Concetti di Sicurezza

Sezione 1

MINACCE AI DATI 1.1

1.1.1 Distinguere tra dati e informazioni

Nel linguaggio di tutti i giorni, le parole *dato* e *informazione* hanno quasi lo stesso significato. In informatica, invece, è importante distinguerle:

- i dati sono numeri, testo o altro (ad esempio immagini) che si riferiscono a fatti non organizzati;
- le informazioni sono dati organizzati in modo da essere utili all'utente.

Un esempio servirà a essere più chiari: in una rubrica telefonica cartacea, costituiscono dei dati i nomi, i cognomi, gli indirizzi, i numeri di telefono che abbiamo annotato, mentre un nome collegato al proprio numero telefonico ed eventualmente anche all'indirizzo, rappresenta un'informazione.

Da questo esempio, si capisce che i dati, presi singolarmente, non hanno grande significato: a cosa servirebbero un paio di cognomi, un numero di telefono, qualche indirizzo, presi a caso, senza alcuna relazione tra loro? Se, invece, a un cognome corrisponde il proprio indirizzo e il proprio numero di telefono, allora abbiamo un'informazione che può esserci utile, perché, attraverso il cognome della persona possiamo risalire al suo indirizzo e ai suoi numeri di telefono.

I dati, quindi, assumono significato quando sono organizzati tra loro in modo da costituire un'informazione.

1.1.2 Comprendere i termini "crimine informatico" e "hacking"

Quando un reato è commesso attraverso l'utilizzo di strumenti informatici, come il computer e Internet, è detto crimine informatico. Tra i più frequenti abbiamo:

- la copia non autorizzata di applicazioni o documenti (file musicali, video, ecc.) protetti dal diritto d'autore;
- l'accesso non autorizzato ai contenuti di un disco o di una banca dati;
- l'intercettazione di dati;
- il furto di identità;
- il phishing (pr. *fiscin*).

I metodi e le tecniche utilizzati per accedere illegalmente ai sistemi informatici altrui (perlopiù di enti o di grandi aziende) sono complessivamente definiti hacking (pr. *àkin*, da "to hack", sign. "smontare"); chi utilizza questi metodi e tecniche è detto hacker (pr. *àker*).

Il vero hacker è un profondo conoscitore dell'informatica, che non accetta le regole e gli interessi economici sempre più presenti nel mondo dei computer e di Internet. Quando riesce a entrare in un sistema protetto, non causa, in genere, danni, ma lascia un segno della sua visita, a volte comunicando il modo in cui è riuscito a superare i sistemi di sicurezza, così che l'azienda o l'ente possano evitare che questo riaccada in futuro.

In quest'ultimo caso si parla di **hacking etico**, così come quando sono le stesse aziende a commissionare l'uso di tecniche di hacking per testare la sicurezza dei propri sistemi e delle proprie reti.

Quando, invece, si accede a sistemi informatici altrui per rubarne i dati, trarne profitto o semplicemente per danneggiarli o distruggerli, si parla di **cracking** (pr. *cràking*, da "to crack", sign. "spaccare") e chi lo pratica è detto **cracker** (pr. *cràker*).

più

Oggi, il termine hacker è usato prevalentemente solo per indicare una persona che provoca danni, il cosiddetto **pirata informatico**. Soprattutto all'estero, perciò, i veri hacker sono chiamati **white hat hacker** (pr. *uàit at àker*, sign. "hacker dal cappello bianco"), per distinguerli dai pirati informatici, definiti **black hat hacker** (pr. *blèk at àker*, sign. "hacker dal cappello nero").

1.1.3

Riconoscere le minacce dolose e accidentali ai dati provocate da singoli individui, fornitori di servizi, organizzazioni esterne

Altre minacce ai dati provengono da persone che hanno accesso ai dati informatici o alle stesse apparecchiature elettroniche e che possono danneggiarli o distruggerli (volontariamente in maniera dolosa, oppure involontariamente in maniera accidentale), oppure rubarli per utilizzarli a scopo personale o per rivenderli.

Queste persone possono essere impiegati della stessa azienda, personale che si occupa della manutenzione dei sistemi informatici, fornitori di servizi, oppure singoli individui od organizzazioni esterne che riescono ad accedere alla rete o direttamente ai dati.

In tutti i casi, è opportuno ricorrere all'utilizzo di account e password (pr. *accàunt* e *pàss-uòrd*; limitano l'accesso ai dati alle sole persone autorizzate; ne parleremo nella Sezione 4 di questo Modulo), e a sistemi di protezione da intrusioni esterne, i cosiddetti firewall (pr. *fàir-uòl*; ne parleremo nel punto 3.1.4).

1.1.4

Riconoscere le minacce ai dati provocate da circostanze straordinarie quali fuoco, inondazioni, guerre, terremoti

I dati conservati nei sistemi informatici o utilizzati dai programmi non sono minacciati solo da persone malintenzionate, ma anche da eventi naturali (incendi, inondazioni, terremoti) o artificiali (guerre, rivolte popolari, fenomeni di vandalismo) in grado di danneggiare o distruggere sia i dati sia le apparecchiature.

Proprio per limitare questi **danni provocati da circostanze straordinarie**, è necessario effettuare una copia di sicurezza dei dati, da conservare in luoghi diversi da quelli dove i dati sono utilizzati (punti 7.1.2 e 7.1.3).

1.1.5

Riconoscere le minacce ai dati provocate all'utilizzo del cloud computing, quali: controllo sui dati, potenziale perdita di riservatezza (privacy)

Il **cloud computing** (pr. clàud compiùting), o più semplicemente **cloud**, è l'insieme di tecnologie che permettono l'accesso a risorse (applicazioni, memorizzazione online, altri servizi, ecc.) disponibili su Internet.

L'utilizzo del cloud è in crescente espansione, considerati i suoi numerosi vantaggi, tra cui la possibilità di accedere alle risorse ovunque sia possibile collegarsi alla rete, con un qualsiasi dispositivo; la condivisione di documenti e file con altri utenti, ecc.

Esistono, però, **minacce ai dati provocate dall'utilizzo del cloud**:

- esiste sempre l'eventualità che, a causa di accessi da parte di persone non autorizzate o dell'azione di malware, avvengano **problemi che riguardano la protezione e il controllo dei dati**;
- per gli stessi motivi, sono possibili **rischi per la privacy**: tutti i nostri dati sono registrati su memorie di massa di proprietà del provider. Inoltre, ogni volta che ci colleghiamo, sono registrate numerose informazioni: orario e durata del collegamento, da dove ci siamo collegati, che tipo di attività svolgiamo in quel momento, ecc.

VALORE DELLE INFORMAZIONI 1.2

1.2.1

Comprendere le caratteristiche fondamentali della sicurezza delle informazioni, quali: confidenzialità, integrità, disponibilità

Le tecniche utilizzate per garantire la sicurezza delle informazioni, devono garantire tre caratteristiche essenziali:

- **confidenzialità (o riservatezza)**: i dati devono essere accessibili solo a persone autorizzate, in nessun modo devono essere diffusi o visibili ad estranei;
- **integrità**: i dati possono essere modificati solo da persone autorizzate e, in ogni caso, se questo avviene, il sistema deve segnalare che è avvenuta una modifica non autorizzata o che i dati sono incompleti;
- **disponibilità**: le persone autorizzate devono poter accedere senza problemi ai dati protetti, il che significa che non devono essere richieste autorizzazioni o chiavi di accesso diverse da quelle in possesso degli utenti e che i dati vanno protetti con copie di sicurezza.

1.2.2

Comprendere i motivi per proteggere le informazioni personali, quali evitare il furto di identità o le frodi, mantenere la riservatezza

Quando le informazioni conservate nei dispositivi elettronici riguardano una persona fisica (ad es. copie digitali di documenti, eventuali credenziali per accedere a una rete informatica, numeri di carte di credito, altre informazioni personali, ecc.) sono dette **informazioni personali** e devono essere protette con attenzione.

Infatti, malintenzionati possono appropriarsene al fine di utilizzarli per sottoscrivere un contratto, acquistare un prodotto, accedere a un servizio, fingendo di essere la persona alla quale appartengono le informazioni. In tutti questi casi si parla di **frodi** e di **furto di identità**, argomenti ai quali è dedicata la Sezione 1.3 (Sicurezza personale).

più

Il **diritto alla riservatezza** (comunemente definito col termine inglese **privacy**, pr. *pràivasi*) è tutelato dalla legge anche per ciò che riguarda l'uso dei sistemi informatici e di Internet. Infatti, la continua diffusione di computer e di Internet fa sì che le informazioni personali da noi comunicate a un ente o a un'azienda possano essere da questi facilmente comunicate ad altri. Attraverso il collegamento incrociato di banche dati, diviene così possibile ottenere un quadro piuttosto completo della personalità di un individuo, compresi aspetti riservati della sua vita (preferenze politiche, sessuali, stato di salute, condizioni economiche, ecc.).
In Italia la **legge 675 del 1996** garantisce il *diritto alla privacy* e impedisce che nostre informazioni personali possano essere utilizzate per fini diversi da quelli da noi concessi, dandoci anche la possibilità di richiederne la cancellazione.

1.2.3

Comprendere i motivi per proteggere informazioni di lavoro su computer e dispositivi mobili, quali: evitare furti, utilizzi fraudolenti, perdite accidentali di dati, sabotaggi

La maggior parte di uffici e aziende conserva, nei propri archivi digitali, informazioni personali dei loro clienti e sono quindi obbligati per legge a tutelarle, per evitare che esse vengano in possesso di malintenzionati che potrebbero usarle per scopi illegali.

Nelle aziende, inoltre, sono a rischio di manomissione o di furto anche informazioni commerciali o finanziarie che riguardano direttamente l'azienda (ad es. progetti, investimenti, rapporti con banche ed enti, ecc.) e che potrebbero essere utilizzate o sabotate da aziende concorrenti.

Per tutti questi motivi, oltre che per il già ricordato rischio di una perdita accidentale di dati, è fondamentale proteggere le informazioni di lavoro memorizzate in computer e dispositivi mobili.

1.2.4

Identificare i principi comuni per la protezione, conservazione e controllo dei dati e della riservatezza, quali: trasparenza, scopi legittimi, proporzionalità delle misure in rapporto ai danni

La diffusione dei sistemi informatici ha condotto le aziende ad affidare a computer e reti interne un'enorme massa di dati, alcuni dei quali rivestono particolare importanza per le aziende stesse, mentre altri devono rimanere riservati perché contengono dati personali riguardanti dipendenti e clienti.

Per questi motivi qualsiasi azienda, indipendentemente dalla sua dimensione, deve preoccuparsi di gestire i problemi legati alla sicurezza dei dati trattati elettronicamente, problemi che consistono principalmente nell'eventualità che persone non autorizzate possano accedere a quei dati e nella possibilità di perdita dei dati stessi, dovuta a disattenzione, malfunzionamenti, virus o altri motivi.

Tra le principali norme da seguire per evitare questi e altri simili rischi, ricordiamo l'adozione di una politica di sicurezza nella gestione dei cosiddetti *dati sensibili*, attraverso la predisposizione di misure necessarie a impedire la perdita di questi dati (in seguito a eventi accidentali, furti, danneggiamento, distruzione) o la loro modifica (specie se si tratta di informazioni riservate). In tal senso sono indispensabili backup periodici dei dati (7.1.3) e procedure di monitoraggio che permettano di risalire alle persone che hanno avuto accesso a dati riservati.

Devono, inoltre, essere predisposte procedure per segnalare eventuali problemi di sicurezza, in modo che anche il solo sospetto di danni o di una diffusione impropria di informazioni riservate possa immediatamente attivare le necessarie contromisure. Infine, non va trascurata la preparazione dei dipendenti (anche tramite appositi corsi, se si tratta di aziende di grandi dimensioni), che devono conoscere le proprie responsabilità riguardo alla sicurezza dei dati: ciò significa educarli a un uso accorto e riservato delle informazioni in loro possesso, a cominciare dall'utilizzo delle password d'accesso.

In Europa, la protezione dei dati personali è regolata da una legge del 1995 (nota anche come "direttiva 95/46/CE") e dai suoi successivi aggiornamenti. Essa stabilisce che il trattamento dei dati personali deve rispettare tre principi:

- trasparenza: ogni persona ha diritto di essere informata quando i suoi dati personali sono in corso di elaborazione;
- scopi legittimi: i dati personali possono essere trattati solo per scopi dichiarati e legittimi;
- proporzionalità: il trattamento dei dati deve limitarsi a quanto strettamente necessario per gli scopi dichiarati, senza nessun eccesso.

1.2.5

Comprendere i termini "soggetti dei dati" e "controllori dei dati" e come si applicano nei due casi i principi di protezione, conservazione e controllo dei dati e della riservatezza

In Italia, le norme che regolano l'utilizzo dei dati sono contenute nel Decreto Legislativo numero 196 dell'anno 2003, noto come "Testo unico sulla privacy" (pr. pràivasi), e nel Decreto Legislativo 5 del 2012, che ha aggiornato il precedente.

Entrambi i decreti fanno riferimento alla già ricordata "Direttiva Europea sulla protezione dei dati" (*European Data Protection Directive*, pr. *iuriopìan déita protècscion dairèctiv*), in base alla quale chi elabora dati personali viene definito controllore di dati, mentre le persone alle quali appartengono quei dati personali sono definite soggetti dei dati.

Punti essenziali di queste leggi sono:

- nessuno può raccogliere e conservare dati personali altrui, senza il consenso scritto dell'interessato;
- l'ente, la società, il professionista che conserva i dati deve nominare un responsabile del trattamento dati, che garantisca il rispetto della legge sulla privacy;
- le persone interessate possono chiedere informazioni riguardo al trattamento dei loro dati e, anche se hanno precedentemente dato il consenso al loro trattamento, possono chiedere che i dati siano cancellati, se ritengono violata la propria riservatezza;
- i dati personali devono essere cancellati non appena cessa il motivo del loro utilizzo.

Se vengono raccolti dati senza il nostro consenso o utilizzati per scopi diversi da quelli permessi, il cittadino può ricorrere al Garante della privacy e, nel caso in cui venga attestato un danno morale o economico, ottenere anche un risarcimento.

Le aziende o gli enti che ci richiedono dati possono utilizzarli, ad esempio, per inviarci periodicamente delle notizie riguardanti le loro attività, per spedirci merce da noi richiesta, per trasmettere il nostro curriculum se siamo in cerca di lavoro. Non sono però autorizzate a utilizzare i dati da noi comunicati per scopi diversi da quelli che abbiamo accettato e devono adottare sistemi idonei a garantire sicurezza e segretezza dei nostri dati.

più Ulteriori informazioni sull'argomento possono essere trovate sul sito dell'autorità garante della privacy, dove è anche possibile porre quesiti: www.garanteprivacy.it

Spesso però, per risparmiare tempo, diamo il nostro consenso senza leggere con attenzione quanto ci viene chiesto di sottoscrivere; così capita molto frequentemente che senza accorgercene autorizziamo l'azienda alla quale comunichiamo i nostri dati a trasmetterli o rivenderli ad altre aziende.

1.2.6

Comprendere l'importanza di attenersi alle linee guida e alle politiche per l'uso dell'ICT e come fare per ottenerle

Da tutto quanto abbiamo detto, è evidente che in ambito professionale e aziendale, quando si utilizzano strumenti informatici, devono essere stabilite e rese note le norme che devono essere seguite da tutto il personale coinvolto.

La scienza che si occupa di archiviare, elaborare, trasformare e trasmettere informazioni attraverso gli strumenti informatici è chiamata ICT (pr. *ai-si-tì*, da "Information & Communication Technology", pr. *informèscion ènd commùnikescion tecnòlogi*).

più

A volte, il termine **ICT** è "italianizzato" in **TIC** (Tecnologie dell'Informazione e della Comunicazione) oppure abbreviato in **IT** ("Information Technology", in italiano "Tecnologia dell'informazione").

Linee guida e politiche per l'uso dell'ICT sono stabilite, perciò, sia a livello generale che locale. A livello nazionale, è ad esempio possibile consultare il sito dell'*Agenzia per l'Italia Digitale* all'indirizzo web www.agid.gov.it. Se, invece, ci troviamo ad operare in una rete locale (come può essere quella di una Scuola o di un'azienda), dovremo far riferimento all'amministratore di quella rete.

1.3 SICUREZZA PERSONALE

1.3.1

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

Con il termine ingegneria sociale (dall'inglese "social engineering", pr. *sòcial ingìnerin*) si indicano le tecniche utilizzate per accedere a informazioni riservate non aggirando protezioni hardware o software, ma studiando il comportamento della persona che ha accesso a quel tipo di informazioni, in modo che sia lei stessa a comunicarle, in maniera diretta o indiretta.

Un esempio per essere più chiari: il pirata informatico telefona a un impiegato di una società, spacciandosi per il gestore delle connessioni Internet e chiedendogli di fornire la password di accesso ad alcuni dati, in quanto è necessaria per risolvere un urgente problema di sicurezza. Di solito, il pirata informatico non telefona a una persona a caso, ma la sceglie sapendo che è in possesso dei dati che gli occorrono, che è più vulnerabile (ad esempio perché molto anziana, oppure poco esperta) e possiede già alcune informazioni che gli servono a confermare la sua falsa identità. Con i social network è ormai semplice acquisire questo tipo di informazioni: il pirata informatico può così telefonicamente rassicurare la persona con cui sta parlando, dicendogli di conoscere personalmente il direttore della società, la sua famiglia, alcuni avvenimenti personali e così via.

1.3.2

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

L'ingegneria sociale utilizza diversi metodi per rubare informazioni personali. Esaminiamo i principali.

Tra i sistemi più diffusi ci sono le chiamate telefoniche: spacciandosi per altre persone (come nell'esempio proposto al punto precedente) oppure fingendo di effettuare un sondaggio che permette di ottenere dei premi, il pirata informatico cerca di ottenere le informazioni che gli occorrono o, quantomeno, notizie che gli permetteranno di giungere successivamente, utilizzando altre tecniche, a quelle informazioni.

Il phishing (pr. *fìscin*) si basa sull'invio di e-mail ingannevoli. Ad esempio, il pirata informatico invia un messaggio che apparentemente sembra provenire da una banca e che, minacciando la chiusura del conto o il blocco di una carta di credito, invita a collegarsi a una pagina web per inserire nome utente e password e confermare la propria identità.

Se l'utente "abbocca all'amo" (questo è il significato letterale del termine "phishing"), le credenziali che digita saranno rubate dal pirata informatico e utilizzate per i suoi scopi.

Lo shoulder surfing (pr. *sciòulde sèefin*) consiste nel rubare le informazioni spiando direttamente la persona: ad esempio mentre digita la propria password al computer, oppure il PIN del bancomat o della carta di credito. L'osservazione può essere effettuata a occhio nudo (ad esempio stando alle spalle della persona, dal che deriva proprio il termine "shoulder surfing" che può essere tradotto con "spiare alle spalle") oppure tramite videocamere nascoste, cannocchiali o altro.

1.3.3

Comprendere il termine "furto di identità" e le sue implicazioni personali, finanziarie, lavorative, legali

Quando il pirata informatico riesce ad acquisire una o più credenziali che permettono l'accesso a un servizio informatico (un singolo computer, una rete di computer, una casella di posta elettronica, un social network, un servizio bancario online, ecc.), avviene il cosiddetto furto di identità, in quanto il pirata può spacciarsi per la persona alla quale ha rubato i dati di accesso.

A quel punto, le conseguenze possono essere diverse:

- personali: il pirata può inviare mail o scrivere messaggi nelle reti sociali e in entrambi i casi il tutto sembrerà essere opera della persona che è stata derubata delle sue credenziali di accesso;
- finanziarie: il pirata può acquistare prodotti online utilizzando la carta di credito del derubato;
- lavorative: queste pratiche possono danneggiare l'azienda per la quale lavora la persona derubata e possono condurre anche al licenziamento della persona stessa;
- legali: le azioni compiute dal pirata informatico appariranno effettuate dal derubato, che dovrà anche risponderne penalmente, cercando di dimostrare la sua innocenza.

1.3.4

Identificare i metodi applicati per il furto di identità, quali acquisire informazioni a partire da oggetti e informazioni scartati (information diving), uso di dispositivi fraudolenti di lettura (skimming); inventare uno scenario pretestuoso (pretexting)

Per acquisire le informazioni necessarie a compiere un furto di identità, il pirata informatico utilizza diversi metodi, dei quali ricordiamo i principali:

- l'information diving (pr. *infórmescion dàivin*) consiste nel frugare tra oggetti e informazioni buttati via: nell'immondizia prodotta quotidianamente da un ufficio o da un ente sono spesso presenti foglietti, appunti, lettere, contenenti dati utili al pirata informatico. Ancora più ricchi di informazioni sono i vecchi computer buttati via da uffici o enti, dei quali i pirati informatici entrano in possesso a volte in maniera organizzata, ad esempio spacciandosi per volontari di società umanitarie che raccolgono vecchi computer per inviarli a paesi poveri. Anche se esistono modelli molto economici di macchine distruggi-documenti ed è abbastanza semplice estrarre un hard disk da un vecchio computer per distruggerlo, la maggioranza di uffici, aziende ed enti non utilizza queste cautele.
- Un metodo più tecnologico è lo skimming (pr. *skìmin*) che ruba i dati incorporati in carte di credito, bancomat o badge, facendoli passare attraverso dispositivi fraudolenti di lettura o acquisendo i dati necessari attraverso l'utilizzo di fotografie e video, grazie ai costi e alle dimensioni ridotti e all'ottima risoluzione di fotocamere e videocamere digitali. Un esempio sono le microcamere nascoste da pirati

informatici negli sportelli bancomat: registrano i dati digitati dai diversi clienti che utilizzano lo sportello nella memoria della microcamera, che a fine giornata il pirata ritira e analizza.
- Vi è poi il cosiddetto pretexting (pr. *prìtextin*), che punta ad acquisire informazioni inventando uno scenario pretestuoso: ad esempio fingendo di essere un superiore, un collega di altro ufficio o filiale, telefonicamente – come nell'esempio del punto 1.3.1 – o tramite l'invio di mail, come nel caso del phishing.

1.4 SICUREZZA DEI FILE

1.4.1

Comprendere gli effetti di attivare/disattivare le impostazioni di sicurezza relative alle macro

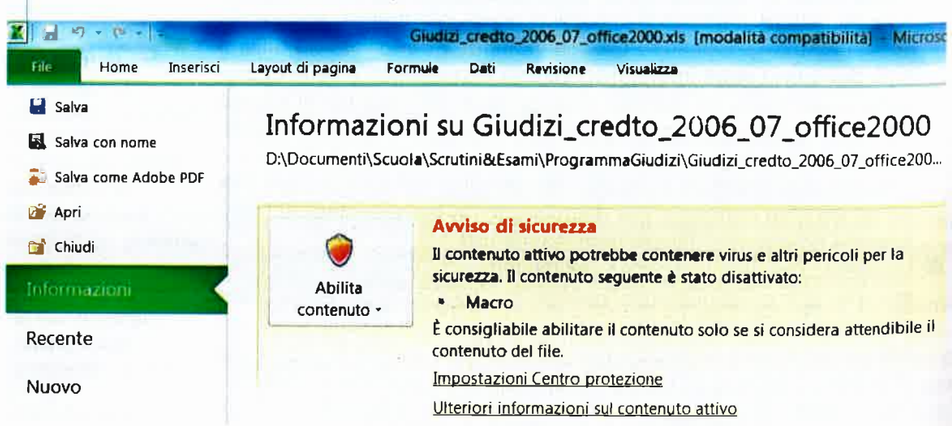
Per effettuare alcune operazioni è necessaria una sequenza di comandi a volte lunga e difficile da memorizzare. Per questo motivo esistono le macro, che permettono, con un solo comando, di eseguire tutte le operazioni che si è provveduto a memorizzare. Ad esempio, con Word si può creare una macro che provveda con un unico comando a numerare tutte le pagine di un documento al quale stiamo lavorando, a crearne un sommario e ad effettuare il salvataggio del file.

Essendo una specie di piccoli programmi, le macro, però, possono nascondere al loro interno dei malware (pr. *màl-uèr*, ad essi è dedicata la seconda Sezione di questo Modulo). Per questo motivo, i programmi segnalano, al momento dell'apertura di un file, la presenza di una macro e chiedono l'autorizzazione ad eseguirla (fig. 1.4.1a).

FIG 1.4.1a

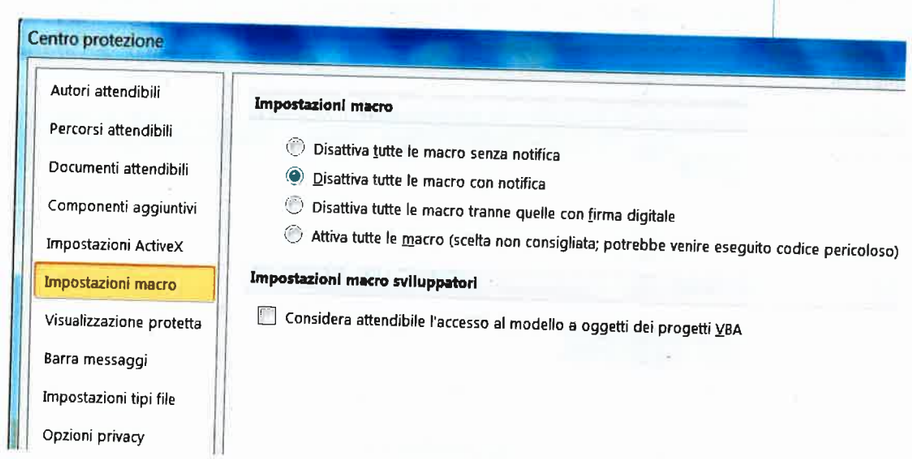
Cliccando sulla scritta "Fare clic per ulteriori dettagli" si otterranno maggiori informazioni (fig. 1.4.1b). Se siamo sicuri della provenienza e dell'affidabilità del file, consentiremo l'esecuzione della macro. In caso contrario e se non è almeno possibile esaminare il file con un antivirus aggiornato, meglio disattivare le macro, anche se questo non consentirà di usufruire di tutte le possibilità offerte dal file.

FIG 1.4.1b



È anche possibile modificare il modo in cui il programma segnala la presenza di macro, accedendo al *Centro protezione*. La procedura con *Word* ed *Excel* è la seguente: *File > Opzioni > Centro protezione > Impostazioni Centro protezione*. A quel punto sarà possibile scegliere tra diverse opzioni (fig. 1.4.1c) che consentono di disattivare le macro con o senza notifica, di abilitare solo le macro fornite di firma digitale (e quindi provenienti da fonti che dovrebbero essere attendibili) oppure di eseguirle automaticamente senza nessun avviso (scelta molto rischiosa).

FIG 1.4.1c



1.4.2

Comprendere i vantaggi e i limiti della cifratura. Comprendere l'importanza di non divulgare o di non perdere la password, la chiave o il certificato di cifratura

Per impedire accessi non autorizzati ai dati – siano essi propri o altrui, come nel caso delle aziende – è fondamentale utilizzare tecniche che, in caso di smarrimento o di furto, impediscano l'utilizzo del dispositivo (smartphone, tablet, portatile o altro) o del supporto di memoria (penna USB, scheda di memoria, disco rigido) nel quale sono memorizzati questi dati.

Ciò è possibile, ad esempio, attraverso la cifratura dei dati o crittografia, che trasforma i dati in una serie di simboli incomprensibili a chi non possieda la "chiave" necessaria a renderli di nuovo utilizzabili.

Un file protetto con una password di apertura viene "cifrato", vale a dire che un eventuale pirata informatico che ne entrasse in possesso e che cercasse comunque di aprirlo con altri programmi, si troverebbe di fronte una serie di simboli senza senso, in quanto non possiede la chiave di cifratura, vale a dire la password che abbiamo impostata.

Esistono comunque dei limiti:

- se dimentichiamo la password, la chiave o il certificato di cifratura non sarà possibile neppure a noi aprire il file;
- se scegliamo una password troppo semplice o prevedibile aumenta il rischio che un pirata informatico possa individuarla;
- vale la consueta raccomandazione di non divulgare per alcun motivo password, chiave o certificato di cifratura.

1.4.3 e 1.4.4

Cifrare un file, una cartella, una unità disco

e

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

Un modo semplice e abbastanza sicuro per proteggere i nostri file di lavoro (documenti, fogli di calcolo, file compressi) da accessi non autorizzati è quello di impostare una password per la loro apertura. Vediamo le procedure necessarie.

Con *Word* occorre cliccare prima sulla scheda *File*, accertarci che sia selezionata l'opzione *Informazioni* nella colonna di sinistra e poi cliccare su *Proteggi documento* per accedere a diverse opzioni (fig. **1.4.4a**); sceglieremo *Crittografa con password* per aprire la finestra *Crittografa documento* (fig. **1.4.4b**), nella quale dovremo digitare la password che sarà necessaria per aprire il file. Il programma ci chiederà di digitare nuovamente la password (per evitare errori di battitura che renderebbero impossibile anche a noi l'apertura successiva del documento), dopo di che per le successive aperture del file sarà richiesta la password.

FIG 1.4.4a

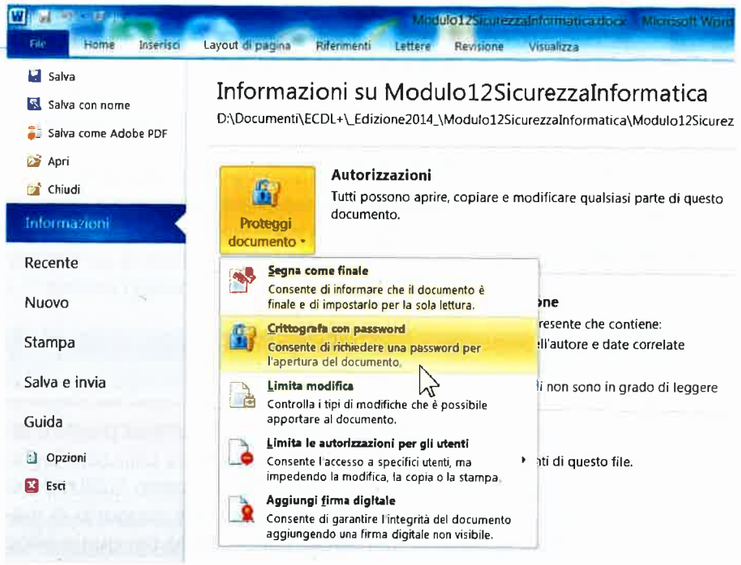
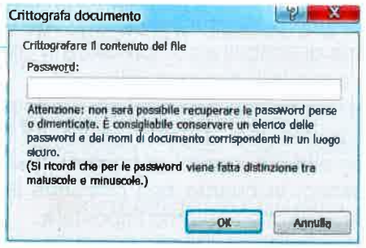


FIG 1.4.4b



Per eliminare la password di apertura basta ripetere l'operazione, stavolta lasciando vuota la casella dove andrebbe inserita la password.

La procedura con *Excel* e altri programmi del pacchetto *Office* è simile, cambia solo qualche minimo particolare, ad esempio in *Excel* il pulsante *Proteggi documento* si chiama *Proteggi cartella di lavoro*.

Si può accedere all'impostazione della password di apertura anche in fase di salvataggio del file, ma la procedura è leggermente più laboriosa. Occorre cliccare prima su *Salva con nome*, poi – nell'omonima finestra che si apre – sul pulsante *Strumenti* che si trova in basso a destra e poi, dal menu a tendina che si apre, su *Opzioni generali*. Nell'omonima finestra che si apre sarà possibile impostare la password di apertura.

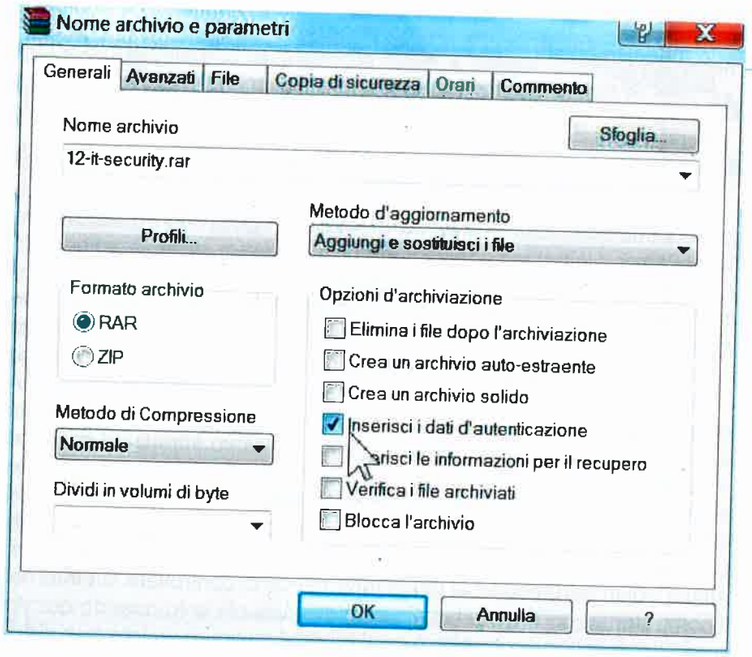
più

Al di sotto della scritta *Autorizzazioni* è indicata l'eventuale protezione applicata al file. Ad esempio, nella figura **1.4.4b** è riportato "Tutti possono aprire, copiare e modificare qualsiasi parte di questo documento", mentre dopo aver applicato una password di apertura sarà indicato "Per aprire il documento è necessaria una password".

È possibile proteggere da aperture indesiderate anche i file compressi, utilizzando uno dei programmi gratuiti di compressione come *WinRar* o *7Zip*, in quanto *Windows* permette di comprimere file ma non di proteggerli con una password.

I programmi di compressione, in genere, aggiungono delle voci di comando al menu contestuale che appare cliccando con il tasto destro su un file o su un gruppo di file. Con il programma *WinRar*, ad esempio, basta cliccare con il tasto destro sul file o sul gruppo di file e poi scegliere il comando *Aggiungi ad un archivio* per poi inserire il segno di spunta nella casella *Inserisci i dati d'autenticazione* (fig. **1.4.4c**); una volta cliccato sul pulsante *OK* il programma ci chiederà di digitare la password. Con il programma *7Zip*, dopo aver scelto *Aggiungi* basterà digitare la password nel campo *Cifratura*.

FIG 1.4.4c



Se si tratta di un file compresso già esistente, dovremo prima aprirlo col programma di compressione e poi scegliere l'opzione necessaria a inserire una password: in *WinRar* l'opzione è *File > Imposta parola chiave predefinita*, in *7Zip* occorre scegliere *Modifica password*.

Sezione 2 Malware

2.1 TIPI E METODI

2.1.1

Comprendere il termine "malware". Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor

Con il termine malware (pr. màl-uèr, deriva dalla contrazione delle parole "MALicious softWARE", sign. "programma maligno") si indica ogni tipo di software creato per arrecare danni al contenuto di un dispositivo elettronico o all'attività di chi lo utilizza.

Poiché esistono molti tipi di malware, i danni da essi provocati sono estremamente diversi: da semplici fastidi come la comparsa di finestre pubblicitarie o rallentamenti del dispositivo, a veri e propri reati come la sottrazione di dati personali o il controllo a distanza del dispositivo infetto.

Nei punti immediatamente successivi illustreremo:

- le modalità con le quali vengono trasmessi i malware: trojan, rootkit, backdoor;
- i malware "infettivi", che creano cioè copie di se stessi per diffondersi in altri dispositivi: virus e worm;
- i principali malware utilizzati per il furto di dati o altre truffe: adware, spyware, botnet, keylogger, dialer.

Vediamo quali sono i principali metodi con i quali si può nascondere il malware.

I trojan (pr. *tròjan*, accettata anche *tròian*) o cavalli di Troia, prendono questo nome perché la loro strategia assomiglia a quella utilizzata da Ulisse per penetrare con i suoi compagni nella città di Troia: nascosti all'interno di un enorme cavallo di legno che doveva sembrare un dono innocente. I trojan, infatti, contengono dei malware nascosti in programmi (ad esempio giochi), file video o audio, oppure sono allegati a mail apparentemente innocue. Una volta avviato il trojan, il malware si installa nel dispositivo e comincia a raccogliere informazioni riservate sulla persona che utilizza quel computer (password, altri codici come ad esempio quelli delle carte di credito utilizzate per acquisti via Internet) per poi inviare tramite Internet queste informazioni ai pirati informatici. Alcuni trojan permettono al pirata informatico di controllare via Internet il computer su cui è installato il virus, ovviamente solo quando questo computer è collegato in rete. A quel punto il malintenzionato può visionare l'intero contenuto del disco, copiarlo, modificarlo o cancellarlo a suo piacimento, in qualche caso addirittura controllare quanto succede nel locale dove si trova l'utilizzatore del dispositivo se a questo sono collegati e accesi un microfono o una web-cam.

I rootkit (pr. *rut-kìt*) sono software che nascondono il funzionamento di altri programmi o processi, in modo che essi non vengano rilevati da antivirus o altri programmi di sicurezza. I rootkit, ad esempio, sono utilizzati per consentire il funzionamento di keylogger (punto 2.1.3) o di altri programmi spia e consentono al pirata informatico di controllare il sistema come se ne fosse il legittimo amministratore.

Le backdoor (pr. *bàk-dòr*, sign. "porta di servizio") sono costituite da software che permette di accedere dall'esterno (tecnicamente si dice

"da remoto") a un sistema, aggirando l'inserimento di password o altre procedure di sicurezza. Alcuni malware, in particolare i trojan, creano delle backdoor per consentire l'accesso non autorizzato del pirata informatico al computer di un'altra persona.

> **più** Anche gli amministratori di sistema creano spesso delle backdoor, in questo caso del tutto lecite, per operare sui computer che sono loro affidati, senza dover digitare password o altro.

2.1.2

Riconoscere i tipi di malware infettivo e comprendere come funzionano, ad esempio, virus e worm

Alcuni malware sono detti "infettivi" perché, una volta eseguiti, non agiscono solo sul dispositivo, ma si moltiplicano, creando copie di loro stessi che sono inserite in programmi o inviate tramite posta elettronica.

Un virus informatico, ad esempio, è un piccolo programma creato per provocare danni ai computer e per diffondersi ad altri computer, così come i veri e propri virus, quelli biologici, si trasmettono da una persona a un'altra. Questo programma viene generalmente nascosto all'interno di altri file che possono essere anche allegati a una mail; quando utilizzate uno di questi file infetti, il virus si diffonde nel vostro computer e negli altri dispositivi eventualmente collegati in rete, andando a nascondersi in altri programmi.

Esistono migliaia di virus, per cui i danni provocati vanno da rallentamenti o malfunzionamenti del computer sino a danni ai file o allo stesso sistema operativo, provocando anche il blocco del dispositivo.

I worm (pr. *uòrm*; sign. "verme") si diffondono attraverso la posta elettronica. Spesso, quando un computer viene contagiato da un worm, comincia a inviare automaticamente delle mail a tutti gli indirizzi presenti nella rubrica dei programmi adoperati per la posta elettronica, sfruttando i momenti nei quali un qualsiasi utente del computer infetto si collega a Internet e senza che la persona stessa se ne accorga. A ognuna di queste mail è allegata una copia dello stesso worm: la persona che riceve quel messaggio, rassicurata dal fatto che conosce il mittente, spesso apre l'allegato che contiene il malware e contagia il proprio computer. Attraverso questa continua moltiplicazione, il worm occupa uno spazio sempre maggiore nella memoria del computer, rallentandone le prestazioni, oltre ad altri problemi che può provocare.

2.1.3

Riconoscere i tipi di malware usati per furto di dati, profitto/estorsione e comprendere come operano, ad esempio adware, spyware, botnet, keylogger e dialer

Alcuni malware sono stati creati per rubare i dati presenti in un dispositivo o in un sistema e poi trasmetterli all'esterno, alla persona che ha inserito il malware, a volte inducendo l'utente a scaricare software differente da quello voluto. Anche essi sono spesso nascosti in allegati di messaggi elettronici o all'interno di file scaricati da Internet. Vediamo quali sono i tipi più diffusi.

Gli adware (pr. *ad-uèr*, da "ADvertising WARE", sign. "prodotto pubblicitario") sono un tipo di malware non particolarmente pericoloso, ma molto invadente: visualizzano sul dispositivo connesso a Internet una serie continua di annunci pubblicitari, attraverso banner e popup. Oltre a rendere difficile la lettura delle pagine web, gli adware possono costituire anche un pericolo per la privacy, quando comunicano le nostre abitudini di navigazione a chi ha creato questo tipo di malware.

più

Il **banner** (pr. *bàna*, accettata *bànner*) appare spesso come un rettangolo largo e poco alto (inserito perlopiù in cima alla pagina web, ma a volte anche al centro o alla fine di essa) che reca al suo interno un'immagine, un video o un testo pubblicitario. Cliccando sul banner ci si collega con un'altra *pagina web* dedicata a quell'argomento.

I **popup** (pr. *popàp*) sono dei riquadri che si sovrappongono alla finestra del browser che stiamo utilizzando per navigare. In questi riquadri sono solitamente contenute delle pubblicità, fastidiose per la navigazione, anche perché a volte occupano il centro dello schermo per costringere l'utente a visualizzarle. In altri casi, però, i popup contengono informazioni a volte indispensabili per poter correttamente navigare nel sito: è il caso dei siti di alcune banche.

Il termine **adware** indica anche una modalità di distribuzione di alcune applicazioni, che sono scaricabili in forma completa e gratuita in cambio della visualizzazione di finestre pubblicitarie personalizzate (in base al tipo di siti visitati più spesso). Esistono programmi che rimuovono questo tipo di adware, ma in genere la loro rimozione blocca il funzionamento dell'applicazione che li ha installati nel nostro computer.

Il ransomware (pr. *ràns*om-uèr) è un malware molto più dannoso, perché blocca il computer o ne cifra i contenuti, chiedendo il pagamento di una somma di denaro per sbloccare il dispositivo ("ransom" in inglese significa "riscatto").

Gli spyware (pr. *spàiuer*) sono piccoli programmi che si installano in maniera subdola nel nostro dispositivo e spiano tutte le nostre attività di navigazione su Internet. In pratica, trasmettono i dati della nostra navigazione a dei server remoti. Queste nostre preferenze saranno poi vendute a società commerciali che in base ai nostri gusti ci invieranno delle mail (il cosiddetto *spam*, del quale parleremo nel punto 6.1.3) o ci faranno apparire – mentre siamo collegati a Internet – delle finestre pubblicitarie collegate a siti che vendono materiale ritenuto di nostro interesse.

Con il termine botnet (pr. *bòtnet*) si indica una infezione che colpisce una intera rete informatica (come quella di una scuola, di un ufficio, di una azienda o di una rete dedicata allo scambio di file e programmi anche se protetti da diritto d'autore), in modo che il pirata informatico che l'ha diffusa riesce a prendere il controllo di tutti i dispositivi collegati a quella rete, senza il consenso dei rispettivi utenti.

I keylogger (pr. *kì-lógar*) sono programmi che registrano tutti i caratteri digitati sulla tastiera (compresi dati privati come password, numeri di carte di credito, ecc.) per poi trasmetterlo a server remoti tramite Internet.

I dialer (pr. *dàialer*) sono dei software che vengono inconsapevolmente scaricati da Internet, in genere cliccando su qualche link presente nel web o contenuto in una mail. Una volta avviato, il dialer interrompe il collegamento con il provider del cliente e collega il modem a un numero telefonico (che di solito comincia con i numeri 709 oppure 899) a tariffazione particolare: così per scaricare una canzone o un logo per telefonino si spendono anche decine di euro. I dialer sono sempre meno diffusi, perché funzionano solo se la connessione a Internet avviene con la tradizionale linea telefonica, componendo un numero telefonico, mentre non hanno effetto con connessioni mobili o ADSL.

PROTEZIONE 2.2

2.2.1 **Comprendere come funziona il software antivirus e quali limitazioni presenta**

Da quando tramite Internet è frequente ricevere file da altre persone (ad esempio come allegati a un messaggio), la Rete è divenuta il principale mezzo di trasmissione di virus, worm, cavalli di Troia, spyware e altri tipi di malware.

Per questo motivo è indispensabile utilizzare un buon programma antivirus, da aggiornare costantemente via Internet, in quanto vengono messi in circolazione sempre nuovi tipi di virus. Di solito l'aggiornamento avviene in modo automatico quando ci si collega a Internet.

Un antivirus controlla i file contenuti nel nostro dispositivo e tutto ciò che in esso viene eseguito. Se, nel controllo, l'antivirus riconosce come sospetto un file, lo segnala all'utente e gli offre alcune opzioni:

- eliminare l'infezione dal file;
- eliminare il file;
- utilizzare il file, a proprio rischio;
- se un file risulta essere "sospetto" viene spostato in una cartella denominata "quarantena".

più

L'antivirus non va usato soltanto per gli allegati che ricevete via Internet, ma per tutti i file che arrivano al vostro computer da qualsiasi fonte: musica o video scaricati, programmi prelevati da Internet, chiavi USB o penne che collegate al computer.

È possibile scaricare per uso personale delle versioni gratuite di validi antivirus per tutti i sistemi operativi; le versioni più recenti di *Windows* includono già *Microsoft Defender* (pr. *màicrosoft defènder*) o *Microsoft Security Essentials* (pr. *màicrosoft sekìuriti essenscials*); altri antivirus hanno costi contenuti. È importante non far funzionare sullo stesso dispositivo più di un antivirus, altrimenti il dispositivo sarà rallentato e ognuno degli antivirus potrebbe segnalare come pericoloso l'altro software antivirus.

In ogni caso, occorre tenere presente che nessun antivirus ci garantisce al 100%, anche se installandone uno valido, aggiornandolo con regolarità e seguendo i consigli di sicurezza forniti in questo Modulo, è improbabile che il vostro dispositivo venga infettato.

Non tutti gli antivirus rilevano ed eliminano spyware e adware, in quanto non sono dei veri e propri virus. In questo caso è possibile scaricare, anche gratuitamente, delle applicazioni specifiche chiamate proprio *antispyware*. Un altro limite degli antivirus è la segnalazione di "falsi positivi", vale a dire file sicuri, che sono invece segnalati come contenenti virus.

più

Per questi motivi è sempre consigliabile essere prudenti, particolarmente nei seguenti casi:

- vanno aperti solo gli allegati ai messaggi elettronici che ci sono stati sicuramente inviate da persone che conosciamo;
- applicazioni e programmi vanno scaricati solo da siti conosciuti e affidabili;
- occorre diffidare di eventuali richieste di scaricare o installare del software;
- tutti i file ricevuti o scaricati devono essere controllati con l'antivirus.

2.2.2

Comprendere che il software antivirus dovrebbe essere installato su tutti i sistemi informatici

Un software antivirus rappresenta, dunque, una necessità non solo per i computer, ma per tutti i sistemi informatici che prevedono una connessione a Internet o ad altre reti.

Come abbiamo detto, sistemi operativi recenti (come *Windows* dalla versione *8* in poi) integrano già un antivirus, ma ne esistono diversi anche per dispositivi come tablet e smartphone che utilizzano altri tipi di sistema operativo (*Android, IoS*, ecc.).

Un antivirus ben configurato e costantemente aggiornato, rende improbabile che un malware possa introdursi nel computer; è comunque consigliabile avviare di tanto in tanto manualmente la scansione del computer, oppure di file o cartelle sospette. Se sono presenti malware, l'antivirus ne indicherà il tipo e suggerirà la procedura da eseguire: se disinfettare, mettere in quarantena oppure eliminare il file.

2.2.3

Comprendere l'importanza di aggiornare regolarmente vari tipi di software, quali antivirus, browser web, plugin, applicazioni, sistema operativo

Il mondo dell'informatica è in continua evoluzione, come dimostrano i nuovi software che sono quotidianamente realizzati. Il malware non fa eccezione a questa regola e anche di esso compaiono ogni giorno nuovi tipi, rapidamente distribuiti in tutto il mondo attraverso Internet.

Quando compare un nuovo malware, gli specialisti delle ditte produttrici di antivirus, sistemi operativi e applicazioni che possono essere contagiate (in particolare browser web e plug-in), si mettono al lavoro e, in breve tempo, inseriscono nella banca dati le nuove istruzioni e le modifiche per debellarlo.

Ovviamente, se non ci colleghiamo con il sito della casa produttrice (cosa che il sistema fa in genere da solo) l'antivirus, il programma antivirus non potrà aggiornarsi e quindi non sarà in grado di riconoscere il nuovo malware e di impedirne il suo ingresso nel nostro computer o in altro dispositivo elettronico. L'unica cosa da fare, in questo caso, è anche la più semplice: lasciare che il sistema proceda autonomamente a inserire gli aggiornamenti quando il dispositivo è connesso a Internet, cosa che fa da solo senza disturbarci mentre navighiamo da un sito all'altro, se non per avvisarci della disponibilità degli aggiornamenti e della loro avvenuta installazione.

Gli aggiornamenti in genere avvengono automaticamente, ma a volte c'è un breve ritardo tra un nuovo virus che compare e l'aggiornamento che serve a segnalarlo e ad eliminarlo.

più

Il **plug-in** o **plugin** (pr. *plaghìn*) è un programma che permette al browser (ma anche ad altri software) di ampliare le proprie funzioni: ad es. poter visualizzare immagini tridimensionali, aprire particolari tipi di file, ecc.

2.2.4

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

Il software anti-virus va automaticamente in funzione all'accensione del dispositivo nel quale è caricato e resta costantemente acceso, controllando tutti i file che vengono eseguiti, ma può anche essere utilizzato per eseguire la scansione di specifiche unità, cartelle o file, il che è utile per controllare file scaricati e allegati di posta elettronica prima di aprirli.

La scansione può anche essere pianificata, in modo che l'antivirus controlli, a intervalli definiti dall'utente, tutti o parte dei file contenuti nel dispositivo. Si può, ad esempio, scegliere di effettuare la scansione in orari il cui il computer è acceso ma non o poco utilizzato.

La scansione si attiva tramite l'interfaccia dell'antivirus, scegliendo tra le diverse opzioni cosa esaminare (unità, file, cartelle), quando e con che intervalli di tempo.

Vediamo, in pratica, come effettuare queste operazioni utilizzando *Microsoft Security Essentials*:

1. avviamo il programma *Microsoft Security Essentials*;
2. scegliamo prima la scheda *Impostazioni* e poi l'opzione *Avanzate*;
3. selezioniamo l'opzione *Analizza unità rimovibili;*
4. clicchiamo su *Salva modifiche* per tornare alla pagina iniziale del programma.

Se vogliamo pianificare la scansione, nella scheda *Impostazioni* dovremo cliccare su *Analisi pianificata* e indicare il giorno e l'orario che preferiamo, per poi cliccare su *Salva modifiche*.

Se, invece, possediamo un computer sul quale è installato *Windows 10*, probabilmente utilizzeremo come antivirus *Windows Defender*, che è già presente nel sistema operativo.

Come quasi tutti gli altri antivirus, *Defender* analizza regolarmente il PC ma è possibile avviare manualmente una scansione oppure pianificarla. Nel primo caso, le operazioni da eseguire sono:

1. avviamo il programma cliccando sul pulsante *Start*, scrivendo nella casella di ricerca *Defender* e poi scegliendo *Windows Defender* dall'elenco dei risultati;
2. nella colonna destra (*Opzioni analisi*) scegliamo tra *Veloce* (l'antivirus controllerà le aree normalmente infettate da malware), *Completa* (verranno controllati tutti i file, l'analisi potrebbe richiedere molto tempo ma sarà comunque possibile utilizzare il computer), *Personalizzata* (dovremo indicare i percorsi e i file da controllare);
3. clicchiamo su *Avvia analisi*.

Per pianificare la scansione con *Windows Defender* occorre utilizzare l'*Utilità di pianificazione*, seguendo questa procedura:

1. clicchiamo sul pulsante *Start*, scriviamo nella casella di ricerca *pianifica* e scegliamo *Pianifica attività* dall'elenco dei risultati;
2. nella colonna di sinistra apriamo (cliccando sul cursore che si trova subito prima del nome) *Libreria Utilità di pianificazione* e quindi selezioniamo *Microsoft > Windows > Windows Defender;*
3. nella colonna di destra clicchiamo su *Crea attività*;
4. nell'omonima finestra che si apre clicchiamo prima sulla scheda *Attivazione* (in alto) e poi sul pulsante *Nuovo* (in basso);
5. a questo punto potremo finalmente scegliere quando dovrà essere avviato automaticamente *Defender* scegliendo tra le molte opzioni disponibili.

Chi usa *Linux* può utilizzare *ClamAv*, che permette sia di scansionare file e cartelle, sia di pianificare scansioni scegliendo *Pianificatore* dal menu *Avanzate*.

2.2.5

Comprendere i rischi associati all'uso di software obsoleto e non supportato, quali: maggiori minacce da parte del malware, incompatibilità

Anche le app e i programmi informatici, il cosiddetto software, hanno un loro ciclo di vita e richiedono perciò un'azione periodica di verifica e manutenzione. Può infatti accadere che a un certo punto quei programmi e quelle app non siano più aggiornati dai produttori e non funzionino – in parte o del tutto – con sistemi operativi o hardware di nuova produzione.

Un software obsoleto e non supportato espone a diversi rischi:

- problemi di compatibilità con le applicazioni più recenti;

- lacune nella sicurezza che possono essere sfruttate dai criminali cibernetici per introdurre malware;
- rallentamenti dell'intera rete della quale fa eventualmente parte il dispositivo che utilizza quel software obsoleto.

In questi casi, è generalmente consigliabile cercare alternative convenienti e in grado di agevolare la propria attività.

2.3 RISOLUZIONE E RIMOZIONE

2.3.1

Comprendere il termine "quarantena" e l'effetto di messa in quarantena file infetti/sospetti

Se l'antivirus individua dei file infetti o sospetti, ma non riesce a "disinfettarli" (vale a dire a ripulirli dal contenuto pericoloso), chiede all'utente se devono essere eliminati, oppure messi in quarantena, vale a dire spostati in un'apposita cartella creata dall'antivirus, nella quale i file resteranno ineseguibili sin quando un aggiornamento del programma antivirus permetterà di renderli nuovamente utilizzabili, oppure sin quando l'utente non deciderà di eseguirli (solo nel caso abbia la sicurezza assoluta che si tratti di una segnalazione errata) oppure di eliminarli definitivamente.

Gli antivirus permettono di scegliere se e in quali casi utilizzare la quarantena.

Ad esempio, con *Microsoft Security Essentials,* cliccando prima su *Impostazioni* e poi su *Azioni predefinite* è possibile scegliere l'azione predefinita da effettuare a seconda del livello di pericolo individuato nel file: potremmo, ad esempio, scegliere di rimuovere il file se il livello di pericolo è giudicato grave e di porlo in quarantena in tutti gli altri casi. È sempre possibile modificare successivamente le proprie scelte.

Se utilizziamo *Defender* per *Windows 10*, dovremo invece cliccare sulla scheda *Cronologia*, poi su *Elementi in quarantena* e infine su *Visualizza dettagli* per vedere l'elenco degli eventuali file posti in quarantena e poter decidere se rimuoverli oppure ripristinarli.

In quest'ultimo caso, ovviamente, dovremo essere assolutamente certi che non contengano malware, altrimenti rischieremmo di infettare tutto il dispositivo.

2.3.2

Mettere in quarantena, eliminare file infetti/sospetti

Se sono presenti malware, l'antivirus ne indicherà il tipo e suggerirà la procedura da eseguire: se disinfettare, mettere in quarantena oppure eliminare il file. Queste opzioni dipendono dal tipo di malware:

- *Disinfetta*: l'antivirus è in grado di eliminare il malware dal file infetto e restituirci il file com'era prima dell'infezione.
- *Metti in quarantena:* l'antivirus non è in grado di disinfettare il file contagiato, lo posiziona quindi in una cartella protetta in attesa di scaricare dalla casa produttrice dell'antivirus un aggiornamento che permetta di eliminare quel tipo di malware.
- *Elimina:* il programma non è in grado di svolgere le prime due operazioni e quindi l'unica soluzione è l'eliminazione del file.

Quest'ultima opzione riguarda spesso i CD e i DVD, sui quali il programma non può intervenire giacché, una volta inciso, il dischetto a lettura ottica non è modificabile. Non essendo possibile eliminare il file da un CD o DVD, i supporti risultano inservibili (a meno di voler infettare il computer nel quale verranno utilizzati).

Contro il malware, a parte la prudenza e i software antivirus (che costituiscono i due elementi più importanti), è possibile adoperare anche risorse online.

I siti web di software antivirus spesso mettono gratuitamente a disposizione degli "scanner on line" che consentono di diagnosticare la presenza di malware. Meno frequente, purtroppo, la possibilità che questi scanner eliminino il malware, in quanto come soluzione viene generalmente proposto l'acquisto o almeno l'installazione in periodo di prova del software antivirus.

Utile risulta anche la consultazione periodica di siti di sistemi operativi, browser web, autorità preposte (ad es. la Polizia di Stato) che aggiornano spesso sulle minacce malware più diffuse e pericolose, a volte rendendo possibile lo scaricamento gratuito di tool (pr. *tul*) di rimozione del codice pericoloso.

Proprio per questo motivo, i malware più pericolosi impediscono la connessione a Internet dei dispositivi che colpiscono. In questi casi è ovviamente possibile utilizzare un altro dispositivo per accedere alle risorse online di cui sopra.

2.3.3

Comprendere che un attacco da malware può essere diagnosticato e risolto usando risorse online quali: siti web di sistemi operativi, anti-virus, browser web, siti web di autorità preposte

Sezione 3 Sicurezza in rete

3.1 RETI E CONNESSIONI

3.1.1

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

In informatica, il termine rete indica un sistema di collegamento tra due o più computer o dispositivi elettronici di altro tipo (tablet, smartphone, ecc.), dotati di una apposita scheda di rete e del relativo software di collegamento, che permette alle persone che utilizzano uno qualsiasi di quei dispositivi di sfruttare non solo le risorse del proprio apparecchio (vale a dire le applicazioni e i dati presenti su esso), ma anche quelle condivise degli altri computer, dispositivi ed eventuali periferiche (ad esempio stampanti o unità di memoria) collegate in rete.

Per fare un esempio: se nel computer di un amico è presente un documento e il mio tablet è collegato alla stessa rete di quel computer, in assenza di eventuali restrizioni poste dal mio amico, posso visualizzare quel documento, anche se materialmente esso non è presente nel mio dispositivo.

Così come è possibile collegare due dispositivi, è possibile collegarne dieci, cento o mille: in ogni caso quella che si realizza è sempre una rete, in inglese network (pr. *nèt-uòrc*), o, più brevemente, net.

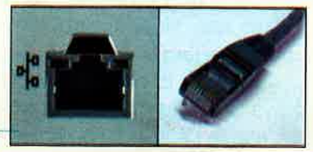
In base alla loro estensione, le reti si dividono principalmente in:

- Reti locali o LAN (pr. *lan*, da "Local Area Network", sign. "rete locale"): limitate a un'area circoscritta (una scuola, un ufficio, un'azienda), in genere non più ampia di 10 km. In una rete LAN esiste di solito un computer principale e più potente, detto server (pr. *sèrver*), che mette le proprie risorse a disposizione degli altri elaboratori della rete, chiamati client (pr. *clàient*). Dal momento che i dispositivi sono collegati attraverso l'utilizzo dei cavi, la rete è detta cablata e di solito garantisce una maggiore sicurezza, in quanto i dispositivi sono collegati in modo fisico e quindi visibile. Inoltre, i cavi assicurano in genere velocità di scambio dei dati maggiori rispetto alle onde radio.

più

Nelle reti cablate, si utilizzano prevalentemente le schede e cavi di rete **Ethernet** (pr. *èter-nèt*), dotati alle loro estremità di connettori chiamati **RJ45**, simili a quelli che si utilizzano nei telefoni moderni, ma leggermente più grandi (fig. **3.1.1a**).

FIG 3.1.1a



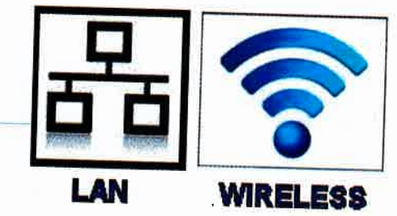
Se la rete non utilizza i fili per collegare i vari dispositivi, ma le onde radio, si aggiunge il prefisso "W" (da "wireless", pr. *uàirless*, sign. "senza filo") ed è quindi detta WLAN (pr. *vù-làn*) o rete locale wireless. Le reti wireless sono più economiche e semplici da installare, non richiedendo la posa di cavi. Se poi non è materialmente possibile far arrivare un cavo per collegare un dispositivo, il wireless è l'unica soluzione possibile. In genere, le WLAN sono protette da una password che impedisce l'accesso alle persone non autorizzate per garantire un accesso sicuro a dati e risorse. in alcuni luoghi pubblici (bar, hotel, locali commerciali, aeroporti, ecc.) esistono WLAN alle quali è possibile accedere liberamente.

- Reti geografiche o WAN (pr. *uàn*, da "Wide Area Network", sign. "rete di area estesa"): collegano tra loro computer distanti tra loro, oppure reti locali, coprendo, quindi, vaste aree. Anche Internet può essere considerata una WAN, per la precisione la più estesa di tutte le WAN.
- VPN (pr. *vì-pì-enne*, da "Virtual Private Network", sign. "rete privata virtuale"): utilizzano Internet (vale a dire una rete pubblica) per creare delle reti private (il cui accesso è quindi consentito solo a persone autorizzate) che collegano computer e dispositivi lontani tra loro. Attraverso una VPN, ad esempio, le aziende creano proprie linee private tra le diverse sedi, in modo da poter sfruttare in sicurezza tutti i servizi dell'azienda. La VPN utilizza un'autentificazione per garantire l'accesso ai soli utenti autorizzati e tecniche di crittografia per evitare il furto di dati.

più

Tutti i sistemi operativi mostrano la disponibilità di una rete attraverso delle icone che compaiono generalmente in basso (nei sistemi *Windows*) o in alto (nei sistemi *Linux* e *Android*), oltre che nel pannello delle configurazioni di rete. Al di là di piccole differenze grafiche, le icone che indicano la disponibilità di connessione LAN o wireless sono in genere quelle della fig. **3.1.1b**.

FIG 3.1.1b



3.1.2

Comprendere che la connessione ad una rete ha implicazioni di sicurezza, quali malware, accessi non autorizzati ai dati, difesa della riservatezza

La connessione in rete – in particolar modo alla più grande di queste reti: Internet – offre vantaggi spesso irrinunciabili: basti pensare all'utilizzo molto limitato che si potrebbe fare di uno smartphone o di un tablet non collegati a Internet.

D'altra parte, la connessione a una rete – sia essa una rete locale, come quella presente in molte scuole, uffici o aziende, oppure Internet – comporta minacce alla sicurezza dei dati. Le principali implicazioni di sicurezza sono:

- trasmissione di malware, che possono essere contenuti in allegati di posta elettronica, pagine web, programmi o altro;
- accessi non autorizzati ai dispositivi collegati e, conseguentemente, a tutti i dati in essi contenuti, a causa di difetti nella sicurezza o infezioni virali;

- **pericoli per la privacy**, sia perché in caso di accessi non autorizzati sono a rischio tutti i dati personali contenuti nei dispositivi collegati in rete, sia perché tutte le operazioni compiute all'interno della rete sono monitorate per ragioni di sicurezza (un amministratore di rete è in grado, ad esempio, di conoscere quando un utente si è collegato alla rete e quali siti ha visitato).

3.1.3

Comprendere il ruolo dell'amministratore di rete nella gestione delle operazioni di autenticazione, autorizzazione e assegnazione degli account all'interno di una rete; verifica e installazione di patch e aggiornamenti di sicurezza importanti, controllo del traffico di rete e trattamento del malware rilevato su una rete

Ogni rete viene gestita da un **amministratore di rete**, che ha la possibilità di effettuare interventi non consentiti agli altri utenti; ad esempio:

- **assegnazione** degli account (necessari per accedere alla rete) ai singoli utenti o a singoli dispositivi;
- **autorizzazione** degli account, assicurandosi che possano collegarsi senza problemi alla rete e stabilendo per ogni account i cosiddetti "privilegi", vale a dire quali operazioni sono permesse e quali vietate;
- **autenticazione** degli ingressi, attraverso password o altre procedure (schede magnetiche, impronte digitali, ecc.) che accertino l'identità di chi vuole accedere alla rete.

Inoltre, l'amministratore di rete ha il compito di controllare la sicurezza del sistema, attraverso le seguenti operazioni:

- **verifica e installazione di patch e aggiornamenti di sicurezza importanti**;
- **controllo del traffico di rete**;
- **trattamento dell'eventuale malware rilevato in rete** al fine di disinfettare, porre in quarantena o eliminare i file pericolosi (come spiegato ai punti 2.3.1 e 2.3.2).

più

La **patch** (pr. *pèc* con la *c* finale pronunciata come nella parola *cena*; sign. "pezza" o "cerotto") è un programma di dimensioni ridotte, destinato a eliminare piccoli o grandi errori di programmazione, che impediscono il corretto funzionamento di un software più grande o di un sistema operativo. Le patch vengono in genere distribuite dagli stessi produttori dei software, allo scopo di rimediare ai difetti riscontrati sino a quel momento (detti bug; pr. *bàg*), in genere in attesa di rilasciare una nuova versione del software.

3.1.4

Comprendere la funzione e i limiti di un firewall in ambiente domestico e di lavoro

Un virus informatico si riproduce nel computer infettando i file e utilizzandoli come mezzo di trasmissione (essendo nascosto al loro interno), per cui può essere bloccato da un antivirus aggiornato. Altri tipi di malware, invece, infettano i computer utilizzando i mezzi di comunicazione tra i dispositivi elettronici (innanzitutto Internet e la posta elettronica) e infiltrandosi come componenti del sistema operativo: per bloccarli non è quindi sempre sufficiente un antivirus, ma occorre un firewall.

Il **firewall** (pr. *fàir-uòl*) è un sistema di sicurezza che determina quali dati possono passare da Internet al dispositivo collegato in quel momento alla rete e viceversa, in modo da cercare di evitare che estranei possano accedere a dati presenti in un computer collegato a Internet, o trasmettere malware.

più

La traduzione letterale di firewall è "muro taglia-fuoco", con riferimento a delle speciali porte o pareti che vengono usate nella costruzione di edifici per impedire il propagarsi di un eventuale incendio da un locale ad un altro, così come un programma firewall ha il compito di impedire il propagarsi di un'infezione nei dispositivi collegati a una rete.

Utilizzati da tempo negli ambienti di lavoro, con la diffusione di Internet e il conseguente aumento del rischio di malware, i firewall sono utilizzati anche in ambiente domestico. Il firewall può essere costituito sia da un software (quasi tutti i sistemi operativi comprendono già al loro interno un firewall) sia da un apparato (ad esempio molti modem-router che servono a collegarsi a Internet dispongono di un firewall) o da un altro PC usato per questa funzione.

Ogni firewall vi segnala sia quando un programma contenuto nel vostro dispositivo cerca per la prima volta di accedere a Internet, sia tutti i tentativi di intrusione subiti dal computer, impedendo che il computer risponda alle istruzioni esterne.

In questi casi, il firewall propone in genere **quattro tipi di scelta**:

- *Sì, solo per questa volta* (viene permesso lo scambio di dati, ma la volta successiva vi verrà riproposta la domanda);
- *Sì, sempre* (sarà sempre consentito quel tipo di scambio di dati);
- *No, solo per questa volta* (viene impedito lo scambio di dati, ma la volta successiva verrà riproposta la domanda);
- *No, sempre* (quel tipo di scambio di dati sarà sempre impedito).

Una cattiva configurazione del firewall è il principale motivo dei suoi limiti: se, ad esempio, l'amministratore della rete blocca tramite il file delle connessioni necessarie a determinati programmi o funzioni, essi non potranno essere utilizzati. Al contrario, se consente connessioni non necessarie, queste potrebbero essere sfruttate da malintenzionati per accedere alla rete. Inoltre, un firewall non rileva la presenza di virus nei dati trasmessi e ricevuti ed è ovviamente impotente in caso di errori del personale interno o di uso di tecniche di "ingegneria sociale" (punto 1.3.1).

In linea generale, è consigliabile autorizzare solamente l'indispensabile: se non siete sicuri di cosa fa un certo programma che chiede l'autorizzazione, non autorizzatelo; autorizzatelo soltanto se l'uso di Internet è impossibile senza quest'autorizzazione.

3.1.5

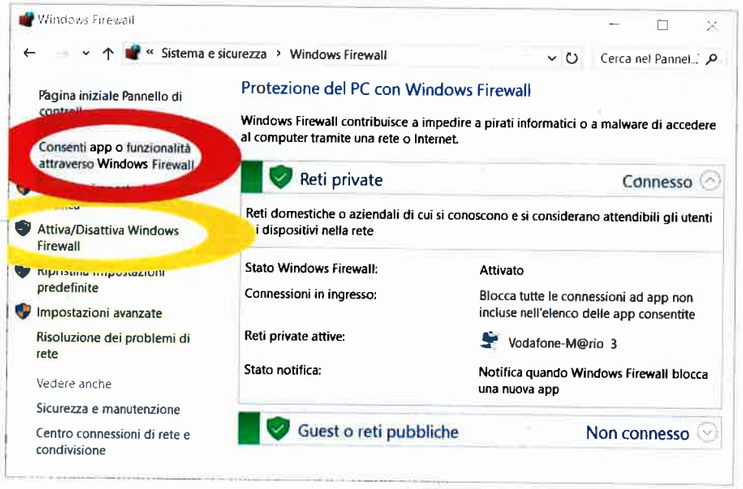
Attivare, disattivare un firewall personale. Consentire o bloccare l'accesso attraverso un firewall personale a un'applicazione, servizio/funzione

Nei computer che utilizzano Windows generalmente si accede al firewall attraverso il Pannello di controllo, cliccando prima su Sistema e sicurezza e poi su Windows Firewall.

Nell'omonima finestra che si apre (fig. **3.1.5a**) troviamo a sinistra una colonna contenente diverse opzioni tra cui:

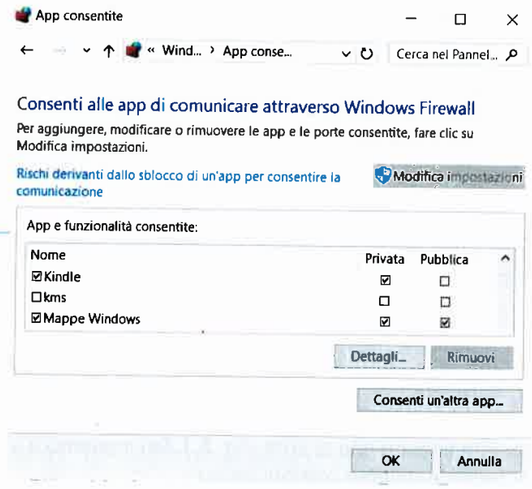
- *Attiva/Disattiva Windows Firewall* per abilitare o disabilitare il servizio (potrebbe esserci richiesto di immettere una password amministrativa o di confermare la scelta);

FIG 3.1.5a



- *Consenti app o funzionalità attraverso Windows Firewall* apre un'ulteriore finestra nella quale potremo consentire o bloccare la connessione ad applicazioni, servizi o funzioni inserendo o disinserendo il segno di spunta nelle relative caselle (potrebbe esserci richiesta una password amministrativa o comparire un riquadro nel quale confermare la scelta). Nella fig. **3.1.5b**, ad esempio è consentita la connessione all'app *Kindle* solo quando siamo collegati in una rete privata (ad es. a casa), mentre è vietata se stiamo utilizzando una rete pubblica (ad es. quella messa gratuitamente a disposizione in alcuni esercizi commerciali o stazioni); è inoltre vietata ogni connessione al servizio *kms* mentre sono consentite le connessioni sia su rete privata che su rete pubblica per il servizio *Mappe di Windows*.

FIG 3.1.5b



Le operazioni sono generalmente simili e abbastanza intuitive anche se utilizziamo altri firewall personali.

SICUREZZA SU RETI WIRELESS 3.2

3.2.1 **Riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti, quali: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access 2), filtraggio MAC (Media Access Control), SSID nascosto (Service Set Identifier)**

Per garantire la sicurezza delle reti wireless si utilizzano sistemi di cifratura dei dati (della cifratura abbiamo parlato al punto 1.4.2), in modo che eventuali malintenzionati che riuscissero a intercettare i dati non sarebbero comunque in grado di leggerli.

Il primo sistema di cifratura ad avere grande diffusione è stato il WEP (pr. *uèp*, da "Wired Equivalent Privacy", sign. "sicurezza della privacy equivalente", con riferimento a una presunta parità con la sicurezza delle connessioni effettuate con i cavi), oggi però quasi completamente sostituito dal più affidabile WPA (pr. *vù-pì-à*, da "Wi-Fi Protected Access", sign. "accesso senza fili protetto"), del quale esiste anche una versione WPA2 che rende ancora più efficace la protezione dei dati inviati e ricevuti.

Per ulteriore sicurezza, può essere utilizzato anche il cosiddetto MAC (pr. *mèk*, da "Media Access Control", sign. "controllo di accesso a livello hardware") o MAC address (pr. *mèk eddrèss*, sign. "indirizzo MAC"), che consiste in un indirizzo scritto in linguaggio esadecimale (vale a dire suddiviso in 6 coppie di cifre; ad esempio: 00:1F:3B:3C:5F:2F), che identifica ogni scheda di rete. Il MAC è impostato di fabbrica e quindi, per una ulteriore sicurezza nelle reti wireless, può essere creata una lista degli indirizzi MAC dei dispositivi autorizzati a utilizzare quella rete. Un estraneo, anche se a conoscenza della password di accesso, non potrebbe accedere alla rete, in quanto non verrebbe riconosciuto come valido l'indirizzo MAC del dispositivo che sta utilizzando. Va comunque tenuto presente che esistono sistemi che consentono a persone esperte di falsificare il MAC di una scheda di rete.

È anche possibile nascondere il nome della propria rete o SSID (da "Service Set Identifier") in modo che essa non compaia a estranei nell'elenco delle reti disponibili a cui connettersi. Anche in questo caso si tratta di un metodo aggirabile, in quanto alla persona estranea basta conoscere il nome della rete per effettuare la connessione.

Non esiste, quindi, un metodo in grado di garantire totalmente la sicurezza di una rete wireless, ma la conoscenza dei diversi metodi e il loro utilizzo – soprattutto in maniera combinata (ad esempio una chiave WPA2 unita a una lista di indirizzi MAC) – assicura un elevato grado di sicurezza.

3.2.2 **Essere consapevoli che usando una rete wireless non protetta si va incontro ad attacchi da parte di intercettatori (eavesdropping), dirottatori di rete (network hijacking), violatori di comunicazioni private (man in the middle)**

Se una rete wireless non è protetta con i metodi indicati al punto precedente, è semplice per un estraneo accedervi o solo per utilizzare gratuitamente la connessione a Internet, oppure per accedere ai dati presenti nei dispositivi e scambiati in rete. Il rischio non è solo del proprietario della rete, ma anche di chi si collega a essa senza averne l'autorizzazione, in quanto anche i suoi dati vengono scambiati senza cifratura.

I principali attacchi ai quali si va incontro usando una rete wireless non protetta sono effettuati da:

- intercettatori o "eavesdropping" (pr. *ivs-dròpin*) che intercettano i dati scambiati in rete. Alcuni pirati informatici, ad esempio, creano volutamente reti wireless non protette, in modo da poter intercettare i