Modulo 4:
SICUREZZA INFORMATICA

1 . DEFINIZIONI

I *dati* sono numeri, lettere, immagini, suoni, simboli ecc., ai quali viene attribuito un significato, affinché rappresentino una realtà, in maniera elementare.
Più dati, elaborati e associati ad altri fattori attraverso un computer, danno vita a un'*informazione*.

1.1 Le finalità dell'IT Security

Lo scopo principale dell'IT Security è quindi garantire la protezione dell'integrità fisica (*hardware*) e logico-funzionale (*software*) di un sistema informatico e dei dati in esso contenuti o scambiati in rete, minimizzandone la vulnerabilità.

1.1.1 Gli standard di sicurezza informatica

Lo standard ISO/27001 è una norma internazionale che definisce i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni
La versione più recente della norma è la ISO/IEC 27001: 2013, che andrà gradualmente a sostituire la versione 2005.

1.1.2 Cosa proteggere?

Nell'ambito dell'IT Security, quindi, si protegge l'insieme delle componenti essenziali del **computer** (sistemi operativi, programmi e dati) e le **reti** che mettono in connessione i singoli dispositivi informatici.
Il **rischio**, in genere, è la risultante dell'equazione tra minaccia/vulnerabilità e contromisure.
La ***minaccia*** rappresenta l'azione capace di nuocere, la ***vulnerabilità*** rappresenta il livello di esposizione rispetto alla minaccia in un determinato contesto, la *contromisura* è l'insieme delle azioni attuate per prevenire la minaccia (anche sensibilizzazione utenti).

Obiettivi della sicurezza informatica

La sicurezza informatica, in generale, consiste nell'assicurare che le risorse hardware e software di un'organizzazione o di un utente siano usate unicamente nei casi e nei modi previsti dalle norme e dagli accordi intercorsi tra le parti.
L'obiettivo della sicurezza informatica è di garantire cinque aspetti dell'ICT:

- l'*integrità dei dati*: devono effettivamente essere quelli che le parti in causa legittimamente sono convinti che siano;
- la *confidenzialità*: solo le persone autorizzate devono poter accedere alle risorse scambiate;
- la *disponibilità*: coloro che ne hanno diritto devono poter sempre accedere a un servizio o alle proprie risorse;
- il *non ripudio*: una transazione o un'azione svolta non può essere negata a posteriori dall'operatore;
- l'*autenticazione*: assicura l'identità di un utente, garantendo a ciascun corrispondente che il suo partner sia effettivamente quello che crede.

1.1.3 I diversi tipi di minacce

Le minacce a cui sono esposti sistemi operativi, dati e informazioni sono riconducibili a due ordini di fenomeni.

- Gli *eventi accidentali*. Si tratta delle conseguenze di eventi non ponderabili e legati a elementi casuali quali, ad esempio, gli eventi atmosferici che determinano l'interruzione

dell'erogazione di energia elettrica e possono avere delle conseguenze sui sistemi operativi e sui dati.

- Gli *eventi indesiderati*. Sono le operazioni compiute da soggetti intenzionati a danneggiare il funzionamento dei dispostivi o a sottrarre informazioni e dati. In questo caso possiamo distinguere ulteriormente tra:
  - attacchi *malevoli*, finalizzati a intaccare il funzionamento dei sistemi,
  - *accesso ai dispositivi da parte di soggetti non autorizzati* e finalizzati alla sottrazione di dati e informazioni.

1.1.4 Crimini informatici e hacker

Chi è l'hacker

Si utilizza per identificare gli autori di crimini informatici. Un hacker, è prima di tutto un programmatore, cioè un utente capace di scrivere il codice con cui sono costruiti i software.

1.1.5 I diversi livelli di protezione

- *passive*, riconducibili ad accorgimenti fisico-materiali, quali, ad esempio, il posizionamento dei server in luoghi sicuri, dotati di sorveglianza;
- *attive*, disponibili anche sul tuo PC.

1.1.6 Esempi pratici di misure di protezione

Login e password

Per accedere a un PC e, poi, a qualsiasi account (di posta elettronica, di una home banking, di Facebook e così via), è necessario *autenticarsi*; è necessario, cioè, farsi riconoscere dal sistema, inserendo una password.

La *One-Time Password* (OTP) è una password valida solo per un accesso o una transazione. Ogni volta che l'utente deve accedere al servizio, crea una password *usa e getta*.

Una volta che hai inserito correttamente *username* e *password* nella login (del tuo PC o della tua casella di posta elettronica, ad esempio), potrai *autenticarti* ed entrare nel sistema. Da questo momento, le tue attività sono tracciate e monitorate da parte di chi gestisce il sistema: questo monitoraggio si definisce ***accountability***.

L'autenticazione a due fattori

È uno dei metodi più sicuri per proteggere i tuoi account.

Il funzionamento è molto semplice: per poter accedere al tuo profilo Facebook o Twitter, oltre all'username e alla password, devi inserire il codice che ti viene spedito istantaneamente tramite SMS, e-mail o che puoi trovare su un'apposita applicazione.

Il metodo più usato è la ricezione di un SMS o di una e-mail contenente il PIN (un codice da 4 a 6 cifre) da inserire nella login per completare l'accesso al tuo profilo. Non è il più sicuro: un pirata informatico può hackerare il sistema e ricevere sul proprio smartphone il codice che hai richiesto tu.

Doppia autenticazione tramite applicazione

Esistono alcune applicazioni (come *Google Authenticator* o *Authy*) che hanno reso molto sicura l'autenticazione.

Quando ci si iscrive a un nuovo servizio, è possibile creare un codice di sicurezza da condividere con lo smartphone attraverso un QR Code.

Come la biometrica migliora la sicurezza informatica

Con il termine biometria in informatica si intende un sistema in grado di riconoscere e identificare un individuo in base ad alcune caratteristiche fisiologiche.

Il sistema di riconoscimento delle informazioni biometriche di una persona viene anche chiamato AIDC (*Automatic Identification and Data Capture*).

Cancellare la Cronologia

1.2 Il concetto di privacy

1.2.2 La social engineering

Si definiscono *social engineering* (ingegneria sociale) e sono a metà tra psicologia e ingegneria: un ingegnere sociale studia il comportamento online della vittima e ne conquista la fiducia, durante conversazioni che indirizza conoscendo quali sono i suoi argomenti preferiti. La *social engineering* è una manipolazione psicologica che induce chi ne è vittima a comportarsi in una determinata maniera o rivelare informazioni personali senza rendersene realmente conto.

1.2.3 Il furto d'identità

Altra attività che rientra nella *social engineering* è il furto di identità e, cioè, il furto di dati personali e sensibili a scopo di frode, (spesso sui social network).

1.2.4 Come difendersi dagli attacchi di ingegneria sociale

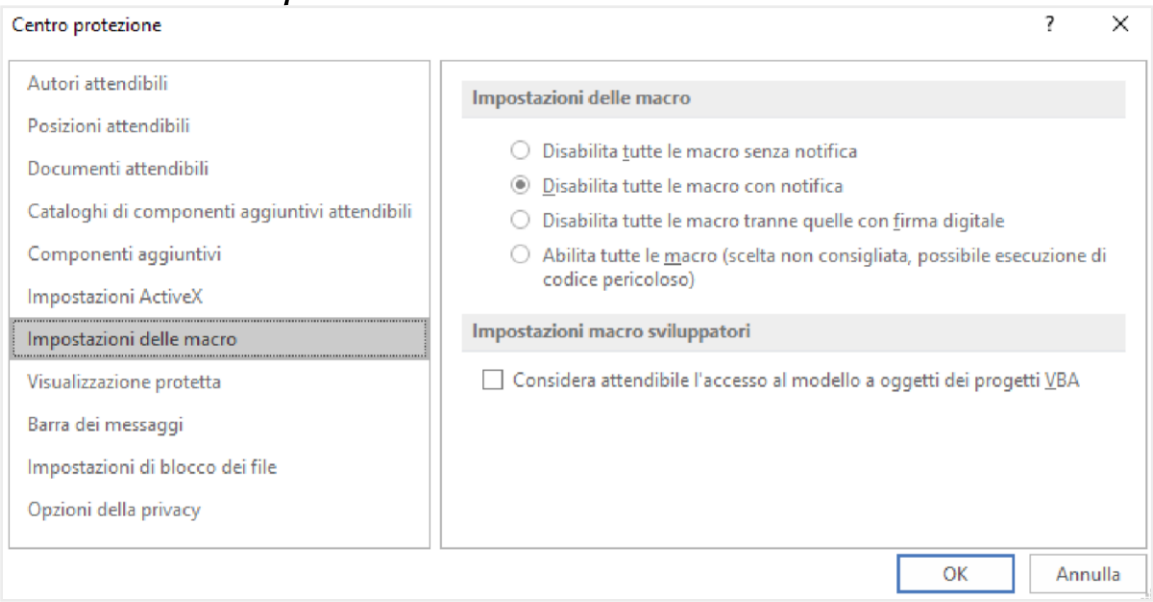
Tenere un certo comportamento online è il modo migliore per evitare problemi anche gravi.
Proteggi le tue transazioni online utilizzando firewall, antivirus e antispyware, e nascondendo la tua connessione wireless domestica. Mantieni aggiornati tutti i software (browser compreso) attraverso gli aggiornamenti automatici.
Fai attenzione a offerte troppo vantaggiose, agli avvisi della banca che comunica l'immediata chiusura del tuo conto se non esegui azioni immediate, agli avvisi di vincita di lotteria o ai rifiuti di un incontro di persona per concludere una transazione.
Crea password complesse, ne abbiamo già parlato. Tieni segreti password e PIN (numeri di identificazione personale) e non inviarli mai per email o con messaggi istantanei. Devi utilizzare password diverse per ognuno dei tuoi account; se utilizzi sempre la stessa, chiunque se ne impadronisca, metterà a rischio tutte le tue informazioni sensibili.
Digita tu stesso gli indirizzi dei siti Web a cui vuoi accedere: se lo fai cliccando su collegamenti contenuti in messaggi in email, SMS, messaggi istantanei o pubblicità pop-up, potresti essere portato su siti legittimi solo in apparenza ma, in realtà, per niente affidabili.
Controlla gli indicatori di protezione delle informazioni dei siti che stai visitando. Se sei in un sito e-commerce e intendi fare un acquisto online, prima di immettere i tuoi dati, verifica che nella barra degli indirizzi, prima del nome del sito, ci sia la dicitura https (la s sta per *secure*) e il logo del lucchetto chiuso. Sono indicatori che ti fanno capire che il sito è sicuro.
Usa solo il tuo PC per fare ogni transazione finanziaria. Non pagare, non fare acquisti o altre attività finanziarie su un computer pubblico o condiviso, oppure su dispositivi come PC portatili e smartphone, che siano connessi a Reti pubbliche wireless. La protezione, in questi casi, non è affidabile.
Usa sempre il buon senso e se hai dubbi di qualsiasi tipo, prima di fare alcunché, chiedi informazioni a qualcuno più esperto di te.

1.3 Misure per la sicurezza dei file

1.3.1 Attivare e disattivare macro

Nei file di Office (Word, Excel e così via), le macro sono delle scorciatoie che, tramite la pressione di combinazioni di tasti e clic del mouse, ti consentono di eseguire in modo veloce attività frequenti.

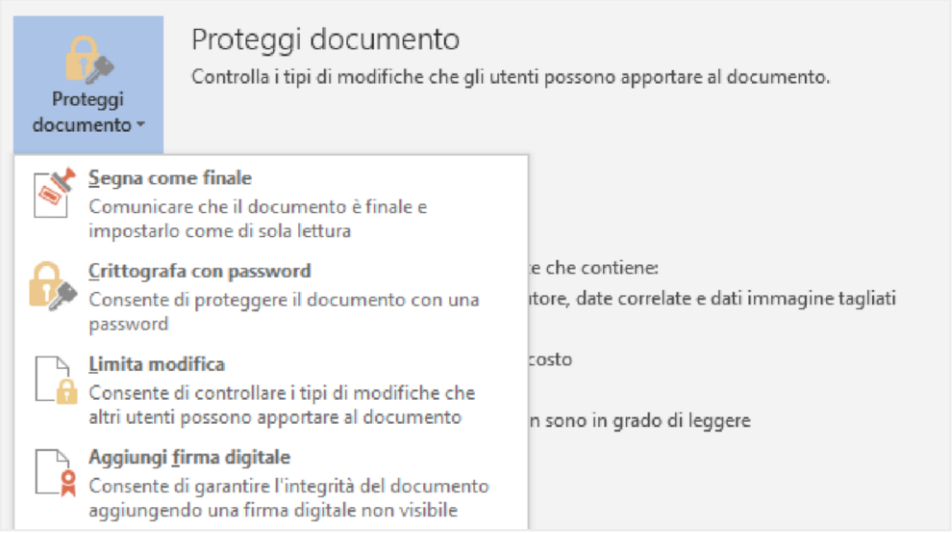
1.3.2 Cambiare le impostazioni delle macro



Per lo stesso motivo, ti consigliamo, inoltre, di non attivare l'opzione *Considera attendibile l'accesso al modello a oggetti dei progetti VBA*.

1.3.3 Cifrare e impostare password per la sicurezza dei nostri file

- Attivare l'opzione *Nascosto*, nella finestra di dialogo *Proprietà*.
- Inserire una password per aprire il file (*File* > pulsante *Proteggi documento)*.



2 . MALWARE

2.1.1 I malware

Malware (contrazione delle parole *malicious* e *software):* indica un qualsiasi programma creato allo scopo di causare danni a un dispositivo su cui viene eseguito e sui dati che vi sono immagazzinati. Ce ne sono di due tipi:

- di tipo parassitario, trasmessi mentre il computer è in funzione;
- del settore d'avvio, trasmessi quando colleghi e tenti di avviare un disco esterno: il virus si aggancia in memoria come se fosse un driver di una periferica ed è difficilissimo da rimuovere.

Il primo malware, conosciuto come *Brain*, fece la sua apparizione nel 1986.

Allora i computer erano davvero molto pochi rispetto a oggi: la propagazione era poi limitata dal fatto che, per infettare un PC, era necessario che vi fosse materialmente inserito un *floppy* infetto.
Brain costituì una vera ispirazione per gli appassionati di *software* che, da allora, iniziarono a gareggiare per dimostrarsi più bravi degli altri nell'accedere a sistemi governativi o sviluppare programmi capaci di diffondersi rapidamente in tutto il mondo (il primo ad avere grande diffusione fu denominato *Morris).*
Fino al 2000, i malware non erano molto dannosi (le finalità erano, appunto, goliardiche) ed erano facilmente rimovibili.
Con il nuovo millennio, le cose sono cambiate di molto: l'aumento esponenziale di connettività e numero di utenti, ha indotto molti a utilizzarli per fini criminali.

2.1.2 I malware più diffusi

Il ***virus*** (termine con cui generalmente, ma erroneamente, vengono indicati tutti i malware) è un piccolo programma, che contiene una sequenza di istruzioni in grado di attivare automaticamente azioni che danneggiano un computer.
Agisce in maniera simile a un virus biologico: è pericoloso, quindi, per la sua tendenza a creare epidemie: parte delle istruzioni del programma infettivo sono deputate alla riproduzione di copie di sé stesso. Dopo la fase riproduttiva, i virus informatici iniziano a svolgere attività di diversa natura e, anche quando non sono direttamente dannosi per il sistema operativo che li ospita, comportano un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso.
In generale, un virus danneggia direttamente solo il software della macchina che lo ospita, anche se può indirettamente provocare danni anche all'hardware, ad esempio causando il surriscaldamento della CPU, fermando la ventola di raffreddamento.
Il ***worm*** (letteralmente traducibile con la parola *verme*) rallenta il sistema attivando operazioni inutili e dannose.
Il ***trojan horse*** è un programma che l'utente scarica perché ha funzionalità utili e desiderate, ma che, se eseguito, avvia, a sua insaputa, (da qui il richiamo al cavallo di Troia), istruzioni dannose per i file.
I ***dialer*** gestiscono la connessione a Internet tramite la vecchia linea telefonica. Possono essere utilizzati per modificare il numero telefonico digitato dall'utente, per chiamare, ad esempio, numeri a tariffa speciale, in modo da trarne profitto illecitamente.
Un ***hijacking*** indirizza su siti diversi da quelli digitati, oppure cambia la pagina predefinita del tuo browser.
La ***zip bomb*** è un programma (di solito compresso) che disattiva le difese del PC per consentire a un altro virus di infettarlo.
Gli ***spyware*** sono usati per spiare le informazioni del sistema sul quale sono installati (abitudini di navigazione, password e altri dati sensibili) che sono quindi acquisite da un terzo interessato ma non autorizzato.

Gli spyware

- *Phishing*: e-mail, con campi da compilare, link o finestre a comparsa, con l'intento di carpire i dati che l'utente dovrebbe inserire per rispondere all'invito o di farlo connettere a specifici siti.
- *Vishing*: usa il telefono per farsi comunicare i dati di accesso.
- *Pharming:* riprodurre un sito Web ufficiale, in modo che il mal capitato inserisca i suoi dati tranquillamente.
- *Sniffing*: intercettazione passiva dei dati che transitano in una rete telematica, attraverso software detti, appunto, *sniffer*.

Come si diffondono gli spyware

- Possono essere installati automaticamente sul tuo PC, attraverso siti Internet infetti;
- Puoi installarli manualmente (ma in maniera involontaria), scegliendo di utilizzare programmi gratuiti (*software freeware*) che riescono facilmente a infettare PC che non abbiano difese sufficientemente alte.

Come riconoscerli?

Si attivano delle azioni che, altrimenti, non si attiverebbero mai.

- *Pop-up pubblicitari*.
- *Modifica di impostazioni che sei certo di non aver cambiato personalmente e non riesci a resettarle*. (pagina iniziale del browser).
- *Componenti aggiuntive che non ricordi di aver scaricato*. (barre degli strumenti superflue).
- *Il computer è lento*.

Prevenire e rimuovere uno spyware

Oltre all'antivirus, ci sono programmi specifici per la rimozione degli *spyware*.

- Ad-Aware SE Personal Edition
- Emsisoft Anti-Malware
- Malwarebytes' Anti-Malware
- HijackThis
- Norman Malware Cleaner
- Spybot - Search and Destroy
- SpywareBlaster
- Spyware Terminator
- SUPERAntispyware

2.1.3 Altre categorie di attacchi informatici: gli attacchi login

Thiefing: sottrarre servizi informatici (collegarsi alla wifi del vicino)

Keylogger: intercettare tutto quello che un utente digita su una tastiera (bancomat). Due tipi:

- *hardware*: dispositivi che vengono collegati al cavo di comunicazione tra la tastiera e il computer o all'interno della tastiera;
- *software*: programmi che controllano e salvano la sequenza di tasti che viene digitata da un utente.

2.2 Gli strumenti di difesa

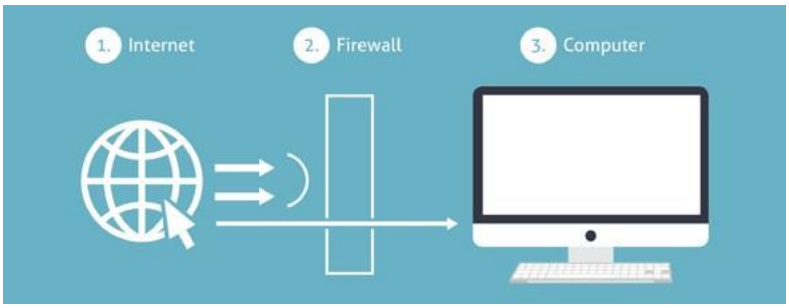
Il principale strumento per la difesa della privacy e dei dati è il tuo buon senso.

2.2.1 A cosa serve il firewall

- bloccare i malware, anche non conosciuti, prima che questi entrino nel computer;
- bloccare all'interno del PC i malware che siano riusciti a entrare, evitando così che possano infettare altri dispositivi eventualmente collegati.

Il firewall:

- impedisce a un malware di infettare la macchina prima che venga individuato dall'antivirus,
- nasconde il computer durante la navigazione, diminuendo al minimo i rischi.



Diversi tipi di firewall

- *a filtraggio di pacchetti*, più comuni, meno costosi e più veloci, ma con alcuni punti deboli
- *a livello di circuito*, livello di protezione più elevato, ma sono più costosi e lenti. Esaminano non soltanto l'intestazione ma anche il contenuto dei *pacchetti* in transito.

2.2.2 L'antivirus

E' un software ideato per:

- prevenire l'infezione,
- rilevare ed eventualmente eliminare programmi malevoli che insidiano la sicurezza dei computer.

2.2.3 Il funzionamento di un software antivirus

L'antivirus identifica la minaccia passando al setaccio il PC, i file e la RAM: in pratica, confronta tutto ciò che è in funzione sul PC con il proprio database delle firme dei malware.
Se identifica un file contenente una di queste firme, lo blocca e segnala subito la cosa.

Le diverse parti dell'antivirus

L'antivirus è composto da tre elementi: il file delle firme, il file di ricerca del virus, il file per l'aggiornamento.

2.2.4 Scansione del sistema

I diversi tipi di scansione disponibili

- *Scansione completa:* analizza file e applicazioni in esecuzione in tutte le unità del computer.
- *Scansione su misura o personalizzata:* consente di selezionare le unità e le cartelle da sottoporre a scansione.
- *Scansione rapida:* verifica l'integrità dei file caricati all'avvio del sistema operativo e la memoria di sistema.
- *Scansione intelligente:* verifica le aree più soggette a infezione.

Antivirus real-time

Analizzano le operazioni eseguite istantaneamente sul PC.

Risultati scansione

Selezionare le *opzioni di correzione*.

- *mettere in quarantena i file infettati*: saranno isolati in una sezione del PC da cui non si possono muovere; puoi ripristinarli in qualunque momento, se necessario;
- *rimuovere* il file in maniera permanente (senza metterlo in quarantena).

2.2.5 L'aggiornamento dell'antivirus

Le organizzazioni che si occupano di raccogliere le segnalazioni di virus si chiamano CERT (*Computer Emergency Response Team*, squadra di risposta alle emergenze informatiche).

2.3 I malware poliformi e l'euristica

Il malware polimorfo è in grado di nascondere il proprio codice: lo fa utilizzando una chiave diversa in ogni tentativo di infezione. È dotato di un motore, anch'esso cifrato, che modifica in maniera casuale la procedura che attiva l'infezione.
Riassumendo, abbiamo imparato che:

- l'antivirus è in grado di eliminare soltanto i malware che riconosce, ossia quelli già presenti nel suo database,
- i nuovi malware (quelli non riconosciuti e quelli che non sono ancora stati scoperti) possono passare completamente inosservati e non essere rilevati.

Oggi tutti gli *antivirus* si aggiornano automaticamente, non appena è disponibile una connessione online.

3. LA SICUREZZA DELLE RETI

3.1.1 Rete e networking

In informatica, si definisce rete un gruppo di computer collegati fra loro in modo da scambiare informazioni sotto forma di dati: è questo il sistema tramite cui, in una rete informatica, è possibile condividere e far circolare elementi *immateriali* tra tutti i dispositivi connessi.

Rete (in inglese, *network*)	Attuazione di una rete (*networking*)
Insieme di computer e periferiche connesse le une alle altre: due computer connessi tra loro costituiscono una *rete minimale*.	Strumenti e compiti che permettono di collegare diversi computer tra loro, affinché possano condividere delle risorse, *in rete*.

3.1.2 Le reti

È possibile classificare le reti informatiche a seconda della dimensione.

Nel modulo dedicato ai principi dell'ICT, abbiamo parlato di rete LAN, *Limited area network* (con estensione limitata), WAN, *Wired Area Network* (si estende su un territorio che può essere molto ampio) e MAN (rete di estensione intermedia).

Ogni rete è costituita, comunque, dai seguenti elementi:

- *Server*: sono i computer che conservano i dati cui possono accedere i client.
- *Client*: sono i computer degli utenti che accedono ai dati forniti dal server di rete.
- *Supporto di connessione*: è il sistema che collega i computer coinvolti.
- *Dati condivisi*: sono i file resi accessibili dal server ai client collegati.
- *Stampanti e altre periferiche condivise*: risorse utilizzabili dagli utenti della rete.

3.1.3 LAN

Qualsiasi dispositivo (server, computer, laptop, stampante, televisore, hard disk, NAS) può diventare *nodo* di una LAN e condividere tutte le proprie risorse con gli altri nodi/dispositivi.

LAN a stella

È il tipo più semplice: tutti i nodi sono collegati a un dispositivo centrale (*centrostella*).

LAN a bus

Tutti i nodi collegati sono agganciati direttamente al medesimo *cavo fisico*: è facile e poco costosa da realizzare ma è anche poco affidabile.

LAN ad anello

È un esempio di rete *peer-to-peer*: tutti i nodi possono ricoprire sia il ruolo di *server* che di *client*, essendo collegati in fila; l'ultimo si dovrà collegare al primo, chiudendo il cerchio.

LAN mesh

Anche la LAN *a maglia* è un esempio tipico di connessione p2p: non esiste un ordine gerarchico tra i nodi, che:

- possono comportarsi, a seconda dei casi, come *server* o *client*;
- sono collegati a un numero variabile di altri nodi, senza seguire uno schema preciso.

3.1.5 Ruolo e compiti dell'IT manager, nel campo della sicurezza

Normalmente le reti sono gestite da un *amministratore di sistema* (IT manager) che deve riconoscere la natura di questi attacchi e mettere in pratica le giuste contromisure.
Per garantire la sicurezza della rete, quindi, l'IT manager deve pianificare e attuare una serie di interventi integrati e finalizzati a:

- difendere i singoli dispositivi connessi alla rete (tramite il firewall e l'aggiornamento dell'antivirus);
- proteggere la rete nel suo complesso;
- proteggere i dati memorizzati nei database.

3.2 Navigare sicuri con le reti wireless

Se una rete wireless non è protetta da password, chiunque, nelle vicinanze, potrebbe collegarsi senza alcuna difficoltà.

3.2.2 Diversi tipi di protezione

Gli sviluppatori di tecnologie Wi-Fi hanno creato vari protocolli di sicurezza per le reti wireless. Vediamo le differenze tra i protocolli WEP, WPA e WPA2

WEP (Wired Equivalent Privacy)

Viene dichiarato standard per la sicurezza Wi-Fi nel settembre del 1999, quando si sostiene che riesce ad assicurare lo stesso livello di sicurezza delle reti cablate.
La WiFi Alliance lo ha abbandonato definitivamente nel 2004 perché non abbastanza sicuro.

WPA (Wi-Fi Protected Access)

Il protocollo WPA è il risultato del potenziamento/miglioramento del WEP. È stato adottato formalmente nel 2003, soprattutto perché compatibile con i dispositivi che utilizzavano il WEP. Esiste la modalità *personal* (reti domestiche) e modalità *enterprise* (reti aziendali)
Questo protocollo, dipendendo molto dalla vecchia tecnologia WEP ed essendo compatibile con lo stesso, è risultato essere molto vulnerabile alle intrusioni.

WPA2

Il protocollo WPA2 è il più sicuro. Persiste la distinzione tra le modalità *personal* e *enterprise*.

3.2.3 Cos'è e come funziona l'hotspot

L'hotspot è un *punto di accesso* a internet che, sfruttando il Wi-Fi, è a disposizione dei device di tutti coloro che sono nelle vicinanze.
L'esercente che offre il servizio, di norma, imposta una password di accesso. In questo modo l'utente è rintracciabile in tutte le sue operazioni.

Hotspot personale: il tethering

Anche uno smartphone può fungere da hotspot (in questo caso si parla di *tethering*).
Sai cos'è il *roaming*? E' la capacità del dispositivo di collegarsi alla rete migliore disponibile.

3.2.5 Diversi tipi di attacchi alle connessioni wireless

- **Intercettazione o eavesdropping:** indica l'atto del malintenzionato di ascoltare conversazioni altrui e di registrare tutte le informazioni utili (come per esempio login e password) che riesce a carpire. Si parla, in definitiva, di una tecnica di intercettazione.
- **Jamming:** il malintenzionato crea interferenze per rendere inutilizzabile un canale di comunicazione via radio.
- **MITM (man-in-the-middle attack):** si interpone in una comunicazione, fingendo di essere una delle parti coinvolte o entrambe.

4 . NAVIGARE IN SICUREZZA

(questa parte è già stata trattata nel modulo 2)

Per approfondimenti consulta la dispensa.

5 . SICUREZZA NELLE COMUNICAZIONI ONLINE

Possiamo distinguere le minacce in due gruppi principali:

- Infiltrazioni *malware* tramite allegati;
- Posta indesiderata.

5.1.1 La cifratura come argine alle infiltrazioni malware

Cifrare vuol dire utilizzare programmi che ci consentono di crittografare un messaggio in modo che non siano più leggibili o alterabili da eventuali intrusi. Alcuni di questi programmi sono online (webmail), altri sono da installare sul PC. Uno di questi è **ProtonMail.** Permette di creare un nuovo indirizzo e-mail su questo sito: le e-mail inviate tra utenti che hanno un indirizzo Protonmail vengono crittografate e decrittografate automaticamente.

Se la mail viene inviata verso un indirizzo di posta normale, si può usare una domanda segreta a cui il destinatario deve rispondere per poter leggere il messaggio.

5.1.2 Firma digitale e crittografia

Differenze tra *firma digitale* e *crittografia* (cifratura).

- Quando si appone la firma digitale a un messaggio, al suo interno vengono incorporate le informazioni che certificano l'identità del mittente;
- Quando un messaggio viene criptato, appare *scritto in codice* e può essere letto soltanto da un destinatario che sia in possesso della chiave adatta a decriptarlo.

La firma digitale garantisce che il messaggio inviato sia stato effettivamente spedito da un mittente certificato; la criptazione fornisce la certezza che il messaggio non sia stato letto o alterato durante la sua trasmissione.

5.1.3 Le caratteristiche del phishing

Il Phishing è il malware più utilizzato per carpire dati in rete in modo fraudolento. Criminali cibernetici inviano e-mail apparentemente ufficiali di banche, fornitori di servizi di pagamento e negozi online, in cui si chiede all'utente di inserire dati, o cliccare su link che rimandano a pagine di login false.

Come riconoscere e-mail fraudolente

- Se ricevi una mail da una banca, un ente pubblico o una grossa azienda, verifica se sei entrato già in contatto o hai fornito il tuo indirizzo alla persona o all'ente che compare come *mittente*.
- Di solito enti e aziende si rivolgono ai loro clienti chiamandoli per nome; i truffatori spesso non hanno questo dato: se un messaggio della tua banca comincia con *Gentili Signori e Signore* o altre forme generiche, ti conviene diffidare.
- Se un messaggio di posta elettronica è pieno di *errori grammaticali*, è molto probabile che si tratta di una truffa: errori di ortografia e informazioni contorte sono un chiaro indizio delle intenzioni fraudolente di quella e-mail, scritta probabilmente in un'altra lingua e poi tradotta da traduttori automatici.
- Se un messaggio contiene un link, ti conviene verificarlo, prima di cliccarci su. Posiziona il mouse sul link e controlla l'indirizzo Internet mostrato in basso a sinistra nella finestra del browser.

Controlla che:

- l'URL coincida con quello che ti aspetti, visto il contento e il mittente;

- siano presenti protocolli HTTP di sicurezza per la trasmissione di dati.

Se hai dubbi, non cliccare sul link e non inserire manualmente l'URL nel tuo browser.

- Nessun negozio online chiede ai propri clienti di trasmettere dati personali tramite e-mail. Se in un messaggio ti trovi davanti a un form da compilare, puoi star certo che si tratta di un tentativo di *phishing*. Stesso discorso vale per i codici PIN.
- Se una mail contiene un invito all'azione immediata è necessario prestare molta attenzione. I truffatori a volte usano le maniere forti per mettere sotto pressione gli utenti e spingerli ad azioni avventate. Il punto è che nessuna azienda minaccia un blocco della carta di credito o il ricorso a un'agenzia di recupero crediti, costringendo così a inserire una password o a scaricare un allegato. Nel dubbio, chiama l'assistenza clienti del mittente.

Cosa fare contro i tentativi di phishing

Se ricevi un'e-mail che sembra un tentativo di *phishing*, spostala nella cartella *Spam* della tua casella di posta e blocca il mittente. In questo modo bloccherai altri eventuali attacchi provenienti dallo stesso mittente.

Puoi, inoltre, contattare l'azienda o la persona per cui si sta spacciando chi vi ha inviato l'email. La maggior parte delle aziende mette a disposizione diverse possibilità di contatto, come per esempio moduli da compilare, con cui è possibile segnalare un tentativo di phishing.

5.1.4 La posta indesiderata

Lo *spam* è un disturbo alla nostra comunicazione online, arrecato da terzi mediante l'invio di messaggi non richiesti.

Lo *spammer* è colui che invia, tutte assieme, tantissime email a scopo pubblicitario o per fare phishing, senza alcun consenso da parte del destinatario, anche per conto di terzi: ci sono aziende che fanno questo per lavoro!

Cosa fare per non essere spammato

- *Non pubblicare il tuo indirizzo e-mail in pagine web*.
- Uno dei trucchi più utilizzati dagli *spammer* per indurti a rispondere e verificare che, in effetti, il tuo indirizzo sia un valido bersaglio, è quello di inserire nei messaggi false opzioni di cancellazioni (del tipo *Se non vuoi ricevere altre mail da noi, clicca qui*). *Non rispondere mai, non serve protestare*.
- Ricordati di *usare e fare usare sempre la copia carbone nascosta (CCN)* per inviare lo stesso messaggio a più persone.
- Quando usi un servizio online (fai un acquisto, ad esempio) *leggi l'informativa sulla privacy* per verificare che non sia prevista la divulgazione del tuo indirizzo ad altre aziende partner: spesso puoi scegliere se lasciare questa libertà o meno al gestore del sito.

5.1.5 Come gestire in sicurezza una casella di posta su Gmail

La *password* (più è complessa più è difficile che altri se ne approprino o possano scoprirla):

- Deve essere composta da almeno 6/8 caratteri,
- Deve contenere numeri, lettere (minuscole e maiuscole) e simboli (! ? _ -)
- Non deve mai essere lasciata in giro (come ad esempio su un post-it o su un foglietto).
- Non devi mai inviarla tramite e-mail e chat.

Strumenti per la sicurezza dell'account Gmail

Gmail mette a disposizione diverse tipologie di strumenti per la sicurezza del tuo account:

- quelli passivi ti permettono di monitorare e segnalare azioni altrui;
- quelli attivi servono a prevenire le azioni altrui; puoi impostarli tu stesso. Il più importante è il filtro anti spam; lo vedremo nella prossima sezione.

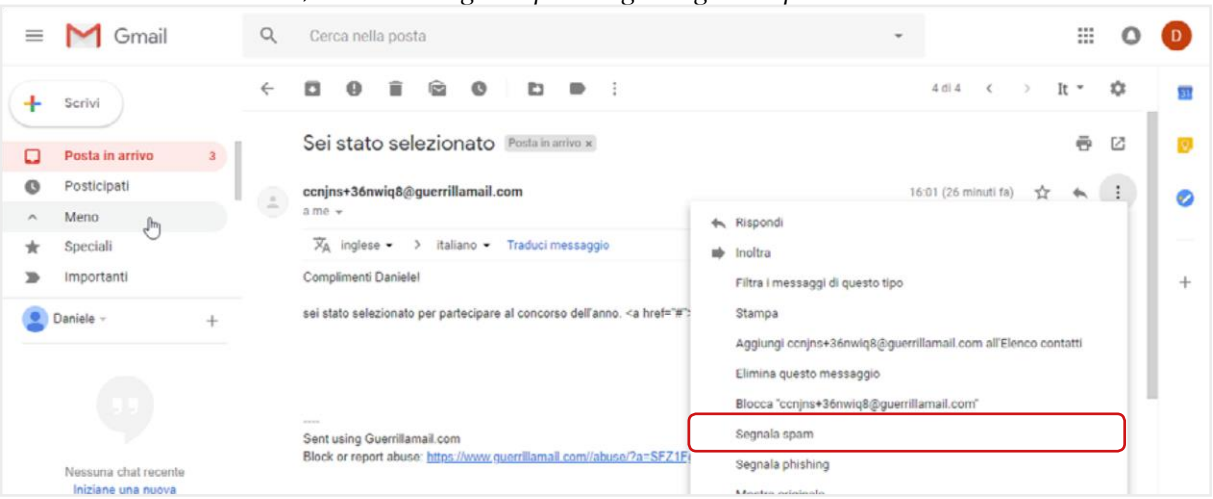
Puoi monitorare le tue ultime attività verificando, ad esempio, che non ci siano stati eventuali *accessi non autorizzati* alla tua casella di posta.

Nella sezione *Dettagli*, nella parte inferiore dell'interfaccia di Gmail, è possibile vedere quando e dove sono stati fatti gli accessi.
Puoi, inoltre, segnalare:

- Un tentativo di *phishing* (messaggi che ti richiedono informazioni personali),
- Mail *spam* (con contenuto non desiderato o per cui non hai mai autorizzato la ricezione o, semplicemente, non desiderata).

In entrambi i casi:

1. Apri il messaggio che desideri segnalare.
2. Clicca sul pulsante *Altro*
3. Nel menu a tendina, clicca su *Segnala phishing* o *Segnala Spam*.



La mail segnalata come *spam*, viene spostata nell'apposita cartella.
Per rimuovere definitivamente queste mail:

1. Fai clic su *Spam* nel menu a sinistra. Se la voce *Spam* non compare, clicca su *Altro*: il menu si espande mostrando tutte le opzioni.
2. Clicca su *Spam*.
3. Seleziona il o i messaggi che desideri eliminare e fai clic sul comando in alto *Elimina definitivamente*.

E' consigliabile segnalare sempre i messaggi che non si desidera ricevere, per aiutare Gmail a rendere più efficiente il sistema che tende a eliminare il problema dello *spam*.
In questa stessa pagina, puoi decidere di *salvare* un messaggio che Gmail o tu stesso hai precedentemente contrassegnato come *spam*.
Selezionalo e fai clic su *Non spam* nella parte superiore dell'interfaccia. Sarà automaticamente spostato nella *Posta in arrivo.*

L' uso di un filtro antispam per le email

Impostare il *filtro antispam* è uno dei modi migliori per rendere sicuro il nostro account.
Quando ricevi una mail indesiderata:

1. Selezionala.
2. Clicca sullo strumento *Altro* nella barra delle etichette.
3. Seleziona la voce *Filtra i messaggi di questo tipo*

4. Accedi a una finestra in cui devi riempire appositi campi che corrispondono ai criteri del tuo nuovo filtro.
Puoi modificare o eliminare filtri esistenti.

5.2 Come gestire gli strumenti di comunicazione online

5.2.1 I possibili rischi alla sicurezza di blog e Social network

Attivazione e gestione di account

Abbiamo visto come attivare, ad esempio, un account di Gmail; le stesse regole circa la creazione e la conservazione delle credenziali vale per ogni altro account tu voglia aprire.

Qui ti proponiamo di riflettere su un altro aspetto e, cioè, circa l'opportunità o meno di pubblicare e condividere determinate informazioni personali tramite i Social.

Da questo punto di vista, infatti, è importante sapere che ogni dato pubblicato può diventare oggetto, non solo di appropriazione indebita, ma anche di analisi e studio.

Sono molti, infatti, coloro che, a seconda dei casi, sono o possono essere interessati… a conoscerti meglio. Qualche esempio?

- Di solito, tra le condizioni che accetti (senza mai leggere!) quando ti iscrivi a un Social, c'è il consenso, rilasciato al gestore del servizio, di trasferire i tuoi dati a terzi per finalità statistiche o, molto più spesso, commerciali. Anche se tu decidessi di cancellare il tuo account, questi dati resterebbero, per il gestore e i terzi, disponibili e utilizzabili. In casi del genere, è certo che riceverai proposte commerciali che non hai mai richiesto, anche dopo che avrai eventualmente chiuso quell'account.
- I tuoi dati possono essere cercati e visionati, a tua insaputa, dall'azienda a cui hai mandato il curriculum, proponendoti come collaboratore. È molto probabile che vogliano farsi un'idea su di te, ancor prima di un eventuale colloquio.
- Se è vero che ognuno di noi è libero di esprimere le proprie idee, anche politiche e/o religiose ed etiche, è altrettanto vero che anche i governi occidentali hanno cominciato ad acquisire dai Social informazioni che ritengono possano essere utili per arginare fenomeni come, ad esempio, quello terroristico. La cronaca di tutti i giorni racconta come arresti ed espulsioni siano, sempre più, la conseguenza di esternazioni fatte e acquisite sui Social.

La sicurezza nei blog

La metà dei blogger sono adolescenti che, nella maggior parte dei casi, indicano la propria età e rivelano il proprio indirizzo e altre informazioni di contatto.

La crescente competitività, inoltre, porta molti a fare di tutto per attrarre l'attenzione: capita spesso, quindi, che i ragazzi pubblichino materiale non adeguato (come, ad esempio, fotografie provocanti di se stessi o di amici).

Sarebbe opportuno che, assieme ai genitori, fossero stabilite regole condivise circa:

- il tempo concesso per restare connessi in Internet o anche solo per utilizzare il PC di casa o lo smartphone;
- la verifica del materiale che i ragazzi intendono pubblicare, prima che siano già online. Anche foto apparentemente innocue, ad esempio, possono causare problemi;
- controllo della piattaforma del blog: se c'è un'area privata protetta da password, è giusto che sia condivisa.

Questi suggerimenti, come quelli che seguono, non possono essere esaustivi ma sono un buon punto di partenza.

- Non fornire informazioni personali (come, ad esempio, cognome, informazioni di contatto, indirizzo di casa, numeri di telefono, indirizzo di posta elettronica, cognomi di amici o familiari, nomi di messaggistica istantanea, età o data di nascita).
- Non pubblicare immagini provocanti di se stessi o di altre persone e accertarsi che le immagini pubblicate non rivelino alcuna informazione personale.

- Riflettere sempre prima di pubblicare qualcosa, poiché il materiale pubblicato sul Web è permanente (aldilà del discusso diritto all'oblio). Chiunque, infatti, può stampare facilmente l'articolo di un blog o salvarlo per sempre sul suo computer.
- Utilizzare i siti di provider più conosciuti, in cui le note legali sono chiare e spiegate.
- Non entrare in competizione con altri blogger. È sempre preferibile avere un approccio positivo e mai mirato alla calunnia o all'attacco degli altri utenti o di persone e istituzioni pubbliche.

La sicurezza nei Social network

Tutti i Social hanno ricche sezioni dedicate all'assistenza degli utenti.
Quella di Facebook, ad esempio (Centro assistenza), dedica molto spazio agli strumenti messi a disposizione per curare privacy e sicurezza.
Augurandoci che quello che abbiamo detto finora stia cominciando a stuzzicare il tuo interesse, ti diamo qualche dritta in proposito.
Tieni sempre presente che:

- Anche il tuo profilo, come quello di molti, è pubblico (visibile, cioè a tutti o quasi),
- Facebook modifica le impostazioni sulla privacy, rendendo pubbliche delle informazioni che prima erano visibili solo agli amici: è importante, quindi, prendere la buona abitudine di rivedere, di tanto in tanto, le impostazioni sulla privacy.

1. Impedisci ai tuoi amici di condividere le tue informazioni.
2. Rimuovi la tua faccia dai suggerimenti di tag.
3. Controlla i tag e decidi se approvare la foto (o video, o post); se non approvi, non verrà pubblicata sul tuo diario e non sarà visibile dai tuoi amici.
4. Restringi il pubblico per i vecchi post.
5. Imposta il livello di privacy che ritieni più appropriato per le informazioni che hai pubblicato sul tuo profilo.
6. Disattiva la ricerca pubblica per evitare che il tuo profilo compaia nei risultati dei motori di ricerca (Google, Bing ecc.).

Sarebbe davvero un buon esercizio, adesso, connetterti al centro assistenza e mettere in pratica questi consigli, aggiornando il tuo profilo Facebook!

Consigli utili

Aldilà delle opzioni che decidi di impostare, ricorda sempre di usare questi strumenti in maniera equilibrata, non facendoti prendere dalle dinamiche di gruppo.

- Se, ad esempio, una tua amica pubblica il suo numero di telefono o foto in cui sono raffigurate in pose non proprio eleganti, non devi sentirti obbligata a farlo anche tu! Se la cerchia dei tuoi amici ti fa dei problemi per cose di questo genere… cambia amici!
- Fai attenzione a pubblicare informazioni personali (foto della tua casa, della tua azienda o della tua scuola, il tuo indirizzo, la data di nascita e il nome per intero): sono informazioni utilissime per chi intende adescare!
- Scegli un username che non contenga alcun dato personale (come Giovanni Roma o Lucia Firenze) e non usate mai come password informazioni personali come il codice fiscale o la data di nascita e così via.
- È buona norma aprire un account email separato, che non contenga il tuo nome per intero, da utilizzare per inviare e ricevere comunicazioni dai siti Web. In questo modo, se vorrai interrompere la connessione con quel sito, ti basta smettere di usare quell'account.
- Non scrivere o pubblicare niente che in futuro possa metterti in imbarazzo. Ciò che viene messo online, rimane online!

5.2.2 Il Social Network Poisoning

Con *Social Network Poisoning* si definisce uno specifico tipo di azioni malevoli messe in atto sui social: si introducono profili artefatti e relazioni inesistenti per contraffare e rendere inaffidabili le informazioni condivise.

Non essendo possibile verificare sempre e in ogni momento la veridicità dei profili degli utenti dei social, è possibile imbattersi in utenti parzialmente o completamente falsi (si parla, in casi del genere, di *fake*). I principali casi di *poisoning* attualmente praticati sono:

- la *sostituzione* e la *simulazione di identità*;
- l'introduzione volontaria di elementi falsi e/o non congrui nel proprio profilo (*profile fuzzing*);
- l'ingresso in gruppi che non hanno a che fare con i propri interessi e relazioni, con il solo intento di fare rumore (*social graph fuzzing*).

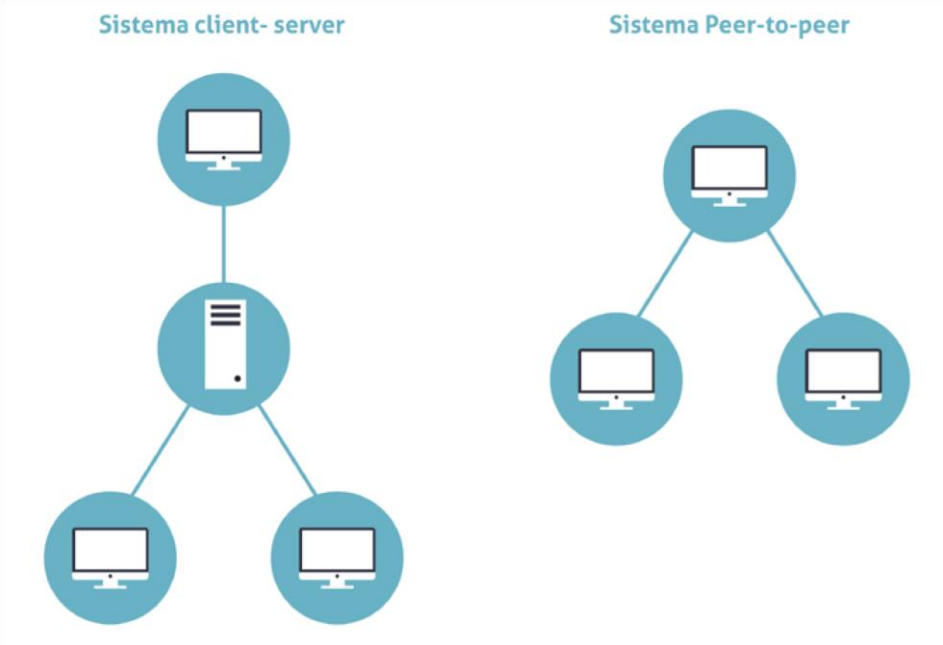
5.2.3 Strumenti per comunicazioni online sicure

Emerge che le applicazioni più usate al mondo hanno moltissime falle.

Una nota di merito va fatta a WhatsApp Con la *crittografia end to end* (E2EE) (protegge la segretezza delle comunicazioni in transito, in modo che non siano visibili nemmeno da chi gestisce i server dell'azienda).

5.3 La tecnologia peer to peer (P2P)

Il P2P è la tecnologia tramite cui gli utenti connessi a Internet possono condividere i file archiviati sul proprio PC, come se fossero in una rete LAN.



5.7 | Sistema Client Server (a sinistra) e Sistema Peer-to-peer (a destra)

5.3.1 Che cosa è il P2P

Con il termine *peer-to-peer* (o rete paritaria o paritetica) si indica una rete in cui i nodi non sono organizzati e suddivisi in client o server, ma sono equivalenti o paritari (in inglese, *peer*).

Questo significa che ogni nodo può essere, allo stesso tempo, *cliente* e *servente* degli altri nodi (detti host) connessi, scambiando con ognuno i file archiviati.

Questa tecnologia è utilizzata soprattutto per condividere musica, film e tanti altri contenuti, in un modo che comporta:

- rischi per la sicurezza degli utenti,
- elementi di illegalità relativi alla violazione dei diritti di *copyright* dei dati scambiati.

5.3.2 I rischi della tecnologia P2P

Indipendentemente dall'applicazione utilizzata (eMule, Napster, MIRC ecc.), è impossibile stabilire a priori l'affidabilità del nodo da cui stiamo scaricando i dati; in pratica, non sappiamo se il PC dell'utente da cui stiamo acquisendo un film, ad esempio, sia infettato con virus o se l'utente stesso non usi questo sistema per riempirci di malware tramite cui accedere, successivamente al nostro PC.

Per funzionare, questi programmi richiedono spesso, ad esempio, di disattivare il *firewall*.

6 . SICUREZZA DEI DATI

6.1.1 Le tecniche di protezione dei dati

Lo storage

Con il termine *storage* (che potremmo tradurre in *sistema di archiviazione dati*) si indicano tutti i supporti hardware e software:

- Organizzati con la specifica finalità di conservare enormi quantità di informazioni in formato elettronico,
- Capaci di garantire la sicurezza delle informazioni conservate.

I diversi tipi di storage

NAS (*Network Attached Storage*). Il dispositivo è collegato a più computer messi in rete tra loro. Questo sistema:

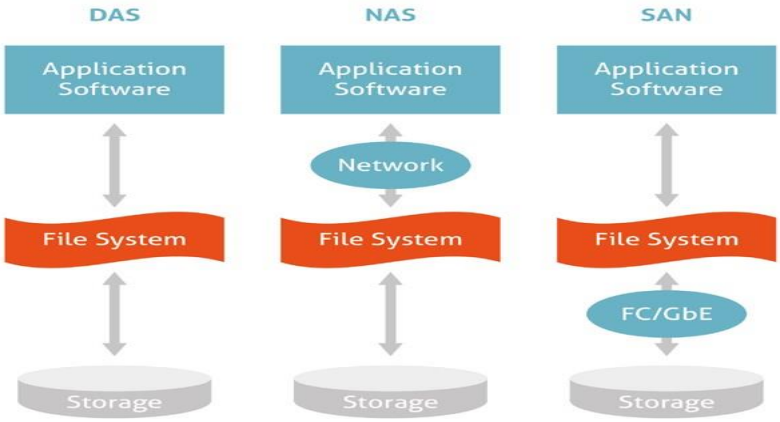
- Permette di centralizzare l'immagazzinamento dei dati in un'unità accessibile a tutti i nodi della rete e specializzata,
- Garantisce che i dati immagazzinati sia molto più al sicuro.

Lo svantaggio è che la grande quantità di dati in transito nella rete locale può determinare rallentamenti e malfunzionamenti del sistema.

DAS (*Direct Attached Storage*). Prima forma di *storage*, consiste in un dispositivo di immagazzinamento di dati che è collegato direttamente a un *server* o a un computer, non avendo alcuna connessione di Rete. Sono diverse le negatività, a confronto con i metodi più moderni: ad esempio,

- È difficile condividere i dati tra più computer.
- L'espansione dello spazio di immagazzinamento è complessa.

SAN (*Storage Area Network*). Sistema di immagazzinamento dati capace di renderli disponibili a computer connessi (normalmente a Internet), ad altissima velocità, grazie all'utilizzo della *fibra ottica* (Gigabit/sec). I vantaggi rispetto ai sistemi DAS è evidente: consente ai *server* e ai *dispositivi di storage* di avere una connettività diretta, con un'ottimizzazione dell'efficienza dello spostamento di dati e processi (come, ad esempio, il *backup* o la *replica dei dati*).



6.1 | I diversi sistemi di storage

6.1.2 Il backup dei dati

È buona norma creare una copia di sicurezza dei propri dati che, in informatica, si definisce *backup*.

È, in sostanza, una copia di riserva da cui puoi recuperare i tuoi dati in caso di perdite accidentali (che possono capitare molto più spesso di quanto si pensi).

Come fare il backup

Una prima forma semplificata di backup è quella di copiare i file che sono sul nostro PC su un supporto esterno:

- Hard disk esterni,
- Supporti rimovibili (CD, DVD, Pen-drive USB, Schede),
- Internet, grazie al Cloud.

A prescindere dal metodo scelto, è buona norma fare almeno una copia al mese dei tuoi dati.

Il punto è che, eccezion fatta per il Cluod, con tutti gli altri supporti corriamo gli stessi rischi visti prima: danneggiamento, perdita, furto.

La soluzione a questi inconvenienti è data dal *backup Windows 10* e, cioè, dallo strumento che Microsoft ci mette a disposizione per salvare automaticamente i dati del PC, evitando di perderli nel momento in cui si dovesse verificare un guasto o altro.

6.1.5 Il Cloud

Un'altra soluzione è il Cloud e, cioè, uno spazio online a tua completa disposizione, in cui trasferire e conservare file.

OneDrive, uno dei tanti servizi disponibili, è il Cloud di Windows 10.

È subito disponibile in maniera gratuita per tutti gli utenti con account Microsoft.

Oltre alle funzioni integrate, puoi utilizzare software gratuiti molto performanti, come, ad esempio, EaseUS Todo Backup Free (compatibile anche con Windows Vista e Windows XP) o fwbackups, per chi utilizza Linux; ce ne sono, comunque, molti altri.

6.2 Il ripristino di sistema

Se continui a visualizzare messaggi di errori che fino a ieri non c'erano o hai installato una serie di programmi che credi possano aver minato la stabilità del tuo PC, puoi risolvere tutto riportando il tuo PC alle condizioni di qualche giorno fa, quando non avevi alcun problema.

6.2.1 Il ripristino su Windows 10

Hai a disposizione una funzione che ti consente di tornare indietro e ripristinare il tuo PC così come era qualche giorno, settimana o, addirittura, qualche mese fa.

1. Digita *Ripristino* in Cortana.
2. Clicca sulla voce che esce in alto, per aprire la finestra di dialogo *Ripristino* del *Pannello di Controllo*.
3. Clicca su *Apri ripristino configurazione di sistema*. Si apre una finestra. Scegli se:
   - Tornare al punto di ripristino immediatamente precedente, mantenendo selezionata l'opzione *Ripristino consigliato*.
   - Sfogliare i diversi punti di ripristino disponibili, spuntando Scegli un punto di ripristino diverso.
4. Clicca su *Avanti.*

Se hai selezionato la seconda opzione, vedrai l'elenco di tutti i punti di ripristino disponibili.

Scegli *Mostra ulteriori punti di ripristino* o *Cerca programmi interessanti* per affinare la ricerca.

5. Seleziona il punto di ripristino che fa più al caso tuo, clicca su *Avanti* > *Fine* > *Si*.

L'operazione può richiedere diversi minuti.

6.3 Eliminare in modo permanente i dati dalle memorie di massa o dai dispositivi

Quando un dato non ti serve più, è buona norma cancellarlo, piuttosto che intasare il tuo computer o il tuo device con file inutili che, a lungo andare, ne limitano le prestazioni.
Per farlo, spostalo nel cestino.

6.3.1 Il cestino

Il cestino è una cartella speciale che contiene tutti i file eliminati. Bada bene, però: questi file sono tutti facilmente recuperabili (tecnicamente, si dice ripristinabili).
Se vuoi ripristinare file cancellati, apri la cartella *cestino*, seleziona i file e clicca su uno dei comandi indicati di seguito.
Per facilitare queste operazioni, ti consigliamo di visualizzare la *barra degli strumenti*, così come hai vedi nella figura precedente. Per farlo, clicca su *Gestisci* e, poi, sull'icona *freccetta in basso* sulla destra della *barra dei menu*.
Se, invece, vuoi che i file nel cestino siano rimossi definitivamente, clicca sul comando *Svuota cestino*.
Devi sapere, però, che anche dopo aver svuotato questa cartella, sul disco rimangono delle tracce che software specifici (come *Glary Utilities* e *Recuva*) possono acquisire per ricostruire integralmente o quasi i file rimossi, a seconda del tempo che passa dalla loro cancellazione e dai successivi utilizzi del computer.

6.3.2 Eliminazione definitiva dei file

Glary Utilities, (lo stesso programma che può recuperare i *file*), ha uno strumento efficace per distruggerli in modo definitivo.
CCleaner è un altro *software* che ti permette di cancellare (*ripulire*, come dice il nome) dal tuo computer tutti i file che non sono più utili. Ne abbiamo già fatto cenno: questo programma è in grado di cancellare anche tutti i file che registrano le tracce della tua navigazione in Internet e che vengono automaticamente salvati sul tuo PC.
Questo tipo di pulizia ha innegabili vantaggi:

- libera spazio di memoria dall'hard disk del tuo PC,
- difende la tua privacy,
- rende più veloce il sistema operativo.