione Plus, realizzata su misura). I capitali assicurati vanno da 500 mila euro fino a 50 milioni di euro. Nel target tutte le aziende, tranne quelle aeronautiche, quelle informatiche e quelle finanziarie. Un occhio di riguardo è rivolto appunto alle Pmi, in particolare a quelle che maneggiano dati sensibili come i retailer.

I danni legati a problemi di sicurezza informatica sono incalcolabili. Negli Usa la perdita di dati può costare a un'azienda anche 5,5 milioni di dollari e le organizzazioni registrano in media ben 122 attacchi cibernetici ogni settimana. In Italia ci sono meno statistiche ma, stando al Rapporto Clusit 2014, dei 1.150 attacchi registrati nel 2013 a livello internazionale, ben 35 si riferiscono a bersagli italiani. L'inadeguatezza dei controlli in un quadro regolamentare sempre più complesso e in rapida evoluzione, ha reso estremamente critica la posizione delle società che non sono in grado di assicurare la tutela dei dati personali posseduti. Tra l'altro la normativa anche in Europa è in via di definizione con nuove regole in arrivo e con sanzioni che potrebbero arrivare al 2%-5% del fatturato, secondo le ipotesi che circolano.

IL FENOMENO IN ITALIA E NEL MONDO

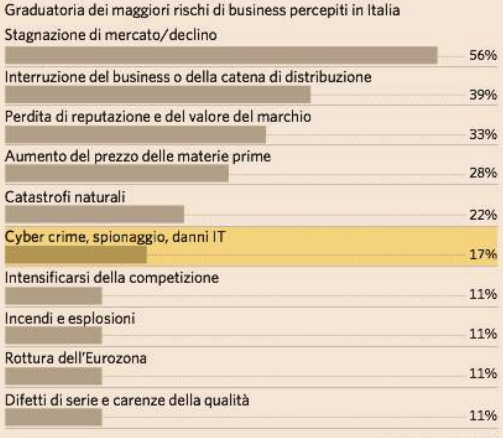
1.150
ATTACCHI RILEVATI NEL 2013
Attacchi a livello internazionale di cui 35 hanno avuto bersagli italiani

20 miliardi
DANNI ANNUI IN ITALIA
Si stima che il cyber crime arrechi all'Italia danni tra i 20 e i 40 mld di €

102 euro
COSTO MEDIO "DATA BREACH"
Costo medio delle violazione di dati personali nel 2013

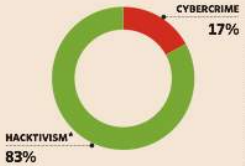
Cosa temono le aziende italiane

Graduatoria dei maggiori rischi di business percepiti in Italia

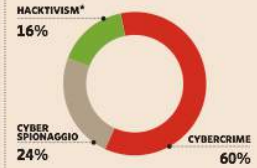


FONTE : Allianz Barometer 2014

CYBER RISK NEL 2013
Distribuzione degli attacchi in Italia



CHI C'È DIETRO
Motivazione degli attacchi



(*) neologismo che deriva dall'unione di due parole, hacking e activism, indica le pratiche dell'azione diretta digitale stile hacker

FONTE: Allianz Barometer 2014

La Notizia

Come ti assicuro dalle insidie del cyber crime

Plus 24 Il Sole 24 Ore

14/6/2014 n. 616, Polizze e sicurezza informatica

http://www.banchedati.ilsole24ore.com/doc.get?uid=finanza-FM20140614011APS

Notizia riprodotta per gentile autorizzazione da Il Sole 24 ORE S.p.A.

Zoomate la pagina per leggere più facilmente l'articolo del quotidiano.

Identificare i metodi applicati dall'ingegneria sociale, quali chiamate telefoniche, phishing, shoulder surfing al fine di carpire informazioni personali

Se volete saperne di più, potete trovare molti esempi interessanti raccontati da Mitnick (uno dei più famosi ex-hacker) nei suoi libri, non certo per imparare a diventare un ingegnere sociale ma al contrario per difendervi dagli attacchi, in particolare in *L'arte dell'inganno. I consigli dell'hacker più famoso del mondo*.

Fra i diversi messi usati nell'ingegneria sociale, le telefonate la fanno da padrone. Un mezzo di comunicazione familiare come il telefono ben si presta a sfruttare l'ingenuità o la buona fede dell'interlocutore, facendogli rivelare informazioni apparentemente innocue ma che, in una catena di telefonate a persone diverse, permettono di giungere a informazioni riservate.

Un'altra tecnica è quella del phishing (esaminata al punto 5.1.5), nota ormai a tutti quelli che usano la posta elettronica: molti dei messaggi di posta indesiderata o spam (descritti al punto 5.1.4) sono relativi a tentativi di phishing in cui il mittente, fingendosi una banca o un gestore di carte di credito richiede di comunicare per conferma le proprie credenziali di accesso al servizio (codice utente e password) per non rischiare il blocco del servizio stesso e l'impossibilità ad accedervi. Non ci crederete ma qualcuno ci casca ancora, non sapendo che nessuna banca chiede informazioni riservate ai propri clienti, men che meno per posta elettronica! Anche se vi sono ulteriori protezioni che impediscono al malintenzionato di prelevare soldi dal vostro conto, può impadronirsi di informazioni per esempio sui vostri acquisti (data, importo, fornitore) o sui vostri introiti (stipendio, datore di lavoro) che gli consentiranno attacchi successivi più convincenti ed efficaci.

Sempre per raccogliere informazioni, e con una parvenza molto più innocua, sono i messaggi di phishng che sembrano provenire dal vostro gestore di posta elettronica e vi chiedono di confermare le vostre credenziali di accesso alla vostra casella, per esempio per verificarne il regolare funzionamento in seguito ad un malfunzionamento. Il fatto che non vi sia nessuna implicazione monetaria diretta abbassa le difese e rende meno sospettoso l'utente che spesso le comunica. Non dovete mai farlo per non consentire l'accesso ai vostri messaggi che rivelano MOLTE informazioni su di voi, utilizzabili per farvi abbassare la guardia in ulteriori attacchi.

Sotto il termini altisonante di *shoulder surfing* si nasconde una tecnica molto semplice e "a bassa tecnologia" per carpire informazioni di accesso quali password o PIN; semplicemente guardando "sopra la spalla" (*shoulder*) di chi inserisce il proprio codice utente, password o PIN in un dispositivo: computer, tablet, smartphone, Bancomat, sistema di pagamento automatizzato, ... e magari impadronendosi successivamente del dispositivo o della tessera.

Tutte tecniche che non richiedono nessuna conoscenza informatica ma sfruttano la destrezza del ladro e l'inattenzione o l'ingenuità del bersaglio.

Abbiamo già parlato di rete e dei pericoli che possono nascere per un individuo che fruisce dei servizi in rete. Il tema va approfondito ed esaminato dal punto di vista dell'impresa che gestisce un'intera rete per le sue comunicazioni interne.

Comprendere il termine rete e riconoscere i più comuni tipi di rete, quali LAN (rete locale), WAN (rete geografica), VPN (rete privata virtuale)

Una rete può essere definita come un insieme di computer (ed eventualmente di altri dispositivi elettronici) collegati fra di loro in modo da consentire la condivisione di risorse comuni (spazio di archiviazione, archivi, stampanti, ...) nonché lo scambio di informazioni da parte degli utenti con vari sistemi di comunicazione. Insito nel concetto di rete è l'insieme delle procedure di sicurezza che garantisce l'accesso ai dati soltanto agli utenti autorizzati. Utenti che dispongono di credenziali di autenticazioni (codice utente e password per esempio) per farsi riconoscere e che accedono ai servizi offerti dalle rete limitatamente ai diritti di cui dispongono nel sistema.

Le reti possono essere classificate in base a diversi criteri.

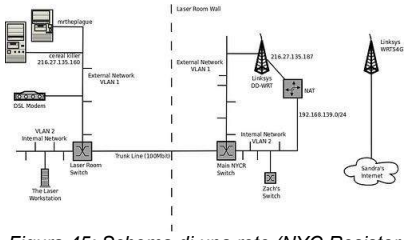


Figura 45: Schema di una rete (NYC Resistor Network)

Un aspetto rilevante è la distanza che separa i calcolatori interconnessi: per consuetudine si classificano le reti in base a criteri spaziali, come un ufficio, uno o più edifici fino ad arrivare alla rete delle reti, Internet, che consente un'interconnessione planetaria. Accettando qualche semplificazione, riportiamo nel prospetto sottostante alcune tipologie frequenti.

Ambito	**Distanza**	**Tipo di rete**
Ufficio, laboratorio	10 m	LAN di ufficio
Edificio (azienda, scuola)	100 m	LAN aziendale
Campus, plesso	1 km	LAN estesa
Città, area geografica	10 km	MAN
Regione, provincia	100 km	WAN
Nazione, continente	1.000 km	WAN estesa
Pianeta	10.000 km	Internet

Si identificano pertanto tre tipi di reti (Figura 45), a seconda della loro estensione:

- LAN (Local Area Network), fra le quali troviamo le WLAN (Wireless Local Area Network)
- MAN (Metropolitan Area Network)
- WAN (Wide Area Network).

Vediamo quali sono le loro caratteristiche e cosa le differenzia:

- *LAN* è una rete locale per il collegamento di PC all'interno di una casa, di un ufficio o di una intera struttura (azienda, scuola, ente). Gli utenti di una LAN operano in una stessa organizzazione, condividendo dati e dispositivi hardware tramite connessioni ad alta velocità (100 Mbps o 1Gbps), elevata sicurezza e affidabilità. Si vanno sempre più affermando le WLAN, reti locali con connessioni wireless (Wi-Fi), che utilizzano onde radio tra i computer in rete. La velocità tipica di una WLAN è di 54 Mbps

- *MAN* è una rete metropolitana, ossia un'estensione delle rete locali in ambito urbano, rese possibili dall'armonizzazione di standard congiunti a cura degli enti ISO e CCITT. Tali reti di solito utilizzano le reti in fibra ottica messe a disposizione dagli operatori di telecomunicazioni. La velocità di una connessione MAN è compresa fra i 2 Mbps e i 140 Mbps. Le reti MAN sono sempre più spesso classificate tra le WAN
- *WAN* è una rete geograficamente estesa, che può collegare reti che si trovano in città diverse. Le reti WAN devono garantire il controllo contro accessi non autorizzati, attraverso la predisposizione di meccanismi di sicurezza.

Nessuna azienda né organizzazione opera in condizioni di isolamento. O perché appartenenti ad una stessa filiera produttiva, o perché facenti parte di uno stesso gruppo o per semplici necessità di scambio di dati e informazioni, tutte hanno esigenze di interconnessione del proprio sistema informatico.

L'estensione della rete all'esterno richiede un'attenzione ancora maggiore alle problematiche di sicurezza e richiede la messa in opera di accorgimenti particolari a protezione delle comunicazioni, per esempio la creazione di cosiddette reti virtuali private (VPN, Virtual Private Network). Per comunicare fra sedi o uffici geograficamente distaccati, un'impresa può creare una propria infrastruttura di rete ma con la diffusione di Internet, si tende per motivi di costo ad abbandonare questo approccio e ad utilizzare invece la stessa rete Internet. In questo caso si parla di rete privata virtuale (in inglese VPN) per indicare una rete di comunicazione privata che utilizza delle infrastrutture di rete pubbliche (Internet). Scopo della VPN sarà di gestire le problematiche di sicurezza che possono derivare dall'uso di una rete condivisa per far transitare informazioni riservate. In particolare il software di gestione della VPN prenderà in carico la cifratura dei dati e l'autenticazione degli utenti, raggiungendo così un elevato livello di sicurezza nella trasmissione

Comprendere lo scopo di un account di rete e come accedere alla rete usando un nome utente e una password

Come più volte ricordato, nome utente e password costituiscono le principali credenziali di autenticazione per l'accesso ad un sistema di elaborazione. Le misure di sicurezza minime richiedono che soltanto gli utenti autorizzati possano accedere alle risorse informatiche, limitatamente ai diritti che gli sono assegnati per la loro attività. Questo vale per un personal computer, per i server o a maggior ragione per le reti, soprattutto se

queste sono di grandi dimensioni e si estendono geograficamente fuori dai locali e dal diretto controllo dell'impresa.

Ogni utente all'interno dell'impresa o dell'organizzazione sarà dotato di un account personale di rete al quale sarà abbinato un codice utente e una password, quest'ultima da scegliere nel rispetto delle regole aziendali e da modificare periodicamente. In questo modo potrà accedere alle funzionalità del sistema di sua pertinenza, ai programmi che è autorizzato ad utilizzare, ai dati utili per lo svolgimento delle sue mansioni. Si ricorda infatti che la funzione del nome utente e della password nell'account di rete è duplice:

- *autenticazione*. Per identificare chi si collega e permettere il collegamento solo a chi è in possesso delle credenziali.
- *autorizzazione*. All'account di rete sono associati i diritti di accesso alle risorse, configurati in modo che ogni utente possa accedere soltanto alle risorse informatiche di cui necessita nell'ambito della sua attività.

Naturalmente il livello di protezione assicurato da questo sistema dipende da molti fattori quali le precauzioni prese per tenere riservate le credenziali e per gestirle nel tempo (non si scrive la password su un foglietto e non si numera progressivamente quando bisogna modificarla pippo01, pippo02, ...); la resistenza agli attacchi di tutti i tipi; la corretta configurazione degli accessi e dei diritti; la fedeltà del collaboratore, ... Non ultimo, la disattivazione dell'account di rete quando cessa il rapporto di lavoro e l'aggiornamento tempestivo dei diritti di accesso quando cambiano le mansioni.

Per questo motivo, negli ambienti che richiedono un maggior livello di sicurezza sono messi in atto dispositivi diversi e più sicuri. In questo, come in tutte le problematiche generali di sicurezza gioca un ruolo importante l'amministratore di rete.

Comprendere il ruolo dell'amministratore di rete nella gestione delle operazioni di autenticazione, autorizzazione e assegnazione degli account all'interno di una rete

L'amministratore di rete è la persona (più di una nel caso di realtà di grandi dimensioni), interna o esterna all'azienda o all'organizzazione, preposta alla gestione tecnica della rete di computer. Assume un ruolo particolarmente importante sulle tematiche di sicurezza ed in particolare deve:

- assicurare il regolare funzionamento delle apparecchiature di rete e dei dispositivi di collegamento
- definire e mettere in opera le misure di sicurezza atte a garantire un corretto livello di protezione della rete
- gestire tutti gli aspetti dell'accesso alla rete da parte degli utenti.

Su quest'ultimo punto in particolare, deve:

- creare gli account utente e assegnare le credenziali di autenticazione (codice utente e password) ai nuovi utenti
- assegnare le autorizzazioni ai nuovi utenti (diritti di accedere ad alcuni dati o programmi e non ad altri, a seconda delle mansioni svolte)
- aggiornare le autorizzazioni degli utenti (per esempio, in caso di cambio di mansioni che portano a gestire dati diversi)
- rimuovere gli account degli utenti che lasciano la struttura.

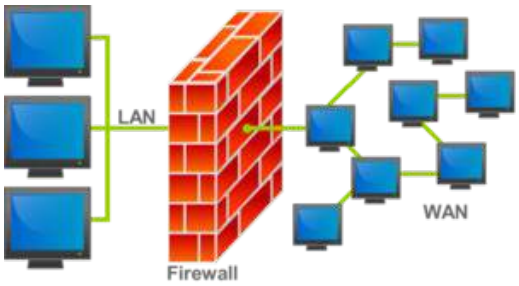


Figura 46: Un firewall

Comprendere la funzione e i limiti di un firewall

Quando le infrastrutture informatiche sono connesse alla rete sono vulnerabili alle intrusioni: molti programmi, tipicamente applicazioni per lo scambio di file, sfruttano la possibilità di accedere ai dati per carpire informazioni riservate, come le password, usando i PC come testa di ponte per entrare in reti aziendali. Per ovviare a questi inconvenienti si ricorre al firewall o "muro tagliafuoco", destinato cioè ad impedire la propagazione del fuoco, e per analogia del *malware*.

Il firewall è un dispositivo software e/o hardware posto a protezione di segmenti di rete, per regolare il traffico in ingresso e in uscita, secondo regole specifiche definite dagli amministratori: in questo modo tutte le connessioni in entrata e in uscita sono filtrate e il transito viene concesso solo a quelle esplicitamente autorizzate. Più in dettaglio, il compiti del firewall sono:

- impedire l'accesso ad Internet di applicazioni presenti sul computer che non sono abilitate ad accedere all'esterno
- impedire l'accesso alla rete interna da parte di applicazioni esterne che non sono abilitate ad accedere all'interno della rete (o del computer)
- filtrare contenuti non adatti al contesto di utilizzo (bambini, attività lavorativa, ...)
- segnalare all'utente e all'amministratore di rete i tentativi di accesso non autorizzati.

Esistono numerosi firewall software, sia Open Source sia commerciali, che rispondono alle più svariate esigenze. Fra quelli FLOSS, si possono citare per Linux:

- *Netfilter/iptables*, per il filtraggio del traffico di rete
- *Firestarter e Shorewall*, come interfacce grafiche a Netfilter/iptables.

Va infine osservato che in un sistema di comunicazione, possono essere installati più firewall, ognuno con uno scopo, un ambito e un gestore diversi: un Personal Firewall sul computer dell'utente, un firewall che separa la rete aziendale da Internet, un firewall presso l'Internet Service Provider.

Anche se rappresentano un valido strumento per filtrare e rendere più sicuro il traffico fra l'interno e l'esterno, i firewall presenta concretamente alcune limitazioni, fra le quali:

- il livello di protezione offerto dal firewall dipende strettamente dal modo in cui è stato configurato. Le regole di filtraggio devono essere molto attentamente analizzate per assicurare un'elevata protezione
- queste regole richiedono una costante attenzione e un regolare aggiornamento per far fronte ai rischi derivanti da nuovi attacchi o nuovi malware
- le regole non devono essere tali da penalizzare la regolare attività lavorativa nell'impresa
- i firewall non hanno nessuna utilità contro gli attacchi alla rete interna provenienti dall'interno. Se un PC è infetto da un malware o un collaboratore malevolo utilizza il suo PC per compiere attacchi dall'interno.

Comprendere il termine "one-time password"

Nelle linee guida sulla sicurezza si richiede che i sistemi informatici consentano agli utenti di cambiare autonomamente la propria password e si raccomanda agli utenti stessi di cambiarla frequentemente. Per maggiore sicurezza alcuni sistemi prevedono un cambio obbligatorio periodico (per esempio ogni 30 giorni). Naturalmente, la durata di validità della password non può essere così breve da penalizzare l'operatività dell'utilizzatore, ma è indubbio che al crescere della durata aumenta la possibilità che la password venga scoperta ed anche che ne sia fatto un utilizzo fraudolento.

Per operazioni critiche, come quelle che hanno risvolti finanziari diretti (bonifici per esempio), sono utilizzate password la cui durata è molto breve (30 secondi o 1 minuto). In questi casi, non è l'utente che la sceglie ma è generata automaticamente da un dispositivo elettronico (Figura 47). La validità nel tempo così ridotta della password ne rende l'intercettazione e soprattutto l'utilizzo improprio molto difficile.

Figura 47: Un generatore di password

Un altro approccio è quello della "one-time password", o password valida una sola volta. L'utente dispone come nel caso precedente di un dispositivo che genera la password oppure la riceve sul proprio telefono portatile in un SMS. Una volta inserita la password sul sito ed eseguita l'operazione, questa perde di validità e non può essere utilizzata per altre operazioni. Oltre a offrire un livello di sicurezza più elevato, questi sistemi in cui la password non è scelta dall'utente ma generata automaticamente, tutelano "malgrado loro" quegli utenti poco sensibili alle tematiche di sicurezza e poco desiderosi di rispettare le buone prassi per la gestione delle password (descritte al punto 3.4.2).

Figura 48: Un lettore di impronte digitali

Molti infatti usano password troppo semplici, magari se il codice utente è il proprio cognome usano il proprio nome come password, aggiungendo un numero progressivo tutte le volte in cui sono costretti a cambiarla: sergio2, sergio3, sergio4, ...

Identificare le comuni tecniche di sicurezza biometriche usate per il controllo degli accessi, quali impronte digitali, scansione dell'occhio

La password, abbinata o no ad un codice utente, è il sistema di controllo degli accessi maggiormente diffuso ma il suo livello di sicurezza non è molto alto. La protezione può essere rafforzata con dispositivi più sicuri come per esempio badge individuali (smartcard) ma anche questi possono essere rubati, oltre a richiedere appositi dispositivi di lettura collegati al personal computer che ne ne hanno finora rallentato la diffusione.

In casi in cui è richiesto un controllo dell'accesso ai dati (o dell'accesso a certi locali) di elevata sicurezza, si ricorre a dispositivi biometrici che sfruttano alcune caratteristiche fisiche dell'individuo anziché la sua conoscenza di una parola chiave. La caratteristica biometrica maggiormente in uso è quella delle impronte digitali (Figura 48). Un apposito lettore (di ridotte dimensioni e costo limitato, tant'è che ne sono addirittura dotai alcuni personal computer portatili) sul quale si passa il dito legge le impronte digitali e le confronta con quelle precedentemente memorizzate. Molto più complessi, voluminosi e costosi sono i dispositivi che effettuano una scansione dell'occhio riconoscendo le caratteristiche dell'iride dell'utente autorizzato.

Si può citare anche fra le tecniche di sicurezza legate a caratteristiche personali la firma grafometrica. La tecnica ,che stanno introducendo alcune banche nei rapporti con i clienti, consiste nel riconoscimento dei movimenti fatti nel firmare un documento. Adoperando un'apposita penna, l'utente firma su una tavoletta che trasmette le informazioni sulla firma ad un programma per confrontarle con quelle precedentemente depositate. Le tecniche di sicurezza biometrica oggi in corso di sperimentazione presentano un livello di protezione maggiore ma fanno nascere diverse problematica in termini di privacy e di misure di sicurezza per la protezione dei dati biometrici di riferimento inizialmente raccolti.

Riconoscere l'importanza di avere una procedura di copie di sicurezza per ovviare alla perdita di dati, di informazioni finanziarie, di segnalibri/cronologia web

Dell'importanza delle copie di sicurezza si è già detto nella parte che illustra come difenderci dai rischi. Addirittura si è suggerito, anche in un uso personale del computer, di pianificare i backup e definire una procedura di copie di sicurezza.

Quest'obiettivo è ancora più stringente per le imprese, vuoi per la natura dei dati che gestiscono, vuoi per il maggior numero di attacchi che possono ricevere, vuoi ancora per i rischi provenienti dall'interno. Diventa quindi di fondamentale importanza che l'intera attività legata alle copie di sicurezza sia pianificata in una vera e propria procedura, indipendentemente dalla dimensione e dalle caratteristiche dell'impresa e dalla gestione, interna o esterna, dell'informatica..

Non è sufficiente per esempio che qualcuno vada a sostituire periodicamente il supporto mobile sul quale vengono fatte le copie oppure ogni tanto a controllare che non sia pieno. Anche perché se il processo non è automatico e per mesi non vi è la necessità di ripristinare i dati, il livello di attenzione diminuisce e ci si "scorda" di fare le copie ...

Come accennato, oltre ad un backup locale può essere fatto un backup remoto. Se il computer è collegato ad una rete locale, tipicamente in situazioni lavorative, l'utente ha spesso a disposizione un'unità di rete (si veda il precedente punto 4.3.1). I file che vengono creati sono quindi prevalentemente memorizzati su questa unità di rete. Non solo questa unità è in un luogo separato rispetto al computer ma il backup regolare è assicurato dai tecnici che gestiscono il sistema informatico. Oltre ad unità personali dei singoli utenti sono spesso disponibili unità comuni (per gruppi di utenti, per ogni reparto, ...) che permettono di condividere dati e di accedervi da diverse postazioni ed anche queste unità sono oggetto di un backup.

Se il computer o il sistema informativo è collegato ad Internet, questo sistema è ulteriormente potenziato. Diversi siti infatti offrono servizi di archiviazione di dati su unità online. Malgrado il possibile inconveniente del rallentamento dovuto alla linea di trasmissione, questo sistema presenta diversi vantaggi per quanto riguarda il backup:

- il backup viene fatto sicuramente in un luogo separato (a volte non si sa nemmeno dove sono i server)
- vi sono numerosi servizi altamente professionali che garantiscono un elevato livello di sicurezza
- i costi sono commisurati all'utilizzo effettivo del sistema, con un costo fisso nullo o molto basso.

Va ricordato che lo scopo delle copie di sicurezza è di poter ripristinare completamente e in tempi brevi i contenuti del sistema informativo in seguito al verificarsi di danneggiamenti e assicurare la continuità dei servizi. A seconda dei sistemi, "contenuti" può significare solo i dati, i dati e i programmi applicativi, i dati, i programmi applicativi e il sistema operativo. Se la procedura di backup si riferisce soltanto ai dati, deve essere integrata con la definizione di procedure di re-installazione del software: l'importante non è di ripristinare i dati ma la funzionalità completa del sistema.

Identificare le caratteristiche di una procedura di copie di sicurezza, quali regolarità/frequenza, pianificazione, collocazione della memoria di massa

Per essere affidabile, una procedura di copie di sicurezza deve definire diverse caratteristiche quali:

- *Regolarità*. Come accennato, le copie di sicurezza non devono essere occasionali o lasciate all'iniziativa di singoli individui. Vanno invece svolte con regolarità, tramite una procedura automatica che esegue il backup ad orari prestabiliti, senza intervento umano. In caso di problema, errore, interruzione, impossibilità di effettuare il backup previsto, la procedura deve inviare una segnalazione automatica all'amministratore del sistema.
- *Frequenza*. La frequenza di esecuzione deve essere stabilita sulla base della quantità di dati da copiare, della loro criticità e del periodo massimo accettabile di perdita dei dati: fare una copia mensile dei dati (per assurdo) significa accettare di perdere fino a un mese di dati ossia quelli aggiunti e modificati dall'ultimo backup. Spesso la frequenza è giornaliera e il backup avviene di notte, periodo tipico di inattività. In situazioni più critiche, la frequenza può essere più alta (due o più volte al giorno)
- *Pianificazione*. Per lo stesso insieme di dati, la copia può essere differenziata per dati da copiare e frequenza di copia. Sono in uso sistemi di copia che, per esempio, copiano i soli dati quotidianamente e l'intero disco una volta alla settimana o una volta al mese, magari su supporti di archiviazione diversi. Nella pianificazione, andrebbero anche definite le procedure di prova periodica di ripristino e le procedure vere e proprie di ripristino in caso di problema.
- *Collocazione*. Fondamentale è la separazione fisica del luogo in cui risiedono ii dati da copiare e quello delle copie. Lasciarli ambedue nello stesso server o nella stessa stanza non è una buona norma in quanto non vengono gestiti i rischi di distruzione o di furto. Le copie di sicurezza vanno fatte su computer o unità

diverse, poste fisicamente in un luogo diverso. Va pertanto scelto il tipo di backup (locale o remoto) che potrà operare su dispositivi locali, su dispositivi collegati alla LAN o addirittura su server di Internet.

La Notizia

2 gennaio 2009

Slashdot (http://slashdot.org), storico e autorevole sito di news informatiche, con un articolo dal titolo apparentemente tecnico *Why Mirroring Is Not a Backup Solution* (Perché avere i dischi duplicati non è una soluzione di backup) racconta di un sito di blog, journalspace.com, nato nel 2002 e vissuto 6 anni, a quanto pare senza aver mai fatto le copie di sicurezza, fino a quando il suo database è andato distrutto, causando la morte dell'azienda. Negli ultima anni, con diverse migliaia di blogger aveva un traffico significativo di 14.000 visitatori al mese.

http://hardware.slashdot.org/story/09/01/02/1546214/why-mirroring-is-not-a-backup-solution

ripreso da Techcrunch all'indirizzo http://techcrunch.com/2009/01/03/journalspace-drama-all-data-lost-without-backup-company-deadpooled/

Va ricordato che le copie di sicurezza sono soltanto uno dei mattoni delle politiche di sicurezza dei dati ed è l'ultimo ricorso, in caso di danneggiamento. Si affiancano infatti a tutti gli altri, destinati a prevenire il furto o la distruzione dei dati nonché ad impedire all'eventuale ladro di utilizzare i dati rubati.