Ministero dell'Istruzione, dell'Università e della Ricerca
Servizio Automazione Informatica e Innovazione Tecnologica

Modulo 1

Infrastrutture informatiche all'interno di un istituto scolastico

ForTIC

Piano Nazionale di Formazione degli Insegnanti sulle Tecnologie dell'Informazione e della Comunicazione

Percorso Formativo C

Materiali didattici a supporto delle attività formative

2002-2004

Promosso da:

- Ministero dell'Istruzione, dell'Università e della Ricerca, Servizio Automazione Informatica e Innovazione Tecnologica
- Ministero dell'Istruzione, dell'Università e della Ricerca, Ufficio Scolastico Regionale della Basilicata

Materiale a cura di:

- Università degli Studi di Bologna, Dipartimento di Scienze dell'Informazione
- Università degli Studi di Bologna, Dipartimento di Elettronica Informatica e Sistemistica

Editing:

CRIAD - Centro di Ricerche e studi per l'Informatica Applicata alla Didattica

Progetto grafico:

Campagna Pubblicitaria - Comunicazione creativa

Scopo e obiettivi del modulo

In questa sezione verrà data una breve descrizione del modulo.
Gli scopi del modulo consistono nel mettere in grado di:

- Identificare e documentare i requisiti *hardware* e *software* dell'infrastruttura informatica dell'istituto scolastico.
- Valutare e raccomandare prodotti *hardware* e *software*.
- Prevenire i problemi e risolverli.
- Identificare e discutere aspetti relativi alla legalità e alla *privacy*.

Il modulo è strutturato nei seguenti argomenti:

- **Identificazione dei bisogni**
  - Identificare e documentare i requisiti *hardware* degli utenti.
  - Identificare e documentare i requisiti *software* degli utenti.
  - Identificare e documentare i bisogni degli utenti di una rete per quel che riguarda l'*hardware*, il *software* e i servizi.
  - Identificare e documentare i requisiti per *hardware* e *software* multimediale.
  - Identificare e documentare i requisiti dei *server* di rete. (C2)
  - Identificare e documentare i requisiti dei *server* per Internet.
- **Valutazione del *software* e dell'*hardware***
  - Valutare e raccomandare prodotti *hardware* e servizi.
  - Applicare i principi dell'ergonomia alla selezione e raccomandazione dei prodotti.
  - Valutare e raccomandare periferiche, prodotti multimediali e servizi.
  - Valutare e raccomandare prodotti *software* e servizi.
  - Valutare e raccomandare *server* di rete e ambienti operativi. (C2)
  - Valutare e raccomandare reti, prodotti di accesso remoto e servizi. (C2)
  - Valutare e raccomandare l'*hardware* necessario per costruire e mantenere un sito *Web*.
- **Prevenzione di problemi e loro soluzione**
  - Descrivere le tecniche e le procedure appropriate per la prevenzione dei problemi e la loro soluzione (stabilizzatori di corrente, UPS, *software* antivirus, *backups* di *software* e dati, piani di sostituzione di componenti *hardware*, modi di conservazione esterna dei *backup*, ecc).
  - Descrivere appropriate pratiche e procedure di sicurezza fisica e protezione di risorse con strumenti *software* (*password*, *software* anti-virus, criptazione dei dati, ecc).
- **Aspetti legali e *privacy***
  - Identificare e discutere elementi di etica professionale.
  - Identificare e discutere aspetti riguardanti le politiche di licenza d'uso dei vari *software*.
  - Identificare e discutere il diritto di proprietà e di licenza del *software*.
  - Identificare e discutere aspetti relativi alla *privacy*.
  - Identificare e discutere aspetti relativi alla crittografazione.
  - Identificare gli aspetti relativi alla responsabilità legale.
  - Identificare e discutere gli aspetti relativi all'accessibilità per disabili.

Introduzione

Prevenzione di problemi e loro soluzione.

Prof.ssa Paola Salomoni
Dott. Diego Gardini

Introduzione

Scopo di questa sezione è introdurre alcune delle metodiche e delle tecnologie che consentono di attuare politiche, efficaci e lineari, di prevenzione dei guasti. Un approccio globale alla protezione dei dati e delle risorse deve essere basato principalmente su politiche di tipo proattivo, ovvero su attività di prevenzione che mirano a ridurre al minimo le **vulnerabilità** del sistema. Alle politiche proattive devono poi essere associate attività di tipo reattivo, che consentano, in caso di danno ormai verificato, di ripristinare il corretto funzionamento del sistema.

In generale, è obiettivo dell'amministratore e del responsabile dei sistemi evitare qualunque minaccia, ovvero qualunque evento o entità che possa danneggiare il sistema compromettendo i dati o i servizi critici. Esistono numerose categorie di minacce, che vanno dagli eventi catastrofici, naturali e non (incendi, terremoti, alluvioni), agli incidenti che coinvolgono le infrastrutture, casuali o intenzionali (taglio di cavi, sospensione dell'erogazione di corrente), ai veri e propri attacchi alla **sicurezza del sistema** .

La valutazione generale dei danni va fatta tenendo in considerazione diversi aspetti:

- gli aspetti tecnici e le tecnologie di supporto alla prevenzione;
- gli aspetti organizzativi, ovvero la definizione di ruoli e procedure che specifichino aree d'azione, limiti e responsabilità, anche attraverso opportune attività di formazione del personale;
- gli aspetti economici e legali.

In questa breve trattazione introdurremo alcuni degli aspetti tecnici, trattando le principali tecniche e procedure per la prevenzione dei problemi e la loro soluzione. È disponibile un approfondimento sulla **sicurezza come forma di prevenzione** , che tratta in modo più specifico le problematiche relative alla sicurezza delle informazioni.

Multiutenza

La protezione dei dati e delle risorse inizia con una fase di definizione dei ruoli in cui a ogni utente sono associati un insieme di criteri di accesso. Il sistema operativo che viene utilizzato deve quindi consentire di definire a quali risorse può accedere ogni utente, proteggendo le altre risorse da eventuali accessi non autorizzati. Deve inoltre offrire un meccanismo di identificazione, tipicamente attraverso uno ***username*** e una ***password*** , che consenta di verificare l'identità degli utenti. Ogni persona che vuole accedere alle risorse del sistema deve farsi riconoscere come utente noto e lo fa specificando l'identificativo (*username*) con cui il sistema lo individua. Deve inoltre fornire la *password* privata associata allo *username*, in modo che il sistema possa verificare la sua identità.

In presenza di ambienti con molti utenti che hanno ruoli differenziati è dunque essenziale optare per sistemi operativi che offrano supporti al controllo degli accessi e all'implementazione di politiche di accesso articolate. Indispensabile è definire a priori quali sono i criteri di accesso alle risorse da parte degli utenti. Sistemi operativi e applicazioni a uso personale, che non prevedano politiche di accesso ai *file* e alle risorse, ma consentano a tutti gli utenti l'accesso a tutte le risorse (quali per esempio *Microsoft Windows98*), rendono impossibile la realizzazione di politiche di protezione e prevenzione significative.

In presenza di utenti che condividono risorse e attività è opportuno definire a priori un insieme di politiche di accesso a postazioni, *file*, stampanti, eccetera, che consenta all'amministratore di semplificare le diverse fasi della gestione. I sistemi operativi multiutente permettono di definire politiche molto articolate, sfruttando come meccanismo base quello dei **gruppi**. Ogni gruppo viene associato alle proprie politiche di accesso alle risorse ed ogni utente viene poi inserito in uno o più gruppi. In questo modo, quando ad un gruppo vengono estesi o ridotti i permessi, la modifica viene applicata automaticamente a ogni utente che ne fa parte.

Backup

Si intende in modo generale con ***backup*** una copia dei dati destinata all'archiviazione che può essere utilizzata in caso di errore per ripristinare uno stato precedente. Le cause di un errore possono essere innumerevoli, ma sono tipicamente riconducibili a due tipologie:

- l'errore prodotto dal ***software***, che può essere causato da un intervento sbagliato dell'amministratore o dell'utente (per esempio una cancellazione irreversibile di *file*), oppure può essere determinato da un malfunzionamento del *software* (anche provocato da un **virus** o da altri tipi di **attacco** alla **sicurezza del sistema**);
- l'errore prodotto dall'***hardware***, che può essere dovuto a un malfunzionamento intrinseco di supporti e componenti (per esempio un disco fisso che si rompe) o causato da eventi esterni che provocano danni all'*hardware* (compresi fenomeni naturali, come un allagamento o un fulmine).

In tutti questi casi le informazioni (o una loro parte) risultano inutilizzabili e per ripristinare lo stato precedente all'errore è necessaria una copia dei dati che sono stati compromessi. L'operazione di ripristino è detta ***restore*** .

Perché il ripristino sia effettivo occorre che la copia di *backup* dei dati sia recente. Più tempo intercorre tra il momento in cui è stato effettuato il *backup* e il momento in cui si verifica l'errore, più gravi saranno gli effetti di quest'ultimo. Per questo motivo è importante pianificare un'attività di *backup* regolare che preveda periodicamente, a scadenze fisse, il *backup* generale dei dati e giornalmente il *backup* dei dati critici. Sono disponibili sistemi che consentono di automatizzare la procedura di *backup* e di avviarla automaticamente quando le risorse sono parzialmente o completamente inutilizzate (per esempio di notte) e sistemi che permettono di centralizzare il *backup* di più macchine in rete.

Tipi di backup

Le procedure di ***backup*** dipendono dal sistema operativo utilizzato, ma, generalmente, è prevista la possibilità di fare *backup* solo dei dati (per esempio della posta elettronica o dei *file* degli utenti), oppure di fare *backup* anche del sistema e delle applicazioni. In questo caso si mantiene copia anche dei *file* di configurazione e dei *file* di sistema, in modo da intervenire sempre esclusivamente con un *restore*. Quest'ultima opzione non sempre è consigliabile poiché esistono diverse occasioni (un esempio tipico è quando l'errore è causato da un attacco alla sicurezza) in cui può essere opportuno reinstallare il sistema operativo.

Il *backup* dei dati è tipicamente una operazione lunga, a causa della grande mole delle informazioni da copiare e della relativa velocità dei **supporti di *backup*** . Per questo motivo non viene sempre effettuato un *backup* completo dei dati, ma vengono a volte utilizzate metodologie di stratificazione delle copie che consentono di effettuare salvataggi parziali. In generale si parla di:

- ***backup* completo** : quando i dati vengono copiati interamente (dal supporto originale al *backup*) e per ripristinarli occorre semplicemente effettuare la copia in senso inverso (dal *backup* al supporto originale). Questo tipo di *backup* è consigliabile quando i dati cambiano molto frequentemente, ma risulta inutilmente lento se i dati sono sostanzialmente stabili e cambiano raramente;
- ***backup* incrementale** : vengono copiati i *file* creati o modificati dall'ultimo *backup* completo o incrementale. Qualora si faccia un successivo *backup* incrementale, questo farà comunque riferimento al precedente. La procedura di *restore* deve quindi prevedere una ricostruzione stratificata a partire dall'ultimo *backup* completo, che passa attraverso tutti i *backup* incrementali effettuati;
- ***backup* differenziale** : vengono copiati i *file* creati o modificati dall'ultimo *backup* completo. Qualora si faccia un successivo *backup* differenziale, questo farà comunque riferimento al *backup* completo e non si avvarrà del *backup* differenziale precedente. La procedura di *backup* è quindi un po' più lenta rispetto al *backup* incrementale, ma è più semplice e veloce la procedura di *restore*, che prevede il recupero dell'ultimo *backup* completo e di un solo *backup* differenziale.

Supporti per il backup

Il ***backup*** dei dati viene fatto su supporti di memoria di massa che offrono grande capacità a basso costo (uno stesso supporto può fornire spazio per il *backup* di più dischi) e alta affidabilità (se in presenza di un errore il *backup* risultasse danneggiato, sarebbe impossibile il ripristino). La velocità è un altro fattore rilevante, meno critico rispetto a quelli citati precedentemente poiché i *backup* lunghi sono frequentemente automatizzati e quindi non risulta essere fondamentale il tempo di esecuzione.

Per tutti questi motivi i *device* dedicati al *backup* sono basati su tecnologie a nastro che hanno alta affidabilità a costi contenuti e sono relativamente veloci nell'accesso sequenziale tipico della procedura di copia. La velocità si misura in termini di *byte* trasferiti al secondo (Bps) e arriva a diversi GB all'ora. Questo tipo di *device* ha capacità molto elevate (nell'ordine delle decine di GB) ed è indicato nei sistemi medio grandi che hanno grandi quantità di dati critici di cui fare frequenti *backup*. Alternativamente possono essere utilizzate unità a cartucce magnetiche rimovibili che hanno minori capacità in termini di memorizzazione e velocità, ma sono più economiche e possono essere efficacemente usate per *backup* meno frequenti e di minori dimensioni.

In alternativa possono essere utilizzati anche supporti non dedicati al *backup*, ma che in particolari condizioni si prestano a questo tipo di attività. Per esempio, i supporti ottici (come CD e DVD, scrivibili e riscrivibili) oppure i supporti magneto-ottici possono essere usati per *backup* di dimensioni medio/piccole. Un'ulteriore alternativa è costituita da dischi fissi aggiuntivi, che possono essere inseriti in un sistema per contenere il *backup* dei dati di quel sistema o di altri. Infine, si possono usare i *floppy* per copie di *file* di pochi KB, che costituiscono una forma personale di *backup*.

Immagini dei dischi

Un meccanismo di ripristino molto efficace consiste nel memorizzare una immagine precisa del disco fisso, settore per settore, e nel riversarla su un diverso supporto di memoria di massa, per esempio un altro disco oppure un CD o un DVD. Viene quindi creata una immagine del disco assolutamente identica all'originale e, se il disco originale risulta danneggiato, è possibile ricostruire la situazione iniziale invertendo il processo di copia. Il disco così ricostruito sarà identico all'originale anche a livello fisico, garantendo il funzionamento del sistema. Questo tipo di processo viene tipicamente attuato attraverso *software* appositi che offrono supporto al *backup* e al ripristino dei dati.

Questo meccanismo può essere usato anche in quelle situazioni in cui molte macchine hanno la stessa dotazione *hardware* e *software* e dunque necessiterebbero di tante installazioni identiche. Una condizione di questo tipo si verifica spesso nei laboratori didattici che hanno frequentemente dotazioni *hardware* identiche, quantomeno per lotti, e necessitano anche di dotazioni *software* sovrapponibili per consentire di effettuare la stessa attività didattica su tutte le postazioni. In questo caso è possibile mettere in atto la procedura di installazione su di un *computer* campione, provvedendo a montare sia il sistema operativo che le applicazioni. Il disco o i dischi del *computer* campione costituiscono dunque una valida base per tutte le installazioni dei *computer* identici a quello scelto e sono perciò candidati a diventare una immagine fisica da ricopiare poi su tutte le postazioni. Partendo dall'immagine del disco (o dei dischi) del *computer* campione è possibile quindi ottenere semplicemente tante installazioni funzionanti con una elementare attività di copia. Questa possibilità consente, a chi gestisce le macchine, di concentrarsi sulla prima installazione, risparmiare tempo sulle successive, ridurre la possibilità che si verifichino errori o si rilevino incompatibilità e infine offre supporto alle installazioni successive che dovessero rendersi opportune a causa di errori.

Due considerazioni, ovvie, introducono vincoli alla procedura appena illustrata. La prima è che, dopo la copia dell'immagine, è comunque necessaria una fase di configurazione delle singole postazioni, che ha come obiettivo quello di personalizzare le installazioni inserendo quei dati, come l'indirizzo IP o il numero di licenza del *software*, che sono diversi in ogni PC. La seconda è che il ripristino da condizioni di errore, fatto attraverso l'immagine iniziale, produce la perdita di tutti quei dati che sono salvati sul disco locale e dunque è sconsigliato qualora gli utenti non disponessero di spazio disco su *file server*.

RAID

Esistono alcune tecniche di controllo dei dischi che migliorano l'affidabilità operando in modo trasparente. La gestione dei dischi denominata **RAID** (*Redundant Array of Independent Disks*) mira a prevenire i danni e a favorire il recupero automatico dei dati. RAID indica un complesso meccanismo di memorizzazione che utilizza più dischi fissi con l'obiettivo di aumentare le prestazioni della memoria di massa in termini di velocità e/o di affidabilità. In particolare i miglioramenti di affidabilità consentono in alcuni tipi di RAID di recuperare automaticamente e in modo trasparente alcuni errori *hardware*.

Le diverse tipologie RAID combinano alcuni meccanismi base:

- lo ***striping*** , una tecnica di miglioramento della velocità di lettura/scrittura che consiste nello spalmare i dati di un blocco in più dischi. Il blocco viene diviso in n sottoblocchi, ognuno dei quali è memorizzato su un disco diverso e ogni lettura innesca n letture (da n dischi), riducendo il tempo di trasferimento e di latenza. Questa tecnica di per sé non incide sulla resa dei dischi poiché non inserisce informazioni di controllo.
- Il ***mirroring*** , in cui ogni disco viene duplicato e dunque esiste una copia di sicurezza di ogni informazione. Il *mirroring*, oltre ad aumentare l'affidabilità, consente l'uso in parallelo dei dischi in lettura. Non migliora invece le prestazioni in scrittura. Le copie vengono gestite direttamente dal sistema, per cui utente e amministratore vedono una sola istanza del *file*. Il *mirroring* prevede una ridondanza totale delle informazioni che dimezza la resa dei dischi.
- I **blocchi di parità** , che consentono di ricostruire porzioni di informazioni andate perse a causa di errori. I blocchi di parità sono blocchi utilizzati per memorizzare informazioni riassuntive (calcolate da apposite funzioni matematiche) sugli n blocchi precedenti e non possono quindi garantire ridondanza totale. Per questo motivo non recuperano da qualunque tipo di difetto, ma solo da errori circoscritti. La ridondanza incide però molto meno del *mirroring* sulla resa dei dischi poiché prevede l'inserimento di un blocco di parità ogni n blocchi dati e dunque una perdita in termini di spazio di un (n+1)-esimo.

Tipologie RAID

Combinando ***striping*** , ***mirroring*** e **blocchi di parità** si ottengono sistemi RAID differenti che offrono diversi gradi di affidabilità e l'aumento delle prestazioni in lettura/scrittura. In particolare:

- **RAID 0**: utilizza ***striping*** per ottenere un miglioramento di prestazioni in lettura e scrittura. È tipicamente utilizzato su dischi di uguali dimensioni in modo da non avere perdite di capacità complessiva. Se si utilizzano 5 dischi da 10 GB si riesce a usare tutti i 50 GB disponibili, che vengono visti come un unico disco, e si velocizzano le letture e le scritture di 5 volte. RAID 0 non prevede ridondanza e se si verifica un guasto su un disco vengono compromesse anche informazioni contenute in *stripe* sugli altri dischi.
- **RAID 1**: utilizza ***mirroring*** per aumentare l'affidabilità del sistema. Recupera da situazioni di danno totale dei dischi. Se si utilizzano 4 dischi da 10 Giga si usano effettivamente solamente 20 GB.
- **RAID 1+0**: utilizza ***striping*** e ***mirroring*** combinati nel modo seguente: i dischi vengono messi in *mirror*, ovvero metà dei dischi sono predisposti per essere copia dell'altra metà. Sono dunque visibili n/2 unità che vengono messe in *striping* per migliorare le prestazioni. È sia molto affidabile (di ogni disco in *stripe* esiste una copia ridondante) che molto veloce. Se si utilizzano 8 dischi da 10 Giga si possono velocizzare le letture e le scritture di 4 volte usando però effettivamente solo 40 GB, visti come un'unica unità.
- **RAID 5**: utilizza ***striping*** e **blocchi di parità** combinati per ottenere un miglioramento di prestazioni e di affidabilità. È meno affidabile rispetto a RAID 1+0, ma rende disponibile all'utente una quantità maggiore di memoria. Se sono disponibili 5 dischi da 10 GB, ne usa uno per la parità e 4 per i blocchi dati effettivi, col risultato che si usano 40 GB e si velocizzano le letture e le scritture di 4 volte. Rispetto alla soluzione con RAID 1+0 si ottengono risultati analoghi con 30 GB in meno. È tollerante rispetto al guasto di un solo disco.

Le tecniche RAID possono essere realizzate via *hardware*, utilizzando appositi *controller* che gestiscono le singole azioni di lettura e di scrittura implementando una strategia RAID, oppure via *software*, attraverso il sistema

operativo, che consente di definire politiche di gestione dell'*hardware* che attuano metodiche RAID.

UPS

Gli eventi esterni che più frequentemente provocano danni ai sistemi sono quelli imputabili alle fluttuazioni nella distribuzione di energia elettrica. Si tratta in alcuni casi di interruzioni improvvise dell'erogazione di corrente (*blackout*) e in altri di sovratensioni e sottotensioni. Tutte queste tipologie di eventi possono provocare seri danni, in particolare agli alimentatori, alle *motherboard*, alle schede di rete e ai dischi.

Per ovviare a questo tipo di problema si possono dotare i sistemi più critici (per esempio i *server*) di un gruppo di continuità (in inglese *Uninterruptible Power Supply*, **UPS**), ovvero di un sistema di alimentazione che ha l'obiettivo di fornire energia anche quando non viene direttamente rifornito perché l'erogazione della rete elettrica si interrompe o è instabile.

Per offrire questo tipo di servizio l'UPS è dotato di batterie, ovvero di accumulatori di energia che forniscono corrente quando la rete non alimenta o quando fornisce energia al di fuori dei limiti di tolleranza ammessi.

Esistono fondamentalmente due tipi di UPS:

- **UPS *off line***: la componente che converte la corrente continua della batteria in quella alternata della rete normalmente è disattivata e gli apparati si alimentano direttamente dalla rete. Viene attivato solo quando manca l'alimentazione elettrica.
- **UPS *on line***, in cui la componente che converte la corrente continua della batteria in quella alternata della rete è sempre attiva e gli apparati si alimentano solo dalle batterie. Questo tipo di UPS tipicamente si occupa anche di stabilizzare l'energia elettrica ovvero di fornire un'alimentazione con tensione stabile e costante e con frequenza fissata. Rispetto agli UPS *off line* ha anche il vantaggio di non dover effettuare commutazioni nel momento del *black out* e di non introdurre dunque interruzioni nell'erogazione.

Virus

I virus fanno parte di una famiglia di attacchi alla sicurezza nota come ***malicious software*** (*malware*), che comprende altri tipi di programmi caratterizzati dal fatto che si diffondono da un *computer* all'altro con lo scopo di produrre danni ai sistemi.

In realtà i virus più recenti mescolano le caratteristiche di diversi tipi di *malware* con lo scopo di diventare più difficili da individuare e più efficaci nel diffondere l'infezione e in particolare spesso sono **virus** e ***worm*** , ovvero *software* che hanno i medesimi meccanismi riproduttivi dei virus, ma che utilizzano (come i *worm*) la rete per propagarsi. Questa caratteristica accomuna la maggior parte dei virus recenti poiché lo scambio di *file* (che è il meccanismo base per il propagarsi dell'infezione) avviene ormai prevalentemente attraverso la rete.

I virus possono essere classificati in base a diverse caratteristiche, tra cui la più significativa è l'ambiente attraverso cui propaga l'infezione e si sviluppa il virus. Sono distinguibili in questa ottica diverse tipologie di virus:

- i ***boot* virus** , che infettano il *Boot Sector* o il *Master Boot Record* dei dischi in modo da essere caricati all'avvio del sistema;
- i ***file* virus** , che infettano, con modalità molto varie, i *file* eseguibili e utilizzano lo scambio di questi ultimi per propagare l'infezione;
- i **macrovirus** , che sono scritti in VBA (*Visual Basic for Application*) un linguaggio per la scrittura di macro negli ambienti applicativi *Office*;
- i ***network* virus**, che si diffondono sfruttando le **vulnerabilità** dei protocolli di Internet.

Su virus e antivirus è disponibile un **approfondimento** .

Antivirus

La migliore difesa contro i virus è ovviamente la prevenzione che va affrontata sia in termini tecnologici che comportamentali. In particolare per prevenire i virus occorre:

- evitare comportamenti rischiosi, quali scambio e *download* di *file* sospetti, installazione di pacchetti non licenziati, apertura degli *attach*. Quest'ultima precauzione è molto importante per difendersi dai macrovirus poiché, se l'allegato non viene eseguito, il virus rimane latente. Aprire i messaggi di posta elettronica può diventare causa di infezione solo se il *client* di posta è impostato per eseguire gli allegati in automatico. Per questo motivo è opportuno disabilitare l'anteprima dei messaggi.
- Aggiornare il *software* in modo da ridurre le vulnerabilità al minimo. L'attacco dei virus viene infatti condotto sfruttando errori nel *software* o nei protocolli e tutte le azioni volte a ridurre il numero di errori presenti nei programmi (come per esempio l'installazione delle *patch*) sono forti forme di prevenzione dei virus.
- Utilizzare un *software* antivirus, ovvero un *software* in grado di identificare i virus e rimuoverli prima che entrino in azione. Per rilevare la presenza di un virus i *software* antivirus cercano all'interno della memoria (centrale e di massa) particolari sequenze di *byte* che costituiscono l'impronta identificativa del virus. La continua produzione di nuovi virus rende quindi indispensabile un aggiornamento continuativo del *software* antivirus per garantirne l'efficacia nel tempo. Alcune volte i *software* antivirus sono in grado di rilevare anche virus di cui non conoscono la sequenza di *byte* identificativa, riscontrando su base probabilistica comportamenti anomali o sospetti.
- Effettuare comunque un *backup* periodico dei dati, in modo da poter ripristinare efficacemente il sistema anche in caso di danni.

Le attività dei *software* antivirus rallentano le prestazioni del sistema, richiedendo continue scansioni della memoria e del disco. Per esempio, è possibile effettuare scansioni periodiche non automatiche di tutto il *filesystem* da attivare in momenti in cui il sistema non è utilizzato. Per questo motivo alcune attività di verifica vengono attivate su richiesta.

Su virus e antivirus è disponibile un **approfondimento** .

Conclusioni

Questa sezione dell'introduzione ha offerto una panoramica molto veloce su alcune delle tecnologie che vengono utilizzate per prevenire i guasti e preservare la disponibilità delle informazioni. In particolare sono state introdotte soluzioni che offrono supporto a tipologie molto differenti di problemi, dall'attacco alla sicurezza dei dati prodotto da un virus ai danni *hardware* che possono essere conseguenza di uno sbalzo di tensione nell'erogazione della corrente elettrica. L'elenco dei problemi, così come quello delle tecnologie che supportano la prevenzione e il recupero, non vuole essere esaustivo, ma vuole invece toccare alcuni dei guasti più frequenti.

Sono stati inoltre evidenziati alcuni aspetti correlati alle tecnologie che hanno in realtà forte impatto su tematiche di tipo organizzativo, quali la gestione degli utenti o la programmazione periodica delle attività di aggiornamento del *software* o delle procedure di *backup*.

Sono disponibili approfondimenti:

- sulla **sicurezza come forma di prevenzione dei problemi** (consigliato per profilo C1)
- su **virus e antivirus** .

Identificazione dei bisogni

Prof.ssa Paola Salomoni
Dott. Diego Gardini

Introduzione

Le Tecnologie dell'Informazione e della Comunicazione (TIC, o anche, in inglese, *Information and Communication Technologies*, ICT) hanno profondamente trasformato le modalità di azione e di comunicazione nella realtà quotidiana e sono penetrate fortemente in ogni contesto favorevole all'innovazione. All'interno delle strutture scolastiche sono presenti almeno due distinte realtà in cui l'uso delle TIC diviene uno strumento fondamentale: l'amministrazione e la didattica.

Gli obiettivi di chi gestisce e amministra le risorse informatiche di un istituto scolastico sono molteplici e devono essere congiunti con la continua esigenza di rinnovamento infrastrutturale e formativo tipico delle TIC. Tra le finalità occorre considerare:

- L'esigenza dell'amministrazione della scuola di avere a disposizione strumenti per la produttività individuale e il *back office* atti a velocizzare e automatizzare le procedure di gestione.
- L'esigenza di studenti e docenti di avere a disposizione strumenti didattici che supportino efficacemente il processo di apprendimento, tra i quali un accesso a Internet efficiente e un sistema di condivisione delle risorse proficuo.
- L'esigenza dell'amministratore dei sistemi di gestire in modo efficace *hardware* e *software*.
- La possibilità di offrire servizi attraverso Internet al personale, agli studenti e alle famiglie.

Il processo di potenziamento delle infrastrutture deve prevedere una attenta analisi dei bisogni reali degli utenti della scuola, dal dirigente all'amministrazione, dai docenti, agli studenti alle famiglie. L'individuazione dei bisogni deve verificare il grado di soddisfacimento prodotto dalle attrezzature attualmente a disposizione e comprendere quali obiettivi gli utenti vogliono realizzare mediante l'acquisizione di nuove risorse informatiche.

Bisogni e obiettivi

I bisogni degli utenti, analizzati e verificati, possono fornire gli elementi base per l'identificazione degli obiettivi di intervento, che vanno definiti in termini generali e poi, in un secondo tempo, specificati e dettagliati in un progetto. Definire gli obiettivi significa progettare di mettere gli utenti in condizione di fruire di un servizio nuovo o di migliorare l'erogazione di un servizio. L'utente quindi non deve limitarsi a spiegare di quale nuova infrastruttura ha bisogno, ma deve definire quale obiettivo attualmente non raggiungibile vuole rendere attuabile con la nuova attrezzatura. Per esempio a fronte di una aumentata esigenza di connettività, l'amministratore può proporre di sostituire più collegamenti via modem con un collegamento a banda larga (**ADSL**). Il singolo utente, che non ha visibilità su tutta l'infrastruttura, potrebbe presentare richieste specifiche meno calzanti.

Uno degli obiettivi da considerare sempre è quello di mantenere aggiornati *hardware* e *software* in modo da non peggiorare i servizi già disponibili rimanendo vincolati a infrastrutture che diventano di giorno in giorno più obsolete. Altri obiettivi, che mirano a definire nuovi servizi, prevedranno l'acquisizione di nuove attrezzature a fronte della disponibilità di nuovi servizi. Gli obiettivi non sono ovviamente tutti raggiungibili, ovvero i bisogni e, più in generale, le richieste degli utenti non sono tutti soddisfabili. Alcuni obiettivi dovranno essere quindi considerati come prioritari e di conseguenza finanziabili, mentre altri verranno rinviati in attesa di maggiori disponibilità.

Un approccio che favorisca le sinergie e la condivisione delle risorse consente di raggiungere un numero maggiore di obiettivi e, dunque, di soddisfare un numero maggiore di bisogni. Per esempio, una stampante in rete può fornire il servizio di stampa a più uffici o una fotocamera digitale può essere utilizzata per soddisfare le esigenze didattiche di più docenti e classi.

La rete

La rete locale è sostanzialmente uno strumento di condivisione delle risorse disponibili all'interno di una scuola. È significativa anche quando connette il numero minimo di *computer*, due, perché consente di condividere tra questi le risorse. Risponde dunque a molti bisogni in modo implicito, poiché permette di mettere a disposizione da più postazioni risorse che altrimenti servirebbero un solo utente alla volta. In particolare la condivisione dell'accesso a Internet (un solo accesso per tutta la scuola), della memoria di massa, delle stampati e delle altre periferiche può consentire di aumentare la dotazione della scuola in termini qualitativi piuttosto che quantitativi.

La rete Internet risponde invece a esigenze di comunicazione con l'esterno e offre supporto allo scambio di informazioni, alla pubblicazione elettronica di materiale ipertestuale e multimediale e al reperimento di materiale pubblicato da altri. La connessione a Internet è dunque un mezzo di scambio e di ricerca e la sua validità in ambito didattico è ormai dimostrata da innumerevoli esperienze. È disponibile in grande parte del territorio nazionale la possibilità di collegarsi a Internet attraverso connessioni **ADSL** (*Asymmetric Digital Subscriber Line*) che forniscono un servizio sempre disponibile e a banda larga.

Una LAN connessa a Internet costituisce dunque un efficace mezzo di comunicazione e condivisione delle risorse.

Accesso a Internet

L'accesso a Internet della scuola può essere sostanzialmente di due tipi:

- **temporaneo** su rete commutata, che avviene usando una linea della rete telefonica pubblica e telefonando a un fornitore di servizi;
- **stabile** (***always on***) su rete dedicata, che non si attiva solo su richiesta (come le connessioni commutate), ma è disponibile 24 ore al giorno.

La connessione commutata ha un costo che dipende dal tempo di connessione (come la telefonata) e può essere realizzata sia su normali linee telefoniche (in questo caso si raggiungono i 56,6 Kbps massimi) che su linee ISDN (in questo caso si arriva a un massimo di 128Kbps, con due connessioni). Le connessioni **ADSL** sono invece di tipo *always on* e offrono un servizio a **banda larga** che arriva a misurarsi in Mbps. Il costo in questo caso è *flat* (indipendente dall'attività o dal tempo) o in alcuni casi può dipendere dalla quantità di traffico generato.

I server

Alcuni obiettivi possono essere efficacemente soddisfatti quando, in presenza di un rete locale della scuola, si gestiscono in modo centralizzato alcuni servizi. In particolare:

- ***domain controller***: *server* che controlla il dominio della LAN, ovvero l'insieme degli utenti, dei gruppi e delle risorse della LAN. Fornisce meccanismi centralizzati d'accesso per cui gli utenti vengono autenticati e gestiti in modo centralizzato.
- ***File server***: *server* che offre la gestione dello spazio disco per gli utenti. Un sistema di accesso ai *file* centralizzato consente agli utenti di utilizzare i propri dati da una qualunque delle postazioni della LAN.
- ***Print server***: *server* che gestisce la/le stampanti, rendendole disponibili da tutte le postazioni della LAN. Mantiene in coda i *task* di stampa.
- *Server* per i servizi Internet: uno o più *server* dedicati a fornire i servizi Internet. In particolare il ***server Web*** rende disponibili i documenti attraverso il protocollo HTTP e dunque è destinato a contenere il sito *Web* della scuola. Il ***mail server*** offre invece servizi *mail* ed è necessario se si vogliono utilizzare molti *account* di posta (come accade quando si vuole offrire la posta a tutti gli studenti e i docenti).

La scelta di fornire servizi centralizzati come quelli descritti agevola anche l'amministratore semplificando

notevolmente alcuni aspetti gestionali come il *management* degli utenti e il ***backup*** .

L'infrastruttura di rete

Le tecnologie *hardware* e *software* e le infrastrutture di rete che sono state brevemente citate danno origine a un'ampia gamma di soluzioni e architetture che possono essere realizzate all'interno di una scuola sia in ambito didattico che come supporto al lavoro dell'amministrazione.

Molte delle competenze necessarie a realizzare un progetto completo di questo tipo sono oggetto dei successivi moduli di questo percorso formativo. Gli esempi che seguono non hanno dunque come obiettivo la definizione di linee guida progettuali, né hanno l'ambizione di trattare in modo esaustivo l'argomento. Sono piuttosto strutturati per delineare le principali funzionalità che possono essere offerte attraverso un'architettura che combini la presenza di una rete locale, l'accesso a Internet e i principali servizi descritti.

Chi intendesse affrontare l'argomento in modo più articolato è invitato farlo attraverso la **bibliografia *on line*** oppure esaminando **i casi di studio** presenti tra gli approfondimenti (consigliati per il profilo C2).

La condivisione delle risorse

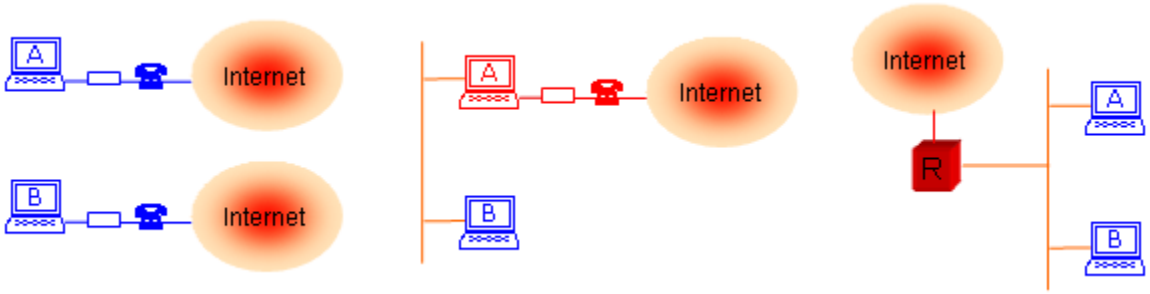
La **rete locale** è fondamentalmente uno strumento di condivisione delle risorse, e in particolare consente di mettere in comune alcune componenti *hardware* che senza la rete risulterebbero utilizzabili esclusivamente da una certa postazione. Si ipotizzi per esempio di avere a disposizione tre postazioni (A, B e C) che costituiscono la dotazione dell'amministrazione o di un piccolo laboratorio. Se si vuole consentire di stampare da ciascuna delle tre postazioni si possono considerare diverse soluzioni tra cui quella più banale è di acquisire tre stampanti, una per ogni PC. Questa soluzione non è facilmente scalabile, ovvero per ogni nuovo PC si rende indispensabile l'acquisizione di una nuova stampante. Non è nemmeno particolarmente conveniente perché con cifre equivalenti è possibile installare una piccola rete locale e condividere l'uso di una sola stampante da tutte le postazioni. La macchina a cui è collegata la stampante (nella figura, A) fungerà quindi da ***print server*** per le altre e dovrà essere sempre accesa quando gli utenti che accedono da B o da C vogliono stampare.

Questa piccola rete locale consente tra l'altro anche l'uso comune di spazio disco, che ha fondamentalmente due scopi: mettere la risorsa fisica (il disco) a disposizione da più postazioni e creare un'area di scambio per i *file* che consente agli utenti di lavorare a più mani sui documenti. Ovviamente il *computer* che funge da *file server* (C, nella figura) dovrà essere acceso perché dalle altre postazioni (A e B) si possa accedere ai *file* contenuti nel disco condiviso.

Connettività Internet

Anche **l'accesso a Internet** può essere condiviso se si dispone di una **rete locale** . Si consideri per esempio un insieme di PC dai quali si vuole rendere possibile navigare. Se l'insieme è molto piccolo (2 o 3) si può dotare ciascun PC di un modem e collegarlo a una linea commutata per consentire l'accesso a Internet attraverso un *provider*. Questa soluzione non è minimamente scalabile e i costi di attivazione delle linee telefoniche suggeriscono di utilizzare una rete locale. In questo caso si può battezzare una delle postazioni (nella figura, A) come quella che verrà

collegata a Internet direttamente. Questa postazione fungerà da ICS (*Internet Connection Server*) ovvero offrirà accesso a Internet anche alle altre postazioni della rete locale. Ovviamente il *computer* A dovrà essere acceso quando si vuole accedere a Internet dal *computer* B.

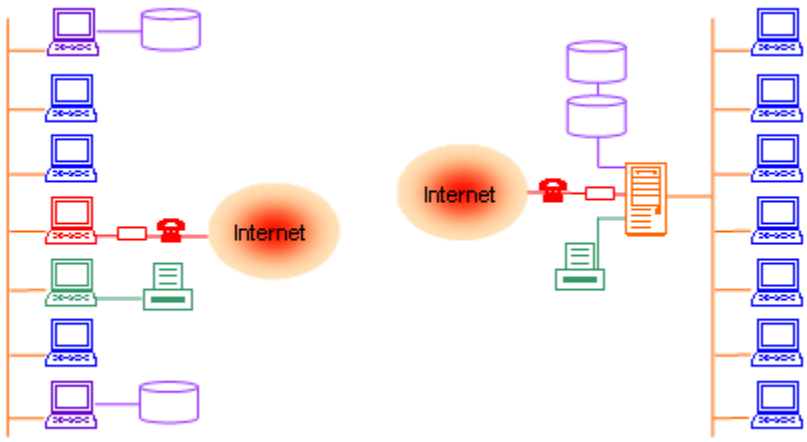


La soluzione supporta efficacemente solo un numero molto limitato di collegamenti a Internet contemporanei. Nel caso di insiemi più numerosi di postazioni, come per esempio avviene nei laboratori, è consigliabile dotarsi di una linea di accesso a Internet a **banda larga** (**ADSL**) che non utilizza nessuna postazione come *Internet Connection Server*, ma è fornita con un opportuno apparato di instradamento che si collega direttamente alla rete locale.

La centralizzazione dei servizi

Ogni servizio offerto richiede l'installazione di appositi *software server*, i quali offrono servizi di condivisione delle risorse. Questi *software* appesantiscono il PC su cui sono installati poiché utilizzano risorse di calcolo e memoria (sia centrale che di massa) che sarebbero altrimenti completamente a disposizione delle applicazioni a uso personale.

Quando il numero di servizi offerti attraverso la rete e il numero di postazioni che ne usufruiscono aumenta, diventa necessario dedicare una macchina a fornire centralmente i servizi ovvero a fungere da *server* per gli altri PC. La macchina *server* resta sempre accesa e di solito non è utilizzata come normale postazione di lavoro, ma opera esclusivamente per fornire i servizi. Sistemi più complessi possono basarsi su più macchine *server*, che offrono sottoinsiemi diversi di servizi, fino a istallare un solo servizio su una o più macchine *server*.



La gestione centralizzata

In un sistema dotato di macchina dedicata ai servizi (macchina *server*) si può sostituire la condivisione di *file*, tipica delle architetture di pari come quelle viste in precedenza, con un vero e proprio ***file server*** che consente una gestione centralizzata delle risorse su disco. Questa scelta è particolarmente adatta a un laboratorio didattico poiché contribuisce a rendere gli archivi raggiungibili con modalità identiche da tutte le postazioni ovvero va nella direzione di rendere indifferente l'uso di una certa postazione rispetto a un'altra.

Un laboratorio didattico basato su una architettura di questo tipo offre anche la possibilità di centralizzare l'amministrazione del sistema. È dunque possibile che la macchina *server* offra anche funzionalità di ***domain controller*** , ovvero si occupi di autenticare gli utenti e di definire a quali risorse hanno diritto di accedere. Questo tipo di centralizzazione semplifica notevolmente il lavoro dell'amministratore del sistema poiché consente di definire una volta per tutte (sul *domain controller*) quali sono gli utenti e quali le rispettive politiche di accesso, senza costringere ad una inutile replicazione degli utenti postazione per postazione e senza spingere a semplificazioni delle politiche di gestione (come l'uso di utenti o *password* condivisi) che creano gravi problemi alla sicurezza del sistema.

Infine, installando anche un ***server Web*** , si può utilizzare la macchina *server* per realizzare alcuni servizi tipici di una Intranet, offrendo un sistema molto efficace per rendere disponibile documentazione sia di tipo amministrativo (circolari, verbali, direttive) che didattico (materiale ipertestuale, dispense, relazioni).

Valutazione del software e dell'hardware

Prof.ssa Paola Salomoni
Dott. Diego Gardini

Introduzione

Scopo di questa articolazione dell'introduzione è illustrare brevemente alcune metodiche di valutazione che possono essere applicate nella scelta delle dotazioni *hardware* e *software* della scuola. Il progetto di un nuovo laboratorio, il cablaggio della rete locale, la scelta del tipo di accesso a Internet sono processi decisionali che devono essere basati su molti fattori tra cui i bisogni espressi dagli utenti, gli obiettivi individuati e i finanziamenti disponibili. Questo tipo di competenze, assieme a una competenza tecnologica generale che consente di scegliere tra una proposta e l'altra e di valutare un progetto, devono essere trovate all'interno della scuola. Possono invece essere acquisite all'esterno le competenze approfondite su specifiche attrezzature, che difficilmente sono riassumibili in una sola persona. Questo tipo di *know-how* è tipico di specialisti di uno specifico settore ma soprattutto è alla base delle attività commerciali in ambito informatico. Chi vende attrezzature ha ovvio interesse a mantenersi aggiornato e a conoscere soluzioni innovative e tecnologie all'avanguardia. Chi acquista può quindi limitare la sua azione al compito, comunque non semplice, di valutare le proposte e giudicarne il grado di corrispondenza con i bisogni e gli obiettivi della scuola.

I contenuti di questa sezione sono volutamente avulsi da riferimenti a specifiche tecnologie, che rischierebbero di rendere immediatamente obsoleta una trattazione che vuole essere introduttiva e generale.

Principi di ergonomia

Con **ergonomia** si intende una disciplina che mira a migliorare sicurezza, salute, *comfort* e benessere dell'utente che utilizza prodotti e servizi. In questo contesto trattiamo brevemente dell'ergonomia di un particolare tipo di prodotto: il *personal computer*, indicato comunemente in questo settore come video terminale. Una attività continuativa al video terminale può dare luogo a disturbi di diversa natura, dovuti al sovraffaticamento visivo, alla postura e alla concentrazione. Adeguando opportunamente le postazioni è possibile ridurre gli effetti di affaticamento e di conseguenza i rischi per la salute.

La legge 626 sulla sicurezza degli ambienti di lavoro tutela anche il lavoro al video terminale e va applicata nella scuola ai lavoratori che lavorano utilizzando il *computer* in maniera continuativa. Non necessariamente va invece applicata in toto nei laboratori didattici perché si presume che gli studenti e i docenti li frequentino per un limitato numero di ore alla settimana e per periodi consecutivi molto brevi (2/3 ore). Tuttavia è buona regola, quando si acquisiscono nuove attrezzature, sia per l'amministrazione che per la didattica, verificare il rispetto delle norme sul lavoro al videoterminale, in modo da garantire al massimo il diritto alla salute degli utenti.

L'ergonomia delle postazioni al *computer* non è vincolata esclusivamente al PC e alle sue periferiche, ma è influenzata fortemente da fattori esterni alla macchina, come la luce ambientale, che può essere più o meno affaticante per la vista, o l'altezza di tavoli e sedie che influisce sulla postura. Per questo motivo la progettazione di postazioni ergonomiche non può prescindere dall'analisi degli ambienti in cui le attrezzature verranno poste e da un progetto di tipo logistico molto attento.

L'hardware e il software

L'infrastruttura tecnologica della scuola è fatta in parte dai PC e dalla rete e in parte da altri strumenti di tipo didattico e non, che completano la dotazione *hardware*. Tra questi vanno annoverati apparati di tipo estremamente comune, come le stampanti e gli *scanner*, che offrono funzionalità utili sia all'amministrazione che alla didattica. Altre infrastrutture sono invece pensate esclusivamente per scopi didattici, come i videoproiettori o le lavagne luminose digitali. Dunque in realtà un laboratorio didattico multimediale e una segreteria scolastica utilizzeranno un insieme di strumenti *hardware* in parte molto simili.

Quello che differenzia invece completamente le due situazioni è il *software*, o meglio le applicazioni che sono a disposizione in laboratorio piuttosto che in segreteria. Ogni applicazione fornisce all'utente una funzione o un'insieme di funzioni che riguardano la realizzazione di un certo compito, per cui compiti completamente diversi sono realizzati da applicazioni differenti. Un insieme di *software* che raggiungono obiettivi diffusi (navigare o scrivere testi) saranno comuni alla segreteria e al laboratorio.

La scelta d'uso di un certo *software* può influenzare la scelta del tipo di PC (ovvero dell'*hardware*) che è destinato a supportarlo. Si pensi per esempio ai requisiti di disco di un *server* o al tipo di scheda video che deve essere usata per applicazioni grafiche 3D.

Attraverso la **bibliografia *on line*** è possibile affrontare casi specifici e trattazioni generali degli argomenti esposti.

Computer

La gamma di PC disponibili sul mercato è estremamente vasta e variegata ed esistono numerose soluzioni che possono rispondere adeguatamente a un certo bisogno. Le differenze principali sono concentrate in caratteristiche delle diverse piattaforme che ne individuano le specificità e rendono un certo PC adatto più di altri a rispondere a un certo scopo. Individuiamo qui brevemente alcune caratteristiche delle tipologie più diffuse:

- ***Server***. Una macchina che offre servizi deve avere caratteristiche di affidabilità, robustezza e tolleranza ai guasti molto maggiori rispetto a un normale PC a uso personale. Deve rimanere sempre accesa e questo incide sul tipo e sul numero delle alimentazioni disponibili. L'affidabilità dei dischi viene spesso elevata utilizzando tecnologie **RAID** e, rispetto alle caratteristiche della rete locale, deve possedere una interfaccia di rete più veloce possibile. Non sono invece essenziali periferiche multimediali, come per esempio la scheda audio. I *server* non dovrebbero essere utilizzati come postazioni di lavoro e quindi non necessitano di monitor e schede video particolarmente avanzate.
- **Postazione di lavoro**. Le postazioni di lavoro del laboratorio e dell'amministrazione possono essere realizzate partendo da piattaforme simili ma avranno caratteristiche differenti, dovute sia al *software* che supporteranno sia al tipo di utilizzo. Generalmente, le macchine del laboratorio possono essere scelte senza particolari requisiti di robustezza e viene tipicamente preferita l'acquisizione di qualche postazione supplementare alla scelta di acquisire macchine di fascia alta. Periodiche reinstallazioni sono comunque da prevedere a causa dell'uso, non particolarmente controllato, di molti *software* da parte di molte persone. Viceversa, le postazioni dell'amministrazione ospitano tipicamente una sola persona, il cui operato è critico per il funzionamento della scuola. Per questo motivo può essere rilevante acquisire attrezzature per cui viene assicurata la tolleranza ai guasti, che quasi tutte le marche rendono disponibili come serie professionale della produzione.
- **Portatile**. La scelta di un PC portatile risponde a ovvi criteri di mobilità che possono essere supportati adeguatamente da una infrastruttura di rete idonea (cablaggio tradizionale con molti punti di accesso diffusi o **rete *wireless***). Esistono diverse tipologie di portatile che mirano a coniugare con differenti prospettive due esigenze di base: la **leggerezza** del PC, che garantisce portabilità ed effettiva mobilità, e la **dotazione**, in termini di caratteristiche computazionali e accessori. Questi due aspetti sono in competizione tra loro: un portatile con *display* più grande e periferiche di I/O integrate (*floppy* e lettore/masterizzatore di CD) è sicuramente più voluminoso e pesante di un portatile con *display* più ridotto e con *device* di I/O esterni. Un

ruolo rilevante ha anche l'autonomia dell'alimentazione, che influisce sul numero e sul volume delle batterie (e quindi sul peso del PC).

In fase di acquisizione è opportuno prevedere la possibilità di stipulare contratti di manutenzione che estendano la garanzia ad almeno tre anni e che offrano un servizio con risoluzione dei guasti sul posto (*on site*). Questo tipo di prestazioni hanno costi generalmente più bassi, se concordati all'acquisto, ed azzerano le spese di manutenzione e di spedizione che, in caso di guasto, possono essere molto elevate.

Multimedia

Sono ormai innumerevoli le applicazioni, di rete e *stand alone*, che sfruttano la multimedialità per offrire servizi innovativi, si pensi ai sistemi di distribuzione di musica su Internet o alla *Web* TV. All'interno delle scuole le attività che hanno evidenziato maggiore applicabilità in contesti didattici sono la fruizione e la produzione di ipermedia.

Fondamentali in un laboratorio per l'editoria multimediale, sia via *Web* che non, sono i *software* di *editing* di immagini e di postproduzione audio e video. Sono disponibili sia soluzioni professionali, piuttosto costose, che soluzioni *freeware* e *shareware* che possono essere utilizzate in modo efficace in ambito didattico. Altre applicazioni interessanti, ma decisamente meno importanti delle precedenti, sono quelle che consentono di produrre animazioni (anche per il *Web*) o mondi virtuali interattivi.

La situazione è più variegata nel settore *hardware* perché alle tradizionali dotazioni del singolo PC (lettore/masterizzatore CD/DVD, casse o cuffie, microfoni, *webcam*) vanno aggiunti apparati di acquisizione e/o riproduzione condivisi, che servono tutto il laboratorio. Alcune attrezzature sono molto diffuse (come *scanner* e stampanti a colori) altre sono invece un po' meno usuali ma non meno importanti, come videocamere e fotocamere digitali, o schede di digitalizzazione con ingressi compositi e S-VHS. La gamma di prodotti *hardware* ovviamente spazia dalle tecnologie acquisibili a costi contenuti ad apparti professionali, che hanno prezzi molto elevati. La scelta degli apparati influenza ovviamente la scelta dei PC sui quali utilizzarli, che devono essere dotati di interfacce per scaricare i media e di capacità di calcolo sufficienti all'elaborazione di immagini, audio e video digitali.

computer connessi in rete e dotati di apparati di acquisizione audio/video (microfono e *webcam*) possono essere usati in applicazioni di video conferenza. Laboratori multimediali di tipo funzionalmente differente, basati in parte su *hardware* e *software* ad hoc, possono essere utili all'apprendimento delle lingue.

Sistemi operativi e servizi

Per i sistemi operativi, come per tutto il *software* in genere esistono numerose politiche di produzione e distribuzione che determinano il tipo di **licenza d'uso** . La scelta del sistema operativo per le postazioni *client* è fortemente influenzata dalle applicazioni che devono utilizzare gli utenti, per cui se una certa applicazione indispensabile gira solo su un particolare sistema operativo, verrà utilizzato quel particolare sistema operativo. Chi sviluppa le applicazioni, d'altro canto, è portato a produrle per le piattaforme più diffuse e questo circolo vizioso alimenta molte forme di consumismo tecnologico che rendono attrezzature nuove (poco usate) già obsolete.

Per i *server* questo tipo di meccanica è vera in parte. Dovendo installare una nuova infrastruttura (senza avere quindi vincoli sulle applicazioni prodotte da situazioni precedenti) è possibile scegliere tra diversi tipi di piattaforma, che offrono un insieme di servizi di base simili e sono dunque in competizione forte tra loro. In particolare, il *software* ***open source*** ha destato recentemente molto interesse in ambito scolastico perché offre, a costi molto bassi (prevalentemente dovuti all'assistenza), servizi comparabili con quelli offerti da sistemi operativi commerciali.

Aspetti legali e privacy

Prof. Avv. Giusella Finocchiaro
Prof.ssa Paola Salomoni

Introduzione

Quest'ultima sezione dell'introduzione è destinata a presentare in modo succinto i principali aspetti normativi correlati alla gestione delle infrastrutture all'interno di un istituto scolastico, in particolare la tutela della ***privacy*** e la **licenza d'uso dei *software*** (a cura di Giusella Finocchiaro).

A questi sono aggiunti alcune tematiche più tecniche che offrono spunto per la messa in opera di strumenti di salvaguardia di alcuni diritti e, in particolare, la **crittografia** , come meccanismo di protezione della riservatezza dei messaggi e i **criteri di accessibilità dei siti *Web* per i disabili** (a cura di Paola Salomoni).

Per alcune delle tematiche trattate in questa sezione, sono disponibili approfondimenti:

- sulla **crittografia** ;
- sulla ***privacy*** ;
- sulle **licenze d'uso del *software*** ;

In questa breve trattazione introdurremo alcuni degli aspetti tecnici, trattando le principali tecniche e procedure per la prevenzione dei problemi e la loro soluzione. È disponibile un approfondimento sulla **sicurezza come forma di prevenzione** , che tratta in modo più specifico le problematiche relative alla sicurezza delle informazioni.

I diritti di utilizzazione economica del software

Secondo il decreto legislativo 518/92 **http://www.giustizia.it/cassazione/leggi/l633_41.html#ART64BIS**, l'autore o il titolare dei diritti di utilizzazione economica dell'opera ha il diritto esclusivo di effettuare:

- la riproduzione del *software* permanente o temporanea, totale o parziale;
- la traduzione, l'adattamento, la trasformazione e ogni altra modificazione del programma;
- qualsiasi forma di distribuzione al pubblico.

Il legittimo acquirente, invece, può:

- riprodurre il programma e tradurre, adattare o trasformare il programma solo se tali attività sono necessarie per l'uso del programma conformemente alla sua destinazione, inclusa la correzione degli errori;
- effettuare una copia di riserva del programma, qualora tale copia sia necessaria per l'uso;
- osservare, studiare o sottoporre a prova di funzionamento il programma.

http://www.giustizia.it/cassazione/leggi/l633_41.html#ART64TER

Il contratto di licenza

Il decreto legislativo detta soltanto le norme generali.

Ampio margine è lasciato alla contrattazione fra l'utilizzatore del *software* e il soggetto che detiene i diritti di utilizzazione economica del *software* (l'autore del programma o l'impresa produttrice di *software* alla quale l'autore ha ceduto i propri diritti).
Il contratto che in dettaglio regolamenta i diritti e i doveri dell'acquirente e dell'utilizzatore di *software* è il contratto di licenza d'uso. Questo contratto è un contratto atipico, cioè non regolamentato dal codice civile, e la definizione del contenuto contrattuale è lasciata all'autonomia delle parti contraenti, le quali possono definire i reciproci diritti e doveri a loro discrezione.

Infatti, il mercato offre una grande varietà di contratti, di tipi di licenze, di prezzi, di obblighi e anche di programmi. Pertanto, non si può dare una definizione unitaria dei programmi per elaboratori esistenti né si possono definire tutti i tipi di programmi esistenti, ma si può soltanto fornire una descrizione delle tipologie più diffuse.
Ad esempio, per stabilire se una duplicazione è abusiva o meno occorre far riferimento al contratto.
Solitamente i contratti di licenza d'uso (cioè i contratti per comprare il programma) limitano l'utilizzo del *software* ad una sola macchina per volta e talvolta la macchina è espressamente individuata nella documentazione contrattuale. Alcuni contratti di licenza d'uso, tuttavia, consentono la riproduzione del programma su un certo numero di macchine.
In genere, i contratti standard di licenza d'uso non consentono l'utilizzazione di un programma da più macchine fra loro collegate in rete. Tuttavia, è possibile stipulare contratti di licenza d'uso che consentano di utilizzare il programma su più macchine o in rete (licenze multiple; a *forfait*; *floating license*, cioè licenze per utilizzare i programmi in rete ma da un numero di utenti prefissato) o inserire in contratto clausole ad hoc.

Tipologie particolari di licenza

4.1. *Open software*

Il titolare dei diritti di utilizzazione economica del *software* può rinunciare ad essi e mettere a disposizioni del pubblico il programma, compreso il codice sorgente, senza richiedere un compenso. La rinuncia ad un diritto è una particolare modalità di esercizio di quel diritto. Sulla base di questo principio si è diffuso il cosiddetto *open software*, che consiste di programmi che sono disponibili sia all'utilizzo che alla modifica da parte di soggetti diversi dall'autore .

Il contratto di licenza d'uso per *open software* più diffuso è costituito dal contratto GNU
http://www.gnu.org/licenses/licenses.html

4.2. Licenza a strappo

Un particolare contratto di licenza d'uso è costituito dal cosiddetto contratto a strappo o contratto di licenza a strappo, *shrink-wrap license*, nell'originaria formulazione statunitense.
In questo caso, il programma è confezionato in un involucro, sul quale sono stampate o attraverso il quale è possibile leggere le condizioni contrattuali. L'apertura dell'involucro costituisce accettazione delle condizioni contrattuali predisposte dal produttore. Le condizioni d'uso del programma sono quelle dei contratti di licenza d'uso più diffusi (uso del programma limitato ad una sola macchina, restrizioni alla possibilità di effettuare copie, garanzia limitata ai soli difetti del supporto materiale, esclusione di altre garanzie e responsabilità). L'acquirente che non intenda accettare il regolamento contrattuale può restituire il prodotto e richiedere la restituzione del prezzo pagato, purché non abbia aperto la confezione. In genere, viene richiesto all'acquirente di compilare e spedire al produttore una cartolina che gli consente di ricevere gli aggiornamenti del *software* e di usufruire delle limitate prestazioni di garanzia accordate dal contratto. La spedizione della cartolina costituisce espressa accettazione del regolamento contrattuale.
Il contratto di licenza a strappo si perfeziona, dunque, con l'atto dell'apertura della confezione. Tale atto vale come accettazione.
L'articolo 1341 c.c. stabilisce che le condizioni generali di contratto predisposte da una parte sono valide nei confronti dell'altra se conoscibili da questa al momento della conclusione del contratto. Dunque, se il regolamento contrattuale è leggibile al momento della conclusione del contratto le condizioni generali di contratto sono da ritenersi valide. L'effettiva conoscenza di esso non ha alcuna rilevanza per il nostro ordinamento, così come non ha alcuna rilevanza l'effettiva conoscenza delle clausole contrattuali al momento della conclusione di un contratto di trasporto, di banca o di assicurazione, eccetera.
Il regolamento contrattuale è da ritenersi accettato al momento della conclusione del contratto, sempre che esso fosse conoscibile. Perché si possa considerare conoscibile, è necessario che le condizioni generali di contratto siano inserite nella confezione in modo da essere visibili e leggibili dall'esterno, al momento della conclusione del contratto, come prescrive l'articolo 1341 c.c.
Non hanno invece alcun effetto le clausole vessatorie presenti nel contratto, che devono essere specificamente approvate per iscritto ai sensi dell'articolo 1341, secondo comma.
Quindi quelle clausole, spesso presenti nei contratti standard di licenza d'uso, che stabiliscono limitazioni di responsabilità, restrizioni alla libertà contrattuale nei rapporti con i terzi e deroghe alla competenza dell'autorità giudiziaria devono considerarsi inefficaci.

4.3. *Software freeware* e *shareware*

Il *software freeware* è *software* distribuito gratuitamente, generalmente in rete, e può essere copiato da chiunque si colleghi con la rete. In genere, reca la scritta *freeware* e il nome dell'autore. Talvolta viene specificato che il programma può essere liberamente copiato, altre volte si invita l'utente ad inviare osservazioni e commenti all'indirizzo specificato.
In questo caso, è evidente la rinuncia da parte dell'autore ai propri diritti di utilizzazione economica dell'opera, quindi il *software freeware* può essere liberamente copiato.
Il *software shareware* presenta molte delle caratteristiche del *software freeware*: è *software* distribuito in rete e può essere copiato da chiunque si colleghi con la rete. In genere, reca la scritta *shareware* e il nome dell'autore.
A differenza che nel *software freeware*, nel *software shareware* si invita l'utente ad inviare un corrispettivo, in genere piuttosto basso, all'indirizzo specificato. Talvolta si precisa che il pagamento del corrispettivo dà diritto agli aggiornamenti del programma.
In questo caso, non si può ritenere che l'autore abbia rinunciato ai propri diritti di utilizzazione economica dell'opera: si tratta di un contratto di licenza d'uso di *software* in cui la distribuzione è effettuata mediante rete e in forme particolari. Pertanto, deve essere corrisposto all'autore il compenso richiesto. Occorre comunque precisare, che per una serie di considerazioni di carattere pratico (in genere si tratta di programmi di modesta rilevanza economica; in genere si tratta di programmi distribuiti dallo stesso autore e non da un'impresa produttrice e in genere l'autore è straniero) non è molto probabile un'azione legale da parte dell'autore.

La cosiddetta legge sulla privacy

La più importante legge italiana in materia di *privacy* è la legge 31 dicembre 1996, numero 675, Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali [**http://www.garanteprivacy.it/garante/prewiew/0,1724,2039,00.html?sezione=115&LANG=1**]1 , più nota come legge sulla *privacy*, la quale attua la direttiva comunitaria 95/46/CE del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati [**http://www.garanteprivacy.it/garante/prewiew/0,1724,380,00.html?sezione=115&LANG=1**]2. È bene chiarire subito che la l. 675/96 - come meglio si vedrà esaminando le definizioni di dato personale e di trattamento già richiamate nel titolo - non disciplina soltanto la *privacy*, cioè i dati riservati, ma piuttosto il trattamento dei dati personali, cioè la circolazione delle informazioni, siano esse riservate o meno.
La legge 675/96 costituisce l'adempimento di altri obblighi internazionali da parte dell'Italia, fra i quali quelli derivanti dall'Accordo di *Schengen* e quelli derivanti dalla Convenzione del Consiglio d'Europa sulla Protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981.

1 Pubblicata nel Supplemento Ordinario alla Gazzetta Ufficiale numero 5 dell'8 gennaio 1997.
2 Pubblicata in G.U.C.E. n. L 281/31 del 23 novembre 1995.

Le disposizioni successive

La legge 675/96 è stata integrata e modificata da molte altre disposizioni normative, cosicché è in corso di predisposizione un Testo unico sulla *privacy*.
Fra le più importanti disposizioni normative che hanno integrato la legge 675/96, si ricordano: il decreto legislativo 9 maggio 1997, numero 123 che ha introdotto la possibilità del consenso in forma orale; il decreto legislativo 28 luglio 1997, numero 255 concernente l'esonero e le semplificazioni delle notificazioni; il decreto legislativo 11 maggio 1999, numero 135, sulle disposizioni in materia di trattamento di dati particolari da parte di soggetti pubblici; il decreto legislativo 30 luglio 1999, numero 281 sul trattamento dei dati per finalità storiche, statistiche e di ricerca scientifica; il decreto legislativo 30 luglio 1999, numero 282, sul trattamento dei dati per garantire la riservatezza in ambito sanitario; il d.p.r. 31 marzo 1998, numero 501, sul funzionamento dell'ufficio del Garante che reca anche norme che disciplinano l'accesso ai dati personali; il decreto legislativo 13 maggio 1998, numero 171, recante disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni; il d.p.r. 28 luglio 1999, numero 318, sull'individuazione delle misure minime di sicurezza; il decreto legislativo 28 dicembre 2001, numero 467, disposizioni correttive ed integrative della normativa in materia di protezione dei dati personali. A ciò si aggiungano le autorizzazioni generali in materia di trattamento dei dati sensibili.

Tutte le norme citate, nonché il testo consolidato della legge 675/96 possono essere reperiti nel sito ufficiale del Garante per il trattamento dei dati personali: **http://www.garanteprivacy.it**.

Sulla *privacy* è disponibile un **approfondimento** .

Intercettazione dei messaggi

I messaggi che passano sulla rete sono in realtà facilmente intercettabili. Esempi di attacchi che mirano all'intercettazione dei messaggi sono lo ***sniffing*** e lo ***spoofing*** dell'indirizzo IP. Oltre a ciò, l'amministratore di una macchina possiede le credenziali per intercettare tutti i dati che passano attraverso quel nodo e quindi un amministratore in malafede può intercettare facilmente messaggi destinati ad altri utenti.

L'intera **sicurezza** del sistema è fortemente compromessa dalla trasmissione di messaggi in chiaro. Un messaggio in chiaro intercettato può infatti essere letto, violando così la **confidenzialità** . Nel caso si tratti di una ***password*** o di una qualunque altra credenziale di identificazione, chi ha intercettato il messaggio avrà modo di sostituirsi al mittente, **abusando della sua identità elettronica** e infrangendo così anche l' **autenticazione** e il **non ripudio** . Con questa credenziale, carpita maliziosamente, sarà poi possibile sostituirsi all'utente nella gestione delle sue risorse, esponendo a rischio infine anche l' **integrità** e la **disponibilità** dei dati.

In realtà questo tipo di problema è percepito come critico soprattutto nel settore commerciale. In questo contesto è più che mai importante che i messaggi:

- non subiscano alterazioni (integrità): il contenuto dell'accordo non deve essere cambiato.
- Abbiano un mittente univocamente identificabile (autenticazione e non ripudio): la sottoscrizione di un messaggio è irreversibile e univoca, come una firma.
- Non vengano letti senza autorizzazione (confidenzialità): deve essere possibile inviare un numero di carta di credito o altre informazioni riservate con la garanzia che solo il destinatario le potrà leggere.

Crittografia

Il problema di inviare messaggi riservati attraverso sistemi di distribuzione non affidabili è sentito da secoli in ambito militare e sono innumerevoli le metodologie più o meno complesse messe in atto per spedire informazioni agli alleati, senza che i nemici possano decifrarle.

La **crittografia** è un procedimento di codifica e decodifica dei messaggi basata su funzioni parametriche, la cui computazione dipende da un parametro detto chiave. Un messaggio crittografato non è direttamente leggibile se non si possiede una funzione e una chiave per decriptarlo.

Il modello su cui è basato un sistema crittografico è il seguente:

- Un mittente A vuole inviare un messaggio M a un destinatario B.
- A cripta il messaggio, ovvero applica al messaggio un metodo di cifratura F con chiave di cifratura K.
- Il messaggio così modificato viene poi spedito via rete a B.
- B riceve un messaggio apparentemente illeggibile ma possiede un metodo di decifratura F' e una chiave K' che consentono di riportare il messaggio in chiaro.

Se un intruso dovesse intercettare il messaggio cifrato non sarebbe in grado di leggerlo a meno di possedere F' e K'.

Le chiavi di cifratura e decifratura possono coincidere e in questo caso si parla di **crittografia a chiave simmetrica** (o a **chiave privata**), oppure possono essere diverse e in questo caso si parla di **crittografia a chiave pubblica** .

Chiave pubblica e chiave privata

I metodi utilizzati tradizionalmente per la crittografia classica erano tutti metodi a chiave simmetrica, basati sull'ipotesi che gli alleati condividessero una chiave nota solo a loro (e per questo detta segreta o anche privata). Quando A vuole spedire a B un messaggio cifrato con un metodo a chiave segreta deve, prima di tutto, fare in modo che B conosca la sua stessa chiave di crittografia, K e, poi, criptare il messaggio con F e K. Quando B riceve il messaggio utilizza F' e K per decriptarlo.

La **crittografia a chiave pubblica** è un metodo asimmetrico basato sull'esistenza di due diverse chiavi, una utilizzata per criptare e una utilizzata per decriptare. Ciascun utente deve quindi possedere due chiavi, una privata che conosce solo lui e una pubblica che rende nota a tutti. Ovviamente esiste una relazione matematica tra **chiave pubblica** e **chiave privata** che deve rendere semplice calcolare la chiave pubblica a partire da quella privata e difficilissimo (o meglio computazionalmente impossibile) calcolare la chiave privata a partire da quella pubblica. La sicurezza di un algoritmo asimmetrico risiede proprio nella difficoltà di individuare la chiave privata, quando si è in possesso di quella pubblica.

Se A vuole inviare un messaggio riservato a B deve dunque procurarsi la chiave pubblica di B (che è disponibile a tutti) e utilizzarla per criptare il messaggio. B sarà l'unico a riuscire a decriptare il messaggio poiché è l'unico in possesso della chiave privata.

I meccanismi di crittografia sono alla base delle diverse forme di certificazione a disposizione su Internet e del funzionamento della firma digitale. Sulla crittografia è disponibile un **approfondimento** .

Criteri di accessibilità dei siti Web

Particolare attenzione è stata rivolta recentemente all'accessibilità dei disabili ai siti *Web* della Pubblica Amministrazione. L'AIPA, attraverso il Gruppo di Lavoro sull'Accessibilità e Tecnologie Informatiche nella Pubblica Amministrazione, ha prodotto una prima bozza di normativa, che va nella direzione di adottare integralmente le raccomandazioni emesse in materia dal *World Wide Web Consortium* (W3C).
In generale i siti progettati attualmente utilizzano stili di presentazione altamente interattivi e a forte contenuto multimediale. Questi siti sono cioè progettati per utenti che non hanno limiti fisici, e dunque sono in grado di interagire attraverso dispositivi che richiedono movimenti manuali fini, né hanno limiti sensoriali, e dunque privilegiano presentazioni di tipo multimediale.

Per valutare il livello di accessibilità di un sito già realizzato possono essere utilizzati appositi strumenti *software* che consentono di verificare automaticamente il rispetto delle condizioni basilari dell'accessibilità. Questa attività permette di correggere errori nella progettazione e nello stile di presentazione e riguadagnare a posteriori la piena accessibilità del sito.

I **riferimenti bibliografici** *on line* consentono di ottenere maggiori informazioni sull'accessibilità dei siti *Web* e in particolare sulle linee guida per la Pubblica Amministrazione.

Approfondimenti

Virus e antivirus

Prof.ssa Paola Salomoni
Dott. Diego Gardini
1.3.1. (Descrivere le tecniche e le procedure appropriate per la prevenzione dei problemi e la loro soluzione)

Introduzione

Il termine **virus** in informatica indica una porzione di codice che ha la caratteristica di autoreplicarsi e inserire se stesso in *file* eseguibili preesistenti sul sistema.

Virus è in realtà una parola latina che significa veleno e che viene utilizzata comunemente in medicina per indicare microrganismi patogeni dell'uomo, degli animali, delle piante e dei batteri. Il virus biologico è un organismo parassita, privo di meccanismi enzimatici propri, che si sviluppa nelle cellule di altri organismi, utilizzando i meccanismi enzimatici di queste ultime. Una volta sviluppatosi nella cellula ospite, il virus si diffonde contagiando altri organismi.

Per analogia il nome virus è stato utilizzato per indicare un tipo di attacco alla sicurezza dei sistemi informatici, basato su un *software* che ha le seguenti caratteristiche:

- non esegue autonomamente ma necessita di un programma eseguibile ospite, che viene infettato, la cui esecuzione attiva il virus;
- si riproduce e si propaga infettando altri sistemi;
- si attiva ed esegue le attività per cui è stato implementato; raramente è innocuo, più spesso produce danni alla **sicurezza** ed in particolare all'integrità dei dati e alla disponibilità dei sistemi;
- è di piccole dimensioni rispetto al sistema che aggredisce.

Ciclo di vita

Il ciclo di vita di un **virus** è caratterizzato da tre attività fondamentali:

- **creazione** del virus: è il momento in cui il virus viene creato dal programmatore e immesso nei primi sistemi;
- **epidemia**: è il momento in cui il virus passa da un *computer* all'altro allargando il suo raggio d'azione;
- **disattivazione**: è il momento in cui il virus viene eliminato, ovvero viene rimosso da tutti i *computer*.

La fase in cui il virus si propaga è a sua volta scandita da diversi momenti:

- **infezione**: quando il virus individua un potenziale sistema ospite, verifica che questo non sia già infettato da una copia di sé e, nel caso sia libero, lo infetta. Il virus resta poi latente per un certo periodo in cui l'unica attività che effettua è tentare di replicare l'infezione, passando da un ospite all'altro;
- **attivazione**: al verificarsi di un certo evento, detto ***trigger***, il virus scatena l'azione vera e propria per la quale è stato progettato, che viene chiamata ***payload*** e in genere è distruttiva e mira alla cancellazione dei dati e all'indisponibilità del sistema in generale.

Anche la fase di disattivazione è articolata:

- **riconoscimento**: il virus viene identificato e viene riconosciuta la stringa identificativa che lo contraddistingue;
- **estirpazione**: utilizzando un antivirus, il virus viene rimosso completamente dal sistema.

Tipologie

I virus fanno parte di una famiglia di attacchi alla sicurezza nota come ***malicious software*** (*malware*) che comprende altri tipi di programmi caratterizzati dal fatto che si diffondono da un *computer* all'altro con lo scopo di produrre danni ai sistemi.

In realtà i virus più recenti mescolano le caratteristiche di diversi tipi di *malware* con lo scopo di diventare più difficili da individuare e più efficaci nel diffondere l'infezione e in particolare spesso sono **virus** e ***worm*** ovvero *software* che hanno i medesimi meccanismi riproduttivi dei virus ma che utilizzano (come i *worm*) la rete per propagarsi. Questa caratteristica accomuna la maggior parte dei virus recenti poiché lo scambio di *file* (che è il meccanismo base per il propagarsi dell'infezione) avviene ormai prevalentemente attraverso la rete.

I virus possono essere classificati in base a diverse caratteristiche, tra cui la più significativa è l'ambiente attraverso cui si propaga l'infezione e si sviluppa il virus. Sono distinguibili in questa ottica diverse tipologie di virus:

- i ***boot* virus** , che infettano il *Boot Sector* o il *Master Boot Record* dei dischi in modo da essere caricati all'avvio del sistema;
- i ***file* virus** , che infettano, con modalità molto varie, i *file* eseguibili e utilizzano lo scambio di questi ultimi per propagare l'infezione;
- i **macrovirus** , che sono scritti in VBA (*Visual Basic for Application*) un linguaggio per la scrittura di macro negli ambienti applicativi *Office*;
- i ***network* virus**, che si diffondono sfruttando le **vulnerabilità** dei protocolli di Internet.

Boot virus

I ***boot* virus** si propagano inserendo una copia di se stessi nel ***Boot Sector*** dei dischetti o nel ***Master Boot Record*** del disco fisso. Una volta riavviato il *computer*, la componente del sistema operativo che si occupa del caricamento, il *bootstrap loader*, porta in memoria il *boot* virus e lo mette in esecuzione.

I *boot* virus sono tipicamente più complessi da realizzare dei *file* virus, perché devono entrare in azione prima che sia caricato il sistema operativo. Devono essere anche implementati utilizzando pochissima memoria in modo da consentire loro di salvarsi nel *Boot Sector* di un dischetto, che è di soli 512 *byte*. *Boot* virus più lunghi si spezzano in una prima parte che invade il *Boot Sector* (o il *Master Boot Record*) e che carica la seconda parte, e in una seconda parte che viene memorizzata in aree poco utilizzate del supporto di memoria di massa (per esempio l'ultima traccia del dischetto). Una volta in memoria, per replicarsi su altri dischetti, il *boot* virus deve intercettare le attività di lettura e scrittura del sistema operativo, facendo attenzione a non insospettire l'utente rallentando troppo le attività di accesso ai *floppy*.

Esempi noti di *boot* virus sono Brain, Ping Pong e Michelangelo [**The Probert E-Text Encyclopaedia**].

File virus

Sono ***file* virus** quei **virus** che utilizzano i *file* come mezzo di diffusione e le proprietà del *file system* per propagarsi. Dovendo entrare in esecuzione, scelgono come ospite un *file* eseguibile (di qualunque tipo, dai .COM alle DLL) che rimane apparentemente inalterato, ma che in realtà diviene pericoloso.

Quando l'utente o il sistema avviano il *file* eseguibile ospite, avviano anche il virus che viene caricato in memoria e inizia l'attività di propagazione. Per non farsi individuare immediatamente il virus lascia eseguire anche il *file* ospite in modo che l'utente non percepisca l'inizio dell'infezione. I meccanismi con cui i *file* virus si agganciano al programma ospite sono innumerevoli e vanno dalla sovrascrittura del codice dell'ospite alla creazione di eseguibili ombra che mascherano l'esecuzione del virus. Un semplice metodo di contraffazione usato da alcuni *file* virus per DOS

consisteva nel scegliere un *file* .EXE e creare un *file* .COM con lo stesso nome. Il nuovo *file* conteneva le istruzioni per il caricamento del virus in memoria e, di seguito, l'esecuzione del *file* .EXE. Il sistema operativo, rispondeva ai comandi digitati dall'utente eseguendo il *file* con estensione .COM (primo tipo di *file* nella sequenza di esecuzione).

Macrovirus

I **macrovirus** sono i virus più diffusi attualmente e sono scritti per eseguire all'interno di applicazioni molto diffuse (tipicamente applicazioni di *office automation* o *client* Internet per la posta e per il *Web*). Sono dunque incorporati in *file* apparentemente innocui, come i *file* .DOC, come se fossero *routine* interne utilizzate dall'autore per calcoli specifici. Il linguaggio utilizzato per le macro viene usato per scrivere il virus.

Poiché gli stessi applicativi sono basati sull'esecuzione di macro predefinite, è relativamente facile scrivere un virus che ha alte probabilità di entrare in esecuzione e dunque di divenire attivo. Per esempio il virus può attivarsi in corrispondenza della macro che viene lanciata all'apertura di un *file*. Questo tipo di virus ha avuto recentemente ampissima diffusione ed esistono numerosi macrovirus che hanno provocato danni su larga scala.

Il problema dei macrovirus è stato in passato sottovalutato e solo dopo diverse epidemie devastanti sono state attivate alcune forme di prevenzione minime, quale la scansione dei *file* documento da parte degli antivirus e la possibilità di impedire l'esecuzione delle macro all'interno delle applicazioni.

Virus polimorfi

Gli **antivirus** basano il riconoscimento dei **virus** , necessario alla loro rimozione, su un codice identificativo univoco che è contenuto nel virus e che è detto **impronta virale** . Un virus diventa quindi particolarmente difficile da individuare se riesce a mascherare la propria impronta ovvero a renderla diversa ogni volta che si replica su un nuovo ospite.

L'impronta virale è costituita da codice eseguibile del virus per cui non può essere tutta alterata per mimetizzare il *software* nocivo. Per nasconderla si può invece **crittografarla** con una funzione che ha alcune caratteristiche casuali e poi replicare il codice del virus criptato e la funzione per decriptarlo.

Questo tipo di virus è detto **virus polimorfo** , poiché contiene un sistema (il *polymorphic engine*) che gestisce le chiavi e le funzioni di cifratura e decifratura. Un virus polimorfo è quindi costituito dal codice del virus, dal *polymorphic engine* (entrambi cifrati) e dalla funzione per decifrarli. Quando il virus polimorfo viene caricato, la funzione di decifratura decripta il virus e il *polymorphic engine*. Il virus lancia poi il *polymorphic engine* ogni volta che vuole ottenere la coppia di funzioni (cifratura, decifratura) che serve a generare una nuova copia mutata di se stesso.

Epidemie

I **virus** maggiormente invasivi e dannosi sono in realtà combinazioni di molte delle tecniche fin qui esposte, di altre tecniche che non sono state trattate per brevità e a queste si aggiungono anche metodologie proprie di altri tipi di ***malicious software*** , come i ***worm*** e i **cavalli di Troia** .

Mescolare le diverse tecniche consente al virus:

- di diffondersi meglio, utilizzando più modalità di trasmissione ovvero di trovare un numero maggiore di potenziali ospiti. In questo caso il virus aumenta la velocità di diffusione e di conseguenza la dimensione. Questo tipo di virus è indicato come **virus multipartito** .
- Di nascondersi meglio, utilizzando più tecniche di mascheramento e meccanismi innovativi. In questo caso il virus aumenta la dimensione dell'epidemia garantendosi un tempo più lungo per essere scoperto e quindi per essere rimosso.

Entrambi questi due fattori determinano quanto vasta sarà l'epidemia del virus. Per contro, per contrastare le epidemie, è cruciale il tempo che occorre alla comunità per individuare il virus e comprendere quali sono i meccanismi di rimozione. A questo scopo vengono mantenuti elenchi aggiornati dei virus e delle loro impronte. Alcuni di questi elenchi costituiscono, di fatto, un osservatorio sull'evolversi delle epidemie [***Wild List***].

La diffusione dei macrovirus

In tempi recenti le epidemie più vaste e dannose sono state prodotte da **macrovirus** , che attualmente sono i virus più diffusi e hanno surclassato le altre tipologie di **virus** .

Diversi sono i motivi che hanno reso superati i *boot* virus e i *file* virus rispetto ai macrovirus. In primo luogo va citato il fatto che i macrovirus hanno un maggior numero di potenziali vittime, poiché sfruttano applicativi diffusissimi e disponibili anche su più piattaforme. A questo fattore va aggiunto il fatto che la maggior parte dei macrovirus sfruttano i servizi Internet (la posta o il *Web*) per infettare nuovi ospiti. La combinazione di questi due fattori rende le epidemie fulminee e devastanti poiché ogni ospite infettato ha il mezzo (la rete) per contagiare moltissimi altri *computer* (tutti in grado di far funzionare la macro che ospita il virus).

Infine va ricordato che un macrovirus viene scritto con un linguaggio di alto livello come *Visual Basic for Application*, che è alla portata di moltissimi programmatori, mentre l'*assembler* che veniva usato per le altre tipologie di virus richiedeva programmatori più esperti. Vediamo nel seguito due macrovirus (**Melissa** e ***Iloveyou***) che hanno segnato la storia recente dei virus.

Melissa

Un virus innovativo dal punto di vista dei meccanismi di diffusione è stato **Melissa** (1999) un **macrovirus** che sfruttava diverse vulnerabilità delle applicazioni di produttività personale della *Microsoft*, per diffondersi attraverso la rete. Si tratta di un ***worm*** scritto in VBA (*Visual Basic for Application*) incorporato in una macro contenuta a sua volta in *file* .DOC.

Melissa opera nel modo seguente:

- arriva un messaggio contenente l'allegato (LIST.DOC) e l'utente lo apre, mandando in esecuzione Melissa;
- il virus si propaga spedendo automaticamente via *email* una copia del *file* .DOC a 50 indirizzi scelti tra quelli contenuti nella rubrica dell'utente colpito;
- una volta propagatosi, il virus diventa nocivo modificando i documenti dell'utente o spedendo sue informazioni personali.

La tecnica di propagazione usata è tale da ingannare l'utente che vede arrivare il messaggio da un suo conoscente e quindi non utilizza particolare prudenza e lo apre.

Nella prima versione la *email* riferiva all'*attach* spiegando che conteneva una lista di *password* per accedere a siti pornografici e, per assicurarsi un efficace inizio dell'infezione, l'autore del virus lo inserì in un *newsgroup* su tematiche sessuali.

Il virus è multipiattaforma, cioé è in grado di infettare utenti che utilizzano sistemi operativi diversi purché siano presenti *Word*, *Outlook* e una connessione a Internet.

Iloveyou

Iloveyou (2000) è un macrovirus *worm* molto famoso che è stato citato dai telegiornali di tutto il mondo che è riuscito a propagare la sua infezione anche in contesti importanti. Le vittime illustri di *Iloveyou* vanno dagli uffici

governativi di diverse nazioni (come il parlamento inglese e gli uffici del Pentagono, della Cia e della *Federal Reserve* americana) ad aziende di rilevanza mondiale (come Vodafone o *Time Warner*).

Per diffondersi *Iloveyou* utilizza lo stesso metodo di **Melissa** , riproduce un *attach* e lo invia ai conoscenti. A differenza di Melissa, che sceglie 50 indirizzi, *Iloveyou* spedisce se stesso a tutti gli indirizzi della rubrica e in questo modo la sua propagazione risulta molto più veloce e capillare. Un'altra differenza da Melissa è nell'azione di *Iloveyou* che è molto più distruttivo: è riuscito a produrre danni per diversi miliardi di dollari.

Iloveyou è scritto in *VBScript* (*Visual Basic Script*) per *Windows Scripting Host* (WSH) e dunque riesce a infettare solo *computer* che hanno installato WSH. Ma WSH viene installato automaticamente in *Windows* 98 e *Windows* 2000 ed è presente in tutte le piattaforme con installato *Internet Explorer* 5.

La diffusione e i danni derivanti da *Iloveyou* hanno spinto *Microsoft* a produrre apposite patch per *Outlook* in modo da limitarne la vulnerabilità.

Nimda

Nimda è un **virus** ***worm*** **multipartito** , scritto in Visual C++, che ha provocato una delle infezioni più diffuse del 2001. Sfrutta diverse vulnerabilità dei sistemi *Microsoft*, infettando molte piattaforme, da *Windows* 95 e *Windows* ME a *Windows* 2000.

Durante l'infezione Nimda effettua numerosi interventi sui *file* del sistema vittima con l'obiettivo di saturare lo spazio fisico dei dischi e di rendere indisponibili le risorse (***denial of service***). Ma la caratteristica più significativa di Nimda è che il virus utilizza contemporaneamente numerosi canali di diffusione per assicurare la propagazione dell'infezione. In particolare i meccanismi di propagazione di Nimda sono:

- ***email***: l'invio di *email* contenenti il virus; gli indirizzi di posta elettronica a cui spedire Nimda sono ottenuti dai *file* .HTM e .HTML memorizzati sul *computer* ospite. Al messaggio, in formato HTML, è allegato un *file* README.EXE, che attiva il virus;
- ***Web***: attacco ai *server* HTTP *Internet Information Server* (IIS): sfruttando le **vulnerabilità** del *software* o possibili *backdoor* lasciate da infezioni virali precedenti, Nimda attacca le macchine su cui sono installati servizi *Web* basati su IIS;
- **LAN**: la propagazione attraverso le risorse condivise della LAN. La diffusione del virus attraverso la LAN avviene con diversi meccanismi, tra i quali la scansione della rete sulla porta HTTP/80 e la creazione di condivisioni dei *drive* locali.

La combinazione dei sistemi di diffusione ha reso l'epidemia di Nimda molto rapida e capillare. Nimda si diffonde infatti molto rapidamente su Internet, attraverso un meccanismo di scelta degli indirizzi bersaglio che passa rapidamente da una comunità di utenti all'altra. Una volta penetrato su un sistema della LAN, Nimda tenta poi di diffondersi sulle stazioni vicine per cercare di compromettere l'intero sottosistema.

Difendersi

Secondo *Computer Economics* gli attacchi da **virus** hanno causato danni nel 2001 per 13,2 miliardi di dollari. La spesa è in forte riduzione rispetto al 2000, anno in cui si è diffuso il virus complessivamente più dannoso a tutto il 2001, ***Iloveyou*** che ha prodotto da solo danni per 8.75 miliardi di dollari.

La migliore difesa contro i virus è ovviamente la **prevenzione** che va affrontata sia in termini tecnologici che comportamentali. In particolare per prevenire i virus occorre:

- evitare comportamenti rischiosi, quali scambio e *download* di *file* sospetti, installazione di pacchetti non licenziati, apertura degli *attach*. Quest'ultima precauzione è molto importante per difendersi dai **macrovirus**

poiché se l'allegato non viene eseguito, il virus rimane latente. Aprire i messaggi di posta elettronica può diventare causa di infezione solo se il *client* di posta è impostato per eseguire gli allegati in automatico. Per questo motivo è opportuno disabilitare l'anteprima dei messaggi.
- Aggiornare il *software* in modo da ridurre le **vulnerabilità** al minimo. L'attacco dei virus viene infatti condotto sfruttando errori nel *software* o nei protocolli e tutte le azioni volte a ridurre il numero di errori presenti nei programmi (come per esempio l'installazione delle *patch*) sono forti forme di prevenzione dei virus.
- Utilizzare un *software* **antivirus** ovvero un *software* in grado di identificare i virus e rimuoverli prima che entrino in azione. Per rilevarli l'antivirus cerca all'interno della memoria (centrale e di massa) l'impronta identificativa del virus. Per questo motivo l'antivirus va tenuto costantemente aggiornato.
- Effettuare comunque un *backup* periodico dei dati in modo da poter ripristinare efficacemente il sistema anche in caso di danni.

Antivirus

Per difendersi dai virus occorre dotarsi di un *software* antivirus che si occupi di:

- prevenire l'infezione, ovvero rilevare il virus prima che abbia realmente infettato il sistema. L'antivirus può scandire a questo scopo i *file* scaricati da Internet, gli *attach* delle *email*, i supporti di memoria di massa removibili. Se l'antivirus entra in funzione in questa fase, il virus non ha ancora avuto modo di riprodursi e di agire per cui non è necessaria una fase di recupero ma è sufficiente la rimozione del codice virale.
- Recuperare dopo una infezione. Il virus ha già infettato l'ospite e in alcuni casi ha anche prodotto danni. L'antivirus non si può limitare a rilevarlo ma deve anche mettere in atto un insieme di meccaniche che consentano di estirparlo, ovvero rimuoverlo dal sistema ospite.

Le verifiche del *software* antivirus vengono tipicamente fatte in via automatica:

- all'avvio del sistema, verificando almeno il *Master Boot Record* e i *file* di sistema.
- Periodicamente, scandendo la memoria centrale.
- Ogniqualvolta si effettua una operazione rischiosa (come l'apertura di un ***attach*** di posta elettronica, l'inserimento di un dischetto nel *drive*, il *download* di un *file*), verificando i *file* potenzialmente pericolosi.

Le attività di recupero sono invece avviate automaticamente ogniqualvolta un virus attivo viene intercettato.

Rilevamento

Le attività di rilevamento effettuate dagli **antivirus** hanno lo scopo di verificare se il *computer* è o no affetto da un **virus** e, se sì, da quale.

L'antivirus cerca il virus, verificando la presenza sulla macchina dell' **impronta virale** , che identifica il virus univocamente e che consente dunque di decidere quali politiche di rimozione applicare. L'antivirus deve essere aggiornato continuamente in modo da avere un insieme di impronte da ricercare il più completo possibile.

L'attività di rilevamento viene fatta con diverse tecniche:

- ***scanning***, ovvero ricerca dell'impronta virale all'interno della memoria, centrale e di massa. Tipicamente l'antivirus verifica spesso la memoria centrale e solo su richiesta i dischi. Lo *scanning* può utilizzare anche tecniche euristiche per individuare virus la cui impronta non sia ancora censita nell'insieme delle sequenze da cercare;
- **monitoraggio** delle attività pericolose o sospette, come per esempio la scrittura in alcune *directory* o di alcuni tipi di *file*;

- ***detection***, ovvero meccanismi di verifica dell'integrità dei dati che calcolano periodicamente il *checksum* dei *file* critici e rilevano così eventuali modifiche indesiderate.

I meccanismi euristici inseriti nelle versioni più efficaci degli antivirus possono scambiare per impronte virali sequenze di *byte* del tutto innocue, evidenziando dunque un **falso positivo** ovvero un caso in cui una porzione di codice o di dati qualunque viene scambiata per virus. Tutte le rilevazioni di potenziali nuovi virus vengono solitamente comunicate dal *software* antivirus al suo produttore che risponde entro breve all'utente, sia in caso di falso positivo che in caso di nuovo virus appena identificato.

Ripristino

La fase successiva al rilevamento di un virus all'interno di un sistema è quella del ripristino, nella quale si cerca di riportare il sistema a uno stato antecedente l'infezione. In fase di ripristino il *software* antivirus deve:

- rimuovere il virus dalla memoria e disattivarlo. Questa operazione è particolarmente critica perché essendo il virus stesso in esecuzione è possibile che contrasti l'azione dell'antivirus. In particolare i virus spesso intercettano parte delle chiamate al sistema operativo.
- Rimuovere il virus dalla memoria di massa, ripristinando il contenuto del disco, sia dei *file* che del *Master Boot Record*, che delle FAT. In particolare il virus deve essere rimosso da tutti i *file* infetti cercando di invertire la procedura invasiva con cui si è replicato. Non sempre è possibile una rimozione indolore e in alcuni casi i *file* infetti hanno perso il loro contenuto originario che non è quindi più ripristinabile.
- Recuperare dai danni, ovvero ripristinare completamente lo stato del *computer* prima che avvenisse l'infezione.

Il recupero completo del sistema dipende dal tipo di aggressione effettuata dal virus e dal tempo che il virus ha avuto per danneggiare il sistema. Per garantirsi la possibilità di un completo ripristino non ci si può affidare esclusivamente allo *scanning* dell'antivirus ma occorre:

- creare i dischetti di emergenza da utilizzare in caso di ripristino del sistema;
- effettuare molto spesso un *backup* dei dati per avere a disposizione all'occorrenza una copia aggiornata degli stessi da utilizzare durante il ripristino.

Antivirus: licenze

Esistono numerosi *software* antivirus che offrono un insieme di funzionalità di base comuni.

Alcuni *software* sono *free*, ovvero completamente gratuiti, ma la maggioranza dei *software* antivirus prevede l'acquisto della **licenza d'uso** . La gran parte dei produttori concede in uso gratuito il *software* in prova per un breve periodo (*shareware* o *evaluation licence*).

Le politiche dei prezzi sono molto variabili, ma solitamente sono previste riduzioni per:

- licenze multiple.
- Licenze *educational*.
- Aggiornamenti di *software* già licenziati o allungamento della durata della licenza.
- Aumento del numero delle licenze in possesso.

Sono previste due tipologie di aggiornamento: l'aggiornamento delle impronte virali, che è gratuito per tutta la durata del contratto, e l'aggiornamento del *software* antivirus (che migliora periodicamente in termini di efficacia). Molti fornitori prevedono licenze con scadenza temporale per cui tutto il pacchetto, compresi gli aggiornamenti delle versioni dell'antivirus, risulta gratuito per il periodo di validità del contratto. In alcuni casi sono disponibili anche

licenze perenni il cui contratto prevede un costo iniziale maggiore e un costo annuale minimo per il mantenimento della licenza.

Molti fornitori offrono anche un contratto di assistenza tecnica, attraverso il quale offrono supporto nel momento della rimozione dei virus. Forme di assistenza vengono date anche via *email* e via *Web*, offrendo informazioni sui nuovi virus, sulle modalità di rimozione e su altre problematiche correlate.

Antivirus: prodotti

Esistono numerosi *software* antivirus che offrono un insieme di funzionalità di base comuni.

Di seguito è riportato un elenco dei più diffusi *software* antivirus con i rispettivi siti:

- *Norton Antivirus* della *Symantec*, **http://www.symantec.com/**
- *McAfee Viruscan* della *Network Associates*, **http://www.mcafee.com**
- *Panda Antivirus* della *Panda software*, **http://www.pandasoftware.com/**
- *PC-Cilling* della *Trend Micro Inc.*, **http://www.trendmicro.com**
- *F-Prot* della *Frisk software International*, **http://www.f-prot.com**
- *F-Secure Anti-Virus* della *F-Secure*, **http://www.f-secure.com**
- *AVG Antivirus* distribuzione *free* della *Grisoft Inc.*, **http://www.grisoft.com/**
- *Inoculate* della *Computer Associate* **http://www.cai.com**
- *Esafe* della *Aladdin*, **http://www.esafe.com**

Funzionalità aggiuntive

I prodotti di **antivirus** , oltre a proteggere le macchine *client*, possono offrire diverse tipologie di funzionalità supplementari:

- possono assicurare la protezione dal lato ***server***, ovvero proteggere *file server* e *print server*. I *server* sono infatti maggiormente vulnerabili in quanto fornitori di servizi e i normali antivirus realizzati per stazioni *client* non riescono a proteggere questo tipo di piattaforme in modo adeguato.
- Possono assicurare, in modo **centralizzato** la protezione dei *client*, consentendo la gestione unificata delle *policy* antivirus e degli aggiornamenti. La protezione dei *client* può avvenire via *Web* e non ed essere completamente trasparente all'utente. Questa funzionalità consente all'amministratore di installare, aggiornare e gestire gli antivirus attraverso un unico sistema integrato senza dover effettuare queste attività da ciascuna postazione *client*. Questo tipo di antivirus offre tipicamente una interfaccia grafica per il controllo del sistema, che tra l'altro produce report sugli attacchi subiti.
- Possono proteggere la **posta** elettronica, agendo sui *server*. Questo tipo di *software* controlla la presenza di virus su tutti i messaggi in transito sul *server* di posta elettronica e in questo modo previene la diffusione dei virus spediti assieme alla *email*, rimuovendoli prima che l'utente possa inavvertitamente attivarli.
- Possono agire direttamente sui protocolli (HTTP, FTP e SMTP) rimuovendo il virus mentre transita sulla rete. Anche in questo caso, il virus non raggiunge l'utente finale e quindi non si rischia un'attivazione involontaria.
- Possono integrare le funzionalità di un ***firewall*** , offrendosi come piattaforma per la gestione integrata della sicurezza del sistema.

Conclusioni

Scopo di questo approfondimento è stato quello di affrontare le tematiche essenziali relative ai *computer* virus, introducendo le principali tipologie di virus, con alcuni casi specifici, e di antivirus. L'argomento è di importanza cruciale sia per affrontare in modo proattivo le problematiche di sicurezza dei dati sia, in modo più generale, per

cercare di prevenire i danni al sistema. La difesa dai virus deve essere affrontata sia attraverso la conoscenza del problema dal punto di vista tecnico, sia attraverso aspetti organizzativi e comportamenti prudenti. Nessuna delle due strategie, da sola, è completamente efficace.

La principale tecnologia di difesa dai virus, l'antivirus, è un supporto ormai indispensabile sia per la prevenzione dell'infezione, che per la sua rimozione e per il successivo ripristino dei sistemi. Esistono numerosi *software* che offrono la possibilità di proteggere le postazioni *client* in modo efficace. In sistemi di media complessità in cui sono presenti *server*, servizi di posta o anche solo un numero elevato di PC deve essere valutata l'opportunità di acquisto di *software* più evoluti che proteggano le piattaforme *server* e che offrano supporto alla gestione degli aggiornamenti.

I **riferimenti bibliografici** *on line* consentono di svolgere autonomamente ulteriori attività di approfondimento, sia su tematiche generali che su aspetti tecnici specifici.

Introduzione alla sicurezza dei sistemi informatici

Prof.ssa Paola Salomoni
Dott. Diego Gardini
1.3.1. (Descrivere le tecniche e le procedure appropriate per la prevenzione dei problemi e la loro soluzione)

Sicurezza

Chi si occupa di **sicurezza informatica** ha, come obiettivo principale, quello di offrire un adeguato grado di protezione dei dati, riducendo i fattori di rischio. In particolare, proteggere i dati significa garantirne:

- la **riservatezza** o **confidenzialità**, ovvero la protezione da letture non autorizzate dei dati memorizzati, elaborati e trasmessi nel sistema, che ha lo scopo di impedire l'utilizzo illegittimo di informazioni riservate.
- L'**integrità**, ovvero la protezione da modifiche non autorizzate dei dati memorizzati, elaborati e trasmessi nel sistema, che ha lo scopo di impedire la manipolazione illegittima delle informazioni. In particolare, garantire l'integrità di un messaggio transitato sulla rete significa assicurare che il messaggio ricevuto sia esattamente quello spedito dal mittente.
- La **disponibilità**, ovvero la capacità di garantire l'accesso ai dati o alle risorse del sistema.
- L' **autenticazione** , ovvero la possibilità di identificare in modo certo e univoco chi invia, manipola e riceve i dati. L'autenticazione è una forma di prova di identità che individua univocamente gli utenti del sistema. L'autenticazione fornisce supporto al non ripudio, che consiste nel dare garanzia che chi trasmette e chi riceve non possano negare di aver inviato e ricevuto il messaggio. Il non ripudio costituisce una prova formale, utilizzabile anche a termine di legge, per dimostrare che una certa persona ha sottoscritto un documento.

Vulnerabilità

La sicurezza delle informazioni è di importanza cruciale in qualunque contesto sociale e lavorativo, anche, ma non solo, in relazione alle leggi relative alla ***privacy*** e alla protezione dei dati. I problemi sono fondamentalmente dovuti a un insieme di fattori che coinvolgono sia aspetti prettamente tecnici e tecnologici che aspetti organizzativi e di comportamento.

In generale i rischi in termini di sicurezza informatica sono da imputarsi alla vulnerabilità, ovvero alla presenza di lacune o insufficienze nel sistema complessivo del trattamento dei dati. La vulnerabilità può essere addebitata:

- al ***software*** (sia il sistema operativo, sia le applicazioni), che ha raggiunto ormai livelli di enorme complessità e di conseguenza contiene sempre più frequentemente errori (accidentali e non). Sfruttando gli errori diviene possibile attivare funzionalità che rendono un *software*, apparentemente innocuo, un pericolo alla sicurezza dei dati.

- Ai **protocolli di rete**. I *computer* in rete interagiscono con gli altri sistemi connessi attraverso protocolli di comunicazione che possono presentare vulnerabilità. In questo caso un sistema intruso si può inserire in una comunicazione con scopo di convincere un sistema vittima a credere che il sistema intruso possa utilizzare legittimamente i suoi servizi.
- Al **comportamento degli utenti**, che non sempre rispettano norme di sicurezza anche di tipo elementare. In realtà la protezione dei dati dipende prevalentemente dagli utenti che utilizzano i sistemi, poiché nessuno strumento tecnologico può sostituirsi al senso di responsabilità e al rispetto delle norme.

La connessione in sé non è invece una causa, ma piuttosto un mezzo, attraverso il quale avvengono i più frequenti e intrusivi attacchi alla sicurezza dei dati.

Metodologie

Gli amministratori e i responsabili dei sistemi informatici possono provvedere al mantenimento della sicurezza delle informazioni e delle risorse attuando metodologie di tipo proattivo e di tipo reattivo.

Le metodologie proattive consistono in attività di prevenzione che mirano a ridurre al minimo le vulnerabilità del sistema sia dal punto di vista organizzativo che da quello tecnologico. Una semplice strategia proattiva consiste, per esempio, nell'installare sistemi *software* **antivirus** per la rilevazione dei **virus** e nel mantenerli periodicamente aggiornati.

Le metodologie reattive vengono invece attuate ad attacco avvenuto per:

- valutare i danni e le violazioni delle norme;
- identificare i colpevoli;
- segnalare correttamente l'attacco ai responsabili legali della struttura;
- ripristinare i dati e il corretto funzionamento del sistema nel più breve tempo possibile.

Una semplice attività di reazione consiste per esempio nella rimozione dei virus, mediante il *software* antivirus che li ha rilevati.

In generale occorre prevedere la possibilità di essere vittima sia di attacchi esterni che interni, ovvero attacchi condotti da persone che operano all'interno della struttura scolastica e che hanno quindi il vantaggio di essere utenti registrati con diritti di accesso alle risorse. Questa seconda eventualità è realistica solo in scuole i cui studenti abbiano una formazione medio/alta su tematiche correlate alle tematiche TIC, quali ad esempio gli Istituti Tecnici Industriali.

Prevenzione: aspetti organizzativi

Dal punto di vista organizzativo, i responsabili dei sistemi informatici devono avere cura di utilizzare essi stessi politiche di amministrazione atte a prevenire attacchi alla sicurezza. Queste politiche si concretizzano tipicamente:

- in fase di acquisizione di nuove risorse, avendo cura di:
  - optare per sistemi operativi, applicazioni e servizi che offrano supporti al controllo degli accessi e all'implementazione di politiche di accesso articolate.
  - Utilizzare esclusivamente *software* per il quale si dispone di licenza d'uso.
  - Definire regolamenti e politiche di accesso che specifichino le responsabilità e le prerogative degli utenti.
  - Definire e implementare politiche di *backup* dei dati
  - Utilizzare *software* per la rilevazione e rimozione dei **virus** (**antivirus**).
  - Utilizzare sistemi (*hardware* e/o *software*) che consentano il monitoraggio della rete e limitino gli

accessi alla rete locale.
- Periodicamente, avendo cura di:
  - aggiornare il *software* scaricando gli opportuni *package*.
  - Aggiornare in particolare gli **antivirus** .
  - Monitorare la rete e i sistemi, alla ricerca di segnali che siano indice di attività potenzialmente pericolose.

Indispensabile è definire a priori quali sono le politiche di accesso alle risorse da parte degli utenti, ovvero chi può accedere a cosa e con che tipo di diritti. Queste politiche devono poi essere implementate utilizzando sistemi operativi e applicazioni che prevedano la gestione di più utenti e meccaniche d'accesso avanzate. Sistemi operativi e applicazioni ad uso personale, che non prevedano politiche di accesso ai *file* e alle risorse, ma consentono a tutti gli utenti l'accesso a tutte le risorse (quali ad esempio *Microsoft Windows98*), rendono impossibile la realizzazione di politiche di sicurezza significative.

Password

Il metodo più semplice per l'accesso illecito a un sistema è quello di impossessarsi indebitamente della ***password*** di un utente autorizzato e, spacciandosi per esso, di compromettere riservatezza, integrità, autenticazione e a volte disponibilità dei dati. A ogni utente sono tipicamente assegnate una o più *password*, tra le quali:

- la *password* di accesso al *computer* o al dominio locale, che impedisce l'utilizzo improprio delle risorse interne (*hardware*, *software* e dati).
- La *password* di accesso alla posta elettronica e ai servizi Internet, che identifica l'utente nell'uso delle risorse esterne.

Nella maggior parte dei casi è lo stesso utente che, utilizzando *password* banali o trascrivendole su promemoria, crea le condizioni perché la credenziale sia scoperta da altri.

Per evitare che questo tipo di problema si verifichi è opportuno:

- fornire agli utenti un insieme di regole di comportamento (da sottoscrivere ad esempio al momento della creazione degli *account*), che li responsabilizzino.
- Suggerire agli utenti di utilizzare *password* che siano contemporaneamente semplici da ricordare e non banali.
- Prevedere meccanismi automatici che costringano gli utenti a cambiare periodicamente la *password*.

Regole di comportamento

Definendo il regolamento d'uso delle risorse e in particolare degli *account*, è opportuno suggerire all'utente come comportarsi nella gestione della ***password*** . Di seguito sono elencati un insieme di semplici suggerimenti che possono costituire una porzione del regolamento:

- Utilizzare *password* di almeno 6 caratteri e di tipo non banale, ovvero contenenti maiuscole, minuscole e segni di interpunzione. Evitare nomi propri, date o altri riferimenti personali facilmente associabili alla propria persona (come il numero di telefono). Non usare parole che possano essere contenute in un dizionario (in qualsiasi lingua).
- La *password* è strettamente personale, per cui è opportuno non comunicare a nessuno la *password* e prestare attenzione nel momento dell'immissione per evitare che possa essere compresa da terzi. In caso di dubbio modificare, appena possibile, la *password*.
- Non trascrivere mai la *password* su promemoria, agende, telefonini o altri supporti. La *password* deve essere ricordata a memoria.

Contestualmente l'utente va responsabilizzato facendogli comprendere che la *password* è il meccanismo di base dell'autenticazione e che terze parti in possesso della sua *password* possono produrre danni ai dati e al sistema in vece sua, sia intenzionalmente che non intenzionalmente.

Altre regole di comportamento da suggerire agli utenti riguardano in generale le loro responsabilità riguardo:

- all'uso corretto delle risorse interne;
- all'uso corretto di Internet e dei suoi servizi (posta elettronica, *chat*, *news*, *Web*, eccetera);
- alla riservatezza delle informazioni.

Infine possono essere suggeriti comportamenti prudenti che evitino la diffusione dei **virus** , come evitare di aprire o visualizzare ***attach*** ai messaggi di posta provenienti da indirizzi sconosciuti o di utilizzare dischetti senza prima verificarli con un antivirus o scaricare *file* da siti sospetti.

Come scegliere una password

La ***password*** deve essere di almeno 6 caratteri e deve contenere lettere maiuscole e minuscole, numeri e/o segni di interpunzione. Deve cioè assomigliare a una sequenza di caratteri scelta a caso tra quelli presenti sulla tastiera. *Password* di almeno 8 caratteri sono fortemente consigliate.

Sequenze di caratteri così strutturate sono però difficili da memorizzare per cui vengono suggeriti meccanismi di costruzione della *password*, che consentano di ottenere parole d'ordine non elementari a partire da informazioni mnemoniche. Il metodo più utilizzato per la generazione di *password* con le caratteristiche suddette è quello di scegliere una frase semplice da ricordare e, partendo da questa, costruire una sequenza di caratteri, tipicamente basata sulle iniziali delle parole. Per esempio partendo da Biancaneve e i sette nani si può facilmente ricordare la *password* B-n&i7na.

Di seguito è riportata una tabella con altri semplici casi:

frase	*password*
Alì Babà e i 40 ladroni	@B&i40La
44 gatti in fila per 6 col resto di 2	44Gifx6r2
Art 1. L'Italia è una repubblica fondata sul lavoro	a1:L'IÈ1R

Prevenzione: aspetti tecnici

In generale è obiettivo dell'amministratore e del responsabile dei sistemi evitare qualunque minaccia ovvero qualunque evento o entità che possa danneggiare il sistema compromettendo i dati o i servizi critici. Esistono numerose categorie di minacce che vanno dagli eventi catastrofici naturali e non (incendi, terremoti, alluvioni), agli incidenti che coinvolgono le infrastrutture, casuali o intenzionali (taglio di cavi, sospensione dell'erogazione di corrente), ai veri e propri attacchi alla sicurezza del sistema.

Un **attacco** è un tentativo di accesso o d'uso non autorizzato dei dati e dei sistemi, che mira a compromettere riservatezza, integrità, disponibilità, autenticazione e/o non ripudio. L'attacco non è di per sé necessariamente fruttuoso, ma può fallire grazie alle politiche di sicurezza proattiva che sono state realizzate. Se l'attacco ha successo, si è di fronte a un incidente che ha inciso sulla sicurezza informatica della struttura.

Si distinguono due tipologie di attacchi:

- **attacchi passivi**, che hanno l'obiettivo di compromettere la riservatezza e l'autenticazione, entrando in

possesso di informazioni private.
- **Attacchi attivi**, che hanno l'obiettivo di compromettere l'integrità e la disponibilità, ovvero mirano ad alterare le informazioni e/o danneggiare i sistemi.

Molto spesso gli attacchi passivi sono effettuati per ottenere le informazioni necessarie a iniziare un attacco attivo.

Alcuni attacchi

Le tipologie di attacco alla sicurezza di sistemi sono fortemente variegate e vengono continuamente prodotti nuovi attacchi che sfruttano le diverse vulnerabilità.

In questo contesto introdurremo diversi attacchi, senza l'ambizione di fare un elenco esaustivo, ma con l'obiettivo di introdurre alcuni tra i meccanismi più diffusi e più pericolosi, ovvero:

- **abuso dell'identità elettronica** ,
- ***exploit*** ,
- ***malicious software*** ,
- ***sniffing*** ,
- ***spoofing*** ,
- ***Denial of service*** .

Abuso dell'identità elettronica

L'identità elettronica degli utenti può essere sostituita in modo malizioso intercettando le credenziali di autenticazione (ad esempio la *password*) sia al di fuori del sistema (attraverso confidenze o promemoria), sia sfruttando vulnerabilità dei sistemi interni (ad esempio con un **cavallo di Troia**), sia mentre queste credenziali transitano sulla rete.

In questo caso, utilizzando le credenziali dell'utente ottenute maliziosamente è possibile sostituirsi ad esso. I problemi più gravi si hanno:

- quando l'abuso produce gravi violazioni alle norme vigenti.
- Quando l'abuso avviene in un contesto commerciale e dà origine a obblighi per la persona la cui identità è stata utilizzata impropriamente.
- Quando viene abusata l'identità dell'amministratore del sistema e, dunque, si è resa possibile la compromissione completa della sicurezza dei dati e delle risorse.

In particolare in questo caso sono colpiti:

- l'autenticazione, poiché qualunque azione compiuta dall'utente sostituito è stata in realtà compiuta da altri.
- Il non ripudio, poiché l'utente abusato può negare di aver partecipato ad una comunicazione e/o di avere sottoscritto un accordo.
- La riservatezza e l'integrità dei dati che sono rispettivamente visibili e scrivibili dall'utente la cui identità è stata utilizzata impropriamente.

Molte volte l'abuso dell'identità elettronica è il primo passo di attacchi più complessi e distruttivi ed è utilizzato proprio per rendere difficile l'identificazione di chi ha compiuto azioni dannose e criminali.

Exploit

Le vulnerabilità dei programmi sono tipicamente generate da un errore nella progettazione o nell'implementazione del *software*. Si indica tipicamente con ***exploit*** l'esecuzione delle azioni necessarie ad approfittare di una vulnerabilità del sistema per sferrare un attacco. La vulnerabilità in se può essere sfruttata solo mettendo in opera un procedimento apposito, il più delle volte complesso, volto a sfruttarla per danneggiare la sicurezza del sistema.

Possono essere vulnerabili sia i sistemi ad uso personale sia i *server*, ma gli *exploit* avvengono più frequentemente sui *server* che, essendo sempre accesi e connessi, sono maggiormente esposti. Le vulnerabilità del *software* possono dipendere a volte da errate configurazioni ed installazioni, fatte dall'amministratore o dagli stessi utenti, che rendono un sistema robusto facilmente accedibile dall'esterno. Ad esempio concedere l'uso di programmi che operano in modalità superutente, aumenta notevolmente il grado di vulnerabilità del sistema operativo.

Esistono appositi *tool* che consentono di scoprire le vulnerabilità presenti in un certo sistema, attraverso un insieme di operazioni di *vulnerability assessment*. La migliore difesa verso la vulnerabilità del *software* resta comunque il frequente aggiornamento e l'installazione di tutti i moduli di correzione offerti dal produttore (*patch*).

Software doloso (malicious software o malware)

Il *software* doloso (***malicious software*** , contratto a volte nel neologismo ***malware***) è un *software* o una porzione di *software* che produce effetti dannosi o non desiderati. Questo tipo di programmi è dunque da considerarsi nocivo, ovvero potenzialmente lesivo della sicurezza del sistema.

Esistono diverse tipologie di *software* doloso tra cui i più noti e diffusi sono **virus**, ***worm*** e **cavalli di Troia**:

- **Cavalli di Troia** : sono programmi apparentemente innocui che una volta eseguiti, effettuano operazioni diverse da quelle per le quali l'utente li aveva utilizzati e tipicamente dannose. Un esempio di cavallo di troia molto semplice è la creazione di una finestra di *login* identica a quella del sistema ma finta, che invia *password* e altre informazioni riservate all'autore del *software* doloso. Spesso quando un sistema viene compromesso l'intruso inserisce cavalli di troia con lo scopo di mascherare l'attacco, procurarsi informazioni aggiuntive e creare un accesso (***backdoor***) da sfruttare successivamente.
- **Virus** : sono porzioni di codice che realizzano tipicamente due attività:
  - quello di replicarsi e inserire se stessi in *file* eseguibili preesistenti sul sistema. Questa attività mira alla diffusione del virus.
  - Quello di compromettere l'integrità delle informazioni e la disponibilità delle risorse. Questa fase attiva del virus viene avviata a scoppio ritardato in modo da consentire una prima fase di diffusione dell'infezione e tipicamente comprende l'aggressione ai dati e ai programmi contenuti nella memoria di massa del sistema.

  Su questo argomento è disponibile un ulteriore **approfondimento** .
- ***Worm*** : sono programmi che utilizzano i servizi di rete per propagarsi da un sistema all'altro. Agiscono creando copie di se stessi sugli *host* ospiti e mettendosi in esecuzione. Sono dunque auto-replicanti e autosufficienti poiché in grado di funzionare senza bisogno di un programma ospite.

Sniffing

Lo ***sniffing*** è un attacco di tipo passivo che mira a compromettere riservatezza e autenticazione effettuando intercettazioni delle comunicazioni. Quando i dati viaggiano non criptati su una rete a mezzo condiviso (come sono tipicamente le LAN) è possibile da un qualsiasi punto della rete intercettare i pacchetti in transito destinati ad altri *host*. È particolarmente critica la fase in cui il *client* invia, in chiaro, a un *server* le informazioni relative all'autenticazione dell'utente. Per questo motivo è opportuno utilizzare servizi che prevedano la trasmissione **cifrata** delle *password*.

L'intercettazione dei dati è fatta attraverso appositi strumenti detti ***sniffer***, che raccolgono le informazioni in transito ed effettuano su di esse diverse operazioni:

- conversione dei pacchetti in una forma leggibile e filtraggio in base a criteri definibili dall'utente. Il filtraggio è tipicamente applicato alle *password* e agli *account*.
- Monitoraggio della rete, sia in termini di performance, che di traffico e di errori, anche attraverso la manutenzione di appositi *log*.

Spoofing

Vengono indicati con il termine ***spoofing*** diversi tipi di attacchi che hanno come meccanica comune quella della sostituzione. In particolare:

- se ci si sostituisce a un utente senza averne diritto, ovvero se si utilizza una qualche forma di abuso dell'identità elettronica, si sta facendo ***user account spoofing***.
- Se si prende il controllo di un canale di comunicazione e su questo si modifica il contenuto dei pacchetti, si sta facendo ***data spoofing***.
- Se si manipola l'indirizzo IP da cui parte una certa connessione in modo da far credere di essere un sistema sorgente differente, si sta facendo ***IP spoofing*** (o ***IP address spoofing***).

Tra questi tipi di attacchi, l'*IP spoofing* è il più noto e diffuso, e ha come obiettivo quello di aggirare i principali controlli attivi effettuati per garantire la sicurezza, che sono appunto basati sul monitoraggio dei numeri IP. Il sistema che effettua l'attacco si spaccia per un diverso IP mentre il sistema che subisce l'attacco invia le risposte all'*host* effettivamente corrispondente all'IP utilizzato per lo *spoofing*.

Lo *spoofing* di indirizzo può essere fatto dall'interno o dall'esterno della sottorete. Lo *spoofing* esterno è più complesso da realizzare perché l'*host* attaccato e quello attaccante non utilizzano mezzi condivisi.

Negazione di servizio (Denial of service)

Gli attacchi di tipo ***Denial of service*** hanno come principale bersaglio la disponibilità delle risorse, in particolare dei sistemi e dei servizi. Lo scopo di chi tenta l'attacco non è quindi quello di ottenere informazioni o di modificarle, quanto quello di impedire ad altri l'accesso alle informazione, anche quando autorizzati, ovvero di negare loro il servizio.

Il risultato di un attacco di questo tipo è dunque l'interruzione di un servizio che risulta indisponibile agli utenti legittimi. Alcune volte questo effetto è ottenuto rendendo le risorse troppo impegnate, in modo da provocare risposte negative a richieste di servizio legittime. Altre volte invece il sistema viene mandato in *crash* e necessita dell'intervento dell'amministratore per riprendere il corretto funzionamento e l'erogazione dei servizi.

Spesso l'attacco ha come obiettivo quello di tenere la vittima occupata, mentre sta avvenendo qualche altra aggressione più critica al sistema. L'autore dell'attacco tipicamente maschera il proprio indirizzo in modo da rendere impossibile o quantomeno molto difficoltoso rintracciarlo. *Denial of service* famosi hanno avuto come bersaglio siti di grandi dimensioni, come ad esempio *Yahoo*.

Due forme molto semplici e diffuse di *Denial of service* sono:

- il ***mail bombing***, che è realizzato inviando a un utente una quantità di posta sufficiente a riempire lo spazio disponibile e dunque bloccare il suo servizio di ricezione.
- La ***bandwidth consumption***, che consiste nel generare una quantità elevatissima di traffico verso una certa destinazione, occupando tutta la larghezza di banda disponibile ed impedendo così ad altri di usufruire dei servizi messi a disposizione da quel nodo.

Alcune contromisure

Di fronte alle innumerevoli tipologie di **attacco** risulta fondamentale operare per ridurre al minimo le vulnerabilità. Oltre alla manutenzione del *software* e alle altre linee guida per la prevenzione dei problemi, è utile e a volte indispensabile dotarsi di tecnologie *hardware* e *software* dedicate alla tutela della sicurezza e alla prevenzione degli attacchi.

Tra queste, ne citiamo alcune particolarmente utili e significative:

- la **crittografia** , che consente di far transitare sulla rete messaggi cifrati nascondendone il contenuto e inoltre offre supporto di base alla certificazione e alla della firma digitale.
- I *software* **antivirus** , che consentono di rilevare e rimuovere i **virus** .
- I ***firewall*** , ovvero sistemi di filtraggio delle informazioni utilizzati per creare una barriera difensiva perimetrale, ovvero per rendere più difficili gli attacchi ai sistemi di una LAN prevenendo gli accessi non autorizzati.

Crittografia

Il successo di alcuni attacchi può essere inibito mediante la trasmissione di messaggi crittografati, ovvero codificati in modo da non poter essere compresi.

Il modello crittografico funziona nel modo seguente: i messaggi da codificare, detti **in chiaro**, sono cifrati mediante una funzione la cui computazione dipende da un parametro detto **chiave**. Il messaggio viene quindi trasmesso in forma crittografata e può essere riportato alla forma in chiaro soltanto da chi possiede la chiave atta alla decifratura. Eventuali intrusi che riuscissero a intercettare la comunicazione, ma non fossero in possesso della chiave di decifratura, non riuscirebbero a ricostruire il messaggio originale.

In tempi passati, quando la **crittografia** veniva utilizzata prevalentemente per uso militare e con mezzi trasmissivi tradizionali, la segretezza del meccanismo veniva riposta in due fattori:

- il metodo con cui avveniva la crittografazione e dunque la decrittografazione, ovvero le funzioni di codifica e di decodifica.
- Le chiavi di crittografazione e decrittografazione ovvero i parametri da passare rispettivamente alle funzioni di codifica e di decodifica.

Sulla rete utilizzare un algoritmo privato di crittografazione può significare limitare il numero dei potenziali destinatari dei messaggi, per cui tipicamente la segretezza è riposta esclusivamente nella chiave. I meccanismi di crittografia sono alla base delle diverse forme di certificazione a disposizione su Internet e del funzionamento della firma digitale.

Su questo argomento è disponibile un ulteriore **approfondimento** .

Antivirus

L'unico sistema efficace per prevenire danni derivanti dalla diffusione di **virus** è l'utilizzo di appositi *software* **antivirus** il cui obiettivo è identificare il virus e rimuoverlo prima che entri in azione. Per rilevare la presenza di un virus i *software* antivirus cercano all'interno della memoria (centrale e di massa) particolari sequenze di *byte* che costituiscono l'impronta identificativa del virus. La continua produzione di nuovi virus rende quindi indispensabile un aggiornamento continuativo del *software* antivirus per garantirne l'efficacia nel tempo. Alcune volte i *software* antivirus sono in grado di rilevare anche virus di cui non conoscono la sequenza di *byte* identificativa, riscontrando su base probabilistica comportamenti anomali o sospetti.

Le verifiche del *software* antivirus vengono tipicamente fatte in via automatica:

- all'avvio del sistema, verificando almeno il *Master Boot Record* e i *file* di sistema.
- Periodicamente, scandendo la memoria centrale.
- Ogniqualvolta si effettua una operazione rischiosa (come l'apertura di un ***attach*** di posta elettronica, l'inserimento di un dischetto nel *drive*, il *download* di un *file*), verificando i *file* potenzialmente pericolosi.

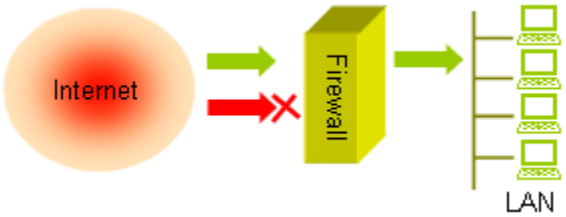
Le attività dei *software* antivirus rallentano le prestazioni del sistema, richiedendo continue scansioni della memoria e del disco. Per esempio è possibile effettuare scansioni periodiche non automatiche di tutto il *filesystem* da attivare in momenti in cui il sistema non è utilizzato. Per questo motivo alcune attività di verifica vengono attivate su richiesta.

Su virus e antivirus è disponibile un ulteriore **approfondimento** .

Firewall

Un ***firewall*** è un sistema connesso alla rete con lo scopo di filtrare i pacchetti in transito. Tipicamente viene posto a bordo della rete con lo scopo di creare una barriera difensiva che aumenti il grado di sicurezza perimetrale, ovvero renda più difficile gli attacchi dall'esterno all'interno del sistema.

Un *firewall* può essere realizzato sia come infrastruttura *hardware* dedicata che utilizzando un *computer* e un opportuno insieme di *software*. Deve essere posto sul bordo (logico) della LAN se si desidera far passare per il *firewall* tutti i pacchetti in entrata e in uscita dalla rete locale. Il *firewall* controlla il flusso dei pacchetti, ovvero decide se consentire o negare l'accesso, implementando delle specifiche politiche di filtraggio del traffico.



Utilizzare un *firewall* significa dunque decidere e implementare delle politiche di sicurezza (*security policy*) che definiscono i criteri di protezione, ad esempio decidendo che è ammesso solo il traffico generato da alcuni servizi (la posta o il *Web*) e non traffico derivante da servizi non standard (che potrebbero rendere possibile o nascondere un attacco).

Si possono distinguere diverse tipologie di *firewall* che utilizzano meccanismi di verifica con differenti livelli di sofisticazione. In particolare i *firewall* più semplici filtrano i pacchetti esaminando le informazioni contenute nell'intestazione e, confrontandole con le *security policy*, decidono se autorizzare o no il transito. Offrono invece una protezione più completa i *firewall* che esaminano anche il contenuto dei pacchetti in transito, con lo scopo di assicurasi che il sistema di destinazione dei messaggi sia realmente in attesa, ad esempio che lo scaricamento di una *mail* sia stato richiesto dal *client*.

Conclusioni

Questa breve trattazione dei problemi correlati alla sicurezza informatica e delle principali metodiche di prevenzione ha avuto lo scopo di introdurre una tematica complessa ed in continua evoluzione. In particolare si è voluto dare enfasi al fatto che un buon sistema organizzativo e un insieme di regole formalizzato, costituiscono un elemento indispensabile nell'attuazione di politiche di prevenzione dei problemi di sicurezza.

Ad esso va affiancato un opportuno insieme di tecnologie *hardware* e *software* che consentono all'amministratore e al responsabile dei sistemi di prevenire le forme più frequenti di attacco e di recuperare in caso in cui questo abbia successo, ripristinando rapidamente le funzionalità dei sistemi.

Sono disponibili approfondimenti relativi alle seguenti tematiche correlate:

- **i virus** ,
- **la crittografia** ,
- **la *privacy*** .

I **riferimenti bibliografici** *on line* consentono di svolgere autonomamente ulteriori attività di approfondimento.

Introduzione alla crittografia

Prof.ssa Paola Salomoni
Dott. Diego Gardini
1.4.5. (Identificare e discutere aspetti relativi alla crittografazione)

Introduzione

I messaggi che passano sulla rete sono in realtà facilmente intercettabili. Esempi di attacchi che mirano all'intercettazione dei messaggi sono lo ***sniffing*** e lo ***spoofing*** dell'indirizzo IP. Oltre a ciò, l'amministratore di una macchina possiede le credenziali per intercettare tutti i dati che passano attraverso quel nodo e quindi un amministratore in malafede può intercettare facilmente messaggi destinati ad altri utenti.

L'intera **sicurezza** del sistema è fortemente compromessa dalla trasmissione di messaggi in chiaro. Un messaggio in chiaro intercettato può infatti essere letto, violando così la **confidenzialità** . Nel caso si tratti di una ***password*** o di una qualunque altra credenziale di identificazione, chi ha intercettato il messaggio avrà modo di sostituirsi al mittente, **abusando della sua identità elettronica** e infrangendo così anche l' **autenticazione** e il **non ripudio** . Con questa credenziale carpita maliziosamente sarà poi possibile sostituirsi all'utente nella gestione delle sue risorse, esponendo a rischio infine anche l' **integrità** e la **disponibilità** dei dati.

In realtà questo tipo di problema è percepito come critico soprattutto nel settore commerciale. In questo contesto è più che mai importante che i messaggi:

- non subiscano alterazioni (integrità): il contenuto dell'accordo non deve essere cambiato.
- Abbiano un mittente univocamente identificabile (autenticazione e non ripudio): la sottoscrizione di un messaggio è irreversibile e univoca, come una firma.
- Non vengano letti senza autorizzazione (confidenzialità): deve essere possibile inviare un numero di carta di credito o altre informazioni riservate con la garanzia che solo il destinatario le potrà leggere.

Crittografia

Il problema di inviare messaggi riservati attraverso sistemi di distribuzione non affidabili è sentito da secoli in ambito militare e sono innumerevoli le metodologie più o meno complesse messe in atto per spedire informazioni agli alleati,

senza che i nemici possano decifrarle.

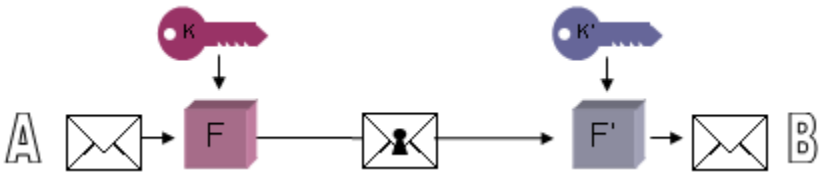
La **crittografia** è un procedimento di codifica e decodifica dei messaggi basata su funzioni parametriche, la cui computazione dipende da un parametro detto chiave. Un messaggio crittografato non è direttamente leggibile se non si possiedono una funzione e una chiave per decriptarlo.

I meccanismi, anche molto evoluti, utilizzati nella crittografia classica, sono in realtà poco adatti ai sistemi basati su *computer* e reti. Una prima differenza sostanziale rispetto al passato risiede nella capacità di calcolo: molti meccanismi indecifrabili dall'uomo in tempi ragionevoli sono in realtà interpretabili velocemente da un attuale calcolatore che è in grado di compiere milioni di operazioni elementari al secondo. Occorre quindi progettare sistemi crittografici con algoritmi così complessi che un intruso, entrato in possesso anche di una grande quantità di testo criptato, non riesca a ricostruire il testo in chiaro corrispondente. Un altro problema deriva dal fatto che nella crittografia classica gli alleati nascondevano ai nemici sia il metodo per crittografare sia la chiave. Sulla rete utilizzare un algoritmo privato di crittografia può significare limitare il numero dei potenziali destinatari dei messaggi, per cui tipicamente la segretezza è riposta esclusivamente nella chiave.

Modello

Il modello su cui è basato un sistema crittografico è il seguente:

- un mittente A vuole inviare un messaggio M a un destinatario B.
- A cripta il messaggio, ovvero applica al messaggio un metodo di cifratura F con chiave di cifratura K.
- Il messaggio così modificato viene poi spedito via rete a B.
- B riceve un messaggio apparentemente illeggibile, ma possiede un metodo di decifratura F' e una chiave K' che consentono di riportare il messaggio in chiaro.

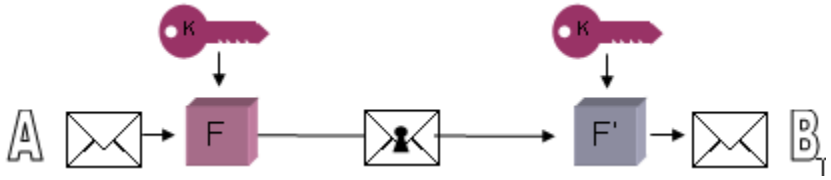


Se un intruso dovesse intercettare il messaggio cifrato non sarebbe in grado di leggerlo a meno di possedere F' e K'.

Le chiavi di cifratura e decifratura possono coincidere e in questo caso si parla di **crittografia a chiave simmetrica** (o a **chiave privata**), oppure possono essere diverse e in questo caso si parla di **crittografia a chiave pubblica** .

Crittografia a chiave privata

I metodi utilizzati tradizionalmente per la crittografia classica erano tutti metodi a chiave simmetrica, basati sull'ipotesi che gli alleati condividessero una chiave nota solo a loro (e per questo detta segreta o anche privata). Quando A vuole spedire a B un messaggio cifrato con un metodo a chiave segreta deve prima di tutto fare in modo che B conosca la sua stessa chiave di crittografia, K, e poi criptare il messaggio con F e K. Quando B riceve il messaggio utilizza F' e K per decriptarlo.



Algoritmi

I moderni sistemi di crittografia a chiave privata utilizzano meccanismi cosiddetti **a blocchi**, che prevedono di scomporre il messaggio da cifrare in blocchi e dunque di operare su di esso per parti. Sui blocchi vengono effettuate operazioni di codifica e trasposizione ricorsive per cui ciascuna parte del messaggio viene rielaborata più volte. La complessità di questo tipo di algoritmi mira a rendere difficile la decodifica da parte di un intercettatore anche quando a essere intercettato è un messaggio lungo che quindi costituisce un caso di prova significativo.

Il più diffuso sistema di cifratura a chiavi segrete si chiama **DES** (*Data Encryption System*) ed è un sistema sviluppato dall'IBM, modificato dalla NSA (*National Security Agency*) e adottato nel 1977 dal governo USA per la protezione dei dati militari. DES è basato su un sistema a blocchi e utilizza chiavi di 64 bit, di cui 8 utilizzati come *checksum* e solo 56 di vera e propria chiave. DES è un algoritmo poco sicuro poiché è pensato per essere efficiente ma anche protetto, su calcolatori di 25 anni fa. La chiave di 56 bit è decisamente troppo corta e quindi, al giorno d'oggi, può essere usato un algoritmo per tentativi per identificarla.

Nonostante ciò, DES è molto utilizzato sia nella sua forma primitiva che in forme più articolate, come a esempio il *Triple DES* (3DES) che tipicamente utilizza blocchi da 64 bit con chiavi a 112 bit. È usato per esempio nella cifratura delle *password Unix* o nei sistemi di autenticazione tipo *Kerberos*.

Sono stati sviluppati molti algoritmi più moderni (e più sicuri) di DES, tra i quali IDEA (*International Data Encription Algorithm*) del 1991 che utilizza chiavi a 128 bit e AES (*Advanced Encryption Standard*) del 2000 che utilizza chiavi lunghe fino a 256 bit.

Problemi

Anche sistemi con chiave simmetrica impossibili da individuare soffrono di alcuni problemi, dovuti al fatto che la chiave deve essere comunicata al destinatario B perché questo possa decifrare il messaggio.

Un primo problema è insito nella trasmissione della chiave che deve quindi a sua volta essere sicura. Se la chiave passa sulla rete in chiaro, allora può essere intercettata e si può compromettere la **riservatezza**del resto della comunicazione. Un altro problema deriva dalla fiducia che B ripone in A: se A comunica dolosamente la *password* all'intercettatore, B utilizza il canale credendolo sicuro quando sicuro non è. Questa eventualità è in realtà molto peggiore del semplice uso di un canale insicuro perché abbassa i livelli di prudenza dell'utente.

Se l'intercettatore ottiene la *password* può inserirsi nella comunicazione fingendo di essere A con B e/o B con A. In questo caso è dunque compromessa anche l'**integrità** dei messaggi, ovvero non vi è garanzia che un messaggio ricevuto sia esattamente quello spedito dal mittente.

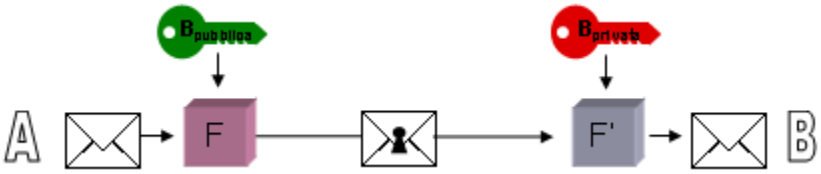
Una soluzione a questo tipo di problema è costituita dalla **crittografia a chiave pubblica** .

Crittografia a chiave pubblica

La **crittografia a chiave pubblica** è un metodo asimmetrico basato sull'esistenza di due diverse chiavi, una utilizzata per criptare e una utilizzata per decriptare. Ciascun utente deve quindi possedere due chiavi, una privata che conosce solo lui e una pubblica che rende nota a tutti. Ovviamente esiste una relazione matematica tra **chiave pubblica** e **chiave privata** che deve rendere semplice calcolare la chiave pubblica a partire da quella privata è difficilissimo (o meglio computazionalmente molto oneroso) calcolare la chiave privata a partire da quella pubblica. La sicurezza di un algoritmo asimmetrico risiede proprio nella difficoltà a individuare la chiave privata, quando si è in possesso di quella pubblica.

Se A vuole inviare un messaggio riservato a B deve dunque procurarsi la chiave pubblica di B (che è disponibile a tutti) e utilizzarla per criptare il messaggio. B sarà l'unico a riuscire a decriptare il messaggio poiché è l'unico in

possesso della chiave privata.

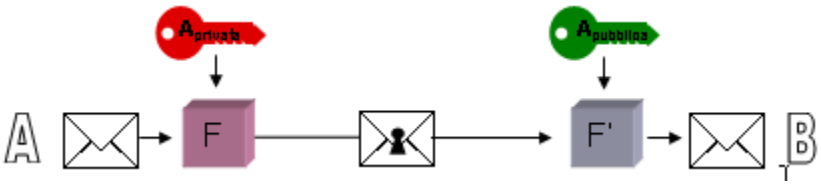


Autenticazione con sistemi a chiave pubblica

I sistemi crittografici a chiave pubblica possono essere utilizzati anche per risolvere problemi inerenti l'autenticazione degli utenti, ovvero per garantire che chi trasmette e chi riceve siano esattamente chi dichiarano di essere. Questo tipo di metodica è alla base della firma digitale e dei certificati.

Se A vuole inviare un messaggio a B e vuole provare a B che il messaggio è effettivamente suo (di A), allora A può criptarlo con la sua chiave privata. B riceverà il messaggio e tenterà di decriptarlo con la chiave pubblica di A. Se l'operazione riesce, allora il messaggio è effettivamente di A, altrimenti B si accorge dell'abuso di identità e può segnalarlo ad A.

Un algoritmo molto diffuso di codifica a chiave pubblica, basato sulla scomposizione in fattori primi di un numero intero, è **RSA** (dal nome dei suoi creatori *Rivest*, *Shamir* e *Adleman*) reso noto nel 1978.



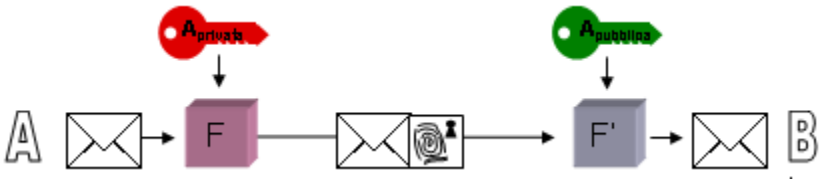
Fingerprint

I sistemi di crittografia a chiave pubblica, incluso RSA, sono piuttosto lenti e la necessità di autenticare un'intera comunicazione può a volte scontrarsi con il ritardo inserito dal criptare l'intero messaggio alla sorgente e dal decriptarlo alla destinazione.

Per rendere più efficiente il meccanismo si utilizza una funzione di ***hash*** attraverso la quale si calcola una stringa identificativa del messaggio, detta ***fingerprint*** (impronta digitale) o ***message digest*** composta da un numero limitato di caratteri (solitamente 128 bit). Questa stringa rappresenta una sintesi del messaggio che è ottenuta attraverso una funzione non invertibile (dato l'*hash* non si risale al messaggio) e che ha una probabilità di generare la stessa *fingerprint* per due messaggi diversi molto bassa. La funzione di *hash* deve inoltre essere molto veloce da calcolare, in modo da rendere significativamente vantaggioso creare il *fingerprint* del messaggio e criptare quello, piuttosto che criptare tutto il messaggio.

A questo punto è possibile autenticare il messaggio limitando l'uso dell'algoritmo di crittografia a chiave pubblica al solo *fingerprint*. Quando A vuole mandare a B un messaggio autenticato e integro, calcola il *fingerprint*, lo cripta con la sua chiave privata e lo aggancia in fondo al messaggio in chiaro. Quando B riceve il messaggio può decriptare con la chiave pubblica di A il *fingerprint* e verificare che esso corrisponde applicando la funzione di *hash* al messaggio ricevuto. Se non c'è conformità tra il *fingerprint* calcolato e quello autenticato, il messaggio non è integro.

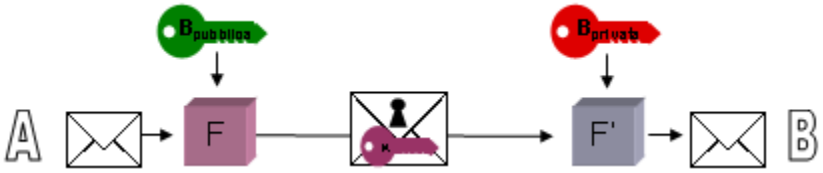
Un algoritmo di *hash* molto utilizzato in crittografia è **MD5** (*Message Digest* 5, 1992) che produce *fingerprint* di 128 bit.



PGP

I sistemi di crittografia propongono spesso soluzioni ibride che utilizzano contemporaneamente più tecniche. Una motivazione a questa scelta è dettata dalla lentezza degli algoritmi a chiave pubblica che impedisce il loro utilizzo in contesti in cui la comunicazione deve essere sollecita. D'altro canto i sistemi a chiave privata hanno il problema della trasmissione sicura della chiave. Una soluzione ibrida di grande successo è PGP (*Pretty Good Privacy*) del 1991 che utilizza come base la cifratura simmetrica di IDEA, la crittografia asimmetrica di RSA e il l'*hashing* di MD5 per le *fingerprint*.

Quando A vuole mandare un messaggio riservato a B, genera casualmente una chiave K e la invia a B criptandola con la chiave pubblica di B. B riceve il messaggio criptato e decriptandolo con la sua chiave privata ottiene K. K è detta **chiave di sessione** poiché la prossima sessione di comunicazione tra A e B avverrà utilizzando K come chiave. A può a questo punto codificare con IDEA il messaggio utilizzando K come chiave. B conosce K e comprende il resto della comunicazione.



Usare PGP

PGP è un *tool* (o meglio un insieme di *tool*) distribuito gratuitamente e disponibile su diverse piattaforme, basato principalmente sulla crittografia a chiave privata di IDEA e sulla crittografia a chiave pubblica di RSA. Il sistema offre supporto a numerose funzionalità tra le quali:

- la **generazione delle chiavi**, pubblica e privata, che vengono prodotte su base casuale a partire da alcuni *input* forniti dall'utente. Ovviamente la chiave privata va mantenuta segreta mentre la chiave pubblica deve essere diffusa il più possibile. La gestione delle chiavi avviene attraverso due *file*: il ***secret ring***, che contiene la chiave privata e va mantenuto segreto, e il ***public ring***, che contiene tutte le chiavi pubbliche note, compresa la propria, e costituisce una specie di rubrica degli utenti riconosciuti.
- La **gestione delle chiavi**, che avviene appunto modificando il *public ring*.
- La **codifica** dei messaggi, attraverso funzioni che consentono di codificare un messaggio, di firmare in chiaro un messaggio e di codificare e firmare un messaggio.
- La **decodifica** dei messaggi, attraverso funzioni che consentono di decodificare messaggi codificati con la propria chiave pubblica, oppure firmati da un mittente di cui si possiede la chiave pubblica oppure codificati e firmati.

Il *download* di PGP può essere fatto a partire dal sito [***The International PGP Home Page***].

Sicurezza del PGP

La crittografia a chiave pubblica riduce di fatto drasticamente la possibilità che un intercettatore si impadronisca della chiave segreta. A fronte di questo vantaggio, la crittografia asimmetrica soffre di un problema correlato con la gestione delle chiavi pubbliche. Non vi è, infatti, alcuna prova che una certa chiave pubblica corrisponda ad una certa persona poiché di per sé non costituisce una prova di identità.

Quando B riceve la chiave pubblica di A:

- non può essere certo che sia realmente di A e non di qualcuno che si spaccia per A. B non ha cioé modo di sapere se è realmente A che utilizza quella chiave.
- Non può sapere se la chiave, che è realmente di A, è stata manipolata e quindi viene usata da terze parti in modo doloso.

Anche in questo caso sono i comportamenti prudenti a difendere gli utenti e i dati:

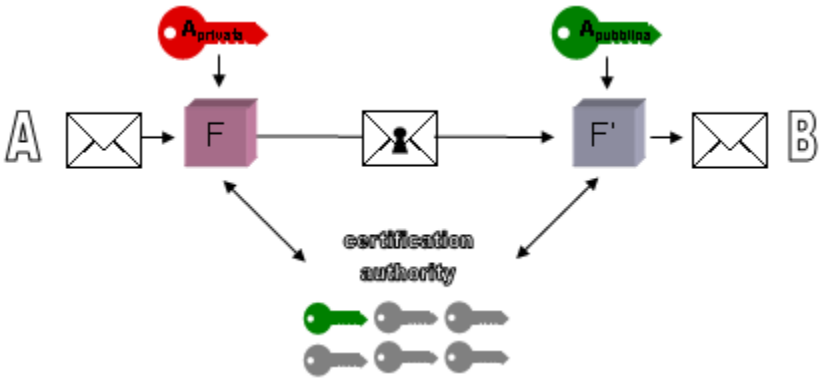
- le chiavi pubbliche sono gestite automaticamente dai *Keyserver*, che sono archivi di chiavi pubbliche accedibili da tutti. I *Keyserver* si aggiornano l'un l'altro automaticamente per rendere consistente l'insieme di informazioni che gestiscono in modo distribuito.
- Il PGP prevede la possibilità di firmare reciprocamente le proprie chiavi. Questo significa che B può sottoscrivere il fatto che la chiave pubblica di A è una certa chiave K. Se io mi fido della chiave pubblica di B, allora questa controfirma mi fa essere fiducioso, in modo transitivo, anche riguardo alla chiave pubblica di A.

Per contro si deve diffidare di chiavi pubbliche poco pubblicizzate o ottenute in modo poco sicuro, per cui è inopportuno controfirmare una chiave e attribuirle credibilità se non si hanno credenziali opportune. Contemporaneamente è importante dare massima diffusione alla propria chiave in modo che sia difficile contraffarla.

Certification authority

Per garantire effettivamente che una chiave pubblica corrisponda a una e una sola persona, e ottenere così quella caratteristica di non ripudio che è indispensabile a condurre a termine attività che abbiano effetti legali (dalla sottoscrizione di un contratto al verbale di un esame universitario) occorre un'istituzione che certifichi le chiavi.

Occorre cioé che la chiave pubblica sia in qualche modo garantita da una terza parte che ne ratifichi la validità. Questa terza parte viene chiamata ***Certification Authority*** .



Certificati digitali

Un **certificato** è un documento elettronico che associa una **chiave pubblica** , e di conseguenza la chiave privata corrispondente, a una particolare identità. Il certificato viene emesso dalla ***Certification Authority*** , che è il garante dell'identità del proprietario del certificato. La *Certification Authority*, per convalidare il certificato emesso, lo firma con la sua chiave pubblica.

Dunque un certificato tipicamente contiene:

- i dati relativi al proprietario, tra cui il nome e la chiave pubblica;
- i dati relativi al certificato, tra cui la data di scadenza e il numero di serie del certificato;

- i dati relativi alla *Certification Authority*, ovvero il nome e la firma digitale.

È la ***Registration Authority*** che si incarica delle pratiche di identificazione prima dell'emissione dei certificati, che possono essere differenziati in base al livello di affidabilità che offrono, ovvero al tipo di procedura utilizzata dalla *Registration Authority* per identificare l'utente. La *Certification Authority*, invece, emette il certificato e ne segue il ciclo vitale, rendendolo pubblico con un sistema *on line* sempre disponibile. Sia le *Registration* che le *Certification Authority* svolgono dunque un ruolo fondamentale e particolarmente delicato, per cui sono scelte tra soggetti altamente affidabili e sopra le parti.

L'insieme costituito da tutte le parti, utenti e *Authority*, nonché dalle tecnologie che queste utilizzano, dai servizi che offrono e dalle politiche di gestione che attuano, è detto PKI (***Public Key Infrastructure***).

Certificati e Web

I certificati digitali sono la tecnologia di base utilizzata nella realizzazione di siti *Web* sicuri. Un sito *Web* può offrire all'utente due funzionalità correlate alla sicurezza della comunicazione e strettamente interdipendenti. La prima consiste nel consentire all'utente di identificare in modo univoco il *server Web*, per garantire che eventuali dati personali o codici di accesso siano inviati a una controparte che è proprio quella che l'utente voleva contattare. La seconda è relativa all'invio sulla rete di dati riservati: supposto che il *server* sia proprio il *server* di riferimento, occorre comunque proteggere da terze parti indiscrete le informazioni che i *client* e *server Web* si vogliono scambiare.

Il *browser* che si collega a un sito *Web* sicuro, utilizza come protocollo **SSL** (*Secure Sockets Layer*) e inizia una sessione sicura chiedendo al *server Web* il suo certificato. Il *server* invia il certificato e il *browser* ne verifica la validità. Solo a questo punto le due parti concordano una chiave di sessione che utilizzeranno per la codifica dei messaggi successivi. È il *client* che genera la chiave di sessione e la cripta con la chiave pubblica del *server Web* (la stessa indicata sul certificato). Solo il *server Web* può quindi leggere il messaggio ed entrare in possesso della chiave di sessione. Questa chiave verrà usate per criptare i messaggi successivi, utilizzando l'algoritmo a chiave privata **DES** .

Il protocollo SSL utilizza url di tipo https:// al posto dell'URL http:// utilizzato dal protocollo HTTP.

Firma digitale

I certificati digitali sono la tecnologia di supporto per dare valore legale alla firma digitale, un sistema che consente a chi sottoscrive il documento di renderne evidente l'autenticità e a chi riceve il documento di verificarne l'integrità.
L'Italia ha dato validità giuridica alla firma digitale attraverso vari interventi normativi che definiscono, tra l'altro, chi può essere certificatore e come deve essere fatto il supporto per la firma digitale.
Oggi in Italia la firma digitale ha lo stesso valore giuridico della firma tradizionale.

Sono distinti tre tipi di certificatori: i certificatori di base, che offrono un relativo livello di qualità e sicurezza, i certificatori qualificati e i certificatori accreditati.
I requisiti dei certificatori accreditati e qualificati sono in corso di elaborazione.

La normativa finora vigente prevede che possano essere certificatori qualificati le società per azioni con capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria e le pubbliche amministrazioni che emettono chiavi pubbliche di competenza in riferimento al proprio ordinamento. La normativa italiana definisce dunque con molto rigore le caratteristiche del certificatore, al punto che il numero dei certificatori è fortemente limitato .

La ragione di questa scelta fortemente vincolante sta nel fatto che la nomina del certificatore qualificato è particolarmente critica poiché questo emette firme digitali con validità e rilevanza a ogni effetto di legge.

Smart card

Per la legge italiana un dispositivo di firma idoneo è un apparato elettronico programmabile solo all'origine, facente parte del sistema di validazione, in grado almeno di conservare in modo protetto le chiavi private e generare al suo interno firme digitali. Il dispositivo di firma è il supporto candidato alla conservazione della chiave privata e deve dunque essere non riproducibile e, in parte, non modificabile. La chiave deve inoltre essere protetta da una procedura di identificazione del titolare (tipicamente l'inserimento di un PIN) e deve essere fatta in modo da non lasciare alcuna traccia della chiave privata sul sistema di validazione.

Il supporto più diffuso che risponde a tutti questi requisiti è la ***smart card*** ovvero una tessera plastificata, con dimensioni di una carta di credito, su cui è integrato un *microchip* programmabile. La *smart card* possiede tutte le caratteristiche richieste poiché è dotata di una ROM non cancellabile, di una EPROM che può contenere i dati del proprietario e di meccanismi di protezione che ne evitano la clonazione.

Il dispositivo di firma non può essere invece realizzato utilizzando un *floppy* o un qualunque altro supporto simile, perché è fondamentale che non possa essere duplicato e che contenga informazioni non modificabili ma programmabili solo all'atto dell'emissione della firma. Inoltre, una chiave pubblica memorizzata su *floppy*, dovrebbe essere trasferita sul sistema di validazione per essere controllata poiché il *floppy* in sé non ha capacità di calcolo.

Conclusioni

Questa breve trattazione ha avuto lo scopo di introdurre la crittografia, descrivendone le principali metodologie e applicazioni. La sicurezza dei dati in generale trae vantaggio dall'uso di questo tipo di tecnologie, ma particolare sostegno viene alle transazioni che devono avere validità legale e che quindi necessitano della garanzia di rispettare integrità, confidenzialità, autenticazione e non ripudio.

In particolare rispondono efficacemente a queste problematiche le tecnologie ibride, che integrano meccaniche tipiche della crittografia a chiave privata con quelle proprie della crittografia a chiave pubblica. Quest'ultima però è davvero sicura solo quando esiste un modo certo per identificare con precisione una persona attraverso la sua chiave pubblica e questa proprietà può essere garantita attraverso l'uso di certificati digitali. I certificati digitali sono utilizzati in svariati contesti, sia in quelli applicativi più diffusi, dall'accesso autenticato ai *server Web* alla posta elettronica, che nelle applicazioni proprietarie, dalla protezione dei dati alla firma digitale.

I **riferimenti bibliografici** consentono di approfondire sia l'argomento in generale e i suoi fondamenti matematici, che gli aspetti più pratici legati alle tecnologie e alle applicazioni, che i principali aspetti normativi correlati.

La tutela giuridica del software e il contratto di licenza d'uso

Prof. Avv. Giusella Finocchiaro

1.4.3. (Identificare e discutere il diritto di proprietà e di licenza del software)

Il software come creazione intellettuale

Il *software* costituisce, dal punto di vista giuridico, una creazione intellettuale.
Le creazioni intellettuali nell'ordinamento giuridico italiano possono essere ricondotte a due distinte categorie: quella delle invenzioni industriali e quella delle opere dell'ingegno.

1.1. Invenzioni industriali e opere dell'ingegno

Sono invenzioni industriali, secondo l'articolo 2585 c.c., le nuove invenzioni atte ad avere un'applicazione industriale, quali un metodo o un processo di lavorazione industriale, una macchina, uno strumento, un utensile o un dispositivo meccanico, un prodotto o un risultato industriale e l'applicazione tecnica di un principio scientifico, purché essa dia immediati risultati industriali.
Sono invece opere dell'ingegno, secondo la definizione dell'articolo 2575 c.c., le opere di carattere creativo che

appartengono alle scienze, alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro e alla cinematografia, qualunque ne sia il modo o la forma di espressione e cioé i libri, le composizioni musicali, i film, eccetera.
Le invenzioni sono giuridicamente tutelate attraverso il **brevetto** (R.D. 29 giugno 1939, numero 1127), mentre le opere dell'ingegno sono tutelate attraverso il **diritto d'autore** o *copyright*, disciplinato dalla legge 22 aprile 1941, numero 633.
http://www.giustizia.it/cassazione/leggi/l633_41.html
Brevetto e diritto d'autore costituiscono due differenti modi di acquisizione del diritto alla tutela giuridica delle creazioni intellettuali, che implicano differenti modi di acquisizione del diritto, differente durata del diritto e differenti strumenti di difesa da eventuali violazioni del diritto stesso.
I diritti sull'invenzione sorgono nel momento in cui l'inventore ha conseguito il brevetto, con effetti che decorrono dalla data in cui la domanda di brevetto è resa accessibile al pubblico. I diritti sulle opere dell'ingegno sorgono, invece, nel momento stesso della creazione dell'opera. Per l'acquisto dei diritti sull' **invenzione industriale** è quindi necessario presentare apposita domanda di brevetto presso l'Ufficio centrale brevetti, mentre per l'acquisto dei diritti relativi all' **opera dell'ingegno** non è richiesta alcuna domanda.
Riguardo, invece, alla durata dei diritti, si ricorda che il diritto all'utilizzazione esclusiva dell'invenzione industriale ha la durata di venti anni dalla data di deposito della domanda. Il diritto all'utilizzazione esclusiva dell'opera dell'ingegno ha, invece, la durata di settanta anni dalla morte dell'autore.
Molto si è dibattuto, sia in Italia che all'estero, sulla tutela giuridica del *software*, se questa fosse da attuarsi attraverso lo strumento brevettuale o invece attraverso la disciplina del diritto d'autore. Questo dibattito, peraltro, era necessariamente preceduto da quello sulla qualificazione giuridica del *software*, come invenzione o come opera dell'ingegno.
Non potendo in questa sede approfondire le ragioni del dibattito dottrinale e anche giurisprudenziale in materia, giova ricordare che la scelta a favore della tutela del *software* attraverso il diritto d'autore è prevalsa sia in Italia che all'estero.
Ciò non esclude che il *software* possa essere tutelato anche, in alcuni casi, attraverso il brevetto e anzi questa forma di tutela è oggetto di un crescente interesse anche legislativo, come risulta da una recente proposta di direttiva.
http://www.innovazione.gov.it/ita/intervento/normativa/allegati/dir_prop_200202.pdf

1.2. Altri strumenti di tutela del *software*

Se la tutela del *software* attraverso la disciplina del diritto d'autore è probabilmente lo strumento di tutela più diffuso, tuttavia, in alcuni casi, altre forme di tutela giuridica possono essere utilizzate.
Innanzitutto, un generale obbligo di fedeltà incombe sul lavoratore dipendente, il quale non può divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa (articolo 2105 c.c.).
Una forma di tutela è rinvenibile anche nelle disposizioni sulla concorrenza sleale, che impongono agli imprenditori di attenersi ai principi della correttezza professionale (articolo 2598 numero 3 c.c.).
Infine, è configurabile una tutela penale mediante l'applicazione delle disposizioni sul segreto. In particolare, l'articolo 623 c.p., concernente il segreto industriale, tutela le notizie destinate a rimanere segrete, sopra scoperte o invenzioni scientifiche o applicazioni industriali, con la precisazione che la giurisprudenza, nella concreta applicazione della norma, non ha ritenuto essere requisito necessario quello della novità delle applicazioni industriali.

La tutela attraverso la disciplina del diritto d'autore

2.1. Le disposizioni principali

La tutela giuridica dei programmi per elaboratore, in Italia, è stata sancita dal decreto legislativo 29 dicembre 1992, numero 518 **http://www.innovazione.gov.it/ita/intervento/normativa/allegati/dl_291292.pdf** attuativo della direttiva 91/250/Cee.
http://www.innovazione.gov.it/ita/intervento/normativa/allegati/dir_140591.pdf
Già in precedenza, la Corte di cassazione si era pronunciata sull'argomento, con la decisione del 6 febbraio 1987, numero 1956, riconoscendo il *software* tutelabile attraverso la disciplina del diritto d'autore.
Il decreto legislativo 518/92 modifica ed integra la disciplina sul diritto d'autore, dettata dalla legge 633/1941.
Il corpo normativo di riferimento è dunque costituito dalla legge sul **diritto d'autore** , legge 633 del 1941 **http://www.giustizia.it/cassazione/leggi/l633_41.html**, mentre le principali integrazioni sono costituite dal decreto legislativo 518/92 e dalla legge 18 agosto 2000, numero 248

http://www.beniculturali.it/normative/dettaglioleggidecreti.asp?Id=418

2.2. L'oggetto della tutela

Oggetto di tutela, in base al diritto d'autore, è soltanto la forma espressiva del programma, non l'idea in esso contenuta.
http://www.giustizia.it/cassazione/leggi/l633_41.html#ART1,
http://www.giustizia.it/cassazione/leggi/l633_41.html#ART2.
Questa tutela limitata corrisponde ad una precisa scelta operata in sede comunitaria a favore della disciplina sul diritto d'autore, con la quale si è ritenuto di non arrestare il progresso tecnologico e scientifico, consentendo la diffusione di algoritmi e principi, ma si è altresì ritenuto di proteggere il singolo programma creato sulla base di quei principi.
I programmi per elaboratore, in qualsiasi forma espressi, e il materiale preparatorio per la progettazione del programma sono ora espressamente menzionati fra le opere protette ai sensi della legge italiana sul diritto d'autore.
I programmi sono tutelati purché originali quali risultato di creazione intellettuale dell'autore. Il grado di creatività richiesto non è precisato dalla legge, ma la giurisprudenza italiana aveva già avuto modo di pronunciarsi in argomento, prima dell'emanazione del decreto legislativo 518/92. In particolare, la Pretura di Pisa con la decisione dell'11 aprile 1984 aveva ritenuto applicabile la tutela accordata dalla legge sul diritto d'autore al programma per elaboratore che si caratterizzi per un proprio 'stile' sostanzialmente originale rispetto ad altri prodotti analoghi e per una determinata forma espressiva nella quale il contenuto di tale programma si traduce.
La Corte di cassazione, con la decisione del 6 febbraio 1987, numero 1956, soffermandosi sui requisiti minimi di creatività del *software* precisava che: L'autore del *software* in tanto produce un risultato creativo in quanto dia apporti nuovi in campo informatico, esprima soluzioni originali ai problemi di elaborazione dati, programmi in modo migliore rispetto al passato determinati contenuti di idee, seppure in misura appena apprezzabile.
Le disposizioni normative non si applicano alle idee e ai principi che stanno alla base del programma, né a quelli che stanno alla base delle sue interfacce. Come, per esempio, ha già avuto modo di affermare la giurisprudenza statunitense, che ha visto contrapposte *Apple* e *Microsoft*, l'interfaccia uomo-macchina di un programma o di un sistema operativo non trovano alcuna tutela giuridica.
Non sono protetti, inoltre, le idee e i principi che stanno alla base della logica, degli algoritmi e dei linguaggi di programmazione.
Il decreto legislativo 29 dicembre 1992, numero 518 non tutela espressamente i manuali, ma la giurisprudenza precedente al decreto legislativo si era già pronunciata in tal senso.

2.3. Durata

Secondo il decreto legislativo 518/92, le disposizioni dello stesso decreto si applicano anche ai programmi creati prima della sua entrata in vigore.
La durata della tutela è di tutta la vita dell'autore e di 70 anni dalla sua morte.
http://www.giustizia.it/cassazione/leggi/l633_41.html#ART24.
Se il programma è un'opera collettiva, la durata della tutela è di 70 anni dalla prima pubblicazione.
Se il *software* è creato e pubblicato dalla Amministrazione dello Stato la durata è ridotta a 20 anni dalla data di pubblicazione, come dispone l'articolo 29.
http://www.giustizia.it/cassazione/leggi/l633_41.html#ART29

2.4.Contenuto del diritto d'autore

Il diritto d'autore sorge con la creazione dell'opera ed il contenuto di questo diritto è costituito da un complesso di diritti patrimoniali e da un complesso di diritti morali sull'opera. I diritti patrimoniali sull'opera, cioé i diritti di utilizzazione economica, sono costituiti dal diritto di pubblicare l'opera, dal diritto di diffonderla, dal diritto di metterla in commercio, dal diritto di elaborarla e dal diritto di tradurla. I diritti elencati sono diritti relativi all'opera nel suo insieme e in ciascuna delle sue parti e possono essere trasferiti a terzi, anche indipendentemente gli uni dagli altri, ai sensi dell'articolo 19 della legge sul diritto d'autore
http://www.giustizia.it/cassazione/leggi/l633_41.html#ART19.
Il trasferimento dei diritti deve essere provato per iscritto ai sensi dell'articolo 110 della legge sul diritto d'autore. I **diritti morali d'autore** , fra i quali il diritto alla paternità dell'opera, il diritto di non pubblicarla, il diritto di opporsi a modificazioni della stessa sono invece inalienabili.
http://www.giustizia.it/cassazione/leggi/l633_41.html#ART20

Dai diritti morali e patrimoniali sul *software*, in quanto opera dell'ingegno, già menzionati, vanno distinti i diritti sulla singola riproduzione del *software*. In particolare, i diritti di utilizzazione economica del *software* o **diritti patrimoniali d'autore** vanno distinti dal semplice diritto di utilizzazione o di uso del *software*, o meglio, della singola riproduzione di *software*.
Si tratta di due differenti ordini di diritti: quelli aventi ad oggetto il *software* in quanto opera dell'ingegno e quelli aventi ad oggetto il *software* in quanto singola riproduzione. I primi si costituiscono sul *software* considerato opera dell'ingegno (bene immateriale), i secondi si costituiscono sulle singole riproduzioni del *software* (bene materiale).

2.5. Titolarità del diritto d'autore

Il titolare dei diritti di utilizzazione economica del programma è l'autore dello stesso. Assai di frequente, tuttavia, gli autori cedono preventivamente i diritti patrimoniali.
Secondo il decreto legislativo 518/92, nel caso in cui l'autore sia un lavoratore dipendente, i diritti di utilizzazione economica del *software* spettano al datore di lavoro, a meno che non sia stato diversamente pattuito. Problemi più complessi si pongono per i diritti di utilizzazione economica del *software* sviluppato da programmatori che siano lavoratori autonomi, sulla base di un **contratto di sviluppo di *software*** .
Nel caso in cui il *software* sia creato dalla pubblica amministrazione o per la pubblica amministrazione si applicano disposizioni particolari, dettate dal decreto legislativo numero 39 del 12 febbraio 1993 **http://www.aipa.it/servizi%5B3/normativa%5B4/leggi%5B1/DLGV39_93.asp**.
Il diritto d'autore sorge, automaticamente, nel momento della creazione del programma. La prova del diritto, cioé la prova che il programma è stato sviluppato da un soggetto, piuttosto che da un altro, può essere fornita mediante il deposito del programma presso l'apposito registro pubblico speciale per i programmi per elaboratore, costituito presso la SIAE. In questo registro viene registrato il nome del titolare dei diritti esclusivi di utilizzazione economica e la data di pubblicazione del programma, intendendosi per pubblicazione il primo atto di esercizio dei diritti esclusivi. Il suddetto registro è stato istituito dal decreto legislativo 518/92 ed è stato regolamentato con il d.p.c.m. 3 gennaio 1994, con il quale sono state determinate le caratteristiche del registro, le modalità di registrazione e le relative tariffe.
La registrazione del programma presso la SIAE comporta l'inversione dell'onere della prova, cioé facilita la prova della titolarità del diritto, poiché si presume che il soggetto che ha registrato il programma ne sia l'autore.
http://www.siae.it.

2.6. I diritti di utilizzazione economica

Secondo il decreto legislativo 518/92 http://www.giustizia.it/cassazione/leggi/l633_41.html#ART64BIS, l'autore o il titolare dei diritti di utilizzazione economica dell'opera ha il diritto esclusivo di effettuare:

- la riproduzione del *software* permanente o temporanea, totale o parziale;
- la traduzione, l'adattamento, la trasformazione e ogni altra modificazione del programma;
- qualsiasi forma di distribuzione al pubblico.

Il legittimo acquirente, invece, può:

- riprodurre il programma e tradurre, adattare o trasformare il programma solo se tali attività sono necessarie per l'uso del programma conformemente alla sua destinazione, inclusa la correzione degli errori;
- effettuare una copia di riserva del programma, qualora tale copia sia necessaria per l'uso;
- osservare, studiare o sottoporre a prova di funzionamento il programma.

http://www.giustizia.it/cassazione/leggi/l633_41.html#ART64TER

2.7. Il *reverse engineering*

Un'altra importante deroga operata dalla direttiva e quindi dalla legge italiana ai diritti esclusivi dell'autore del programma è costituita dalla disposizione relativa alla decompilazione o *reverse engineering*, cioé alla possibilità di scomporre un programma al fine di ottenere le informazioni necessarie per conseguirne l'interoperabilità con altri programmi. **http://www.giustizia.it/cassazione/leggi/l633_41.html#ART64QUATER**

Il decreto legislativo stabilisce che non è necessaria l'autorizzazione dell'autore del programma per gli atti di traduzione del codice e di riproduzione della sua forma, quando tali atti siano indispensabili per ottenere le informazioni necessarie per conseguire l'interoperabilità di un programma, creato autonomamente, con altri programmi. Devono concorrere tuttavia alcune condizioni: che gli atti siano compiuti dal licenziatario o da altra persona avente diritto, che le informazioni non siano già facilmente accessibili e che gli atti siano limitati alle parti del programma originale, necessarie per conseguire l'interoperabilità. Non è consentita l'utilizzazione delle informazioni così ricavate a fini diversi, né la comunicazione delle informazioni a terzi, né la loro utilizzazione per lo sviluppo, la produzione o la commercializzazione di programmi sostanzialmente simili o per altri atti che violino il diritto d'autore. Come norma di chiusura, viene stabilito che le disposizioni relative alla decompilazione non possono essere interpretate in modo da consentire che la loro applicazione rechi indebitamente pregiudizio agli interessi del titolare del diritto o entri in conflitto con il normale impiego del programma.

2.8. Misure cautelari e sanzioni

La violazione delle disposizioni del decreto legislativo 518/92 consente il ricorso a misure cautelari e comporta l'applicazione di sanzioni civili e penali, disposte dallo stesso decreto legislativo, oltre che dalla legge sul diritto d'autore.
I provvedimenti che possono essere ordinati dall'autorità giudiziaria prima dell'emanazione della sentenza definitiva, secondo la legge sul diritto d'autore, sono:

- la descrizione (articolo 161 l. d. a.)
- la perizia (articolo 161 l. d. a.)
- il sequestro (articolo 161 l. d. a.)
- il sequestro dei proventi (articolo 161 l. d. a.)

http://www.giustizia.it/cassazione/leggi/l633_41.html#ART161
Descrizione e sequestro di programmi e manuali sono già stati disposti dalla giurisprudenza italiana inaudita altera parte.
La giurisprudenza italiana ha inoltre accolto domande di provvedimenti d'urgenza ex articolo 700 c.p.c. e di reintegrazione possessoria.
I provvedimenti definitivi che possono essere adottati dall'autorità giudiziaria, secondo la legge sul diritto d'autore, sono, oltre all'accertamento del diritto:

- la rimozione o distruzione degli esemplari frutto dell'attività illegittima (articolo 158 l. d. a.)
- il risarcimento del danno (articolo 158 l. d. a.)
- la pubblicazione della sentenza (articolo 166 l. d. a.)

Le sanzioni penali secondo l'articolo 171 della legge sul diritto d'autore
http://www.giustizia.it/cassazione/leggi/l633_41.html#ART171, sono costituite dalla multa da L.100.000 a L. 4.000.000 per chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma:

- riproduce, (...), diffonde,(...) un'opera altrui;
- ...
- riproduce un numero di esemplari (...) maggiore di quello che aveva diritto di riprodurre.

Rientra in questa fattispecie il caso di colui che copia il *software* per uso personale.
http://www.giustizia.it/cassazione/leggi/l633_41.html#ART171-BIS
L'articolo 171 bis della legge sul diritto d'autore, introdotto dal decreto legislativo 518/92, e modificato anche dalla legge 248/2000 dispone che chiunque abusivamente duplica per trarne profitto programmi per elaboratore, o, ai medesimi fini, importa, distribuisce, vende, detiene a scopo commerciale, o concede in locazione programmi non contrassegnati dalla SIAE è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da L. 5.000.000 a L. 30.000.000 (...)
Il decreto legislativo individua due fattispecie. Gli elementi costitutivi della prima fattispecie sono:

- l'abusiva duplicazione e

- il fine di profitto

Rientra in questa fattispecie, per esempio, il caso della riproduzione del *software* in ambito professionale.
Gli elementi costitutivi della seconda fattispecie sono:

- il fine di profitto e
- il compimento di atti di commercializzazione.

Rientra in questa fattispecie, per esempio, il caso del rivenditore di *software* copiato.
La sanzione prevista è costituita dalla pena della reclusione da tre mesi a tre anni e della multa da L. 5.000.000 a L. 30.000.000.
La stessa pena si applica se il fatto concerne i cosiddetti copiatori, se unicamente intesi a consentire o facilitare la rimozione arbitraria o l'elusione funzionale dei dispositivi applicati a protezione del *software*.
La pena non è inferiore a due anni di reclusione e la multa a L.30.000.000 se il fatto è di rilevante gravità o se il programma è stato precedentemente distribuito, venduto o concesso in locazione su supporti contrassegnati dalla SIAE.

Il contratto di licenza d'uso

Il decreto legislativo detta soltanto le norme generali.
Ampio margine è lasciato alla contrattazione fra l'utilizzatore del *software* e il soggetto che detiene i diritti di utilizzazione economica del *software* (l'autore del programma o l'impresa produttrice di *software* alla quale l'autore ha ceduto i propri diritti).
Il contratto che in dettaglio regolamenta i diritti e i doveri dell'acquirente e dell'utilizzatore di *software* è il **contratto di licenza d'uso** . Questo contratto è un contratto atipico, cioé non regolamentato dal codice civile, e la definizione del contenuto contrattuale è lasciata all'autonomia delle parti contraenti, le quali possono definire i reciproci diritti e doveri a loro discrezione.
Infatti, il mercato offre una grande varietà di contratti, di tipi di licenze, di prezzi, di obblighi e anche di programmi. Pertanto, non si può dare una definizione unitaria dei programmi per elaboratori esistenti né si possono definire tutti i tipi di programmi esistenti, ma si può soltanto fornire una descrizione delle tipologie più diffuse.
Ad esempio, per stabilire se una duplicazione è abusiva o meno, occorre far riferimento al contratto.
Solitamente i contratti di licenza d'uso (cioé i contratti per comprare il programma) limitano l'utilizzo del *software* ad una sola macchina per volta e talvolta la macchina è espressamente individuata nella documentazione contrattuale.
Alcuni contratti di licenza d'uso, tuttavia, consentono la riproduzione del programma su un certo numero di macchine.
In genere i contratti standard di licenza d'uso non consentono l'utilizzazione di un programma da più macchine fra loro collegate in rete. Tuttavia, è possibile stipulare contratti di licenza d'uso che consentano di utilizzare il programma su più macchine o in rete (licenze multiple; a *forfait*; *floating license*, cioé licenze per utilizzare i programmi in rete ma da un numero di utenti prefissato) o inserire in contratto clausole ad hoc.

3.1. *Open software*

Il titolare dei diritti di utilizzazione economica del *software* può rinunciare ad essi e mettere a disposizioni del pubblico il programma, compreso il codice sorgente, senza richiedere un compenso. La rinuncia ad un diritto è una particolare modalità di esercizio di quel diritto. Sulla base di questo principio si è diffuso il cosiddetto *open software*, che consiste di programmi che sono disponibili sia all'utilizzo che alla modifica da parte di soggetti diversi dall'autore.
Il contratto di licenza d'uso per *open software* più diffuso è costituito dal contratto GNU
http://www.gnu.org/licenses/licenses.html

3.2. Licenza a strappo

Un particolare contratto di licenza d'uso è costituito dal cosiddetto contratto a strappo o **contratto di licenza a strappo**, *shrink-wrap license*, nell'originaria formulazione statunitense.
In questo caso, il programma è confezionato in un involucro, sul quale sono stampate o attraverso il quale è possibile leggere le condizioni contrattuali. L'apertura dell'involucro costituisce accettazione delle condizioni contrattuali predisposte dal produttore. Le condizioni d'uso del programma sono quelle dei contratti di licenza d'uso più diffusi

(uso del programma limitato ad una sola macchina, restrizioni alla possibilità di effettuare copie, garanzia limitata ai soli difetti del supporto materiale, esclusione di altre garanzie e responsabilità). L'acquirente che non intenda accettare il regolamento contrattuale può restituire il prodotto e richiedere la restituzione del prezzo pagato, purché non abbia aperto la confezione. In genere, viene richiesto all'acquirente di compilare e spedire al produttore una cartolina che gli consente di ricevere gli aggiornamenti del *software* e di usufruire delle limitate prestazioni di garanzia accordate dal contratto. La spedizione della cartolina costituisce espressa accettazione del regolamento contrattuale.
Il contratto di licenza a strappo si perfeziona, dunque, con l'atto dell'apertura della confezione. Tale atto vale come accettazione.
L'articolo 1341 c.c. stabilisce che le condizioni generali di contratto predisposte da una parte sono valide nei confronti dell'altra se conoscibili da questa al momento della conclusione del contratto. Dunque, se il regolamento contrattuale è leggibile al momento della conclusione del contratto le condizioni generali di contratto sono da ritenersi valide. L'effettiva conoscenza di esso non ha alcuna rilevanza per il nostro ordinamento, così come non ha alcuna rilevanza l'effettiva conoscenza delle clausole contrattuali al momento della conclusione di un contratto di trasporto, di banca o di assicurazione, eccetera.
Il regolamento contrattuale è da ritenersi accettato al momento della conclusione del contratto, sempre che esso fosse conoscibile. Perché si possa considerare conoscibile è necessario che le condizioni generali di contratto siano inserite nella confezione in modo da essere visibili e leggibili dall'esterno, al momento della conclusione del contratto, come prescrive l'articolo 1341 c.c.
Non hanno invece alcun effetto le clausole vessatorie presenti nel contratto, che devono essere specificatamente approvate per iscritto ai sensi dell'articolo 1341, secondo comma.
Quindi quelle clausole, spesso presenti nei contratti standard di licenza d'uso, che stabiliscono limitazioni di responsabilità, restrizioni alla libertà contrattuale nei rapporti con i terzi e deroghe alla competenza dell'autorità giudiziaria devono considerarsi inefficaci.

3.3. *Software freeware* e *shareware*

Il *software freeware* è *software* distribuito gratuitamente, generalmente in rete, e può essere copiato da chiunque si colleghi con la rete. In genere, reca la scritta *freeware* e il nome dell'autore. Talvolta viene specificato che il programma può essere liberamente copiato, altre volte si invita l'utente ad inviare osservazioni e commenti all'indirizzo specificato.
In questo caso, è evidente la rinuncia da parte dell'autore ai propri diritti di utilizzazione economica dell'opera, quindi il *software freeware* può essere liberamente copiato.
Il *software shareware* presenta molte delle caratteristiche del *software freeware*: è *software* distribuito in rete e può essere copiato da chiunque si colleghi con la rete. In genere, reca la scritta *shareware* e il nome dell'autore.
A differenza che nel *software freeware*, nel *software shareware* si invita l'utente ad inviare un corrispettivo, in genere piuttosto basso, all'indirizzo specificato. Talvolta si precisa che il pagamento del corrispettivo dà diritto agli aggiornamenti del programma.
In questo caso, non si può ritenere che l'autore abbia rinunciato ai propri diritti di utilizzazione economica dell'opera: si tratta di un contratto di licenza d'uso di *software* in cui la distribuzione è effettuata mediante rete e in forme particolari. Pertanto, deve essere corrisposto all'autore il compenso richiesto. Occorre comunque precisare che per una serie di considerazioni di carattere pratico (in genere si tratta di programmi di modesta rilevanza economica; in genere si tratta di programmi distribuiti dallo stesso autore e non da un'impresa produttrice, e in genere l'autore è straniero) non è molto probabile un'azione legale da parte dell'autore.

Alcuni casi particolari di utilizzo di software nelle scuole

Si illustrano di seguito alcuni casi particolari di utilizzo di *software* nelle scuole, sulla base di alcuni quesiti già posti in passato.

4.1. *Software* donato da un rivenditore

Per le donazioni future si consiglia di acquisire documentazione scritta, ad esempio una lettera del rivenditore.
Se in passato è stato donato *software* originale (dischetti originali e manuali d'uso originali) ma non c'è documentazione che provi la donazione, la prova della legittima detenzione del *software* sarà costituita dall'originalità

del materiale detenuto.
Infine, nel caso in cui il *software* donato dal rivenditore sia una copia, non si sarà passibili di sanzioni solo se si potrà dimostrare che la copia era stata effettuata dal rivenditore.

4.2. *Software* donato da un insegnante

Si consiglia di fare riferimento al contratto di comodato (prestito) con il quale, in questa circostanza, l'insegnante presta alla scuola il programma, a titolo gratuito. Anche in questo caso è opportuno acquisire documentazione scritta, ad esempio una lettera dell'insegnante.
Il contratto di comodato è lecito se non è vietato dal **contratto di licenza d'uso** del programma, che occorre controllare.

4.3. *Software* fuori commercio

Se il *software* è detenuto in buona fede da più di dieci anni prima dell'entrata in vigore del decreto legislativo 518/92, deve ritenersene acquisito il diritto di uso.
Se, invece, non è trascorso tale periodo di tempo, il *software* è detenuto irregolarmente. In questo caso, la situazione può essere sanata mediante gli opportuni contatti con la casa produttrice, anche se è meno probabile che quest'ultima promuova un'azione legale.

4.4. *Software* sviluppato da un insegnante

Nel caso in cui un insegnante abbia sviluppato un programma, detto programma è tutelato dalla disciplina della legge sul **diritto d'autore** , modificata dal decreto legislativo 518/92, sopra illustrato.
Il diritto d'autore sorge, automaticamente, nel momento della creazione del programma. La prova di tale diritto, cioé la prova che il programma è stato sviluppato da un certo insegnante, piuttosto che da un altro, può essere fornita mediante il deposito del programma presso l'apposito registro pubblico speciale per i programmi per elaboratore, costituito presso la SIAE.
La registrazione del programma presso la SIAE comporta l'inversione dell'onere della prova, cioé facilita la prova della titolarità del diritto, poiché si presume che il soggetto che ha registrato il programma ne sia l'autore. La registrazione presso la SIAE non è, tuttavia, l'unico mezzo di prova.
L'autore del *software*, se non ha ceduto ad altri i diritti di utilizzazione economica del programma (ad esempio ad un'impresa produttrice di *software*), ha la piena disponibilità di tali diritti e quindi può distribuire gratuitamente il programma, conservando il diritto morale d'autore, cioé il diritto di essere riconosciuto autore dell'opera.

La tutela giuridica delle banche di dati e delle opere multimediali

La tutela giuridica delle banche dati è oggetto di una specifica direttiva comunitaria, la direttiva 96/9/CE, attuata in Italia con il decreto legislativo 6 maggio 1999, numero 169
http://www.parlamento.it/parlam/leggi/deleghe/99169dl.htm, il quale ha modificato la legge sul **diritto d'autore** (legge 22 aprile 1941, numero 633).
La creazione di una banca dati comporta generalmente un notevole investimento in termini di risorse economiche e di ricerca: le attività necessarie vanno dal reperimento dei dati e delle informazioni, alla loro organizzazione in maniera sistematica e agevole per la consultazione.
Questo investimento è minacciato dal fatto che, una volta costituita la banca dati, una copia delle informazioni e dei dati in essa contenuti può essere agevolmente effettuata, anche allo scopo di costituire una nuova banca dati.
Qual è la tutela giuridica della banca dati?
Il singolo dato o la singola informazione, cioé l'elemento che costituisce la banca dati, non è suscettibile di tutela: nella fattispecie, non è configurabile un diritto che tuteli chi ha raccolto delle informazioni per il solo fatto di averle raccolte (diverso e complementare problema è quello della tutela del soggetto al quale le informazioni si riferiscono).
È, invece, tutelabile giuridicamente la banca dati nel suo complesso, in quanto raccolta di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili grazie a mezzi elettronici o in altro modo, come oggi dispone l'articolo 2 della legge sul diritto d'autore
http://www.giustizia.it/cassazione/leggi/l633_41.html#ART2.
L'ordinamento italiano non prevedeva, fino al decreto legislativo 169/99 una tutela giuridica specifica delle banche

dati.
In altri ordinamenti, le banche di dati erano già espressamente incluse nell'ambito di applicazione della disciplina del diritto d'autore oppure la loro protezione giuridica era realizzata mediante una specifica disciplina.
Nel nostro ordinamento, la principale forma di tutela praticabile era ed è ancora costituita dall'applicazione della disciplina sul diritto d'autore (in questi senso è la decisione della Pretura di Roma del 14 dicembre 1989). Essa, tuttavia, presuppone l'originalità dell'opera, con riguardo alla sua particolare struttura, e questo requisito non sempre è proprio della banca dati, la quale può essere piuttosto qualificata dalla completezza, nonché dalla qualità e dalla tipologia di informazioni in essa contenute (si pensi, ad esempio alle raccolte di giurisprudenza su CD-ROM).
Un altro strumento di tutela delle banche dati previsto dall'ordinamento italiano è costituito dalle disposizioni a tutela della concorrenza, che tuttavia rivelano altre difficoltà di applicazione.
Una particolare forma di tutela, nuova per l'ordinamento italiano, ma non per quelli di altri Paesi, è quella introdotta dalla direttiva sulla tutela giuridica delle banche dati e dal decreto attuativo.
La direttiva introduce, infatti, un **diritto sui generis** a favore del creatore della banca dati, che consiste nel diritto di vietare operazioni di estrazione e/o reimpiego della totalità o di una parte sostanziale del contenuto della stessa.
Questo diritto ha la durata di quindici anni e sorge con la costituzione della banca dati ed è analiticamente disciplinato dall'articolo 102-bis della legge sul diritto d'autore.
L'esistenza del diritto sui generis fa salvi il diritto d'autore sulla banca dati, ove configurabile, e i diritti sulle opere facenti parte della banca dati, nonché i diritti sul *software* utilizzato per l'impostazione o il funzionamento della banca dati.
Sono nulle le disposizioni contrattuali che impediscano al legittimo utente della banca dati di estrarre e reimpiegare parti non sostanziali della banca dati, valutate in termini quantitativi e qualitativi o che non gli consentano l'impiego normale della banca dati, ai sensi dell'102-ter della legge sul diritto d'autore.
Soluzioni analoghe a quelle sopra prospettate trovano, nel nostro ordinamento, il problema della tutela giuridica delle opere multimediali, che tuttavia non sono oggetto di autonoma definizione legislativa.
Un'opera multimediale può essere definita come un'opera costituita dalla combinazione di diversi contenuti: testo, grafica, illustrazioni, filmati, animazioni, fotografia, musica, eccetera. L'opera può essere distribuita su CD-ROM o *on line*.
I contenuti dell'opera multimediale sono fra loro collegati mediante un particolare schema logico, ideato dall'autore, che costituisce la peculiare struttura e organizzazione interna dell'opera.
I contenuti dell'opera multimediale, cioé il testo, la grafica, le illustrazioni, la fotografia, costituiscono, a loro volta, opere o parti di opere.
Sotto il profilo giuridico, si possono individuare quantomeno i seguenti beni da tutelare:

- l'opera multimediale, integralmente considerata, caratterizzata dalla peculiare struttura e organizzazione interna dell'opera
- le opere o le parti di opere che ne fanno parte
- il *software* strumentale alla fruizione dell'opera.

Le opere o le parti di opere che fanno parte dell'opera multimediale, nonché il *software* strumentale alla fruizione dell'opera sono tutelati attraverso la disciplina del diritto d'autore, secondo i limiti e le modalità specificamente previsti dalla legge per ciascuno di essi (ad esempio, per la protezione del *software* troverà applicazione la legge sul diritto d'autore, come modificata dal decreto legislativo 518/92).
Per tutelare l'opera multimediale nel suo complesso e, quindi, la peculiare struttura dell'opera, invece, potrà applicarsi la disciplina del diritto d'autore, ma dovrà essere soddisfatto il requisito del carattere creativo dell'opera. Inoltre, come risulta dalle concrete applicazioni della legge a tutela del *software*, la protezione giuridica conseguita attraverso la disciplina sul diritto d'autore è piuttosto fragile.
Si consideri, inoltre, l'ulteriore elemento di complessità rappresentato dal fatto che il diritto d'autore è costituito da un fascio di diritti che, nel caso di opera multimediale, insiste su beni soggetti, per loro stessa natura, a continue modificazioni.
I diritti d'autore sull'opera multimediale sono dunque costituiti dal diritto dell'autore dell'opera multimediale, dai diritti degli autori delle opere che ne fanno parte, dal diritto dell'autore del *software*. Ognuno di questi soggetti è titolare di un insieme di diritti morali e patrimoniali, fra i quali: il diritto di opporsi a modificazioni dell'opera, il diritto di distribuzione dell'opera, il diritto di rielaborare l'opera, il diritto di modificare l'opera e il diritto di tradurla.
Inoltre, può verificarsi che sulle opere insistano altre privative come il **brevetto** o il marchio.
In questo quadro di grande complessità si delineano chiaramente alcuni interessi contrapposti.
Innanzitutto, il diritto del produttore dell'opera che ha effettuato un notevole investimento in termini di risorse

umane, finanziarie e tecnologiche.
In secondo luogo, il diritto dell'autore dell'opera multimediale, cioé il diritto di chi ha organizzato l'opera con una particolare struttura e ha creato i collegamenti all'interno di essa.
In terzo luogo, i diritti degli autori e dei produttori delle opere contenute nell'opera multimediale, nonché i diritti dell'autore del *software*.
Mentre questi ultimi appaiono, prima facie, riconducibili a schemi noti nell'ambito della disciplina sul diritto d'autore, seppure di notevole complessità quanto alla loro gestione in sede contrattuale e assai problematici quanto alla definizione degli accordi di licenza, gli altri diritti sono definiti dalla tutela giuridica delle banche di dati.
Si contrappongono agli interessi di protezione giuridica dell'opera, considerati nel loro insieme, gli interessi dei potenziali concorrenti, cioé di quei soggetti che volendo produrre un'opera analoga, sono contrari alla definizione di una privativa.
Si contrappone, inoltre, agli interessi di protezione giuridica dell'opera, l'interesse del potenziale utilizzatore del singolo esemplare dell' **opera dell'ingegno** , il quale aspira ad un ampio raggio di facoltà.
La problematica è affrontata dal decreto legislativo 169/99, già ricordato. Nell'ampia definizione recata dalla legge sul diritto d'autore di banca dati come raccolta di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili grazie a mezzi elettronici o in altro modo pare essere compresa anche l'opera multimediale.
Si configura, quindi, a protezione del creatore dell'opera, accanto alla tutela già prevista dal diritto d'autore, un diritto sui generis volto ad impedire l'estrazione e/o il reimpiego non autorizzati della totalità o di una parte sostanziale del contenuto della banca dati.
Il legislatore italiano ha per la prima volta utilizzato il termine multimediale nella recente legge 248/2000 che ha apportato nuove modifiche alla legge sul diritto d'autore. Con la legge citata sono state introdotte o inasprite le sanzioni penali a tutela delle banche dati e delle opere multimediali.
Ha recentemente arricchito lo scenario la direttiva 2001/29/CE sull'armonizzazione di alcuni aspetti del diritto d'autore e diritti connessi **http://www.innovazione.gov.it/ita/intervento/normativa/allegati/dir_220501.pdf**.

La tutela della privacy

Prof. Avv. Giusella Finocchiaro

1.4.4. (Identificare e discutere aspetti relativi alla privacy)

Il quadro normativo italiano

1.1. La cosiddetta legge sulla *privacy*

La più importante legge italiana in materia di *privacy* è la legge 31 dicembre 1996, numero 675, Tutela delle persone e di altri soggetti rispetto al **trattamento** dei dati personali [**Legge num. 675**1] , più nota come legge sulla *privacy*, la quale attua la direttiva comunitaria 95/46/CE del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati [**Direttiva 95/46/CE**2] .
È bene chiarire subito che la legge 675/96 - come meglio si vedrà esaminando le definizioni di **dato personale** e di trattamento già richiamate nel titolo - non disciplina soltanto la *privacy*, cioè i dati riservati, ma piuttosto il trattamento dei dati personali, cioè la circolazione delle informazioni, siano esse riservate o meno.
La legge 675/96 costituisce l'adempimento di altri obblighi internazionali da parte dell'Italia, fra i quali quelli derivanti dall'Accordo di *Schengen* e quelli derivanti dalla Convenzione del Consiglio d'Europa sulla Protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981.

1 Pubblicata nel Supplemento Ordinario alla Gazzetta Ufficiale numero 5 dell'8 gennaio 1997.
2 Pubblicata in G.U.C.E. numero L 281/31 del 23 novembre 1995.

1.2. Le disposizioni successive

La legge 675/96 è stata integrata e modificata da molte altre disposizioni normative, cosicché è in corso di predisposizione un Testo Unico sulla *privacy*.
Fra le più importanti disposizioni normative che hanno integrato la legge 675/96, si ricordano: il decreto legislativo 9 maggio 1997, numero 123 che ha introdotto la possibilità del consenso in forma orale; il decreto legislativo 28 luglio 1997, numero 255 concernente l'esonero e le semplificazioni delle notificazioni; il decreto legislativo 11 maggio 1999, numero 135, sulle disposizioni in materia di trattamento di dati particolari da parte di soggetti pubblici; il decreto

legislativo 30 luglio 1999, numero 281 sul trattamento dei dati per finalità storiche, statistiche e di ricerca scientifica; il decreto legislativo 30 luglio 1999, numero 282, sul trattamento dei dati per garantire la riservatezza in ambito sanitario; il d.p.r. 31 marzo 1998, numero 501, sul funzionamento dell'ufficio del Garante che reca anche norme che disciplinano l'accesso ai dati personali; il decreto legislativo 13 maggio 1998, numero 171, recante disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni; il d.p.r. 28 luglio 1999, numero 318, sull'individuazione delle **misure minime di sicurezza** ; il decreto legislativo 28 dicembre 2001, numero 467, disposizioni correttive ed integrative della normativa in materia di protezione dei dati personali. A ciò si aggiungano le autorizzazioni generali in materia di trattamento dei **dati sensibili** .
Tutte le norme citate, nonché il testo consolidato della legge 675/96 possono essere reperiti nel sito ufficiale del Garante per il trattamento dei dati personali: **http://www.garanteprivacy.it**.

Ambito di applicazione

La legge 675/96 prevede che le disposizioni in essa contenute siano applicabili al **trattamento** di dati personali, come di seguito definito, da chiunque effettuato nel territorio dello Stato.
La legge si applica, dunque, al trattamento di dati svolto con o senza l'ausilio di mezzi elettronici, al trattamento effettuato in Italia di dati detenuti in Italia o all'estero, alle banche di dati pubbliche e alle banche di dati private.
Non rientra nel campo di applicazione della legge, se non limitatamente, il trattamento di dati personali effettuato da persone fisiche a fini esclusivamente personali, sempre che i dati non siano destinati alla **comunicazione** sistematica o alla **diffusione** . È il caso, ad esempio, della rubrica personale, della quale non deve essere notificata la costituzione, ma che deve essere custodita conformemente alle disposizioni legislative in materia di sicurezza, come dispone l'articolo 3 della legge 675/96 [**Articolo 3**].
È prevista, inoltre, l'esclusione di particolari trattamenti dall'ambito di applicazione della legge, come, ad esempio, del trattamento dei dati coperti da segreto di Stato o del trattamento dei dati effettuato dagli uffici giudiziari.

Definizioni

La legge fornisce alcune definizioni, indispensabili alla comprensione dell'articolato, contenute nell'articolo 1 [**Articolo 1**].

3.1. I dati

Una banca di dati è qualsiasi complesso di dati personali, ripartito in una o più unità dislocate in uno o più siti, organizzato secondo una pluralità di criteri determinati tali da facilitarne il **trattamento** . Una banca di dati può essere unica, quindi, anche se articolata in più sedi.
È amplissima la definizione di **dato personale** che designa qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
Il dato personale è, quindi, qualunque informazione riferibile a qualunque soggetto.
Il dato personale non è necessariamente un dato riservato.
Sono, invece, esclusi dall'ambito di applicazione della legge i **dati anonimi** . È definito dato anonimo il dato che in origine, o a seguito di trattamento, non può essere associato a un **interessato** identificato o identificabile.
Si tratta del dato privo di nome e cognome, ma anche privo di ogni riferimento indiretto al soggetto cui si riferisce: privo, ad esempio di riferimento ad un codice o ad un numero identificativo, quale il numero d'ordine nel registro.

3.2. Le operazioni sui dati

La legge sulla *privacy* si applica indifferentemente al trattamento di dati con mezzi informatici e al trattamento di dati effettuato con altri mezzi, ad esempio cartacei. Riguarda, dunque, i dati in rete così come i dati contenuti negli archivi o nei registri cartacei.
Il trattamento dei dati consiste in qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la **comunicazione** , la **diffusione** , la cancellazione e la distruzione di dati. La definizione di trattamento

comprende, in sostanza, qualunque operazione effettuata, con o senza mezzi automatizzati, sui dati.
La legge italiana disciplina specificamente, nell'ambito del trattamento dei dati, la comunicazione e la diffusione dei dati.
Per comunicazione si intende il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione: è il caso di un'informazione resa, per esempio, dall'insegnante ad un genitore.
Per diffusione si intende il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione: è il caso, ad esempio, della pubblicazione dei risultati degli scrutini mediante affissione in bacheca [**Pubblicazione dei risultati degli scrutini**] [**Pubblicazione esiti scrutini non viola la *privacy***], oppure della pubblicazione di informazioni su Internet, nel sito dell'istituto scolastico.

Dati sensibili

La legge in esame, in linea con le disposizioni dalla direttiva comunitaria, ha previsto regole particolari in relazione ai cosiddetti **dati sensibili** cioè ai dati che riguardano più da vicino la personalità etico-sociale dell'individuo e le sue caratteristiche psico-sanitarie, secondo la definizione contenuta nella Relazione al disegno di legge.
Sono definiti dati sensibili i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale [**Dati sensibili**]. Il trattamento illecito di questi dati è potenzialmente idoneo a recare un più grave pregiudizio alla persona alla quale i dati si riferiscono.
Il **trattamento** dei dati sensibili da parte di soggetti pubblici, esclusi gli enti pubblici economici, è consentito solo se autorizzato da espressa disposizione di legge nella quale siano specificati i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite.
Una particolare disciplina è prevista per i dati inerenti alla salute.

L'organizzazione

La legge 675/96 ha un forte impatto organizzativo e individua tre figure: **titolare** , **responsabile** e **incaricato** .

5.1. Il titolare

Il titolare è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità e alle modalità del **trattamento** di dati personali, ivi compreso il profilo della sicurezza, come dispone l'articolo 1 [**Articolo 1**].
Si tratta del soggetto che assume le decisioni sulle finalità e sulle modalità del trattamento dei dati.
Titolare del trattamento è l'istituto scolastico e la titolarità è esercitata dal dirigente scolastico.
Con riguardo all'esercizio della titolarità si ricorda il parere espresso dal Garante per la protezione dei dati personali [***Privacy*: chi sono i titolari e i responsabili del trattamento dei dati nelle imprese e nelle amministrazioni pubbliche**].

5.2. Il responsabile/i responsabili

La legge introduce un'altra figura di notevole rilievo, costituita dal responsabile del trattamento. Il responsabile è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali, come dispone l'articolo 1 [**Articolo 1**]. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste.
Il responsabile deve essere un soggetto che fornisce, per esperienza, capacità e affidabilità, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza [**Articolo 1**].
I compiti del responsabile devono essere analiticamente previsti per iscritto e variano di caso in caso.
Il responsabile del trattamento dei dati personali non può che essere espressamente designato: ad esempio, non

potrà considerarsi responsabile del trattamento di dati personali, ai sensi della legge 675/96, senza un atto formale di designazione o di nomina, in cui siano per iscritto elencati i suoi nuovi compiti, il responsabile del sistema informativo di un ente.
È bene ricordare che le decisioni strategiche restano di competenza del titolare, anche se viene nominato un responsabile.
Nella scuola possono essere nominati dei responsabili interni: uno o più docenti, tecnici, responsabili di laboratorio, eccetera.
Ma è opportuno che siano nominati anche dei responsabili esterni se i dati sono trattati da altri soggetti: per esempio, in caso di contratto di *outsourcing*.

5.3. Gli incaricati

Mentre il titolare e il responsabile possono essere anche persone giuridiche, la terza figura individuata dalla legge, cioè l'incaricato del trattamento dei dati, che è la persona incaricata di compiere le operazioni dal titolare del trattamento, è una persona fisica [**Incaricato del trattamento dei dati**].
Negli istituti scolastici dovrebbero essere nominati incaricati di trattamento tutti i soggetti che trattano dati personali: per esempio, tutti i docenti e il personale amministrativo.

Presupposto di legittimità del trattamento dei dati

Il presupposto di legittimità del **trattamento** dei dati è diverso a seconda che il trattamento sia effettuato da soggetti privati o da soggetti pubblici.

6.1. Trattamento effettuato da una scuola privata

Se il trattamento è effettuato da un soggetto privato, la legge richiede che sia espresso il consenso da parte del soggetto al quale i dati si riferiscono: il trattamento nonché la **comunicazione** e la **diffusione** dei dati, da parte di soggetti privati e da parte di enti pubblici economici, sono consentiti solo previo il consenso dell' **interessato** , che deve essere documentato per iscritto, o quando ricorrano alcune circostanze equipollenti al consenso, elencate dall'articolo 12 della legge 675/96 [**Articolo 12**].

6.2. Trattamento effettuato da una scuola pubblica

Se il trattamento è effettuato da un soggetto pubblico, l'ente **titolare** del trattamento dei dati personali non deve richiedere il consenso. Il trattamento è lecito soltanto per lo svolgimento di funzioni istituzionali dell'ente, nei limiti previsti da leggi e regolamenti.
Dunque regole differenti si applicano al trattamento dei dati personali effettuato da parte di una scuola pubblica e di una scuola privata: in particolare, l'istituto scolastico pubblico non è tenuto a richiedere il consenso dello studente per il trattamento dei suoi dati personali.

La comunicazione e la diffusione dei dati

In relazione alla **comunicazione** e alla **diffusione** dei dati, rispettivamente definite, come si ricorderà, dalla legge, il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall' **interessato** , in qualunque forma, anche mediante la loro messa a disposizione o consultazione [**Comunicazione e diffusione a soggetti determinati**] e il dare conoscenza dei dati personali a uno o più soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione [**Comunicazione e diffusione a soggetti indeterminati**], occorre distinguere il caso in cui la comunicazione e la diffusione siano effettuate da un soggetto pubblico e il caso in cui siano effettuate da un soggetto privato.
L' articolo 20 [**Articolo 20**] dispone che per la comunicazione e la diffusione effettuate da parte di soggetti privati o di enti pubblici economici è necessario il consenso espresso dell'interessato, oppure il ricorrere di circostanze equipollenti al consenso.
Invece, l'articolo 27 [**Articolo 27**] dispone che la comunicazione e la diffusione di dati personali da parte di soggetti

pubblici ad altri soggetti pubblici, esclusi gli enti pubblici economici, devono essere previste da norme di legge o di regolamento, o risultare necessarie per lo svolgimento delle funzioni istituzionali. Se la comunicazione e la diffusione di dati non sono previste da normativa specifica, le amministrazioni devono darne comunicazione al Garante, il quale può vietarle.
La comunicazione e la diffusione di dati personali da parte di soggetti pubblici a privati o enti pubblici economici sono consentite solo se previste da disposizioni di legge o di regolamento.
In quest'ultimo caso, i soggetti pubblici non possono genericamente richiamarsi allo svolgimento delle funzioni istituzionali ed è necessario che la comunicazione e la diffusione di dati a soggetti privati siano effettuate attraverso regole espresse e precostituite.
Di conseguenza, le amministrazioni pubbliche non possono in mancanza di specifiche disposizioni legislative o regolamentari, comunicare e diffondere dati a soggetti privati, diversi dal soggetto al quale i dati si riferiscono.

Alcuni casi di comunicazione di dati scolastici

a) Comunicazione di dati per l'orientamento, la formazione e l'inserimento professionale

La comunicazione dei dati concernenti gli esiti scolastici, intermedi e finali, degli studenti e di altri dati personali non sensibili né attinenti a provvedimenti giudiziari, è stata disciplinata dall'articolo 17 del decreto legislativo 30 luglio 1999, numero 281 che ha inserito l'articolo 330 bis nel decreto legislativo 16 aprile 1994, numero 297 [**Articolo 330 bis**]. Ivi si dispone che le scuole e gli istituti scolastici di istruzione secondaria possono comunicare e diffondere i dati sopra menzionati, su richiesta degli interessati, cioè degli studenti, anche a privati e per via telematica, e con la finalità di agevolare l'orientamento, la formazione e l'inserimento professionale.
La scuola che voglia quindi comunicare alle imprese interessate i dati degli studenti per agevolare il loro inserimento nel modo del lavoro ne deve acquisire il consenso.
Se i dati riguardano studenti già diplomati, per i quali tale consenso non può essere acquisito prontamente, i dati possono essere comunicati o diffusi decorsi trenta giorni dalla notizia che le scuole e gli istituti scolastici, ovvero il Ministero rendono nota mediante annunci al pubblico [**Diplomati e mondo del lavoro**].
[**Articolo 17**].
Il nuovo articolo 330 bis ha trovato applicazione anche nel caso di una richiesta presentata ad una scuola da un docente universitario degli elenchi dei diplomati degli anni 1971/72 e 1972/73 per l'effettuazione di una ricerca. Sulla questione specifica si è pronunciato il Garante per la protezione dei dati personali [**Istituto tecnico industriale statale 'Tullio Buzzi' - Parere relativo alla divulgazione di dati personali relativi a diplomati - 1 febbraio 2000**]

b) Comunicazione di dati per la ricerca e la collaborazione in campo scientifico e tecnologico

Va inoltre ricordato che la comunicazione di dati relativi ad attività di studio e di ricerca, a laureati, a docenti, a tecnici, eccetera può essere effettuata dalle pubbliche amministrazioni al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico, come dispone l'articolo 6, quarto comma del decreto legislativo 204/1998 [**Articolo 6**]. Ivi si dispone che al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico le pubbliche amministrazioni, ivi comprese le università e gli enti di ricerca, ferme restando le disposizioni di cui all'articolo 13, comma 1, lettera d, della legge 31 dicembre 1996, numero 675, possono con autonome determinazioni comunicare e diffondere, anche a privati e per via telematica, dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione di quelli sensibili o attinenti a provvedimenti giudiziari, di cui agli articoli 22 e 24 della predetta legge. I dati di cui al presente comma non costituiscono documenti amministrativi ai sensi e per gli effetti di cui agli articoli dal 22 al 27 della legge 7 agosto 1990, numero 241. I predetti dati possono essere successivamente trattati per le sole finalità in base alle quali sono comunicati o diffusi.

c) Pubblicazione dei dati degli esiti degli scrutini

Il Garante ha avuto modo di precisare, in risposta ai quesiti posti da alcuni presidi che la pubblicazione degli esiti degli scrutini non costituisce in alcun modo violazione della normativa a tutela della *privacy* [**Pubblicazione dei risultati degli scrutini**] [**Pubblicazione esiti scrutini non viola la *privacy***].

d) Altri casi

La comunicazione e la diffusione dei dati, da chiunque effettuate, sono comunque permesse nei casi in cui esse siano necessarie per finalità di ricerca scientifica o di statistica e si tratti di dati anonimi o quando siano necessarie per finalità di difesa dello Stato, per la prevenzione, l'accertamento e la repressione di reati [**Comunicazione e diffusione dei dati per finalità di ricerca scientifica o di statistica**].

I diritti dell'interessato

8.1. L'informativa

La legge stabilisce nell'articolo 10 [**Articolo 10**] il diritto dell' **interessato** (nel caso specifico, dello studente) di essere informato.
Per potere validamente prestare il proprio consenso, qualora il consenso sia richiesto, e, in generale, per potere esercitare il controllo, l'interessato deve disporre di alcune informazioni precisate nell'articolato e cioè di informazioni concernenti:

- le finalità e le modalità del **trattamento** cui sono destinati i dati;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto di rispondere;
- i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di **diffusione** dei dati medesimi;
- i diritti che gli sono riconosciuti dalla legge;
- le finalità e le modalità del trattamento;
- il **titolare** e il **responsabile** del trattamento dei dati.

Giova precisare che l'interessato deve essere informato, secondo quanto precisato dall'articolo 10, anche nel caso in cui il suo consenso non sia richiesto: ad esempio, qualora i dati siano raccolti da un soggetto pubblico.
Le informazioni devono essere fornite all'interessato per iscritto, al più tardi al momento della prima **comunicazione** dei dati.

8.2. Il diritto di accesso e di rettifica

I diritti di accesso e di rettifica della persona interessata sono dettagliatamente disciplinati nell'articolo 13 [**Articolo 13**] e si articolano nel diritto dell'interessato di conoscere, mediante accesso gratuito al registro dei trattamenti, tenuto dal Garante, l'esistenza di trattamenti di dati che possano riguardarlo e nel diritto di ricevere le informazioni essenziali sul titolare e sul responsabile del trattamento dei dati, nonché sulle finalità e le modalità del trattamento.
Nei confronti del titolare o del responsabile del trattamento sono riconosciuti all'interessato i seguenti diritti:

- il diritto di ottenere, senza ritardo, la conferma dell'esistenza o meno di trattamenti di dati che lo riguardano, informazioni sui dati e sulla logica del trattamento, nonché di ottenere la comunicazione dei dati;
- il diritto di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge;
- il diritto di rettifica, cioè di integrare, aggiornare e rettificare i dati;
- il diritto di ottenere l'attestazione che le operazioni di cancellazione e di rettifica siano state portate a conoscenza dei terzi;
- il diritto di opporsi, per motivi legittimi, al trattamento dei dati che lo riguardano, ancorché pertinenti allo scopo della raccolta.

Le scuole, come tutti i soggetti titolari di trattamenti di dati personali, devono consentire all'interessato, cioè allo studente, di esercitare i diritti che la legge gli riconosce , anche predisponendo un'organizzazione adeguata.

8.2.1. Modalità di esercizio dei diritti dell'interessato

In generale, il titolare del trattamento dei dati può richiedere all'interessato, ove non risulti confermata l'esistenza di dati che lo riguardano, soltanto un contributo spese non superiore ai costi effettivamente sopportati per l'esercizio dei diritti menzionati, come dispone l'articolo 17 del d.p.r. 31 marzo 1998, numero 501 [**Articolo 17**].
I diritti sopra elencati possono essere esercitati anche da persone fisiche diverse dall'interessato o da associazioni. In relazione ai dati personali concernenti persone decedute, i suddetti diritti possono essere esercitati da chiunque vi abbia interesse.
Le modalità di esercizio dei diritti sopra elencati sono stabilite dettagliatamente dal d.p.r. 501/98 [**D.P.R. 31 marzo 1998, numero 501**], sul funzionamento dell'ufficio del Garante che reca anche norme che disciplinano l'accesso ai dati personali. In particolare, si dispone che l'interessato deve provare la propria identità, anche esibendo o allegando copia di un documento di riconoscimento.

Gli obblighi del titolare: la notificazione

Chi costituisce una banca di dati o intende procedere al **trattamento** di dati personali o cessa il trattamento dei dati è tenuto a darne notificazione al Garante [**Notificazione**]. Così la scuola e per essa il dirigente scolastico.
La notificazione deve contenere alcuni elementi informativi previsti dalla legge e ogni variazione relativa al contenuto della notificazione comporta l'aggiornamento di quest'ultima.
L'omessa o incompleta notificazione è sanzionata penalmente [**Sanzione**] .

(segue) Gli obblighi del titolare: la qualità dei dati

Come dispone l'articolo 9 [**Articolo 9**], i dati personali oggetto di **trattamento** devono essere:

- trattati lealmente e lecitamente;
- raccolti e registrati per scopi determinati, espliciti e legittimi, e successivamente trattati in modo non incompatibile con tali scopi;
- esatti e, se necessario, aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti e successivamente trattati;
- conservati in una forma che consenta l'identificazione dell' **interessato** per un periodo di tempo non superiore a quello necessari o per gli scopi per i quali i dati sono stati raccolti e successivamente trattati.

L'articolo 9 della legge 675/96 è stato richiamato dal Garante con riferimento alla conservazione dei dati contenuti nei temi scolastici
[**I temi in classe non violano la *privacy***].
In caso di violazione delle modalità di raccolta o dei requisiti dei dati personali, sopra elencati, la legge consente all'interessato che, in conseguenza di ciò, abbia subito un danno, di richiedere il risarcimento del danno non patrimoniale [**Risarcimento**].

La sicurezza

11.1. Le misure di sicurezza

La legge sulla Tutela delle persone rispetto al **trattamento** dei dati personali, presenta un profilo di particolare interesse: quello della sicurezza informatica [**Approfondimento sulla sicurezza**].
I rischi individuati dalla legge sono costituiti dai rischi:

- di distruzione o perdita, anche accidentale, dei dati;
- di accesso non autorizzato;
- di trattamento non consentito o non conforme alle finalità della raccolta.

L'articolo 15 [**Articolo 15**] dispone che i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche

caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi sopra elencati.
La legge 675/96 non detta misure di carattere tecnico, rinviando la definizione in concreto delle **misure minime di sicurezza** da adottare in via preventiva ad un regolamento, attualmente costituito dal d.p.r. 28 luglio 1999, numero 318 [**D.P.R. 28 luglio 1999, numero 318**].
La mancata adozione delle misure minime di sicurezza configura il reato di omessa adozione di misure necessarie alla sicurezza dei dati, introdotto dall'articolo 36 della legge 675/96 [**Articolo 36**].
La norma ha come potenziali destinatari non solo il **titolare** del trattamento, ma anche il **responsabile** , nel caso in cui questi fosse responsabili per la sicurezza.

11.2. Le misure minime di sicurezza

Le misure minime sono dettate dal d.p.r. 318/99 [**D.P.R. 28 luglio 1999, numero 318**].
Esse sono distinte in trattamento informatizzato dei dati mediante il trattamento non automatizzato dei dati personali.

Nel caso di trattamento informatizzato dei dati personali si distinguono inoltre a seconda che:

- gli elaboratori non siano accessibili da altri elaboratori o terminali;
- gli elaboratori siano accessibili attraverso reti non disponibili al pubblico;
- gli elaboratori siano accessibili attraverso reti disponibili al pubblico;
- gli elaboratori siano accessibili in rete per fini esclusivamente personali.

In estrema sintesi, le misure minime di sicurezza sono costituite da:

- l'adozione di *password* [**Approfondimento sulla sicurezza**]
- l'individuazione dei soggetti preposti alla gestione delle *password*

Se il trattamento è effettuato mediante elaboratori accessibili attraverso reti, a queste misure si aggiungono:

- l'adozione di un codice identificativo personale per ogni utente
- l'adozione di programmi antivirus [**Approfondimento su virus e antivirus**]

Si precisa inoltre che lo stesso codice non può essere assegnato a persone diverse e che deve essere prevista la disattivazione del codice in caso di perdita della qualità del soggetto o di mancato utilizzo.
Se il trattamento ha ad oggetto **dati sensibili** o dati giudiziari ed è effettuato mediante elaboratori accessibili attraverso reti disponibili al pubblico, occorre anche predisporre annualmente un documento programmatico sulla sicurezza per definire:

- la protezione dei locali e procedure per l'accesso
- i criteri per assicurare l'integrità dei dati
- i criteri per assicurare la sicurezza delle trasmissioni
- l'elaborazione di un piano di formazione

11.3. Responsabilità civile

L'adozione delle misure minime di sicurezza consente di evitare la responsabilità penale, ma non è sufficiente per evitare la **responsabilità civile**
L'articolo 18 prevede una particolare ipotesi di responsabilità civile, attribuendo estremo rilievo alle conoscenze tecniche del settore. La legge dispone, infatti che chiunque cagiona danno ad altri per effetto del trattamento dei dati personali, è tenuto al risarcimento ai sensi dell'articolo 2050 del Codice civile.
L'articolo 18 della legge introduce il regime di responsabilità oggettiva per il danno cagionato per effetto del trattamento dei dati personali. Ciò comporta che il titolare del trattamento dei dati, a cui sia richiesto il risarcimento del danno, per liberarsi debba fornire l'assai difficile prova di avere adottato tutte le misure idonee ad evitare il danno, quale che sia il costo delle misure di sicurezza.

Ai fini penalistici, perché non si configuri il reato di omessa adozione di misure necessarie alla sicurezza dei dati, il titolare del trattamento dei dati deve adottare le misure minime di sicurezza di cui all'articolo 15, commi 2 e 3, cui fa espresso riferimento l'articolo 36 della legge, che introduce il reato citato [**Articolo 15**].
Ai fini civilistici, per liberarsi da responsabilità, non sarebbe sufficiente neanche l'adozione delle misure di sicurezza tali da ridurre al minimo i rischi. Infatti, ai sensi dell'articolo 18, per liberarsi da responsabilità civile, il titolare del trattamento dei dati deve fornire la prova di avere adottato tutte le misure idonee ad evitare il danno. Di conseguenza, il criterio di valutazione dell'idoneità delle misure adottate sarebbe costituito dallo stato dell'arte.

Adempimenti essenziali

Senza alcuna pretesa di esaustività, si indicano di seguito alcuni adempimenti essenziali:

- nominare uno o più responsabili;
- nominare gli incaricati;
- fare il censimento dei trattamenti nell'organizzazione per potere effettuare le notificazioni;
- emanare un regolamento sul **trattamento** , la **comunicazione** e la **diffusione** dei dati;
- predisporre l'informativa;
- predisporre un modulo per la richiesta del consenso alla comunicazione dei dati con la finalità di agevolare l'orientamento, la formazione e l'inserimento professionale;
- predisporre un modulo per la richiesta del consenso al trattamento dei dati, se si tratta di scuola privata;
- verificare l'adozione delle **misure minime di sicurezza** ;
- adottare un piano per aumentare le misure di sicurezza e, se del caso, il documento programmatico per la sicurezza.

Infrastrutture e servizi per la connettività: due casi di studio

Prof.ssa Paola Salomoni,
Dott. Diego Gardini
1.1.3. (Identificare e documentare i bisogni degli utenti di una rete per quel che riguarda l'hardware il software e i servizi),
1.2.6. (Valutare e raccomandare reti, prodotti di accesso remoto e servizi)

Introduzione

La disponibilità di linee **ADSL** (*Asymmetric Digital Subscriber Line*) a costi contenuti o a volte gratuitamente (nell'ambito di convenzioni ad hoc con alcuni fornitori del servizio), ha reso possibile anche per le scuole usufruire di connessioni a Internet che siano *always on* e a banda larga.

Le connessioni ***always on*** (sempre in linea) sono connessioni dedicate che non si attivano solo su richiesta (come le connessioni commutate) ma sono a disposizione 24 ore su 24. Questo tipo di linea è dunque adatta a trasformare la scuola da un soggetto che usufruisce dei servizi Internet a un soggetto che può offrire esso stesso servizi, al proprio personale, agli studenti, ai genitori e a terze parti interessate. Una connessione *always on* consente dunque, per esempio, di ospitare a scuola un *server Web* visibile dall'esterno, oppure di gestire un *server* di posta per fornire a tutti gli studenti un *account* di posta elettronica e gestire opportune *mailing list*.

Le connessioni **a larga banda** offrono larghezze di banda misurabili in Mbps e sono dunque adatte a fornire connettività Internet ad alcune decine di stazioni mantenendo un elevato grado di interattività. Questo tipo di connessione consente inoltre di fruire di servizi multimediali innovativi, quali per esempio i sistemi di *e-learning* e risulta quindi particolarmente interessante in ambiente scolastico.

Riprogettare la connettività

Questo approfondimento presenta due casi di studio, nei quali l'introduzione della tecnologia **ADSL** come supporto

alla connettività Internet ha introdotto modifiche strutturali alle infrastrutture della rete locale. Per ciascuno dei due casi sono riportate le principali scelte progettuali, avendo cura di citare le tecnologie utilizzate e di motivare le decisioni prese. Maggiori informazioni sulle specifiche tecnologie verranno fornite nei moduli successivi. Non sono stati riportati i costi delle infrastrutture perché questo tipo di informazioni sono soggette a una fortissima obsolescenza.

In particolare nel **primo caso** , la relativa complessità delle esigenze della scuola e in particolare la scelta di utilizzare la connessione ADSL anche per collegare a Internet le macchine dell'amministrazione, ha portato all'introduzione nell'architettura della rete di un *firewall*. Il *firewall* viene utilizzato per raggiungere diversi scopi:

- aumentare la **sicurezza** perimetrale,
- aumentare la sicurezza interna,
- limitare le attività degli utenti a un insieme di operazioni consentite.

Il **secondo caso** integra l'innovazione apportata dall'introduzione di una connessione *always on*, con aspetti di mobilità introdotti attraverso l'uso di tecnologie ***wireless*** . La scelta delle connessione ADSL e il conseguente ripensamento della struttura interna della LAN, ha infatti creato l'occasione per valutare l'opportunità di installare una rete *wireless* che offra supporto alla mobilità degli utenti e consenta di portare la rete nelle aule e negli uffici con interventi di cablaggio molto limitati.

Un primo caso di studio

In vista dello spostamento in una nuova struttura, un Istituto Tecnico Industriale imposta un nuovo progetto di connettività che ha come obiettivo finale quello di collegare a Internet stabilmente e a banda larga sia i laboratori didattici che le segreterie. Nel precedente edificio la connessione a Internet avveniva mediante due linee commutate ISDN, una per l'amministrazione e una per i laboratori.

L'istituto ha due laboratori didattici che sono composti da attrezzature recenti e che verranno spostati senza integrazioni. Nel primo laboratorio sono collocate 13 postazioni e nel secondo 15. La segreteria opera invece su 4 postazioni. Sono presenti inoltre due *server* che fungono da *controller* di dominio (per l' **autenticazione** degli utenti), *file server* e *server* stampa rispettivamente per la segreteria e per i laboratori.

Il progetto deve considerare:

- la scelta del fornitore del servizio di accesso.
- Il cablaggio della rete locale.
- Le problematiche di **sicurezza** e la prevenzione degli **attacchi** , sia interni che esterni.
- Il progetto di nuovi servizi da offrire agli utenti, tra i quali la posta elettronica e la possibilità di consultare da casa la posizione personale degli studenti.

Cablaggio

Il progetto dell'edificio prevedeva la realizzazione di un cablaggio strutturato molto esteso, messo in opera in fase di costruzione del plesso.

Il cablaggio disponibile è basato sulle seguenti scelte operative:

- connettere ogni aula dell'istituto con un centro stella, posto in un armadio di permutazione, attraverso due prese per aula;
- realizzare una sottorete per ciascuno dei due laboratori (per ospitare fino a 20 postazioni) e una per la segreteria (per ospitare fino a 8 postazioni).

Sono stati utilizzati doppini di tipo UTP (*Unshielded Twisted Pair*) categoria 5, che supportano *Fast Ethernet* (fino a 100 Mbit/sec).

Apparati attivi

Posto che la posa in opera dei cavi era già stata stabilita dal progetto di costruzione dell'edificio, la realizzazione della LAN deve essere completata attraverso la collocazione e connessione degli apparati attivi.

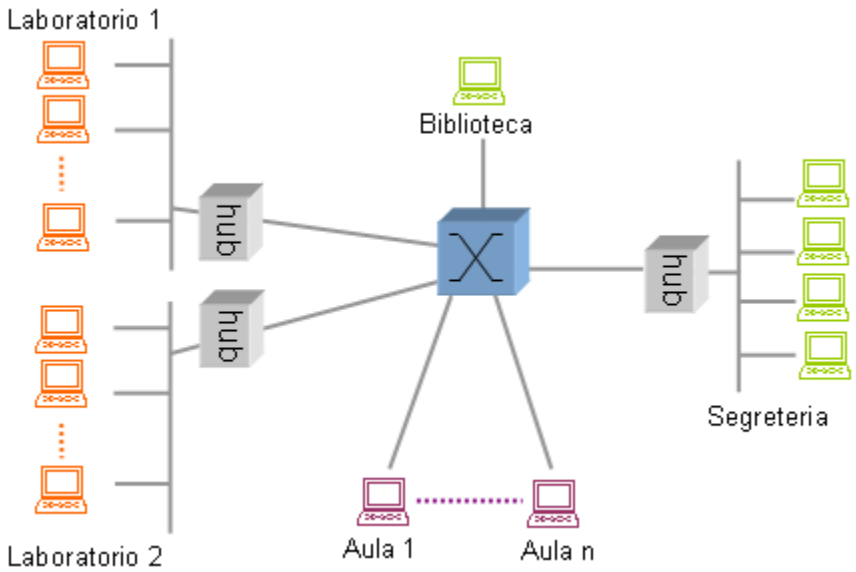
L'istituto è dotato di calcolatori per lo più recenti, equipaggiati con schede di rete a 10/100 Mbit/sec che nel vecchio edificio erano connessi tra loro tramite *hub* a 100 Mbit/sec. Sono dunque disponibili due *hub* a 100 Mbps da 16 porte che erano utilizzati nei laboratori e un *hub* a 100 Mbps a 8 porte utilizzato in segreteria.

Per la connessioni delle portanti tra i vari laboratori e la segreteria è stato scelto uno *switch* di livello 2, con 24 porte, ovvero un apparato attivo in grado di instradare i pacchetti esclusivamente verso l'indirizzo (di livello 2) destinatario. Questa scelta va nella duplice direzione di migliorare le prestazioni e aumentare la **sicurezza** del sistema. Il numero di porte è sufficiente a coprire le esigenze iniziali dell'Istituto, ma l'apparto dovrà essere integrato se si vorrà installare un *computer* per aula.

Per i laboratori didattici e per la segreteria si opta per il riuso degli *hub* preesistenti e utilizzati già nel vecchio edificio, fatta salva l'opportunità di sostituirli in futuro con altri *switch*. Gli *hub* sono infatti apparati di livello 1 che hanno il solo compito di rimbalzare il segnale sulle porte a disposizione e quindi non effettuano uso selettivo delle risorse e, condividendo il canale, rendono possibili attacchi alla sicurezza dei dati. Gli *switch* sostitutivi consentirebbero di aumentare le prestazioni, la sicurezza e il numero di postazioni collegabili.

LAN

Una prima possibile configurazione della LAN è dunque la seguente:



Connettività Internet

Per la connettività Internet si è scelto un collegamento **ADSL** , di tipo permanente, che comprende l'utilizzo di un indirizzo IP statico, la registrazione e gestione di un dominio di secondo livello, la fornitura e installazione di un *router* ADSL. Il costo del contratto è di tipo *flat*, ovvero prevede un prezzo fisso mensile senza tenere conto del traffico.

La fornitura offre una velocità di 640 kbit/sec per il *download* e di 128 kbit/sec per l'*upload*, con una banda garantita verso qualunque destinazione di 20kbit/sec in *download* e 10 kbit/sec in *upload*. Infine il contratto prevede l'utilizzo di 50 MB di spazio disco e di 5 indirizzi di posta elettronica.

Si aprono dunque, rispetto alla configurazione della LAN appena prospettata due diverse tipologie di problema:

- la necessità di mascherare gli indirizzi della LAN dietro all'unico indirizzo IP routabile che è in possesso dell'istituto. Questo tipo di attività può essere realizzata mediante un sistema NAT/PAT che è integrato nel *router* ADSL fornito assieme al collegamento a Internet.
- La necessità di proteggere la rete locale e le sue risorse, poiché il collegamento stabile aumenta fortemente i rischi di attacco alla sicurezza del sistema. La rete può essere protetta mediante un ***firewall*** .

TIR

Nelle forniture **ADSL** il *router* viene anche indicato con l'acronimo TIR (Terminazione Intelligente di Rete) e tipicamente è in grado di fornire servizi aggiuntivi, rispetto al normale instradamento IP. In particolare le funzionalità aggiuntive più frequenti sono:

- il **NAT** (*Network Address Translation*), un servizio che offre la possibilità di collegare un numero qualunque di postazioni pur avendo un solo indirizzo IP pubblico. Il NAT è realizzato mappando le comunicazioni su indirizzi IP privati, visibili solo all'interno della rete.
- Il **PAT** (*Port Address Translation*) che consente a stazioni interne alla rete privata di fornire servizi a *client* della rete pubblica. Il PAT mappa le porte dei *server* della rete privata su porte logiche del TIR e reinstrada le comunicazioni di conseguenza.

Il TIR compreso nel contratto sottoscritto dall'istituto comprende funzionalità di NAT e PAT.

Sicurezza

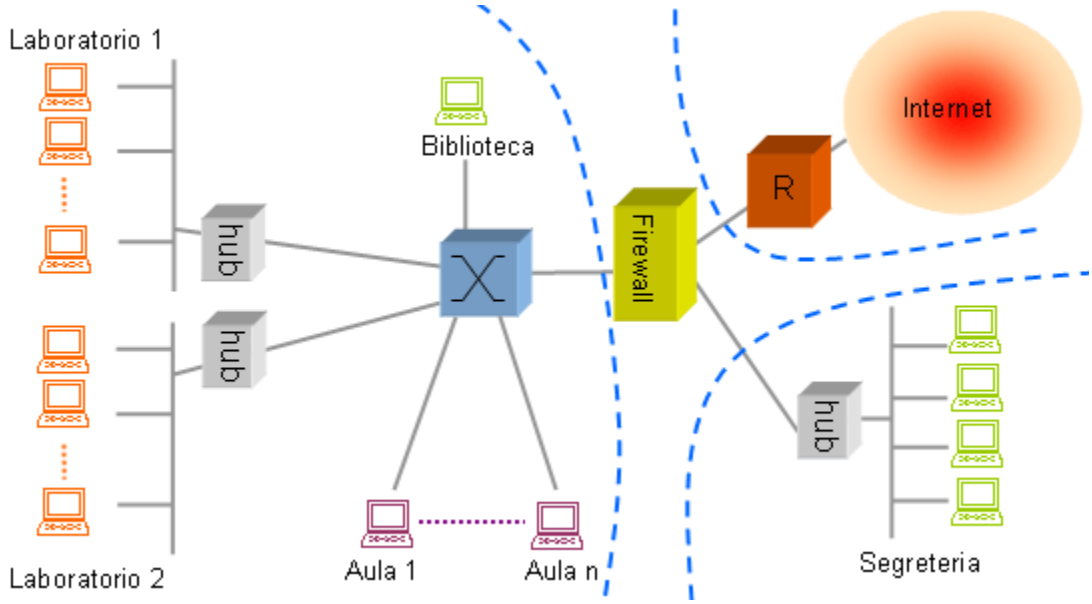
Due problematiche di **sicurezza** sostengono il progettista nella scelta di utilizzare un ***firewall*** per ridurre i rischi derivanti dall'architettura di rete finora prospettata:

- la connessione stabile rende maggiore il rischio d'attacco poiché le risorse sono sempre a disposizione di un eventuale intruso che miri a impossessarsene e/o a danneggiarle. A rischio sono sia le macchine dei laboratori che quelle dell'amministrazione e queste ultime devono essere protette con maggiore efficacia perché contengono dati sensibili.
- Gli studenti dell'istituto hanno, già in passato, dato prova di possedere abilità informatiche sufficienti a sferrare con successo attacchi alla sicurezza. In questo caso rispetto agli attacchi diretti verso l'esterno della rete, sono più critici gli attacchi interni che potrebbero essere rivolti alle macchine dell'ammistrazione e ai dati (sensibili e non) in esse contenuti.

Per questo motivo è opportuno installare un *firewall* che effettui una sorveglianza non solo perimetrale ma anche interna. Il *firewall* dividerà dunque la LAN in tre sottoreti, una per i laboratori, una per l'amministrazione e, infine, una che include esclusivamente il *router* e diviene quindi la via di transito verso l'esterno del sistema.

Firewall

La configurazione completa della LAN è dunque la seguente:



I nuovi servizi

In fase di stesura del progetto vengono definiti alcuni nuovi servizi che si vogliono rendere disponibili agli studenti, al personale e alle famiglie. Vengono inoltre suggerite linee guida nella scelta delle risorse *hardware* e *software* di supporto ai nuovi servizi, rinviando a una futura analisi la scelta delle specifiche piattaforme e applicazioni e la fattibilità economica relativa.

In particolare, sentiti gli utenti finali (studenti, docenti e famiglie), risultano interessanti i seguenti servizi:

- un servizio di posta elettronica che assegni a ogni studente e a ogni docente una casella di posta in modo da incentivare le comunicazioni attraverso questo medium. Non sono evidentemente sufficienti le 5 caselle fornite dal *provider* d'accesso per cui per realizzare questo servizio si prevede di utilizzare un *server* di posta che fornisca supporto ai principali protocolli (SMTP, POP e IMAP). Considerate le funzionalità del *server*, si consiglia di valutare la possibilità di basare il servizio su piattaforme ***open source***.
- Un sistema basato su *Web* che consenta di utilizzare Internet per accedere ai dati sul rendimento scolastico degli allievi, sia in termini di valutazione dei risultati che in termini di presenze/assenze e ritardi. Il sistema dovrà prevedere una forma di autenticazione degli utenti in modo che solo persone autorizzate dall'Istituto (tipicamente i genitori) possano accedere alle informazioni e integrarsi con gli applicativi disponibili presso la segreteria.

Secondo caso

Un liceo classico è sito in un palazzo storico nel centro di una città e ha infrastrutture informatiche prevalentemente concentrate in due luoghi: il laboratorio multimediale e la segreteria. Il liceo ha recentemente sostituito la connessione commutata via ISDN del laboratorio con una connessione stabile a banda larga basata su tecnologia ADSL e vorrebbe utilizzare la nuova linea anche per garantire connettività a Internet a tutte le altre postazioni site nel palazzo.

Il progetto ha l'obiettivo di verificare la possibilità di cablare tutto l'edificio mediante una infrastruttura mista *wired* e *wireless* che integri il cablaggio basato su cavi con tecnologie senza fili. Attraverso questa infrastruttura la linea ADSL deve poter diventare il mezzo di accesso a Internet anche per gli elaboratori della segreteria e per le postazioni site nella biblioteca e nell'aula magna.

La connettività *wireless* deve essere realizzabile in due fasi: in una prima fase deve esser offerta copertura *wireless*

alle aree dell'amministrazione, al laboratorio multimediale, all'aula magna e alle aree di studio e ricreazione di studenti e docenti. Una seconda fase deve rendere possibile la copertura di tutto il resto dell'edificio.

WLAN

Con il termine inglese *wireless* si indica una specifica tipologia di comunicazioni che utilizza come mezzo fisico per il trasporto dei dati l'etere. Un segmento del mercato *wireless* particolarmente significativo e stabile è costituito dalle *Wireless* LAN (**WLAN**) il cui obiettivo principale è quello di integrare, piuttosto che sostituire, le tradizionali LAN, fornendo connettività mobile agli utenti. In edifici in cui è complesso installare tradizionali reti via cavo, per particolari modelli strutturali o in edifici storici e soggetti a vincoli delle Belle Arti, le WLAN sono la soluzione ottimale per offrire connettività, sia dal punto di vista delle prestazioni che dal punto di vista economico.

In particolare nel settore delle applicazioni didattiche le WLAN hanno trovato un fertile terreno applicativo offrendo diverse tipologie di servizi, che risultano innovativi sia dal punto di vista della connettività che delle funzionalità. Sono ormai diverse le scuole che hanno affiancato al cablaggio via cavo con installazioni di reti con l'obiettivo di integrare meglio la presenza del personal *computer* all'interno delle classi e di favorire la mobilità dei docenti.

WiFi

IEEE **802.11** è il primo standard sviluppato per le WLAN e può essere comparato con lo standard 802.3 definito per le reti locali basate su *Ethernet*. Lo scopo di 802.11 è quello di definire un set di regole operative tali che apparati costruiti da differenti produttori possano operare tra di loro in maniera trasparente, proprio come avviene per tutti gli apparati basati sulla tradizionale tecnologia *Ethernet*.

Questo standard è basato sull'architettura cellulare, ovvero la LAN viene vista e definita come un insieme di più **celle**, in cui ogni cella è controllata da una stazione base chiamata punto di accesso o ***Access Point*** . Premesso questo, possiamo dire che una LAN può essere formata da una singola cella con un singolo punto di accesso oppure da un insieme di celle dove i vari punti di accesso sono collegati tra loro attraverso un *backbone* che viene realizzato su una rete cablata *Ethernet* ma può essere anch'esso *wireless*.

La tipologia di WLAN più diffusa è nota come ***WiFi*** (*Wireless fidelity*) ed è definita dallo standard 802.11b (della famiglia 802.11) che opera a 2,4Ghz di frequenza e raggiunge un *transfer rate* di 11Mbps.

La struttura

Il liceo ha sede in due edifici: un palazzo principale, che ospita l'amministrazione, la biblioteca, la maggior parte delle aule e i laboratori, e un fabbricato separato in cui sono collocate le palestre. L'edificio principale è strutturato su due piani: al piano terra trovano ubicazione l'amministrazione, l'aula magna, la biblioteca, la sala di studio, il laboratorio multimediale e alcune aule. Il primo piano ospita le altre aule e il laboratorio di scienze. La linea ADSL arriva con un *router* nel laboratorio. I *computer* del laboratorio multimediale sono collegati tra di loro attraverso un *hub* a 100 Mbps. L'amministrazione ha un cablaggio interno a 100 Mbps attraverso un *hub* a 8 porte.

Il progetto deve prevedere l'acquisizione delle infrastrutture necessarie a:

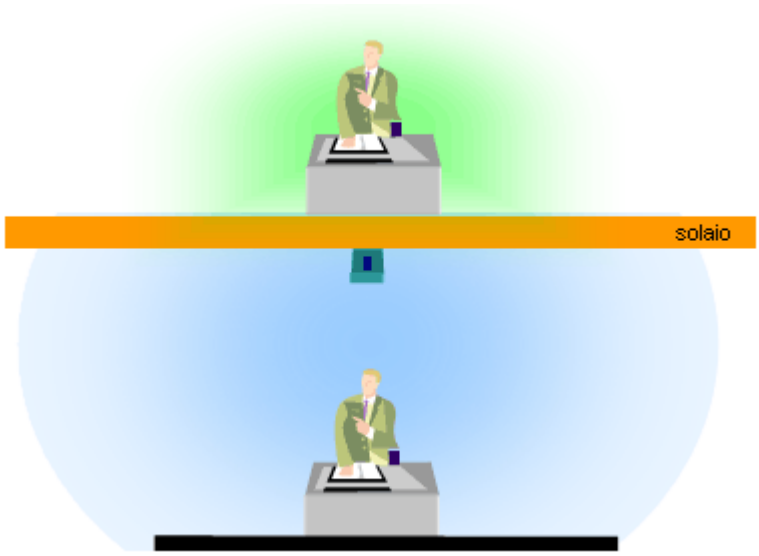
- collegare (via cavo) l'amministrazione alla linea ADSL;
- offrire copertura *wireless* alle aree indicate come primarie (tutte collocate al piano terra dell'edificio principale);
- prevedere i lavori di ampliamento della copertura *wireless* a tutte le aule (piano terra e primo piano).

Ampliamento della LAN

Il cablaggio tradizionale deve assicurare la connessione della rete dell'amministrazione alla linea **ADSL** . Viene quindi prevista la posa di un cavo che realizzi questo collegamento e l'acquisto di uno *switch* a 100 Mbps con 16 porte. Allo *switch*, che fungerà da centro stella della LAN, andranno collegati: il *router* ADSL, l'*hub* del laboratorio multimediale e l'*hub* dell'amministrazione. La scelta di uno *switch* consente di aumentare il grado si sicurezza della rete, limitando le aree a mezzo condiviso. Questa scelta è particolarmente critica se si prevede l'integrazione con apparati *wireless*.

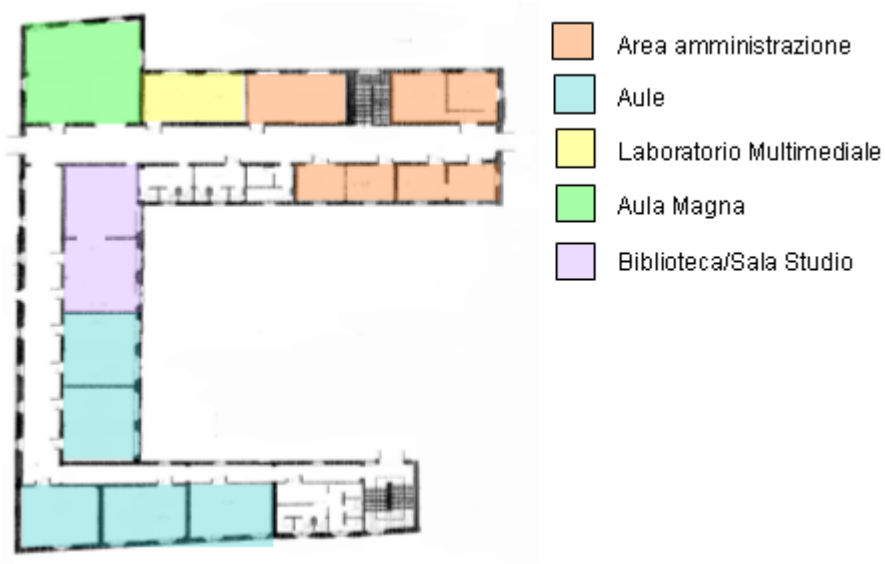
Il cablaggio tradizionale deve inoltre raggiungere tutti gli *access point*. Sono disponibili in commercio anche apparati che consentono di costruire il *backbone* tra gli *access point* utilizzando *link wireless*, ma hanno costi più elevati dei normali apparati WLAN. Per questo motivo viene scelta la stesura di cavi dallo *switch* centro stella (posto nel laboratorio multimediale) ai singoli ***access point*** . I punti di posa degli *access point* devono essere definiti dopo una attenta analisi della topologia della scuola e solo dopo aver effettuato opportune misurazioni. Il segnale radio si attenua infatti quando attraversa ostacoli fisici (quali i muri) e dunque per essere certi che il segnale copra tutta l'area indicata come primaria, occorre fare misure di ricezione. Una misura particolarmente utile risulta quella volta a comprendere il tipo di attenuazione prodotto dal solaio posto tra il piano terra e il primo piano.

Essendo l'edificio antico (e dunque il solaio realizzato senza cemento armato) è possibile che l'attenuazione prodotta dal solaio sia minima e dunque che gli apparati usati per coprire il piano terra, se posti sufficientemente vicini al soffitto, offrano copertura anche a parte del primo piano.



Il piano terra

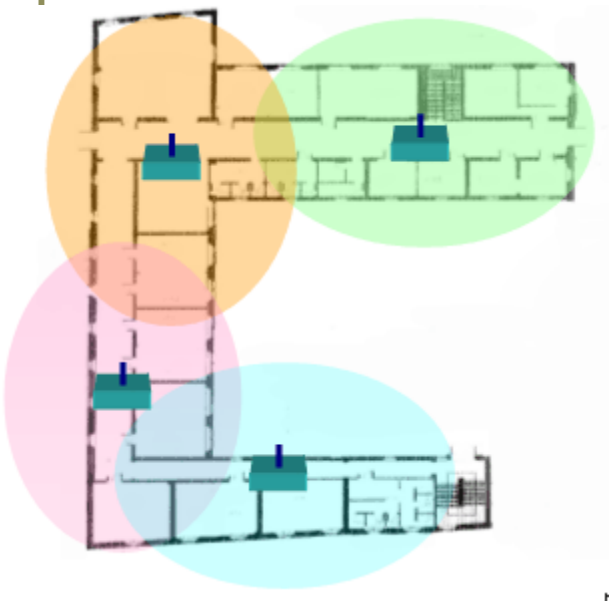
Il piano terra del liceo è rappresentato dalla seguente piantina, dalla quale risulta evidente che le zone da coprire nella prima fase sono tutte attigue.



Copertura del piano terra

Dalle misurazioni effettuate risultano sufficienti due *access point* (collocati rispettivamente di fronte all'aula magna e sopra alla segreteria per coprire tutta l'area richiesta nella prima fase. Il segnale supera il solaio con un'attenuazione accettabile, per cui al primo piano arriva nitido oltre il metro da terra (distanza a cui verranno tenute le tipicamente schede di rete). Le misure sono state fatte da uno dei potenziali fornitori con AP identici a quelli che verranno installati nella scuola.

Copertura delle aule



Per offrire connettività *wireless* a tutte le aule (piano terra e primo piano) sono dunque sufficienti 4 apparati, i due previsti per la fase iniziale più altri due che possono essere acquisiti e collegati al centro stella in una fase successiva.

Scelta degli apparati

Gli apparati *WiFi* disponibili sono innumerevoli e hanno costi molto variabili a seconda delle funzionalità che offrono. In particolare sono offerti alcuni servizi aggiuntivi che possono essere interessanti in casi specifici:

- apparati ***access point*** con *backbone wireless*: sono AP dotati di più schede *wireless*. Tipicamente una scheda è utilizzata per l'accesso dei terminali mobili e una per il *backbone*. Hanno il vantaggio di non richiedere il cablaggio LAN tradizionale.
- Apparati *access point* alimentati attraverso il cavo di rete: sono AP che ricevono alimentazione attraverso il doppino che li collega alla rete. Per utilizzarli occorre che lo *switch* sia in grado di alimentarli o che esista un altro apparato che viene aggiunto alla rete al solo scopo di fornire l'alimentazione agli *access point*.
- Apparati con funzionalità aggiuntive per la **sicurezza** e la gestione della rete. Le reti *wireless* sono infrastrutture poco sicure: il loro raggio d'azione esce a volte dalle aree per le quali sono impiantate e l'algoritmo di crittografia utilizzato ha diverse falle note da tempo. Sono in commercio apparati che offrono supporto a funzionalità per il miglioramento della sicurezza che implementano a questo scopo diverse strategie. Altre funzionalità di supporto alla gestione realizzano per esempio politiche di assegnazione dinamica degli indirizzi IP (**DHCP** e **NAT**).

Nel progetto del Liceo trovano applicazione semplici apparati di accesso senza funzionalità aggiuntive, che possono essere reperiti a costi molto limitati.

Conclusioni

I due casi mostrati hanno avuto lo scopo di presentare due diverse situazioni in cui la connettività *always on* a banda larga messa a disposizione dalle linee ADSL ha offerto lo spunto per ripensare alla rete locale della scuola e ridefinirne i servizi.

L'esposizione ha, in entrambi i casi, mirato a illustrare gli aspetti più innovativi delle scelte progettuali, tralasciando

volutamente gli aspetti più tecnici e quelli più consueti.

Entrambi i progetti sono stati realizzati seguendo criteri di scalabilità, ovvero sono state acquisite infrastrutture che consentono la messa in opera di un primo nucleo di nuovi servizi, delineando già un insieme di possibili migliorie da realizzare nel breve periodo. Per questo motivo le trattazioni non sono esaustive e lasciano aperte ampie possibilità di miglioramento dell'infrastruttura in termini di servizi, sicurezza, prestazioni. I possibili potenziamenti sono individuati dai rispettivi progetti, ma rimandati a successivi interventi di finanziamento.

Bibliografia

1.1 Identificazione dei bisogni

Rete e scuola

Come non cadere nella rete: Guida alla progettazione di un cablaggio strutturato per le scuole secondarie superiori; Cisco; **http://www.cisco.com/global/IT/solutions/pdf/edu_smb.pdf**
F. Cremascoli e M. Gualdoni; *La lavagna elettronica: Guida all'insegnamento multimediale;* 2000Laterza
La lavagna elettronica: Guida all'insegnamento multimediale; F. Cremascoli e M. Gualdoni;
http://www.laterza.it/laterza/libri-online/cremascoli/cremascoli.htm
Reti informatiche per la didattica: Guida di riferimento allo sviluppo di un progetto di rete di istituto; A. Boezi;
http://www.docenti.org/reti/logica.htm
Per costruire la rete delle scuole: Situazione della telematica scolastica e progetto per la rete in Emilia-Romagna; M. Nanni, G. Ortolani; **http://kidmir.bo.cnr.it/scuolan/libro/copertina.htm**

1.2 Valutazione del software e dell'hardware

Ergonomia

GLOSSARIO DI ERGONOMIA, Consultabile e scaricabile attraverso il sito dell'INAIL; F. Marcolin, G. Mian, A. Ossicini, F. Luisi, S. Pischiottin, L. Vecchi Brumatti;
http://www.inail.it/medicinaeriabilitazione/pubblicazioni/glossario/indice.htm
Donald A. Norman; *LA CAFFETTIERA DEL MASOCHISTA: Psicopatologia degli oggetti quotidiani;* 1990Giunti
D. Lgs. 626/94, ATTUAZIONE DELLE DIRETTIVE 89/391/CEE, 89/654/CEE, 89/655/CEE, 89/656/CEE, 90/269/CEE, 90/270/CEE, 90/394/CEE, 90/679/CEE, 93/88/CEE, 95/63/CE, 97/42, 98/24 E 99/38 RIGUARDANTI IL MIGLIORAMENTO DELLA SICUREZZA E DELLA SALUTE DEI LAVORATORI DURANTE IL LAVORO; ;
http://www.giustizia.it/cassazione/leggi/dlg626_94.html

Open Source

Osservatorio Tecnologico, Software nella Scuola; ;
http://www.osservatoriotecnologico.net/software/default.htm

1.3 Prevenzione di problemi e loro soluzione

Multiutenza

A. Silberschatz, P. Galvin; *Sistemi Operativi (quinta ed.);* 1999Addison Wesley

Backup

Guida dell'amministratore di sistema di Linux: Capitolo 10. I Backup; Lars Wirzenius;
http://ildp.pluto.linux.it/guide/GuidaSysadm/c2264.html
Documentazione su Microsoft Windows2000 Server: Backup e ripristino dei dati; Microsoft Corp.;
http://www.microsoft.com/windows2000/it/server/help/backup_overview.htm

1.4 Aspetti legali e privacy

Accessibilità

Accessibilità dei siti Web; OTE Osservatorio Tecnologico;
http://www.osservatoriotecnologico.net/Internet/accessibilita.htm
Accessibilità e tecnologie informatiche nella PA; AIPA; **http://www.aipa.it/attivita[2/gruppi[18/accessibilita[3/**

Approfondimenti

Introduzione alla sicurezza dei sistemi informatici

William Stallings; *Sicurezza delle reti: Applicazioni e standard;* 2001Addison Wesley
Dieter Gollman; *Computer Security;* 1999John Wiley & Sons
Guida alla sicurezza dei PC; Stefano Bendandi; **http://www.html.it/sicurezza_pc/index.html**
Sicurezza nelle reti locali; OTE Osservatorio Tecnologico;
http://www.osservatoriotecnologico.net/RETI/sicurezza.htm
Dispense del corso di Sicurezza su Reti; Alfredo De Santis; **http://www.dia.unisa.it/ads.dir/corso-security/www/CORSO-0102/**

Virus e Antivirus

[TheProbertE-TextEncyclopaedia] *The Probert E-Text Encyclopaedia;*
http://www.sneaker.net.au/docs/encyclo/GIL1.HTM
Proteggi il tuo PC: I Portatili. Capitolo 4: Virus e Antivirus;
http://education.mondadori.it/libri/Download/Capitoli/334_cap04.pdf
Virus Enciclopedia; Trendmicro; **http://www.trendmicro.com/vinfo/virusencyclo/**
[WildList] *Wild List;* **http://www.wildlist.org**

Introduzione alla crittografia

La firma digitale; Ministero per l'innovazione tecnologica;
http://www.innovazione.gov.it/ita/egovernment/infrastrutture/firma_digitale.shtml
William Stallings; *Sicurezza delle reti: Applicazioni e standard;* 2001Addison Wesley
Introduzione alla crittografia; Pierre Loidreau;
http://www.linuxfocus.org/Italiano/May2002/article243.shtml
Dieter Gollman; *Computer Security;* 1999John Wiley & Sons
Crittografia e PGP; Matteo Zinato; **http://www.html.it/crittografia/index.html**
Dispense del corso di Sicurezza su Reti; Alfredo De Santis; **http://www.dia.unisa.it/ads.dir/corso-security/www/CORSO-0102/**
Introduzione ai problemi legati alla crittografia e alla firma elettronica; Daniele Giacomini;
http://lagash.dft.unipa.it/AL/al287.htm
[TheInternationalPGPHomePage] *The International PGP Home Page;*
http://www.serve.com/nimrod/pgp.html
Introduzione alla firma digitale; Interlex; **http://www.interlex.it/docdigit/intro/indice.htm**

Infrastrutture e servizi per la connettività: due casi di studio

Tecnologia WIreless (Guida al WiFI); Daniele Pauletto; **http://ewireless.interfree.it/**
Legislazione sulle WLAN; Wireless.it; **http://www.wireless.it/legislazione.html**
Wireless LAN Security FAQ; **http://www.airgate.it/faq/wlsfaq.htm**
Wi-Fi: realizzare reti senza fili; Fabio Boneschi; **http://www.hwupgrade.it/articoli/647/1.html**

La tutela giuridica del software e il contratto di licenza d'uso

G. Alpa (a cura di); *La tutela giuridica del software;* 1984Giuffré
L. Chimienti; *La tutela del software nel diritto d'autore;* 2000Giuffré

B. Cunegatti; *Aspetti legali dell'opera multimediale;* 2000Guerini e Associati
G. Finocchiaro; *I contratti ad oggetto informatico;* 1993Cedam
P. Frassi; *Creazioni utili e diritto d'autore;* 1997Giuffré
E. Giannantonio; *La tutela giuridica delle topografie dei prodotti a semiconduttori;* 1990Giuffré
R. Ristuccia e V. Zeno Zencovich; *Il software nella dottrina, nella giurisprudenza e nel D. LGS. 518/92 (Seconda Edizione);* 1993Giuffré
V. Zeno Zencovich; *Le leggi sulla tutela dei programmi per elaboratore in Italia e nel mondo;* 1990Giuffré
l. 22 aprile 1941, n. 633;
http://www.innovazione.gov.it/ita/intervento/normativa/allegati/legge_220441.pdf
d. lgs. 29 dicembre 1992, n. 518;
http://www.innovazione.gov.it/ita/intervento/normativa/allegati/dl_291292.pdf
l. 18 agosto 2000, n. 248;
http://www.innovazione.gov.it/ita/intervento/normativa/allegati/legge_180800.pdf
d. lgs. 6 maggio 1999, n. 169;
http://www.innovazione.gov.it/ita/intervento/normativa/allegati/dl_060599.pdf

La tutela della privacy

AA. VV.; *Società dell'informazione tutela della riservatezza. Atti del congresso svoltosi a Stresa dal 16 al 17 maggio 1997;* 1998Giuffré
C.M. Bianca, F.D. Busnelli, A. Bellelli, F.P. Luiso, E. Navarretta, S. Patti, P.M. Vecchi; *Tutela della privacy, ne Le nuove leggi civili commentate;* 1999n. 2-3, marzo-giugno
G. Buttarelli; *Banche dati e tutela della riservatezza;* 1997Giuffré
G. Finocchiaro; *Diritto di Internet. Scritti e materiali per il corso;* 2001Zanichelli
Garante per la protezione dei dati personali; *Cittadini e società dell'informazione. Bollettino;* periodicoPresidenza del Consiglio dei ministri - Dipartimento per l'informazione e l'editoria
Garante per la protezione dei dati personali; *Relazione per l'anno 1997-1998-1999-2000-2001;* periodicoPresidenza del Consiglio dei ministri - Dipartimento per l'informazione e l'editoria
E. Giannantonio, M.G. Losano, V. Zeno Zencovich; *La tutela dei dati personali. Commentario alla l. 675/1996;* 1997Cedam
V. Italia, M. Della Torre, G. Perulli, A. Zucchetti; *Privacy e accesso ai documenti amministrativi;* 1999Giuffré
Sito ufficiale del Garante per il trattamento dei dati personali; **http://www.garanteprivacy.it**
l. 31 dicembre 1996, n. 675, 'Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali';
http://www.garanteprivacy.it/garante/prewiew/0,1724,2039,00.html?sezione=115&LANG=1
d.p.r. 28 luglio 1999, n. 318; **http://www.garanteprivacy.it/garante/prewiew/0,1724,1371,00.html?sezione=115&LANG=1**

Glossario

ACCESS POINT: stazione base che controlla l'accesso a una cella della **Wireless** LAN.

ADSL: (*Asymmetric Digital Subscriber Line*) è un sistema di comunicazione digitale che utilizza il supporto fisico di un doppino telefonico per offrire un servizio *always on* e a banda larga. La comunicazione è asimmetrica nel senso che sono fornite larghezze di banda differenti in *download* e in *upload*. La linea rimane utilizzabile contemporaneamente per le normali telefonate e per la comunicazione asimmetrica dei dati.

ANTIVIRUS: è un *software* il cui obiettivo è identificare i **virus** e rimuoverli prima che entrino in azione. Per rilevarli l'antivirus cerca all'interno della memoria (centrale e di massa) particolari sequenze di *byte* che costituiscono l'impronta identificativa del virus.

ATTACCO: è un tentativo di accesso o d'uso non autorizzato dei dati e dei sistemi, che mira a comprometterne la **sicurezza** .

ATTACH: insieme di uno o più *file* allegati ai messaggi di posta elettronica.

AUTENTICAZIONE: è uno degli obiettivi della **sicurezza** informatica che ha lo scopo di provare in modo univoco l'identità degli utenti di un sistema.

BACKUP: copia dei dati destinata all'archiviazione che può essere utilizzata in caso di errore, quando le informazioni (o una loro parte) risultano inutilizzabili, per ripristinare uno stato precedente recuperando i dati che sono stati compromessi.

BACKUP COMPLETO: ***backup*** in cui i dati vengono copiati interamente dal supporto originale al *backup* e ripristinati effettuando la copia in senso inverso (dal *backup* al supporto originale).

BACKUP INCREMENTALE: ***backup*** in cui vengono copiati i *file* creati o modificati dall'ultimo ***backup* completo** o incrementale. Qualora si faccia un successivo *backup* incrementale, questo farà comunque riferimento al precedente.

BACKUP DIFFERENZIALE: ***backup*** in cui vengono copiati i *file* creati o modificati dall'ultimo ***backup* completo** . Qualora si faccia un successivo *backup* differenziale, questo farà comunque riferimento all'ultimo *backup* completo, ignorando i precedenti *backup* differenziali.

BLOCCHI DI PARITÀ: è una tecnica di miglioramento dell'affidabilità in cui alcuni blocchi, detti blocchi di parità, sono utilizzati per memorizzare informazioni riassuntive, calcolate tramite apposite funzioni matematiche, su alcuni blocchi precedenti. Non garantisce ridondanza totale come invece fa il ***mirroring*** .

BOOT SECTOR: è il settore del dischetto che contiene il *bootstrap loader* ovvero la *routine* di avvio del sistema operativo.

BOOT VIRUS: sono **virus** che si propagano inserendo una copia di se stessi nel ***Boot Sector*** dei dischetti o nel ***Master Boot Record*** del disco fisso.

BREVETTO: atto amministrativo che attribuisce all'inventore la facoltà esclusiva di attuare un'invenzione e di trarne profitto.

CAVALLO DI TROIA: è un programma (di tipo ***malicious software***) apparentemente innocuo che una volta eseguito, effettua operazioni diverse da quelle per le quali l'utente lo aveva lanciato.

CERTIFICATION AUTHORITY: soggetto di fiducia, che emette, regola ed elimina i **certificati digitali** .

CERTIFICATO DIGITALE: è un documento elettronico che associa una **chiave pubblica** , e di conseguenza la chiave privata corrispondente, a una particolare identità. Il certificato viene emesso dalla ***Certification Authority*** .

CHIAVE DI SESSIONE: Sequenza di caratteri, di lunghezza arbitraria, la cui validità è limitata ad una sessione di comunicazione. Tipicamente è concordata mediante tecniche a chiave pubblica e utilizzata per crittografia a chiave privata.

CHIAVE PRIVATA: Sequenza di caratteri, di lunghezza arbitraria, utilizzata in coppia con la chiave pubblica nella crittografia a chiave pubblica. Deve essere conosciuta solo dal proprietario.

CHIAVE PUBBLICA: Sequenza di caratteri, di lunghezza arbitraria, utilizzata in coppia con la chiave privata nella crittografia a chiave pubblica. Deve essere resa pubblica.

COMUNICAZIONE: dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

CONTRATTO DI LICENZA D'USO: contratto che ha ad oggetto l'utilizzo di un programma.

CONTRATTO DI SVILUPPO DI SOFTWARE: contratto che ha ad oggetto la creazione o la modificazione di un

programma.

CRITTOGRAFIA: procedimento di codifica e decodifica dei messaggi basata su funzioni parametriche, la cui computazione dipende da un parametro detto chiave.

CRITTOGRAFIA A CHIAVE PRIVATA: metodo crittografico che utilizza una sola chiave condivisa da mittente e destinatario per criptare e decriptare il messaggio.

CRITTOGRAFIA A CHIAVE PUBBLICA: è un metodo asimmetrico basato sull'esistenza di due diverse chiavi, una utilizzata per criptare e una utilizzata per decriptare. Ciascun utente deve quindi possedere due chiavi, una privata che conosce solo lui e una pubblica che rende nota a tutti.

DATO PERSONALE: qualunque informazione riferibile, anche indirettamente, a persona fisica, persona giuridica, ente o associazione.

DATO ANONIMO: il dato che in origine, o a seguito di trattamento, non può essere associato a un interessato identificato o identificabile.

DATI SENSIBILI: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

DENIAL OF SERVICE: è un **attacco** che ha come principale bersaglio la disponibilità delle risorse, in particolare dei sistemi e dei servizi.

DES: (*Data Encryption Standard*) algoritmo di cifratura a **chiave privata** basato su codifica a blocchi e chiave di 56 bit.

DHCP: (*Dynamic Host Configuration Protocol*) è un protocollo per la gestione dinamica di indirizzi IP. I *client* ottengono l'indirizzo IP da un DHCP *server* che gestisce l'assegnazione degli indirizzi in modo dinamico, ovvero assegna a ogni richiesta un indirizzo tra quelli disponibili.

DIFFUSIONE: dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

DIRITTO D'AUTORE: insieme dei diritti morali e patrimoniali riconosciuti all'autore di un'opera dell'ingegno, quale un programma per elaboratore.

DIRITTI MORALE D'AUTORE: diritti incedibili riconosciuti all'autore dell'opera, quali il diritto ad essere riconosciuto autore, il diritto di non pubblicare l'opera, il diritto di opporsi alle pubblicazioni che possano recare pregiudizio alla reputazione dell'autore, il diritto di ritirare l'opera dal commercio qualora ricorrano gravi ragioni morali.

DIRITTI PATRIMONIALI D'AUTORE: diritti trasferibili di utilizzazione economica dell'opera. Sono costituiti dal diritto di pubblicare l'opera, dal diritto di diffonderla, dal diritto di metterla in commercio, dal diritto di elaborarla e dal diritto di tradurla.

DIRITTO SUI GENERIS: diritto del titolare di una banca di dati o di un'opera multimediale di impedire l'estrazione e/o il reimpiego non autorizzati della totalità o di una parte sostanziale del contenuto della banca dati.

DOMAIN CONTROLLER: *server* che controlla il dominio della LAN ovvero l'insieme degli utenti, dei gruppi e delle risorse della LAN. Fornisce meccanismi centralizzati d'accesso per cui gli utenti vengono autenticati e gestiti in modo centralizzato.

ERGONOMIA: disciplina che mira a migliorare sicurezza, salute, *comfort* e benessere dell'utente che utilizza prodotti e

servizi. L'ergonomia del video terminale ha lo scopo di adeguare le postazioni per ridurre gli effetti di affaticamento e di conseguenza i rischi per la salute, prodotti dal lavoro continuativo col *computer*.

EXPLOIT: esecuzione delle azioni necessarie ad approfittare di una vulnerabilità del sistema per sferrare un **attacco** .

FILE SERVER: *server* che offre la gestione dello spazio disco per gli utenti. Un sistema di accesso ai *file* centralizzato consente agli utenti di utilizzare i propri dati da una qualunque delle postazioni della LAN.

FIREWALL: è un sistema connesso alla rete con lo scopo di filtrare i pacchetti in transito che viene tipicamente utilizzato con lo scopo di creare una barriera difensiva che aumenti il grado di **sicurezza** perimetrale di una rete.

FIRMA DIGITALE: tecnologia che mira a garantire **autenticazione** e **integrità** dei documenti elettronici, basata sull'uso di **certificati digitali** .

IMPRONTA VIRALE: è un codice identificativo che il **virus** inserisce nel *software* ospite e che viene utilizzato per identificarlo.

INCARICATO: il soggetto, nominato dal titolare o dal responsabile, che tratta i dati personali.

INTERESSATO: il soggetto al quale si riferiscono i dati personali.

INVENZIONE INDUSTRIALE: opera suscettibile di un'applicazione industriale.

HASH: funzione che calcola una stringa di lunghezza fissata a partire da una stringa più lunga. In crittografia si utilizzano funzioni *hash* non reversibili che non consentono di ricostruire la stringa originale a partire dal valore di *hash*.

MACROVIRUS: sono **virus** costruiti con linguaggi di *script* per le macro (VBA, *Visual Basic for Application*) e incorporati in *file* creati con pacchetti di produttività personale (come per esempio i *file* .DOC).

MAIL SERVER: offre servizi *mail* ed è necessario se si vogliono di utilizzare molti *account* di posta (come accade quando si vuole offrire la posta a tutti gli studenti e i docenti).

MALICIOUS SOFTWARE: è un *software* o una porzione di *software* che produce effetti dannosi o non desiderati. Sono esempi di *malicious software* i **cavalli di Troia** , i **virus** e i ***worm*** .

MASTER BOOT RECORD: è il settore del disco fisso che contiene il *bootstrap loader* ovvero la *routine* di avvio del sistema operativo.

MD5: (*Message Digest* 5, 1992) è un algoritmo di *hash* utilizzato per produrre ***fingerprint*** di un messaggio.

MESSAGE DIGEST/FINGERPRINT: sequenza di caratteri molto ridotta che rappresenta un messaggio più lungo.

MIRRORING: è una tecnica di miglioramento dell'affidabilità in cui ogni disco viene moltiplicato (almeno duplicato) e dunque esiste almeno una copia di sicurezza di ogni informazione.

MISURE MINIME DI SICUREZZA: le misure previste dal d.p.r. 318/99.

NAT: (*Network Address Translation*) è una tecnica con la quale un *router* interviene sui pacchetti, allo scopo di sostituire indirizzi IP pubblici con indirizzi della rete privata e viceversa.

OPERA DELL'INGEGNO: opera di carattere creativo appartenente alle scienze, alla letteratura, alla musica, eccetera, quale che ne sia il modo o la forma di espressione.

PASSWORD: sequenza di caratteri utilizzati come credenziale di **autenticazione** per provare l'identità di un utente.

PAT: (*Port Addres Translation*) servizio aggiuntivo del **NAT** che consente di gestire la sostituzione anche a livello TCP e UDP.

PGP: è un insieme di *tool* che integra crittografia a chiave privata e crittografia a chiave pubblica per garantire **riservatezza**, **integrità** e **autenticazione** .

PKI: l'insieme costituito da tutte le parti che operano per la certificazione (utenti e *authority*) nonché dalle tecnologie che queste utilizzano, dai servizi che offrono e dalle politiche di gestione che attuano.

PRINT SERVER: *Server* che gestisce la/le stampanti, rendendole disponibili da tutte le postazioni della LAN. Mantiene in coda i *task* di stampa.

RAID: (*Redundant Array of Independent Disks*) indica un complesso meccanismo di memorizzazione che utilizza più dischi fissi con l'obiettivo di aumentare le prestazioni della memoria di massa in termini di velocità e di affidabilità. È basato sulla combinazione di ***striping*** , ***mirroring*** e **blocchi di parità** .

REGISTRATION AUTHORITY: ente di fiducia che effettua l'identificazione dei soggetti che richiedono il **certificato digitale** .

RESPONSABILE: il soggetto preposto dal titolare ad un trattamento dei dati personale.

RESPONSABILITÀ CIVILE: obbligazione di risarcire il danno cagionato.

RESTORE: operazione di recupero dei dati da una copia di ***backup*** che mira a ripristinare una situazione stabile antecedente al verificarsi di un errore.

RSA: algoritmo di crittografia a chiave pubblica reso noto nel 1978. L'acronimo RSA è derivato dal nome dei suoi creatori *Rivest*, *Shamir* e *Adleman*.

SICUREZZA INFORMATICA: insieme di misure atte a preservare confidenzialità, integrità e disponibilità, dei dati e delle risorse *hardware* e *software* utilizzate per la loro gestione.

SMART CARD: tessera plastificata delle dimensioni di una carta di credito, su cui è integrato un *microchip* programmabile. La *smart card* è un supporto utilizzato per la **firma digitale** .

SNIFFING: è un **attacco** di tipo passivo che mira a compromettere riservatezza e **autenticazione** effettuando intercettazioni delle comunicazioni.

SPOOFING: indica diversi tipi di **attacco** che hanno come meccanica comune quella della sostituzione: degli indirizzi di rete (*IP address spoofing*), degli utenti (*user account spoofing*), del contenuto dei messaggi (*data spoofing*).

SSL: (*Secure Sockets Layer*) protocollo utilizzato per la navigazione *Web* sicura che consente all'utente di identificare in modo univoco il *server Web*, e cripta la comunicazione tra *client* e *server*. È basato sull'uso di **certificati digitali** .

STRIPING: è una tecnica di miglioramento della velocità di lettura/scrittura che consiste nello spalmare i dati di un blocco in più dischi. Il blocco viene diviso in n sottoblocchi ognuno dei quali è memorizzato su un disco diverso e ogni lettura innesca n letture (da n dischi), riducendo il tempo di trasferimento e di latenza.

TITOLARE: il soggetto che assume le decisioni sulle modalità e le finalità del trattamento.

TRATTAMENTO: qualunque operazione effettuata sui dati personali, come mezzi informatizzati o non informatizzati.

UPS: (*Uninterruptible Power Supply*) gruppo di continuità ovvero sistema di alimentazione che ha l'obiettivo di fornire energia anche quando non viene direttamente rifornito perché l'erogazione della rete elettrica si interrompe o è instabile.

USERNAME: l'identificativo dell'utente all'interno del sistema. È associato a una ***password*** che consente di verificare l'identità dell'utente.

VIRUS: sono porzioni di codice (di tipo ***malicious software***) che hanno la caratteristica di autoreplicarsi e inserire se stessi in *file* eseguibili preesistenti sul sistema. Una volta diffusa l'infezione compromettono l'integrità delle informazioni e la disponibilità delle risorse.

VIRUS MULTIPARTITO: è un virus che utilizza più modalità di trasmissione contemporaneamente.

VIRUS POLIMORFO: è un **virus** che modifica il proprio codice a ogni infezione per rendere più difficile il riconoscimento. È costituito dal codice del virus, dal *polymorphic engine* (entrambi **criptati**) e dalla funzione per decifrarli. Il *polymorphic engine* calcola la coppia di funzioni (cifratura, decifratura) che serve a generare una nuova copia del virus mutata.

WEB SERVER: rende disponibili i documenti attraverso il protocollo HTTP e dunque è destinato a contenere il sito Web della scuola.

WIRELESS: indica una specifica tipologia di comunicazioni che utilizza come mezzo fisico per il trasporto dei dati l'etere.

WIFI: (*Wireless Fidelity*) indica una ***Wireless*** LAN basata sullo standard 802.11b (della famiglia **802.11**) che opera a 2,4Ghz di frequenza e raggiunge una larghezza di banda massima 11Mbps.

WORM: sono programmi (di tipo ***malicious software***) che utilizzano i servizi di rete per propagarsi da un sistema all'altro e agiscono creando copie di se stessi sugli *host* ospiti e mettendosi in esecuzione.

802.11: è lo standard sviluppato per le *Wireless* LAN e può essere comparato con lo standard 802.3 definito per le reti locali basate su *Ethernet*.

Autori

Hanno realizzato il materiale di questo modulo:

Prof.ssa Giusella Finocchiaro
Professore associato di diritto di Internet nell'Università di Bologna.
Avvocato e titolare dello Studio Legale Finocchiaro, specializzato in diritto dell'informatica.
Autrice di sei monografie (fra cui: Diritto di Internet, Zanichelli, Bologna, 2001; La firma digitale, nel Commentario del codice civile Scialoja-Branca, diretto da F. Galgano, Zanichelli, Bologna-Roma, 2000) e di oltre 50 articoli e contributi, pubblicati su riviste italiane e internazionali.
Ha fatto parte di alcuni organismi internazionali, quali il Gruppo di esperti dell'UNCITRAL (Commissione delle Nazioni Unite sul commercio internazionale) sulle firme elettroniche(1997-2001) e il Gruppo di esperti dell'ITC-WTO sul commercio elettronico.
Ha lavorato in progetti internazionali concernenti il commercio elettronico e argomenti collegati.
Insegna anche all'Università L. Bocconi di Milano, dal 1994.
Collabora con Il Sole-24 Ore sui temi di *cyber*diritto, dal 1995.

Dott. Diego Gardini
Funzionario dell'Area Tecnica, Tecnico Scientifica ed Elaborazione Dati, presso il Polo Scientifico-Didattico di Cesena

dell'Università di Bologna. È responsabile del coordinamento del personale tecnico per le esigenze delle attività informatiche dell'amministrazione del Polo Scientifico-Didattico di Cesena e del Corso di Laurea in Scienze dell'Informazione. È responsabile del coordinamento degli acquisti informatici e del supporto tecnico informatico per tutte le strutture afferenti al Polo Scientifico-Didattico di Cesena dell'Università di Bologna. È referente per i collegamenti di rete per tutte le strutture afferenti al Polo Scientifico-Didattico di Cesena. Ha collaborato con il centro *the Abdus salam - international centre for theoretical physics* (ICTP) di Trieste nell'ambito del programma scientifico dell'attività UNU/ICTP *Autumn Training Activity on Networking and Radiocommunications*.

Prof.ssa Paola Salomoni
Professore Associato di Informatica presso l'Università di Bologna, dove insegna Sistemi Operativi e Sistemi Multimediali. È docente del corso di Ipermedia in Rete nell'ambito del Master in Tecnologie e applicazioni multimediali dell'Università degli Studi di Bologna di cui è anche vice-direttore. È codocente del corso di *Design* Multimediale nell'ambito del Master in Comunicazione e Tecnologie dell'Informazione tenuto presso AlmaWeb - *Graduate School of Information Technology, Management and Communication* dell'Università degli Studi di Bologna. Ha pubblicato su numerose riviste nazionali e internazionali su tematiche correlate alle applicazioni multimediali distribuite, con particolare attenzione alle reti *wireless*, e ai sistemi multimediali per il *distance learning*.