Uso sicuro della rete e browser per bambini

di Giovanni Marcianò (http://margi.bmm.it)

BIOGRAFIA

dal 1992 segue attivamente l'impiego didattico delle TIC, dal 1999 si occupa di metodologia didattica nelle azioni di FAD per il personale della scuola, fa parte della *Società Italiana per l'e-Learning* (Politecnico di Milano). Promuove da anni il costruttivismo come modello d'impiego delle TIC nella scuola dell'infanzia ed elementare. Dal 2001 ha curato diverse iniziative di studio e promozione dell'uso consapevole delle TIC a scuola e in famiglia.

SOMMARIO

Premessa e guida alla lettura

Dalla metà degli anni '90 l'Amministrazione scolastica ha svolto una crescente azione mirata a dotare le scuole italiane di ogni ordine e grado di infrastrutture tecnologiche al passo coi tempi [1]. Non solo computer, ma anche reti interne (LAN) e accesso a Internet.

Sempre più numerose sono anche state le occasioni di formazione per gli insegnanti, inizialmente per avvicinarsi a questi strumenti, poi anche per padroneggiarne le innumerevoli potenzialità di supporto all'attività didattica. Dai corsi previsti nei progetti 1A del PSTD [2], al piano nazionale UMTS "ForTic" [3]: un crescendo di occasioni

[1] Dai progetti sperimentali Telecomunicando e Multilab, ai piani nazionali come il PSTD 1997-2000 (Programma di Sviluppo Tecnologie Didattiche). Nel 2001 ulteriori finanziamenti con la CM 152, e nel 2002 con la CM 114, quest'ultima comprendente un chiaro indirizzo verso l'impiego sistematico di Internet sia per l'attività amministrativa che didattica.

[2] 30 ore di "alfabetizzazione", in cui la parte finale del programma di massima riguardava per l'appunto Internet e il suo uso. Il PSTD ha riguardato tutte le Istituzioni scolastiche italiane.

[3] CCMM 55 e 116/2002. La denominazione "UMTS" indica la fonte della risorsa finanziaria – 150 mld di lire - che fu destinata a questo piano, che giungeva dall'asta delle licenze UMTS. ForTic da "Piano Nazionale di **For**mazione alle **TIC** - Tecnologie dell'Informazione e della Comunicazione". 120 ore di formazione, 60 in aula e 60 di autoformazione a distanza per quasi 190.000 docenti in servizio.

per far crescere le competenze professionali specifiche nell'impiego delle nuove tecnologie nel corpo docente della scuola italiana.

Tutto ciò ha reso ormai normale che le scuole si connettano al vasto mondo di Internet per svolgere esperienze formative, per condurre in modo più efficace ed efficiente le funzioni amministrative, per tenersi informati sulle ultime norme o su nuove opportunità didattiche. Via Internet si può facilmente fare ricerca, comunicare, documentare il proprio lavoro pubblicando i lavori realizzati in classe.

Ma sempre meno si può ignorare che Internet è anche una potenziale fonte di rischi, tanto più rilevanti quanto meno è diffusa una cultura relativa ai modi legittimi di usarlo e alla consapevolezza delle funzioni che la Rete rende possibili, funzioni spesso utili ma che possono nascondere rischi di cui è necessario essere consapevoli, come primo livello preventivo di sicurezza.

In questo contributo, per la nuova azione formativa del personale docente, intendo sottoporre alcuni elementi per lo sviluppo di una cultura d'uso corretto e consapevole di Internet, tramite il richiamo a norme vigenti, con l'indicazione di prassi opportune, l'invito a un sempre più professionale e consapevole uso.

Infine qualche indicazione su strumenti specifici, ma ben sapendo che il tema qui trattato non trova, e non troverà, soluzioni "automatiche". Ogni applicazione informatica per la sicurezza può solo aiutare chi è consapevole, chi sa quali rischi son possibili. E non è giusto trasformare un insegnante in un tecnico informatico. Ma di certo sono da conoscere alcuni strumenti che fondono l'attenzione alla sicurezza con pari attenzione alle esigenze didattiche dell'insegnante.

Le indicazioni qui riportate sono riferite a un uso generico delle infrastrutture di rete. L'attenzione è rivolta prevalentemente all'insegnante che vuole accompagnare i propri alunni a conoscere la rete e le se grandi potenzialità. E che in questa esperienza vuol procedere al riparo dai rischi che son presenti.

1) Valori dell'uso consapevole

Seymour Papert, intervistato nel 1997 mentre era ospite in Italia [4], alla domanda:

> *"In Italia, alcuni parlano di rendere effettivo un regolamento per difendere i bambini dal rischio delle tecnologie, per avere delle regole da seguire. Navigare in Internet può costituire un pericolo, per bambini e ragazzi, nell'avvicinarsi a contenuti come la pornografia, o la violenza."*

rispondeva già con un forte scetticismo verso facili soluzioni tecnologiche, o divieti espliciti, o anche all'idea di poter "tenere fuori" dalla scuola o dalle case Internet. Poneva invece già allora, in coerenza con la sua pedagogia del vivere quotidiano nel III millennio[5], le basi per valorizzare il rapporto adulto – bambino, che proprio intorno al tema della sicurezza in rete può trovare un forte senso educativo [6]. Diceva infatti:

> *Prima di tutto, non credo che funzionerà, e la gente perde il proprio tempo a pensare ad una soluzione del genere. La vera soluzione si trova nel dare fiducia ai bambini. Dobbiamo discutere di queste cose con i nostri bambini. Se vediamo che non riescono a parlare di quello che vedono, c'è qualcosa di sbagliato nel nostro*

[4] http://www.mediamente.rai.it/home/bibliote/intervis/p/papert.htm
[5] v. Papert S., The Connected Family: bridging the digital generation gap (1996). http://www.connectedfamily.com
[6] educativa nel senso etimologico del termine, di *accompagnamento per la crescita*. Non certo come nuova materia di studio.

> *rapporto con i bambini. Credo che sia più importante per le famiglie pensare perché ci sia un problema, piuttosto che pensare a delle soluzioni tecnologiche. La soluzione sta nella natura della famiglia e nella relazione con la gente. Conosco molti bambini; i miei nipotini passano molto tempo con i computer e non penso che facciano nulla di male. Occasionalmente si imbattono in qualcosa che non va bene e ne parlano. Dicono: "Abbiamo visto una cosa buffa". Ne discutono. Penso non ci sia del male.*

Dobbiamo quindi pensare alle tecnologie come una nuova occasione, un nuovo motivo di relazione educativa con i giovani. Dal 1997 ad oggi tutti siamo ormai coscienti di quanto le tecnologie digitali affascinino i giovani. La realtà statunitense a cui Papert riferiva il quotidiano dei suoi nipotini è ormai scenario corrente anche in Italia. Resta però un elemento importante fortemente critico: quanto le famiglie, ma anche la scuola, sono preparati a questo nuovo fronte dell'educazione? Proseguiva Papert dicendo:

> *Però, certi genitori non sanno che cosa fanno i propri bambini, e molti bambini non si fidano dei genitori, oppure, addirittura, alcuni bambini pensano che quando i genitori dicono: "Non fare questo", si tratti di una buona cosa da farsi. Se questo è il proprio rapporto con i bambini, si deve essere coscienti di avere un grave problema, e si deve cercare di risolverlo. E allora, naturalmente, questi bambini vogliono spiare delle cose e non dire ai genitori quello che hanno visto, e le cose vanno di male in peggio. In questi casi la tecnologia aggrava un problema che esisteva già. Non crea il problema. Ma penso che contenga la possibilità di soluzione.*

In questa ultima considerazione, sul fatto che le tecnologie finiscano per amplificare dinamiche relazionali già presenti, c'è molto da riflettere. E proprio su questo piano, quello della positiva relazione tra adulti e bambini, ancor più tra adulti e ragazzi, che ritengo importante che si maturi nella scuola una forte esperienza che possa essere di riferimento alle famiglie.

Educare non è mai stato facile; la scuola nell'era moderna è nata proprio perché l'educazione presuppone una professionalità specifica, di cui gli Stati si son fatti responsabili attraverso la Scuola pubblica di Stato, e l'istruzione obbligatoria. Il che non ha tolto, e non toglie, alla famiglia l'importante ruolo da sempre avuto, ma porta la scuola ad essere un valido ausilio nel momento in cui il bambino è in grado di esplorare il mondo che lo circonda. Ieri un mondo fisico, oggi anche virtuale.

Vorrei che il tema dell'uso consapevole delle tecnologie rientrasse in questo corretto contesto di educazione congiunta, nella scuola e in famiglia. La scuola, in questo momento, è certamente più in grado di raccogliere questa sfida rispetto alla famiglia. A scuola l'impiego delle tecnologie riferite all'attività didattica è sempre più comune. Se svolto con attenzione al corretto uso, allora rappresenta l'occasione per propagare anche verso i genitori, spesso coinvolti dai figli nell'uso domestico di Internet, una "cultura della sicurezza" sempre meno opzionale per la formazione dei giovani.

> *Lavorare con i bambini, con i computer, offre ai genitori e ai bambini l'opportunità di sviluppare progetti più collaborativi, di apprendere insieme, di condividere qualcosa di molto ricco, in cui i bambini sono, in effetti, molto bravi ad apprendere e possono insegnare ai genitori. Penso che attraverso queste tecnologie abbiamo molta più opportunità di migliorare la vita dei bambini e la relazione tra i bambini e i genitori, piuttosto che il contrario. Ma i genitori devono comprendere che devono passare del tempo, devono imparare ad usare il computer, e devono essere disposti ad avere una mente più aperta su quello che i bambini debbano apprendere e di quello che non debbano apprendere, e di come l'apprendimento*

> *debba funzionare. Il computer rende solo visibile un problema che c'era già nell'attitudine dei genitori.*

È quest'ultimo punto, "*una mente più aperta su quello che i bambini debbano apprendere"*, che è importante avere chiarezza, prima di tutto a scuola. Se intendiamo il ricorso alle TIC semplicemente come un modo più efficiente di scrivere, calcolare e disegnare, allora il problema della sicurezza non esiste.

Se invece alle TIC chiediamo l'accesso a patrimoni di informazione senza limiti, l'estensione dei confini comunicativi oltre il chiuso dell'aula, impegnando gli alunni a confrontarsi con l'uso di questo strumento che ha modificato radicalmente tanti uso quotidiani del nostro recente passato – si pensi solo al servizio di posta elettronica – allora è proprio il fronte della sicurezza quello in cui la funzione educante della scuola ha ampio spazio d'espressione, con gli alunni e tramite essi anche con le loro famiglie.

Vediamo quindi cosa è bene avere presente, conoscere, non tanto per un'applicazione diretta, quanto per saper cogliere i migliori orientamenti in un campo affatto immobile, in cui nuovi servizi – e quindi nuovi potenziali rischi – nascono quotidianamente.

2) Navigazione sicura

Attraverso l'infrastruttura di rete locale (LAN) nella scuola è ormai un caso comune avere accesso istantaneo a Internet da ogni postazione, nei laboratori e non solo. L'evoluzione tecnologica e del mercato ha reso la realizzazione di una rete d'istituto molto economica a fronte dei benefici che porta, e per questo le indicazioni del Ministero - in più occasioni di finanziamento – incoraggiavano l'investimento su questo fronte. Con tecnologie tradizionali, via cavo, ove possibile. E ora anche con ricorso alla tecnologia wireless – WiFi – dove situazioni infrastrutturali rendono complessa la stesura di cavi nelle sedi scolastiche.

Come ogni altro servizio della scuola – biblioteca, palestra, mensa ecc. – è regolamentato per garantirene il corretto uso da parte del personale e degli allievi, così dovrebbe essere pure per la LAN. La definizione, in ogni Istituzione scolastica, delle "regole condivise per l'uso della rete locale e dei servizi su di essa attivati" introduce direttamente il tema dell'uso sicuro e consapevole, a garanzia di evitare danni all'infrastruttura, alle persone, alla scuola in genere. L'insieme delle regole d'uso viene tecnicamente definito "policy".

a) La policy d'Istituto

La definizione della Policy d'Istituto spetta istituzionalmente al Dirigente scolastico che, come per il Regolamento d'Istituto, ne garantisce l'applicazione. E questo è un aspetto formale, che incide sul valore delle regole. Prima però queste regole devono essere individuate, ed espresse. E come non esiste un unico "Regolamento d'Istituto" valido in generale nella scuola, parimenti la Policy d'Istituto deve essere scritta con stretto riferimento alla realtà della singola Istituzione scolastica.

I punti generali su cui concentrare la propria attenzione nella stesura del documento che definisce la Policy d'Istituto sono principalmente questi:

i) regolamentare

- **chi** e **come** può avere accesso alle **postazioni** in rete della scuola, prevedendo i diversi casi a seconda dei soggetti operanti nell'Istituto: personale in servizio, allievi, eventuali soggetti esterni alla scuola
- **chi** e **come** può accedere ai **servizi** resi disponibili sui computer in rete, sempre con riferimento ai diversi soggetti operanti nell'Istituto;
- **come** si garantisce la tutela della **privacy** nell'uso degli strumenti tecnologici d'Istituto.

ii) adottare strumenti hardware e/o software

- per prevenire l'uso improprio dell'accesso a Internet. Ad esempio è importante definire con chiarezza come provvedere alla gestione del log [7] relativo al traffico generato sulla LAN in uscita e in entrata verso Internet;
- per evitare danni causati da virus o da altro software [8] che viola le norme sopra definite;
- contro il rischio di intrusioni indesiderate dall'esterno della LAN;
- per ridurre al minimo i tempi di recupero della piena funzionalità dell'infrastruttura in caso di guasto del sistema.

È importante che le regole (policy), una volta definite vengano comprese nel Regolamento d'Istituto. Così rappresentano una linea di condotta precisa e chiara cui tutti gli utenti debbano attenersi. È evidente che queste regole devono avere una valenza formativa, e non solo sanzionatoria, perché il loro scopo è principalmente quello di aiutare gli utenti meno esperti a orientarsi in merito a temi come la tutela della privacy, la libertà di espressione, il rischio di plagio, la necessità di identificazione e identità di rete, l'etica della rete, la conoscenza dei vincoli legali, il rischio di molestie via Internet e così via. Una fetta di legalità da garantire non sono nel reale quotidiano, ma anche nel virtuale.

L'aver definito all'interno dell'Istituzione scolastica regole chiare è una buona base per lavorare serenamente, sicuri di aver posto in atto quanto possibile in chiave di prevenzione. Dato che poi il Regolamento di Istituto viene di solito distribuito agli studenti all'inizio dell'anno scolastico, l'inserimento al suo interno delle regole condivise per l'uso della rete permette alla scuola di informare anche le famiglie, divulgando elementi di quella cultura del corretto uso delle TIC a cui accennavo in premessa.

Dovrebbe essere affissa nei laboratori e nei luoghi di accesso alla rete (biblioteche, aule, postazioni singole) oltre che pubblicata sul sito della scuola. La policy è bene che si estenda all'uso della rete da parte di tutti i dipendenti della scuola, per essere effettiva e non simbolica.

Un aiuto alla stesura delle regole condivise da inserire nel Regolamento d'Istituto è reperibile nei documenti per la sottoscrizione della "Politica d'Uso Accettabile e Sicura della Scuola esemplare" curate dall'"European schoolnet" , disponibili anche il lingua italiana. L'Ufficio Scolastico Regionale per il Piemonte ha attivo un forum dedicato al

[7] Ovvero il registro che riporta gli indirizzi, l'orario, e vari altri elementi delle richieste / risposte in entrata / uscita. È un'operazione automatica, che spesso è curata anche dal fornitore del servizio di accesso a Internet. Ma bisogna sapere, in caso servisse, chi contattare.

[8] Ad esempio il cosiddetto "*spyware*", che legge informazioni sul computer e di soppiatto lo invia a qualcuno via Internet. Con rischio di violazione della privacy.

tema [9], aperto a tutti, in cui molte scuola han depositato loro documenti. È possibile accedere anche ad approfondimenti presenti sul sito del MIUR [10] e del Governo [11].

b) L'accesso al world wide web

Il "Monitoraggio Tecnologie Didattiche" svolto dal Ministero [12] indica come la scuola sia l'ultimo dei luoghi in cui i ragazzi in età dell'obbligo scolastico hanno occasione di connettersi a Internet . Il dato può apparire rassicurante dal punto di vista della tutela dei minori verso l'esposizione ai rischi della rete, ma anche preoccupante per il mancato ruolo di guida che la scuola dovrebbe svolgere verso gli alunni e le famiglie.

Riporto qui alcune indicazioni che possono essere di riferimento, che si propongono anche come tema di approfondimento nel contesto d'aula di questa azione formativa. Oltre che – ovviamente – al momento della programmazione didattica e di stesura del POF nella propria sede di servizio.

i) scuola primaria

Il Monitoraggio prima citato indica che il 68% degli alunni di Circoli didattici che hanno utilizzato almeno qualche volta Internet, l'hanno fatto da casa. Solo l'11% da scuola. Il 54% di chi si è connesso almeno qualche volta a Internet l'ha fatto per svolgere ricerche assegnate come compito scolastico.

Di certo nell'ultimo anno il contesto sarà mutato, alzando anche un po' la percentuale di alunni che hanno potuto conoscere Internet a scuola. Ma son sicuro che la prevalenza delle ricerche su Internet resta. È possibile che tali attività di ricerca si svolgano a scuola, almeno come prima esperienza, educando gli alunni all'uso degli strumenti loro appositamente dedicati? Da qualche anno su Internet sono disponibili appositi motori di ricerca per minori, di cui chi opera a scuola deve avere conoscenza per privilegiare tali strumenti, che offrono certamente maggiori garanzie di tutela dei minori rispetto agli equivalenti strumenti d'uso generico.

E anche nell'assegnare agli alunni compiti di ricerca da svolgere a casa, gli insegnanti sarebbe bene curare che i bambini riportino sul diario personale, insieme all'argomento assegnato, gli strumenti adatti a una ricerca su Internet sicura [13]. Tale indicazione può anche essere data direttamente alle famiglie degli alunni che ricorrono a Internet per lo svolgimento dei compiti a casa.

D'altro canto, sono sempre più numerosi e in lingua italiana i siti Internet appositamente dedicati alla navigazione dei bambini, ricchi di consigli per genitori e insegnanti, e anche rivolti a precise fasce d'età o a tematiche infantili. I docenti formati dai corsi ForTic - percorso B hanno avuto occasione di approfondire questi aspetti, e di poter essere un riferimento interno alla scuola per avere informazioni aggiornate sul tema.

Sempre per tenersi aggiornati, si possono seguire siti come kidsfreeware [14] che tra le tante risorse free per bambini ha anche sezioni specifiche su browser e altri strumenti per Internet (sezione: surfing the web); e anche i suggerimenti e le informazioni

---

[9] Forum "UsoSicuro", accessibile previa registrazione online su http://www.siscas.net/forum/usosicuro
[10] v. http://www.istruzione.it/innovazione/tecnologie/consapevole.shtml
[11] v. http://www.italia.gov.it/chihapauradellarete/index.html
[12] v. MIUR "*Progetto Monitoraggio tecnologie didattiche*", abstract, 2003, p. 10 - http://www.istruzione.it/innovazione/news/2003/allegati/abstract_monitoraggi.pdf
[13] A titolo d'esempio si vedano http://www.baol.it/ - http://www.simpaticoland.com/
[14] http://www.kidsfreeware.com

messe a disposizione su Internet dalle forze della Polizia di Stato [15] e dell'Arma dei Carabinieri [16].

Dal quadro generale descritto, composto da molte risorse liberamente fruibili in rete, si collocano a parte strumenti a pagamento. Essenzialmente distinguibili in due tipologie: filtri e browser dedicati.

I primi possono essere previsti da chi fornisce l'accesso a Internet, come esempio cito Davide.it [17] un provider italiano nato proprio per offrire connessioni filtrate. In questo caso la scuola non ha alcun onere di tipo tecnico, nulla da installare, aggiornare ecc. ma beneficia del lavoro "a monte" fatto da chi collega la scuola a Internet, il provider. In questo caso un provider speciale.

Sul fronte dei browser per bambini cito un prodotto italiano [18], nato da poco e di cui ho avuto modo di seguire la sperimentazione in 11 scuole piemontesi: Il Veliero [19]. Rimando per i dettagli al laboratorio "Il Veliero – navigazione, e-mail e chat sicuri".

ii) scuola secondaria

Molti aspetti riferiti alla scuola primaria valgono anche nei contesti di scuola secondaria di primo e di secondo grado. La diversa età degli alunni e le più ampie tematiche disciplinari comportano un uso più maturo e ampio delle nuove tecnologie, con l'adozione di strumenti software e di servizi di rete standard, in luogo di quelli dedicati prima presentati.

Fermo restando il fatto che non è possibile una sicurezza totale garantita da accorgimenti tecnologici, ciò non significa che non si debbano attivare tutte le misure tecniche possibili per un efficace controllo della navigazione. Dopo di che, proprio per la mancanza di garanzie assolute dal lato tecnico, è importante porre la propria attenzione alle valenze educative e agli obiettivi formativi della scuola. Così come i Regolamenti d'Istituto indirizzano il comportamento personale degli allievi verso la correttezza nei confronti degli adulti, dei compagni, dei locali scolastici, altrettanto può essere fatto in merito al comportamento che gli alunni devono avere nell'impiego dell'accesso a Internet che la scuola mette a loro disposizione.

La programmazione didattica della scuola può prevedere, tra gli obiettivi formativi, il corretto e maturo rapporto con le nuove tecnologie da parte degli allievi, facendo rientrare a pieno titolo nelle funzioni educative della scuola la formazione dei giovani all'uso corretto delle risorse di rete dell'Istituto e di Internet.

3) Comunicazione sicura

a) Posta elettronica

Il servizio di posta elettronica è, dopo la navigazione, certamente il più conosciuto e utilizzato dagli utenti di Internet. Permette di unire i vantaggi della rete mondiale Internet, che annulla le distanze, con la tradizione della corrispondenza testuale.

---

[15] v. http://www.poliziadistato.it/pds/cittadino/consigli/internet.htm
[16] v. http://www.carabinieri.it/cittadino/consigli/tematici/internet.htm
[17] v. http://www.davide.it
[18] esiste un altro browser, di cui si può trovare la versione tradotta in italiano, Kiwe. v. http://www.kiwe.net/kiwebrowser.htm
[19] v. www.ilveliero.info

L'uso a scuola del servizio di posta elettronica è già molto diffuso e praticato, a tutti i livelli. Tra gli adulti, ma anche tra i ragazzi. Quello che appare più evidente è un uso prevalentemente "privato" di questo servizio. Il MIUR con "Scriviamocinrete" ha messo a disposizione del personale scolastico una casella di posta elettronica istituzionale, nella forma nome.cognome@istruzione.it [20].

Il fatto che il gestore del servizio di posta elettronica sia il MIUR qualifica il titolare di una casella istituzionale per il ruolo professionale che riveste. Infatti il Ministero assegna l'account non in modo generico, ma dopo la verifica del fatto che il richiedente sia un dirigente scolastico o un docente in servizio a tempo indeterminato.

i) Gli insegnanti

Sono sempre più numerosi gli insegnanti che si trovano ad impiegare la posta elettronica per comunicare con colleghi e anche con genitori dei propri allievi.

Trattandosi di comunicazione tra soggetti maggiorenni non presenta particolare rischi, se non quelli tipici del servizio di posta elettronica [21]. L'impiego dell'account nel dominio istruzione.it autentica il corrispondente con cui si scambiano messaggi. Nel caso di account diversi (cosa normale nel caso dei genitori) è bene avere la certezza che dietro l'indirizzo utilizzato per l'invio vi sia davvero la persona con cui intendiamo corrispondere.

Una certa cautela è infatti da porre nell'acquisizione di tale indirizzo, e nella definizione di questa modalità di conduzione del rapporto scuola-famiglia. Solo il colloquio diretto coi genitori permette di avere questa sicurezza all'atto dell'avvio di uno scambio di e-mail. Non sono rari i casi in cui nostri colleghi han scoperto che il servizio di posta, a casa, viene gestito dai figli, e non dai genitori.

ii) Posta tra insegnanti e alunni

Rispetto al contenuto della corrispondenza con i propri alunni per via elettronica valgono ovviamente gli stessi riferimenti di correttezza da applicare alla corrispondenza tradizionale. L'uso della posta elettronica richiede ulteriori cautele.

In primo luogo, gli indirizzi personali di posta degli alunni non devono essere divulgati. Questa cautela va applicata in modo molto attento se l'indirizzo è personale dell'alunno, è comunque opportuna anche nel caso in cui il ragazzo utilizzi un indirizzo familiare. Si deve privilegiare quindi l'invio diretto al singolo indirizzo di mail piuttosto che a liste.

Nel caso di invii a gruppi di alunni o a gruppi compositi si devono evitare liste di indirizzi nei campi "To:" oppure "Cc:" [22], preferendo in questi casi il campo "Bcc:" che resterà nascosto ai destinatari. Si privilegi inoltre l'uso di un client di posta piuttosto che il servizio webmail: solo col client di posta la documentazione del traffico in uscita e in arrivo resterà sul proprio personal computer a propria completa disposizione.

Un secondo fronte di attenzione deve essere quello dell'impiego della casella di posta degli alunni per l'iscrizione a servizi di rete di vario genere. Ormai quasi tutti i servizi messi a disposizione sulla rete, laddove richiedono una registrazione per usufruirne,

---

[20] v. http://www.istruzione.it/posta_docenti

[21] A questo proposito è bene essere al corrente delle norme di "galateo in rete" (*netiquette*) consultabile all'indirizzo http://www.istruzione.it/posta_docenti/netiquette.pdf

[22] nelle versioni italiane dei client di posta "A:" e "Cc:". Questi campi sono visibili a tutti i destinatari, e così tutti gli indirizzi di posta possono essere acquisiti dai destinatari del messaggio.

fanno capo alla mail personale quale strumento di verifica dell'identità del nuovo iscritto. Dato che ogni servizio attivato, anche completamente gratuito, comporta la sottoscrizione di un contratto, appare chiara la cautela da porre in tale operazione. Inoltre molti servizi invitano colui che si iscrive, ma anche a volte lo vincolano, a concedere l'autorizzazione all'uso della propria e-mail per l'inoltro di informazioni di vario tipo, spesso commerciali, da parte del gestore del servizio ma anche di terze parti. Ben si comprende come tale prassi risulti non opportuna.

L'esigenza di adottare particolari cautele non deve scoraggiare dall'uso della posta elettronica! Non è ignorando gli aspetti di criticità che si risolvono i problemi connessi con il suo corretto uso. Una soluzione che affronta alla base molti di tali problemi e che si invita a tenere nella massima considerazione attiene la gestione in proprio, da parte della singola Istituzione scolastica o di Reti di scuole, del servizio di posta elettronica per gli alunni. Laddove la generazione e gestione degli account di posta degli alunni fosse amministrata direttamente da personale della scuola tutti i rischi e le relative cautele assumerebbero una rilevanza decisamente minore, in quanto ogni disguido o indesiderato effetto sarebbe facilmente recuperabile o annullabile. Non è una cosa semplice, ma ultimamente più frequente.

iii) Gli alunni

Come per ogni attività scolastica è bene che gli alunni utilizzino a scuola la posta elettronica personale solo per attività didattiche programmate dai propri insegnanti. Anche se l'uso della posta avviene in spazi e orari didatticamente significativi, restano alcuni aspetti da valutare attentamente. Vediamoli.

Il primo elemento da considerare riguarda i contenuti ricevuti/inviati, e attiene il corretto rapporto tra l'alunno e l'Istituto, sia in merito all'uso diligente delle strutture e dei servizi messi a disposizione dalla scuola, sia per il valore formativo che questa attività, se svolta a scuola, deve rivestire. Mentre l'alunno può essere responsabilizzato in merito alla posta che invia, incerto resta il contenuto della posta che egli può ricevere. La posta elettronica è oggi il principale canale di diffusione di malfare, in grado di danneggiare un computer in svariati modi, comportando quindi disfunzioni varie.

Un secondo e più complesso aspetto riguarda la gestione dei dati sensibili o personali - e quindi riservati - che la configurazione e l'uso di un programma di posta (client) comporta. Va ricordato, a questo proposito, che i servizi di ricezione/invio della posta possono essere disabilitati, o configurati in modalità opportuna coerentemente con quanto definito a livello della policy d'Istituto. È comunque opportuno che gli alunni siano indirizzati a usare il servizio di webmail, che permette il controllo della propria casella e lo svolgimento di corrispondenza senza depositare dati sensibili nel client di posta del computer della scuola. Infatti, usando il servizio di webmail, i contenuti della corrispondenza, così come i dati relativi all'account e alla password di accesso dell'alunno, sono gestiti a livello del server, e ciò elimina l'onere di gestione di dati sensibili e/o personali da parte della scuola.

iv) Software per la posta sicura

Vi sono prodotti commerciali appositamente sviluppati per l'uso sicuro della posta da parte dei piccoli utenti di Internet. In italiano vi è MyM@il, un vero e proprio client di posta per bambini, e Il Veliero, già citato per la navigazione sul web, che nella versione per la scuola comprende un sistema interno di posta. Due modalità diverse di

affrontare il delicato problema, conciliando le esigenze comunicative delle classi di scuola elementare con la sicurezza.

- MyM@il è un client di posta elettronica per bambini. L'interfaccia utente è a misura di bambino ed è dotato di funzioni apposite per evitare di entrare in contatto con sconosciuti, sia nell'invio che nella ricezione da persone non "autorizzate". Prevede un modulo server, per gestire il servizio tramite la LAN scolastica. Ovviamente il sistema va "programmato" attivando opportunamente le funzioni di protezione, in modo che il bambino si colleghi ad Internet, invii e riceva e-mail "protetto" da messaggi imprevisti o indesiderati. Le opzioni fondamentali di protezione, tutte configurabili, sono:
  - protezione da *remailer* anonimi, canale frequente di messaggi indesiderati da mittenti resi anonimi da servizi di *anonimizer*
  - controllo del contenuto dell'email ricevuta, che non contenga vocaboli pericolosi o volgari
  - blocco e-mail da utenti sconosciuti, in base alla lista utenti redatta dal genitore o dall'insegnante
  - blocco *attachment*, per evitare i rischi connessi agli allegati, bloccando quelli provenienti da tutti gli utenti, o solo da utenti sconosciuti
  - *black list*: è la lista di indirizzi di posta elettronica o di domini, che si intende bloccare. Ogni e-mail proveniente da un indirizzo o da un dominio "black" verrà bloccata
  - report utente: la registrazione (log file) delle azioni dell'utente.

- Il Veliero invece adotta una diversa strategia. Sfruttando l'architettura di tipo *virtual intranet* tra le scuole registrate, affianca alla modalità di comunicazione sincrona sicura tra le classi (chat, istant message) anche la posta, che dal punto di vista dell'utilizzo replica quasi perfettamente iun client di posta elettronica tradizionale. Di fatto utilizza un protocollo proprietario (non SMTP) ed una rete dedicata. Questo comporta che non sia possibile la trasmissione e la ricezione di messaggi di posta a chiunque, ma solo tra gli appartenenti alla rete del Veliero, senza alcuna possibilità di interferenza (SPAM). La comunità del Veliero scuola, intesa come l'insieme delle postazioni laboratorio, è strutturata secondo una gerarchia di entità, quali:

  regione -> città -> scuola -> classe.

  Ogni classe può ricevere e inviare messaggi alle altre classi, c'è la possibilità che siano gli stessi bambini a creare le bozze di messaggio da inviare e che sia poi l'insegnante, dalla sua postazione di controllo, a perfezionare ed effettivamente inviare tali messaggi. I messaggi ricevuti possono essere aperti dall'insegnante e all'occorrenza essere visualizzati su ogni postazione dei bambini. Allo stato attuale non è prevista la possibilità di inviare allegati, limitando l'uso della posta elettronica alla pura funzione di comunicazione asincrona.

Adottando una gestione interna della posta tramite account propri, oppure impiegando ausili software dedicati, l'impiego sicuro della posta permette certamente molti impieghi didatticamente significativi. Inoltre, come ho già ricordato, si persegue l'obiettivo formativo di un'educazione all'accorta e consapevole gestione degli strumenti di comunicazione. Un obiettivo importante purché i diritti e i doveri del

moderno cittadino corrono ogni giorno di più sui canali della comunicazione digitale. Il servizio di posta elettronica rappresenta un potente strumento di interazione che si deve imparare a usare in modo sempre più attento, conoscendone le valenze di "identità in rete" che spesso rappresenta.

b) Comunicazione sincrona

Siti internet e posta elettronica sono servizi "asincroni": chi genera la pagina web o scrive una e-mail e chi consulta il sito o legge il messaggio operano in tempi diversi, da pochi minuti a mesi e anni. Nella comunicazione sincrona si richiede la contemporanea presenza in rete dei soggetti coinvolti.

Sul web sono disponibili molti strumenti di comunicazione sincrona, alcuni molto noti e diffusi, altri meno. Tra i servizi più conosciuti quelli di chat, utilizzati anche con funzione formativa o di assistenza a distanza, e di istant messaging, che permettono di raggiungere in tempo reale il destinatario con un breve avviso. La sempre maggiore velocità nella trasmissione dei dati ha favorito l'evoluzione dei servizi di comunicazione sincrona, originariamente basati sulla comunicazione testuale, ampliando oggi le possibilità di comunicazione anche all'audio e al video.

L'avvento di chat vocali riduce l'aspetto dattilografico [23], valorizzando invece la potenza comunicativa immediata della voce rispetto a brevi frasi battute di getto. In questo caso la possibilità di condurre a costi nulli [24] colloqui su scala nazionale o anche internazionale va presa in seria considerazione, permettendo agli insegnanti attività con fini didattici in determinati spazi orari programmati con gli interlocutori.

Quando poi alla voce si affianca anche il video, e si possono quindi vedere gli interlocutori con cui si sta dialogando, la comunicazione assume le caratteristiche della video-conferenza. Si tenga comunque conto che l'aggiunta del video assorbe un'ulteriore quota della banda disponibile, per cui potrebbe rallentare altri servizi contemporaneamente attivi sulla connessione a Internet della scuola.

A fronte di questi aspetti incoraggianti verso l'impiego dei servizi disponibili di comunicazione sincrona, vi sono elementi in evoluzione tutti da valutare con attenzione. Infatti la disponibilità di questi servizi è oggi connessa all'appartenenza alle cosiddette "comunità virtuali", in cui bisogna registrarsi assumendo una identità (ID) che - verificata tramite la password personale - qualifica chi accede ai servizi verso i terzi. Anche qui si deve procedere con attenzione valutando tutti gli aspetti correlati a queste procedure, che in cambio di un servizio gratuito comunque richiedono qualcosa, ad esempio la ricezione di comunicazioni pubblicitarie.

Nell'impiego da parte degli alunni si valuti con attenzione l'offerta specifica rivolta alla scuola da parte di organizzazioni [25] che promuovono attività didattiche in rete. In tali casi i servizi di chat e simili sono offerti con la dovuta attenzione all'utenza scolastica.

Partecipare a iniziative on-line rivolte alla scuola e promosse da agenzie nazionali, europee o internazionali può costituire una valida prima esperienza a cui riferire

---

[23] Saper scrivere con le 10 dita senza guardare le tastiera risulta spesso un vantaggio innegabile per chi comunica in modo sincrono tramite messaggi testuali.

[24] Ciò vale nel caso di contratti di accesso ad Internet di tipo a costo fisso (flat) e senza limiti di traffico, tipici nelle connessioni veloci xDSL, il costo non è invece nullo se il volume di traffico è fatturato (contratti "a traffico").

[25] A solo titolo d'esempio si visiti Webscuola (www.webscuola.it), che da anni offre in rete iniziative didattiche on-line per la scuola italiana, nata e promossa anche col sostegno del Ministero nel 1998.

ulteriori programmazioni e progetti didattici. Essendo le opportunità ogni anno differenti, non è possibile dare qui esatte indicazioni.

c) Altre forme di comunicazione in rete

Esistono altre forme di comunicazione in rete oltre quelle già esaminate. Alcune considerazioni già esposte restano valide anche in questi contesti. Inoltre:

i) Forum

l'attivazione o la partecipazione a forum rappresenta una opportunità estremamente interessante di collaborazione in rete. Forum su specifici argomenti sono spesso attivati a supporto di azioni formative, e permettono al gruppo che vi partecipa di comunicare in modo asincrono - come con la posta elettronica - ma condividendo con i componenti del gruppo il dibattito in corso, e ritrovando sempre al loro posto i messaggi scambiati.

Elemento importante dei forum è la figura del moderatore, in grado di operare un controllo attivo sui contributi inviati e approvare o meno i messaggi che vengono inoltrati al gruppo. È sempre opportuna l'attivazione, nel contesto scolastico, di forum moderati, in cui il ruolo di moderatore va svolto dai docenti, con un po' d'esperienza e padronanza dello strumento.

ii) Blog

È un fenomeno da poco diffusosi in Europa e in Italia, e rappresenta l'ultimo fenomeno di comunicazione di massa della popolazione giovanile; in Italia sta coinvolgendo prevalentemente il mondo degli adolescenti.

Utilizzando un servizio di rete apposito, i ragazzi possono pubblicare in tempo reale i loro elaborati (testi ma anche elementi multimediali, foto, grafica, suoni ecc.) sulla rete Internet, realizzando quasi un proprio sito personale. E tutto ciò senza particolari software o competenze specifiche, ma tutto direttamente on-line, utilizzando qualsiasi computer connesso a Internet.

Tale opportunità ha portato al proliferare di materiali pubblicati su Internet prodotti anche da ragazzi, che in luogo del tradizionale e personalissimo diario hanno scelto la rete come custode dei loro pensieri, poesie e confidenze. L'indirizzo del proprio blog personale è diventato un segno distintivo, da condividere con gli amici.

Si cita il caso del fenomeno blog a dimostrazione del fatto che la rete Internet continua a essere una infrastruttura su cui vengono attivati servizi di comunicazione e di diffusione delle informazioni a volte nuovi e quasi sempre di immediato e semplice uso. In tal modo si rende possibile l'estensione a larghe fasce di utenti di attività e iniziative sino a poco prima riservate agli specialisti del settore.

Il blog ha molte potenzialità rispetto alla didattica, permettendo un'azione di scrittura in rete molto potente col minimo di infrastruttura hw/sw [26]. Sapersi orientare di fronte alle innovazioni fa capo anche alla diffusione di quella cultura del corretto uso delle TIC a cui queste linee d'indirizzo mirano.

---

[26] Si veda l'area dedicata http://blog.scuolaer.it/ della rete delle scuole dell'Emilia Romagna, con un'ampia rassegna di lavori della scuola. Inoltre http://www.schoolblogs.com/ che opera a livello internazionale. Ma anche il Blog della IIIA scuola media di Olgiate Comasco: http://www.raccontifantascienza.splinder.com/ un'esercizio di scrittura di racconti di fantascienza svolto su Splinder, un servizio generico ce permette di realizzare blog personali.

BIBLIOGRAFIA

Aa.Vv. *Internet 2004. Manuale per l'uso della rete.* Laterza. Bari 2003.

Aa.Vv. *SchoolNetGuide – il mio bambino ed io in linea*. Swisscom SA. Zurigo 2004.

Azzena D., Marcianò G., Tortorici M. *Un ragno per amico – Indicazioni alle scuole per usare bene e in sicurezza Internet e le LAN.* USR Piemonte. Torino 2003.

Bianchi G., Marcianò G., Tortorici M. *Intranet/Internet nelle scuole*, In *Rassegna dell'Istruzione.* Le Monnier, Firenze LVIII, 1, 2003/04, 58-62.

Fleck R.A Jr.., McQueen T. *Internet Access, Usage, and Policies in Colleges and Universities*, First Monday, 4, 11 (November 1999).

Lastrego C., Tagliapietra G., Testa F. *Tommasone cyberpoliziotto*. Firenze. Fatatrac 2003.

Prece J. *Comunità online*. *Progettare l'usabilità, promuovere la società*. Tecniche nuove. Milano 2001.

SITOGRAFIA

I. SAFE USE OF THE INTERNET – Pilot awareness programme
http://www.netaware.org/it/website.html
La DGXIII dell'UE ha affidato a due organismi internazionali, Fleishman Hillard e Childnet International, l'incarico di varare un programma propedeutico di ricerca e una serie di programmi pilota le cui raccomandazioni contribuiranno alla formulazione da parte della Commissione Europea di un piano d'azione completo sull'uso sicuro di Internet. Il programma di lavoro si articola in 6 sezioni distinte. Per una presentazione in Powerpoint delle varie fasi del programma, su questo sito il file Awareness.ppt

II. EUN SchoolNet INSIGHT - knowledge base for new technology and education
http://insight.eun.org/eun.org2/eun/en/Insight_SchoolPractice/entry_page.cfm?id_area=391
Informazioni aggiornate sull'uso didattico delle TIC con attenzione alle policy e alle scelte gestionali opportune per I decisori della scuola ad ogni livello. Sono disponibili tre tipi di documenti che analizzano le policy adottate: Rapporti nazionali, Policy Briefings e Rapporti speciali. Alcuni documenti sono riservati, ma la maggior parte dei rapporti sono consultabili. Si raccomanda per la panoramica aggiornata sulle scelte in atto nei diversi Paesi europei.

III. SWISSCOM – Progetto scuole
http://www.swisscom.com/GHQ/content/Schulen_ans_Internet/SchoolNetGuides
Swisscom offre ai cantoni e alla Federazione Svizzera delle Scuole Private (FSSP) di realizzare gratuitamente una rete scolastica che collega tutte le reti locali (LAN, Local Area Network) delle scuole in un´unica infrastruttura di comunicazione. Concretamente, ciò significa che se la scuola dispone già di una LAN, riceveun accesso a internet a banda larga in funzione del numero di PC in

uso nell'istituto e collegati alla rete scolastica del cantone. L'attenzione alla sicurezza è presentata in appositi opuscoli disponibili in formato PDF.

IV. INDIRE – Progetto PERINE (Pedagogcal and Educational Research Information – Network for Europe)
http://www.bdp.it/perine
Un progetto che nasce per iniziativa dei membri della rete 12 ('Information Centres and Libraries in Educational Research') dell' EERA (European Educational Research Association), con l'obiettivo di facilitare l'accesso all'informazione che sta alla base della ricerca educativa. Attraverso una stretta collaborazione tra fornitori di servizi di informazione nel settore, ricercatori ed utenti, la rete si propone di censire a livello europeo fonti di informazione e risorse Internet che possono sostenere la ricerca educativa e promuovere collaborazione e pratiche di qualità nel trattamento e nell'uso di tale informazione. L'uso sicuro sarà uno dei temi su cui operare.

V. MIUR - USR per il Piemonte – area UsoSicuro
http://www.piemonte.istruzione.it/tic/internet_sicuro.shtml
Documentazioni e forum sul tema dell'uso sicuro a scuola, degli adempimenti richiesti dal DPS (Documento Programmatico Sicurezza) nelle realtà scolastiche, esempi di PUA (Policy di Uso Accettabile) delle scuole piemontesi

VI. MINISTERO ISTRUZIONE UNIVERSITÀ E RICERCA
http://www.istruzione.it/innovazione/tecnologie/consapevole.shtml
Segnala le criticità d'uso di Internet a scuola. Oltre ad essere evidente la necessità della presenza dell'insegnante come guida durante le sessioni, si rende indispensabile l'adozione di soluzioni che proteggano i minori che navigano sulla rete. Il MIUR offre una serie di indicazioni e di esperienze utili alla soluzione di tali problemi; inoltre, nell'intento di individuare nuove soluzioni più valide, ha accolto favorevolmente l'invito del Ministro dell'Innovazione Tecnologica e del Ministro delle Comunicazioni di far parte del Comitato Tecnico per l'uso Consapevole di Internet. Si possono trovare link a risorse disponibili in rete.

VII. POLIZIA POSTALE
http://www.poliziadistato.it/pds/informatica/
Vigilare sull'uso distorto delle tecnologie per impedire che divengano veicolo di illegalità. E' questo lo scopo che si prefigge la polizia postale e delle comunicazioni impegnata a contrastare le attività illecite compiute attraverso i mezzi di comunicazione, assumendo un ruolo fondamentale nella lotta alla criminalità che sempre più spesso naviga su internet.
A seguito dell'entrata in vigore della legge 269 del 1998, che ha previsto nuovi strumenti investigativi. A fini preventivi è stata inoltre intensificata l'attività di monitoraggio della rete riguardo alcuni fenomeni come la pedofilia, le sette religiose ed altre organizzazioni di vario tipo le cui attività potrebbero sconfinare in manifestazioni criminali o di odio razziale. Attraverso il Servizio centrale, i 19 compartimenti con competenza regionale, e le 76 sezioni con competenza provinciale, la polizia postale e delle comunicazioni assicura una presenza articolata e diffusa su tutto il territorio nazionale. Inoltre tutti i suoi uffici sono stati dotati di indirizzi e-mail ai quali è possibile chiedere informazioni o inviare segnalazioni di violazione di norme penali nei settori relativi alla specialità.

VIII. 114 EMERGENZA INFANZIA
http://www.114.it/
Il 114 è una linea telefonica di emergenza accessibile gratuitamente da telefonia fissa 24 ore su 24 da parte di chiunque intenda segnalare situazioni di emergenza in cui la salute psico-fisica di bambini o adolescenti è in pericolo o in cui il bambino o l'adolescente sono a rischio di trauma, rendendo necessario un intervento immediato di tutela attraverso il coinvolgimento di specifici Servizi e Istituzioni del territorio. Attraverso il Servizio Emergenza Infanzia 114 è anche possibile segnalare situazioni di disagio derivanti da immagini messaggi e dialoghi diffusi attraverso televisione, radio, carta stampata e Internet.

IX. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
http://www.garanteprivacy.it /
L'attività del Garante, iniziata nel 1997, ha riguardato ogni settore della vita sociale economica e culturale del Paese in cui si sia manifestata l'esigenza della protezione dei dati personali. I compiti del Garante sono attualmente specificati nell'art. 31 della legge 675/1996, dove vengono indicati, tra l'altro, il controllo della conformità dei trattamenti di dati personali a leggi e regolamenti e la segnalazione ai titolari o ai responsabili dei trattamenti delle modifiche da adottare per conseguire tale conformità; e anche l'indicazione degli accorgimenti da adottare nell'uso dei dati "semi-sensibili". Un riferimento istituzionale importante.

X. KIDSFREE
http://kidsfreeware.com
una ricca collezione di freesoftware per bambini. Una sezione è tutta dedicata a browser free per l'accesso sicuro a Internet

XI. MYM@IL – client di posta per bambini
http://www.mymail.it
client di posta elettronica per bambini dai 6 anni in su che permette di muovere i primi passi nel mondo della posta elettronica in maniera facile e sicura. MyM@il è in grado di comunicare attraverso Internet ed inviare e ricevere messaggi di posta elettronica. Il pacchetto MyM@il include il client di posta elettronica vero e proprio, MyConfig per la configurazione e la gestione degli utenti di MyM@il, un Tutorial realizzato per i bambini, un gioco per testare la preparazione sul mondo della posta elettronica. Sul sito le informazioni aggiornate.

XII. IL VELIERO
http://www.ilveliero.info
browser per bambini realizzato in Italia per la navigazione e comunicazione sicura in internet da casa e da scuola. Consente di visitare i siti selezionati dagli esperti, scelti in base ai contenuti proposti, all'adeguatezza del linguaggio, alla qualità grafica e alla facilità nella navigazione. Al tempo stesso offre al Nostromo (il genitore, l'insegnante o un altro supervisore) la possibilità di abilitare ulteriori nuovi siti per i propri Naviganti. Il Veliero è anche una comunità interattiva che comunica, tramite lo scambio di messaggi, e-mail e chat sicura.

GLOSSARIO

fonte:
Glossario della Sicurezza, Edipi, Milano 2004.
http://www.edipi.com/glossario.php

ANSI, American National Standards Institute

E' l'organizzazione che si occupa degli standard americani relativi a vari settori, compresi informatica e comunicazioni. E' un l'organismo responsabile dell'approvazione di numerose normative (standards) che vengono spesso nominate, in inglese, ad esempio Ansi C, la versione del linguaggio di programmazione C approvata dall'Ansi. Fondato nel 1918, l'Asi è un istituto no-profit, coordina il settore privato statunitense intorno ad un sistema normativo volontario e supportato dalle organizzazioni pubbliche e private. La federazione Ansi rappresenta gli interessi di circa 1.400 associati quali aziende, organizzazioni, agenzie governative,membri istituzionali e internazionali e rappresenta gli Usa nelle sessioni di lavoro nei lavori internazionali. Ansi è membro di Iso, Internationale Organization for Standardization, svolge un ruolo attivo nell'organo direttivo come membro permanente. Tramite l'Usnc, Ansi è uno dei 12 membri dell'Iec, International Electrotechnical Commission.

BIOMETRIA – TECNICHE BIOMETRICHE

La Biometria è un metodo matematico per misurare i dati biologici, è la scienza che usa la tecnologia digitale per identificare gli individui attraverso le loro caratteristiche fisiche. Le impronte digitali, la voce, la faccia, l'occhio di ciascun individuo sono caratteristici dell'individuo e unici. Quindi potenziali chiavi 'uniche' per accedere a servizi protetti da un sistema di sicurezza: basta digitalizzare una di queste caratteristiche e inserirla in una banca dati. Un identificatore biometrico cattura un'immagine della caratteristica da utilizzare per il riconoscimento, la elabora e la archivia per confronti successivi e all'occorrenza si interfaccia con il sistema di controllo che confronta le immagini con quelle presenti nel database. Ad esempio l'iride è una caratteristica assolutamente unica. Per il processo di riconoscimento dell'iride la tecnologia si avvale anche di alcune raffinatezze come registrare e misurare i tempi di dilatazione e contrazione della pupilla per accertare che davanti al sistema di sicurezza ci sia la faccia di un essere umano e non la foto del suo occhio.

BUFFER OVERFLOW

Spesso i sistemi operativi permettono a certi programmi di operare con determinati privilegi anche a livello di utente, permettendogli così di avere il controllo totale sulla macchina. Il problema in questo caso si verifica nel momento in cui un hacker è in grado di intervenire sulla funzionalità di tali programmi: se interviene a quel livello è anche in grado di impossessarsi e di controllare la macchina sulla quale è installata l'applicazione target. Per difendersi dal buffer overflow che rappresenta una delle principali cause di compromissione nel 2001, ci si deve affidare a programmatori che devono

impostare le macchine e le applicazioni secondo il principio del least privilege, cioè assegnare ai programmi esclusivamente i privilegi di cui necessitano.

CERTIFICATION AUTHORITY (CA)
REGISTRATION AUTHORITY (RA)

Enti pubblici o privati garanti della corrispondenza tra l'identità del titolare del certificato e la coppia di chiavi (pubblica e privata) cui il certificato è riferito. La Certification Authority è un'entità che gode della fiducia di tutti gli utenti che operano nel sistema. La CA deve essere depositaria di fiducia in quanto deve garantire che ogni Chiave Pubblica sia legata al proprietario attraverso un certificato. La CA si avvale di altre entità chiamate Autorità di Registrazione (Registration Authority) per garantire che l'utente richiedente un certificato sia esattamente quello riportato nel certificato. La CA fornisce tre servizi base ai suoi utenti finali: emissione del Certificato, emissione della Lista dei Certificati Revocati, rinnovo del Certificato, revoca del Certificato. La CA realizza quindi un sistema di controllo che garantisce che la chiave privata di un determinato certificato è sicuramente in possesso di una sola persona, della cui identità il sistema si fa garante. Si può trattare di un sistema interno all'azienda, o di grandi società di certificazione indipendenti come VeriSign, Thawte, oltre a Ssb, Telecom Italia, Sia, Poste.it, ecc. La Registration Authority (RA) è l'entità che provvede ad identificare con certezza i soggetti che richiedono un certificato digitale (@Sign) registrandone i dati tramite procedure. L'attività di Registration Authority è tra le più delicate e significative tra quelle svolte dagli Enti Certificatori. Il Certificato digitale di seguito definito è rilasciato da un Ente Certificatore iscritto dall'Aipa nell'Elenco Pubblico dei Certificatori sulla base di precise regole tecniche e di sicurezza, e come tale garantisce circa l'identità del possessore

CHIAVI DI SICUREZZA

Chiavi pubbliche (asimmetriche) e chiavi private (simmetriche). La crittografia di documenti è uno strumento per trasferire informazioni riservate tra persone. Queste ultime devono naturalmente avere la chiave di lettura per de-crittare i documenti: la chiave di decodifica in mano al mittente e al destinatario è una chiave privata detta anche simmetrica. Tale sistema presenta alcuni problemi: la chiave privata segreta deve essere inviata su un canale sicuro (chi garantisce il canale?), non garantisce la non ripudiabilità dell'informazione (il mittente che nega l'invio di un documento), è di difficile applicazione in un contesto di comunicazioni via rete, in quanto il numero di chiavi segrete crescerebbe in maniera esponenziale per ogni destinatario con cui si volesse instaurare una comunicazione confidenziale. La soluzione è quindi un sistema di sicurezza pubblico, o asimmetrico. La prima proposta in questo senso risale al 1976 per cui si prevedeva l'utilizzazione di una coppia di chiavi per persona, una pubblica, cioè nota a tutti, ed una privata, correlate tra loro. La doppia chiave permette la confidenzailità, nel senso che il mittente che vuole inviare un messaggio non decifrabile da altri se non dal destinatario, codifica il messaggio in chiaro con la chiave pubblica del destinatario stesso: il destinatario potrà decodificare il messaggio con la sua chiave privata. La doppia chiave permette inoltre l'utilizzo

della Firma Digitale. Se il mittente vuole rivendicare la paternità dei un documento, è sufficiente che applichi al documento la sua chiave privata. Il destinatario potrà leggere il contenuto e verificarne la provenienza con il solo ausilio della chiave pubblica del mittente. Quindi in sintesi una Chiave Privata è uno dei due elementi della coppia di chiavi di sicurezza, quello destinato a essere conosciuto dal soggetto titolare. Serve per apporre la firma digitale sul documento informatico o serve per decifrare un documento informatico in precedenza cifrato mediante la corrispondente chiave pubblica. La Chiave Pubblica è l'elemento della coppia di chiavi di sicurezza destinato a essere reso pubblico, con il quale si verifica la firma digitale posta sul documento informatico dal titolare delle chiavi private o si cifrano i documenti informatici da trasmettere al titolare delle predette chiavi.

CLUSIT

Riproponiamo, in modo più articolato, il lemma Clusit, Associazione Italiana per la Sicurezza Informatica Clusit è una associazione "no profit" con sede presso l'Università degli studi di Milano, Dipartimento di Scienze dell'Informazione. Gli obiettivi principali che l'Associazione persegue sono la creazione e la diffusione di una cultura della sicurezza informatica presso le aziende private, gli enti della pubblica amministrazione e le organizzazioni economiche del nostro paese. Il Clusit intende: Promuovere e favorire iniziative per la diffusione di tutti gli aspetti della sicurezza informatica. Contribuire sia a livello comunitario che italiano alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica. Concorrere alla definizione di percorsi di formazione per la preparazione delle diverse figure professionali operanti nel settore della sicurezza informatica. Promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà. Il Clusit si inserisce in un network europeo di associazioni analoghe. In collaborazione con le altre associazioni europee Il Clusit partecipa a progetti dell'Unione Europea e ha accesso ai lavori del G8. Il Clusit si propone come il luogo dove far convivere tutte le realtà coinvolte dal problema della sicurezza informatica così da costituire un unico punto di riferimento per chi vuole conoscere lo stato dell'arte in materia. Il Clusit mette le proprie competenze a disposizione delle aziende, che sono alla ricerca di informazioni oggettive che consentano loro di orientare al meglio le loro scelte in materia di sicurezza informatica, ma anche dei privati cittadini, sempre più interessati alle nuove tecnologie ma estremamente sensibili al problema della protezione della privacy e preoccupati per i pericoli della nuova criminalità informatica. Tra le manifestazioni organizzate dal Clusit per il 2002 InfoSecurity (23-24-25 gennaio 2002 alla Fiera di Milano) e master Universitari in Sicurezza Informatica (Università degli Studi di Milano - gennaio-giugno 2002 ; Regione Calabria). (tel. 349.7768882; www.clusit.it)

COMPUTER RISK ANALYSIS

Metodologia che utilizza strumenti tipicamente software per eseguire l'analisi del rischio informatico. L'analisi procede su successioni di moduli destinati all'identificazione e valutazione degli asset e all'analisi della vulnerabilità e delle minacce al sistema informatico e quindi al calcolo del rischio. I moduli di analisi possono realizzare attività di identificazione dei servizi e del flusso di dati,

mappatura e valutazione degli asset, con conseguente rilevazione del grado di vulnerabilità ed esposizione al rischio. I software specifici sono in grado di automatizzare l'elaborazione e di produrre report dettagliati.

CRITTOGRAFIA

La crittografia è una metodologia che permette di scambiarsi informazioni confidenziali. L'obiettivo della crittografia è di rendere privata una comunicazione che si svolge su un mezzo pubblico (nella nostra Era tipicamente Internet), potenzialmente insicuro a cui chiunque può avere facile accesso. La crittografia su basa su una serie di principi: Segretezza, solo il destinatario è in grado di leggere il messaggio crittografato; Autenticità, il destinatario del documento è sicuro dell'origine del messaggio; Integrità, il destinatario è sicuro che il messaggio non abbia subito modifiche durante la trasmissione; Non Ripudiabilità, il destinatario può avere, senza possibilità di incertezza, sicurezza dell'origine del messaggio al mittente. Le prime notizie di un sistema di crittografia si trovano negli scritti di Plutarco che descrive un metodo di scrittura nascosta adottato dagli spartani: una striscia di cuoio attorno ad un bastone caratterizzato da un certo diametro su cui il messaggio veniva scritto su colonne. Srotolata la striscia di cuoio il testo era incomprensibile e solo arrotolandola su un bastone di uguale dimensione a quello del mittente era leggibile. In Grecia, veniva usato anche il disco di Enea il Tattico, un disco con 24 fori per ciascuna lettera dell'alfabeto. La codifica del messaggio avveniva passando un filo attraverso i fori corrispondenti alle lettere. Giulio Cesare usava un sistema che consisteva nello scrivere i messaggi spostando tutte le lettere dell'alfabeto di 3 posizioni: tale sistema è noto come cifrario monoalfabetico. Nel Medioevo e nei secoli dopo si utilizzarono sistemi sempre più complessi: verso la fine dell'Ottocento arriva la tecnologia con macchine in grado di cifrare e decifare automaticamente i messaggi. Il disco di Wheatstone era un sistema formato da due dischi concentrici. Durante la seconda guerra mondiale i tedeschi utilizzarono una macchina di cifratura chiamata Enigma, composta di vari dischi che ruotavano alla pressione di ogni tasto. In risposta gli inglesi costruirono una macchina chiamata Colossus in grado di decifrarne i loro messaggi.

CSI - Computer Security Institute

Fondato nel 1974 a San Francisco, il Csi è un'associazione formata da esperti nel campo della sicurezza che può contare su migliaia di consulenti in ogni parte del mondo e che offre una vasta gamma di programmi didattici e informativi destinati ad aiutare i responsabili della sicurezza a proteggere efficacemente le risorse informatiche di aziende ed enti pubblici.

D R M – Digital Rigths Management

Il Digital Rights Management è una tecnologia che permette ai proprietari di contenuti di testo digitali (tipicamente e-book e documenti aziendali) di distribuirli in maniera sicura attraverso Internet, in modo tale da impedirne la duplicazione e la distribuzione fuori dai propri canali. La diffusione di libri elettronici in Rete offre evidenti vantaggi e potenzialità: riduzione dei costi legati alla carta, all'inchiostro e alla stampa, ma anche la capacità di avere una

piattaforma che consenta un accesso immediato da parte dei clienti ai propri contenuti, consentendo sia una distribuzione più capillare che un migliore time-to-market. In questo contesto bisogna ricordare che il copyright dell'autore e della casa editrice vanno salvaguardati nel passaggio dal libro cartaceo al libro elettronico. Proprio per fare questo è stata sviluppata una tecnologia, chiamata D.R.M. (Digital Rights Management), che permette ai proprietari di contenuti digitali di distribuirli in maniera sicura attraverso la Rete, in modo tale da impedirne la duplicazione e la distribuzione fuori dai propri canali. La tecnologia D.R.M. funziona in modo da permettere un facile download degli eBook, facendo ottenere all'acquirente una licenza che gli permetta di accedere a diversi livelli di utilizzo del file. Senza questa licenza il file non può essere letto dall'utente. Infatti, l'eBook è criptato e solamente con la "chiave personalizzata" rilasciata a seguito dell'acquisto è possibile accedere ai contenuti che saranno, comunque, protetti da copie e stampe non autorizzate dalla "chiave". (tratto da CartaDigitale.it)

DENIAL OF SERVICE

Il termine Denial of Service (abbreviato in DoS) indica un attacco in un sistema informativo aziendale il cui scopo è quello di produrre una perdita di funzionalità, più o meno prolungata nel tempo. Questo tipo di attacco, non ha come obiettivo quello di guadagnare un certo controllo della macchina, ma quello di impedire alla macchina di svolgere alcune operazioni.

DISASTER RECOVERY

I sistemi di Disaster Recovery sono in genere soluzioni di back up che duplicano i dati delle aziende. Le soluzioni per il Disaster Recovery sono quindi focalizzate sulla salvaguardia del dato e sulla garanzia di poter ripristinare il supporto informatico in funzione del business aziendale. La moltitudine di pericoli che il moderno data centre deve affrontare, ha posto il Disaster Recovery tra le strategie di investimenti in Information Technology di molte aziende. I crimini via Internet, i virus, le cadute di tensione, gli errori umani, gli incendi ed altro ancora (i fatti dell'11 settembre ne sono un esempio, con interi sistemi informatici distrutti in pochi minuti) influiscono fortemente sul business, con un significativo impatto sulla capacità organizzativa. In questo contesto, la pianificazione di una strategia di disaster recovery è un imperativo per qualsiasi business: la vera sfida consiste nel realizzarla in maniera efficace e a costi vantaggiosi. Con l'attuale trend economico ed il rallentamento degli investimenti tecnologici, il fattore più importante consiste nell'offrire, in modo flessibile, da parte delle aziende fornitrici, il giusto livello di protezione per ciascuna applicazione, su tutti i sistemi operativi e le piattaforme hardware.

DOCUMENTO PROGRAMMATICO PER LA SICUREZZA

In tema di misure di sicurezza dei dati aziendali sensibili che viaggiano su computer collegati ad Internet, si fa riferimento al D.P.R. n° 318 del 28 luglio 1999 che prevede appunto la stesura di un "Documento programmatico per la sicurezza dei dati". Il Dpr prevede che tale Documento redatto in ambito di policy di sicurezza aziendali, descriva i criteri tecnici ed organizzativi relativi alla

protezione delle aree e dei locali interessati dalle misure di sicurezza; le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi; la tutela dell'integrità dei dati; la sicurezza nella trasmissione dei dati, ivi comprese le restrizioni di accesso per via telematica; il piano di formazione degli incaricati del trattamento. Per l'omessa adozione, anche colposa delle misure di sicurezza previste dal regolamento la pena, attribuibile a chiunque, e di una reclusione fino a 2 anni o ad una ammenda fino a oltre 40 mila euro.

ETHICAL HACKING

E' un servizio di ricerca delle vulnerabilità basato su una metodologia con cui lo specialista, come un hacker, cerca di impossessarsi di un sistema: ciò consente in una fase successiva di attuare le azioni necessarie per difendere adeguatamente il sistema. L'attività di hacking etico è a fini costruttivi e comporta l'utilizzo di competenze, inventiva e creatività al fine di penetrare un sistema informativo per preservarne la sicurezza. L'Ethical Hacking si avvale di una metodologia operativa che comporta due tipi di simulazione: la prima, dall'esterno, mediante l'uso della rete Internet, riproduce il modus operandi di un hacker/cracker; la seconda, dall'interno, ricalca l'attacco effettuato da persone con un accesso o una conoscenza delle risorse interne dell'azienda. La documentazione finale, consegnata al committente, è pertanto costituita dagli elementi provati e fornisce indicazioni sulle possibili strade da intraprendere per un miglioramento del livello di sicurezza.

FIREWALL

Firewall significa "muro di fuoco". E' uno degli strumenti principali della sicurezza informatica, progettato per impedire accessi non autorizzati a/da reti private. Il suo utilizzo tipico quindi è quello di impedire agli utenti provenienti da Internet l'accesso non autorizzato ad una Intranet. Un firewall si occupa di filtrare i dati che passano da un computer ad un altro sulla rete, quindi applica un modello di sicurezza di tipo "perimetrale", per tenere fuori tutto ciò che non è necessario far entrare. Per reti private o Intranet con medi e alti livelli di complessità, o con necessità di particolari sicurezze, sono utilizzati anche firewall che creano serie di divisioni 'interne', per evitare che accessi non autorizzati a una macchina mettano in pericolo il resto del sistema. Il firewall divide il traffico in ammesso, rifiutato o ignorato, stabilisce un insieme di regole che definiscono a quali servizi esterni possono accedere gli utenti della Intranet e a quali servizi della Intranet o rete privata possono accedere Pc/utenti dall'esterno. Un firewall può essere un dispositivo hardware oppure un software posto come già detto fra la rete locale (Lan, local area network) ed Internet, con protezioni di vario livello. Livello di Rete, denominato screening router, che esamina ogni pacchetto di dati per valutare se farlo passare dalla rete locale oppure bloccarlo. A livello dell'Applicazione, denominato server proxy, che comunica con server esterni alla rete per conto degli utenti interni alla rete locale. Livello di Circuiti, simile al server proxy, ma crea un circuito tra client e server. Il Dipartimento della Difesa statunitense ha pubblicato un manuale per la sicurezza delle reti, chiamato "Orange Book" dove sono definiti i requisiti minimi di un firewall e le classi di sicurezza che vanno dal livello D (il più basso) al livello A (il più alto), suddivise ognuna in sottoclassi, per un totale di sette livelli di sicurezza

FIRMA DIGITALE

La Firma Digitale è l'equivalente elettronico-informatico della firma autografa: ha il medesimo valore legale e il vantaggio della sicurezza. La Firma Digitale oltre ad avere valore legale garantisce l'autenticità cioè l'identità dell'autore del documento; la sua integrità, il destinatario verificare che il documento non sia stato manomesso; ed infine il non ripudio: l'autore non può non riconoscere un documento firmato. La firma digitale si è resa necessaria per regolare i rapporti elettronici tra utenti informatici, per un uso sicuro di Internet e per lo sviluppo delle transazioni online. Le aree maggiormente interessati dalla diffusione della Firma Digitale sono il commercio elettronico, il rapporto telematico tra pubblica amministrazione e privati cittadini e la trasmissione di documenti elettronici via e-mail (si parla di "Infrastruttura a Chiave Pubblica", la famosa Pki, Public Key Infrastructure). L'Aipa (Autorità per l'Informatica nella Pubblica Amministrazione) ha svolto un'intensa attività per la diffusione della cultura della Firma Digitale, che l'ha portato alla realizzazione di una serie di regolamenti. Tale regolamenti stabiliscono quali sono gli scenari di riferimento giuridici, tecnologici ed organizzativi per ottenere quanto necessario ad un efficace utilizzo della firma. Il processo di firma digitale richiede che l'utente effettui una serie di azioni necessarie alla predisposizione delle chiavi utilizzate dal sistema di crittografia su cui il meccanismo di firma si basa. In particolare occorre (www.aipa.it): la registrazione dell'utente presso una Autorità di Certificazione (AC), la generazione di una coppia di chiavi (Ks, chiave segreta e Kp, chiave pubblica), la certificazione della chiave pubblica, la registrazione della chiave pubblica. Dopo tali operazione l'utente è in grado di firmare elettronicamente qualunque documento, sfruttando la sua chiave segreta , durante il periodo di validità della certificazione della corrispondente chiave pubblica. E' possibile chiedere una revoca della certificazione della chiave pubblica, quando si ritiene che la segretezza della sua chiave privata sia stata compromessa. All'Aipa è demandato il compito di curare l'elenco pubblico dei certificatori, enti che garantiscono l'identità dei soggetti che utilizzano la firma digitale. L'Italia si è posta all'avanguardia in tema di Firma Digitale: è stato uno dei primi Paesi in Europa ad aver legiferato (L. 59/97 e D.P.R. 513/97).

GARR

Il Garr, Gruppo per l'Armonizzazione delle Reti della Ricerca, è composto da tutte le Entità che rappresentano la Comunità Accademica e della Ricerca Scientifica in Italia. I principali compiti istituzionali del Garr verso la propria comunità sono: realizzare e gestire la rete dell'Università e della Ricerca Scientifica Italiana (attualmente tramite il "Progetto Garr-B"), nonché l'interconnessione con le altre reti per la ricerca europee, mondiali e con Internet in generale; fornire i servizi operativi ed i servizi applicativi in rete; favorire il coordinamento e la collaborazione tra le attività di Ricerca (a livello nazionale ed internazionale) tramite i servizi telematici, compresi anche la ricerca e lo sviluppo nei servizi telematici stessi; favorire l'aggiornamento, la conoscenza e lo scambio di informazioni sui servizi telematici, anche tramite l'organizzazione di Corsi ed Incontri. Il Progetto di Rete Garr-B mira alla creazione di una rete a larga banda al servizio della comunità accademica e scientifica italiana.

GARR-CERT

Scopo del servizio operativo Garr-Cert è la gestione degli incidenti di sicurezza informatici in cui siano coinvolti enti collegati alla rete Garr. In particolare, compiti di Garr-Cert sono: assistere gli utenti nella gestione degli incidenti di sicurezza; rispondere alle segnalazioni di incidenti, avvertendo gli utenti coinvolti e seguendone gli sviluppi; diffondere informazioni sulle vulnerabilità più comuni e sugli strumenti di sicurezza da adottare; assistere gli utenti nel realizzare le misure preventive ritenute necessarie per ridurre a livelli accettabili il rischio di incidenti; emanare direttive sui requisiti minimi di sicurezza per le macchine con accesso alla rete, verificandone il rispetto; gestire corsi di aggiornamento tecnico, a tutti i livelli, e in particolare per utenti finali; mantenersi aggiornato allo stato dell'arte degli strumenti e metodologie per la sicurezza; provare strumenti esistenti, e svilupparne di nuovi per esigenze specifiche.

HACKER

Gli Hacker sono degli esperti informatici che mirano, attraverso attacchi a siti Internet o reti pubbliche o private, a fornire elementi per individuare i limiti di un programma o di un sistema di sicurezza. Questa è la faccia buona della professione dell'hacker. La faccia cattiva è rappresentata da soggetti che possono diventare criminali che attaccano le istituzioni o le aziende private, modificano le pagine dei siti istituzionali o delle multinazionali, accedendo e modificando dati nei loro computer, organizzano truffe. Il termine hacker deriva da "hack" che indica gli scherzi con cui si divertivano gli studenti del Mit (Massachussetts institute of technology) negli anni settanta. In particolare si definivano hackers alcuni tra gli studenti che lavoravano al Signal and power subcommitee. Quest'ultima era la sottocommissione per lo studio dei segnali e dell'energia, un sottogruppo del Tmrc, una delle diverse associazioni universitarie che vertevano su interessi particolari. Da alcuni anni, molti hackers vengono assunti da grosse aziende per controllare il loro software e la sicurezza delle loro reti, perchè particolarmente abili nell'intrufolarsi nel sistema informatico. Oltre agli hacker esistonp i crakers, il cui obiettivo principale sono i sistemi operativi e i preakers, che conoscono il sistema telefonico ed il modo di raggirarlo.

IAT - Istituto per le Applicazioni Telematiche

L'Istituto per le Applicazioni Telematiche si occupa di ricerca scientifica e tecnologica nel settore delle applicazioni telematiche e delle reti di comunicazione, quindi con ampie competenze sui temi della sicurezza e della riservatezza dei dati. Lo Iat è stato fondato nell'ambito del Cnr, consiglio nazionale delle ricerche, nel gennaio 1997.

Obiettivi dell'istituto, oltre a svolgere attività di ricerca nel settore delle tecnologie della informazione, sono le attività finalizzate allo sviluppo e alla sperimentazione di strumenti informatici e telematici, trasferire le conoscenze sviluppate nei settori di competenza anche a vantaggio della pubblica amministrazione, e del sistema produttivo, favorire lo sviluppo dei rapporti internazionali e svolgere attività di formazione sfruttando le conoscenze presenti in Istituto. Le principali linee di ricerca in cui è impegnato l'istituto sono le

seguenti: tecnologie dell'informazione, architetture di rete e relative tecnologie, sicurezza delle reti e riservatezza dell'informazione, applicazioni multimediali in rete, sistemi informatici distribuiti a gestione centralizzata e supporti telematici per la gestione dell'informazione.

INTRUSION DETECTION

I servizi di Intrusion Detection, che rientrano nelle attività di monitoraggio di una rete, servono ad individuare tentativi d'attacco del network o più in generale alterazioni delle configurazioni dei sistemi informativi in rete. Questi strumenti consentono di controllare in maniera costante eventuali intrusioni analizzando la rete con un meccanismo automatico in tempo reale. Le capacità di rilevamento delle intrusioni, comprendono diverse attività tra cui attività di Exploits, che indica un tentativo di accedere o compromettere i sistemi della rete; attività di DoS (Denial-of-Service), che indica il tentativo di usare ampiezza di banda della rete locale; attività di Reconnaissance, che serve ad indicare se qualcuno sta mappando la rete per identificare potenziali bersagli; attività di Misuse, che indica il tentativo di violare le regole aziendali. Con sistemi di Intrusion Detection gli utenti possono rilevare e interrompere le attività di rete non autorizzate sia che provengano dall'interno che dall'esterno della rete.

ISO, International Organization for Standardization

Organismo fondato nel 1946 responsabile della creazione degli standard internazionali in molti settori, tra cui elaboratori e trasmissione dei dati. Iso è una federazione non governativa a cui partecipano circa 130 enti normatori internazionali Iso: promuove lo sviluppo e l'unificazione normativa per consentire scambi di prodotti, beni e servizi; coordina gli ambiti di progetto diversi, tecnico-scientifico ed economico; opera e legifera in base ad articolati accordi internazionali. Sono poi i singoli Paesi aderenti all'accordo, tramite gli enti di standardizzazione nazionali, ad introdurre le "International Standard" nelle norme nazionali. I lavori per pervenire alla pubblicazione di norme di standardizzazione sono affidati a comitati a cui partecipano rappresentanti di industrie, istituti di ricerca, istituzioni governative, organizzazioni dei consumatori.

NIPC - National Infrastructure Protection Center

In risposta al crescente numero di denunce relative ai crimini perpetrati ai danni dei principali componenti del mondo economico e informatico, l'Fbi ha dato vita al Nipc, una struttura con distaccamenti presso le sedi principali e le Regional Computer Intrusion Squad dell'Fbi sparse in tutti gli Stati Uniti. Il Nipc, una partnership tra varie agenzie federali e l'industria privata, è concepita per fungere da principale strumento del governo per prevenire e combattere gli attacchi informatici alle infrastrutture del Paese, come sistemi di telecomunicazioni, impianti di energia, trasporti, sistemi bancari, servizi di emergenza e uffici pubblici. La missione delle Regional Computer Intrusion Squad è quella di investigare sulle violazioni indicate nel Computer Fraud and Abuse Act, comprese le intrusioni nelle reti di computer pubbliche e private, le attività di

spionaggio industriale, la pirateria informatica e altri crimini legati alle attività elettroniche.

NOC, Network Operation Center

All'interno di molte aziende specializzate in sicurezza opera una struttura specializzata nella fornitura di servizi di e-security in outsourcing, che rappresenta lo strumento operativo di cui il fornitore si è dotato per seguire costantemente i suoi clienti: si tratta di un centro di controllo denominato Noc (Network Operation Center), appositamente strutturato per garantire un presidio attivo 24 ore su 24, gestito da personale specializzato, in grado di individuare i tentativi di intrusione e bloccarli con estrema tempestività

PENETRATION TEST

I servizi di Penetration Test consistono in un'attività preventiva: servono ad individuare eventuali vulnerabilità nei dispositivi hardware e software di una rete. Questa attività consente di predisporre misure necessarie per prevenire eventuali rischi di blocco dei sistemi informativi a seguito di attacchi o tentativi di intrusione. Effettuare un test di penetrazione significa cercare, dall'esterno del perimetro di difesa, di violarlo ricorrendo a tecniche di hacking. Dal momento che difficilmente si è in grado di effettuare questo tipo di operazione si deve ricorrere a consulenti esterni.

PGP, Pretty Good Privacy

E' uno dei più popolari formati di crittografia, anche perché è semplice da usare ed è ben integrato con diverse piattaforme IT.
Il programma ha il pregio di tutelare, in modo molto semplice, la privacy degli utenti. Tutti i dati che questi scambiano in rete sono protetti e non possono essere letti da nessuno, consentendo di comunicare in modo sicuro con chiunque. Il Pgp, datato 1991, realizza un sistema di crittografia ibrido che sfrutta una cifratura simmetrica, più veloce, per l'intero documento e la cifratura con chiavi asimmetriche, più complessa e di esecuzione più lenta, per proteggere la chiave simmetrica. La sicurezza degli algoritmi utilizzati nel programma non è mai stata provata matematicamente, ma è garantita sia dal suo uso abbastanza diffuso, sia dalla opposizione che il governo statunitense ha sempre dimostrato nei confronti della sua diffusione, attraverso una legge, la International Traffic Arms Regulations (Itar). Per informazioni sul programma si può consultare il sito www.pgpi.com.

POLITICHE DI SICUREZZA

Lo Politiche di Sicurezza servono per gestire e applicare i sistemi di gestione della sicurezza all'interno di una organizzazione. Il principale obiettivo di una politica di sicurezza è proteggere le risorse dell'azienda. Spesso le procedure connesse alla protezione del patrimonio aziendale impattano notevolmente sulla produttività degli utenti: per definire le politiche di sicurezza quindi è necessario valutare quale è il livello ottimale di protezione dei dati aziendali, bilanciandolo con l'effetto che si viene a creare per la produttività. Nella definizione delle politiche

di sicurezza è necessario tenere presente tutti i problemi di protezione delle risorse, tra i cui aspetti si trovano le politiche di gestione, del controllo di accesso, della riservatezza dei dati, dell'integratità dei dati e della loro gestione.

Porta Logica

Una Porta (detta anche Porta logica), nel contesto delle reti informatiche, è una specie di 'canale di comunicazione' tra client e server. Ogni servizio (o protocollo) ha una porta logica preferenziale da usare (come esempio, il protocollo Http utilizza la porta logica 80 sul server). Le porte logiche sono 65.535, le prime 1024 sono quelle utilizzate da servizi di sistema, a parte su sistemi Linux dove queste porte sono estese fino alla 32.768. Una delle più frequenti vulnerabilità nei sistemi informatici è data appunto dal troppo numero di porte aperte in un sistema: più porte logiche sono aperte, maggiori sono i pericoli di intrusione dall'esterno

ROUTER

Un router è un dispositivo (hardware o software) che gestisce la connessione tra due o più reti. E' un dispositivo fondamentale per collegare reti anche di tipo diverso, attraverso le quali gestisce l'instradamento dei messaggi. I router progettati per lavorare in Internet sono in grado di inviare i messaggi da una rete all'altra scegliendo la strada più breve o una alternativa in caso di reti con traffico elevato o fuori uso. I router hanno il compito di far passare i pacchetti di dati da una rete all'altra in modo da avvicinarli alla destinazione creando quindi una catena di router ognuno dei quali sa l'indirizzo del successivo sulla Rete grazie a tabelle costantemente aggiornate. Un caso di utilizzo di un router è il collegamento di una rete locale di tipo privato a una rete di tipo pubblico come ad esempio avviene nelle società con possibilità per tutti le postazioni di lavoro di accedere ad Internet attraverso una connessione dedicata.

SECURITY AUDITING

E' un'attività che si può ricondurre alla categoria di servizi di Vulnerability Monitoring, con la peculiarità di essere svolta su server e servizi perimetrali L'Internet security auditing è quindi un'attività che viene condotta al fine di rilevare eventuali vulnerabilità nella rete aziendale sia dei sistemi operativi che degli applicativi installati. Vengono verificate anche le policy di sicurezza aziendali.

SINGLE SIGN-ON

Il Single Sign-On prevede che la parte client di un sistema venga riconosciuta solo una volta nel corso di una sessione al momento di accesso ad una applicazione basata su server: questa abilitazione iniziale offre all'utente la possibilità di accedere a tutti i server a cui il client è autorizzato dall'amministratore, senza quindi bisogno di imputare successivi login.
Un sistema basato su Single Sign-On semplifica le operazioni di accesso alle applicazioni ma non rappresenta il massimo in termini di sicurezza in quanto, secondo una definizione proposta da Cryptonet, il passo da singolo punto di

accesso (single point of access) e singolo punto di attacco (single point of attack) è breve. Alcune soluzioni prevedono che un Single Sign-On offra sì la possibilità di imputare un solo login per sessione ma che questo sia autorizzato a partire da sistemi di strong authentication come possono essere i certificati di identità digitale emessi da una Pki, chiave personale di identificazione.

SMTP

SMTP (Simple mail transfer protocol, Protocollo semplice per il trasporto di posta) gestisce il trasferimento della posta dal sistema di posta di un calcolatore a quello di un altro. Smtp si occupa della posta diretta a uteni di computer remoti: è il sistema di posta locale a tenere per ciascun utente una indirizzo di e-mail in cui depositare o ricevere la posta. Protocollo per lo scambio di messaggi di posta elettronica in rete Internet, Intranet o Extranet, Smtp può gestire messaggi formattati ed allegati grafici, audio, video e multimediali.

SNIFFER

Lo sniffer, o meglio "attacco a sniffer", è un metodo utilizzato dagli hacker per impossessarsi di una user-Id e della relativa password di un legittimo utente per accedere ad una rete locale. Dopo essere entrato nella rete (attraverso porte che necessariamente si aprono su Internet), l'hacker prende le informazioni "osservando" e copiando i pacchetti di dati degli utenti legittimi della rete Intranet o Lan (local area network). Una accortezza necessaria ad evitare attacchi a sniffer è l'uso della crittografia per le informazioni scambiate sulla rete. Un altro tipo di difesa efficace è l'utilizzo di un firewall che filtra i pacchetti provenienti da Internet. Lo sniffer può essere di due tipi: attivo o passivo. Molto pericoloso per la sicurezza è lo sniffing attivo l'hacker costringe la rete ad accettarlo come se fosse un utente fidato. Una variante del metodo Sniffer è l'attacco a spoofing: la base di partenza è lo sniffing attivo, ma dopo questa operazione, l'hacker cambia il proprio indirizzo con quello di un utente valido ed inoltra richieste al server che vengono prontamente eseguite. Generalmente l'attacco a spoofing viene condotto sulla posta elettronica.

SSL

Ssl, Secure Socket Layer, è un protocollo che consente, grazie a tecniche crittografiche, il trasferimento di dati tramite la rete Internet in modo sicuro. Il suo funzionamento è basato su un sistema a doppia chiave e i certificati digitali. In pratica esistono due chiavi: una per cifrare i dati inviati, l'altra per decifrarli. La seconda è conosciuta solamente da chi riceve i dati. Ssl è utilizzato per le transazioni sicure online.

STANDARD BS 7799

La Certificazione di conformità allo standard BS 7799 offre alle aziende uno strumento per garantire agli interlocutori commerciali e ai clienti la validità del proprio sistema di sicurezza: la certificazione obbliga inoltre a tenerlo costantemente sotto controllo con verifiche periodiche, come avviene abitualmente con i sistemi di Qualità. La Certificazione può essere rilasciata ad

un'azienda, reparto, impianto o altra unità e può essere successivamente estesa a qualsiasi sistema di gestione. La norma risponde alla domanda di enti, amministrazioni pubbliche, aziende industriali e commerciali, che richiedono una struttura comune per sviluppare le modalità di gestione dei rispettivi sistemi di sicurezza, migliorando la fiducia nelle relazioni interaziendali

TROJAN HORSE

Un Trojan Horse è un qualsiasi programma che ha una funzione visibile e una funzione nascosta, un esempio può essere un programma che esegue un gioco mentre segretamente invia file via e-mail. Un esempio di Trojan Horse può essere una piccola applicazione che visualizza un'animazione e che discretamente cerca file dell'utente interessanti e li rispedisce attraverso la connessione.

USERNET

Usernet (Unione per la Sicurezza E la Riservatezza dei NETworks) è una associazione fondata da Gruppo Webegg, Servizi Interbancari, Tuv Italia, Northon M.C. e Studio Legale Tamburrini Savi & Associati. Usernet è nata nel 2000 con lo scopo di approfondire le tematiche e i problemi legati all'Ict, la sicurezza delle reti, l'accesso alle informazioni del Web, in particolare con uno sguardo rivolto alle aziende che vogliono operare su Internet. Usernet organizza corsi di formazione, studi workshop, help desk on line, bollettini informativi e convegni per veicolare i contenuti che riguardano la sicurezza per l'e-commerce e l'e-business. I momenti di formazione sono concentrati in tre appuntamenti durante l'anno, che approfondiscono tre profili, legale, tecnico e organizzativo. L'Associazione, nelle sue diverse attività, ha sempre come riferimento la normativa internazionale (BS7799) e offre agli uomini d'azienda la possibilità di valutare, sulla base di criteri oggettivi, la sicurezza e l'affidabilità dei sistemi informativi aziendali. www.usernet.it

VIRUS

I virus informatici sono in sostanza brevi stringhe di codici in grado di danneggiare o cancellare dati, file o software memorizzati sul disco fisso di un computer. Da un punto di vista informatico un virus non è altro che un programma che si attiva e comincia a diffondersi in modo totalmente indipendente dalla volontà dell'utente. Il computer può venire infettato da un virus effettuando il download di un file infetto da Internet o copiando un file infetto da un dischetto. Una volta insinuatosi tra i file del computer, il virus può cominciare immediatamente a danneggiare o distruggere dati, oppure può attendere il verificarsi di un determinato evento o il sopraggiungere di una data stabilita che inneschi la sua carica distruttiva. I virus erano inizialmente composti di poche righe di linguaggio Assembler, poi cominciarono a svilupparsi sempre di più potenti e complessi: oggi si contano almeno 8 nuovi virus al giorno. Esistono diverse tipologie di Virus. File Viruses, attaccano i file eseguibili: .exe, .bat, .com, byn. Eccetera; Boot Viruses, virus del settore di avvio o virus di boot, risiedono nel settore di avvio del disco rigido e si attivano nello stesso momento in cui il computer viene acceso; Macro Virus che non si diffondono attraverso i normali

programmi ma nei documenti (tipo Word ed Excel). Un discorso a parte meritano i Trojani o ''Cavalli di Troia'', file all'apparenza innocui. I trojan vengono inviati tramite messaggi di posta elettronica, file ricevuti via chat o scaricati via internet, file contenenti macro, ecc... Una volta installati nel Pc i Trojan aprono un accesso ad un computer remoto facendo si che lo stesso abbia il pieno controllo del computer attaccato.

VPN - Virtual Private Network

Nel momento in cui si vogliono collegare tra loro, in modo sicuro, due o più filiali della stessa azienda, è necessario prevedere una connessione che possa garantire la sicurezza dei dati trasferiti da una sede all'altra. La soluzione è una Vpn (rete privata virtuale) che realizza una connessione permanente per ogni singola sede, un canale riservato e sicuro. Per Vpn si intende un collegamento che appoggiandosi su una connessione pubblica rende disponibili tutti i servizi della rete interna anche ad utenti remoti. Il riconoscimento avviene attraverso una procedura di autenticazione. Virtual Private Network vuol dire creare una rete aziendale su tutto il territorio per scambiare dati ed informazioni. Una rete privata virtuale costituisce un collegamento a livello dell'infrastruttura di rete, piuttosto che a livello delle applicazioni. La rete privata virtuale può essere realizzata secondo due tipologie. La prima collega una filiale periferica alla sede centrale ed è caratterizzata da router e firewall che trasformano in dati cifrati tutto il traffico che li attraversa. Il secondo tipo di VPN è rappresentato dal collegamento tra il notebook sul campo oppure il Pc a casa, verso una filiale o verso la sede centrale. Il collegamento può essere attivato mediante un qualsiasi ISP (Internet service provider). I vantaggi della Vpn sono: convenienza, gli utenti remoti possono collegarsi alle risorse di rete via Internet provider al prezzo di una chiamata locale; flessibilità, nuovi utenti vengono aggiunti con facilità senza nuove apparecchiature o linee dedicate; affidabilità, le Vpn sfruttano i mezzi delle infrastrutture della rete pubblica; sicurezza, le Vpn utilizzano sistemi di cifratura per proteggere il traffico privato.

VULNERABILITY ASSESSMENT

I sistemi di vulnerability assessment sono in grado di effettuare esami in profondità per rilevare problemi che possono rappresentare vulnerabilità della sicurezza nei sistemi informatici. I sistemi di vulnerability assessment vengono aggiornati continuamente per poter simulare l'attacco con i più recenti prodotti sviluppati dall'industria del crimine elettronico. Il servizio di Vulnerability Assessment che viene proposto da diverse società di consulenza, che realizzano software e soluzioni di security o semplicemente da associazioni dedite alla lotta alla criminalità informatica, ha come obiettivo la valutazione del livello di protezione e dell'efficacia dei sistemi di sicurezza adottati e quindi di prevenire eventuali attacchi basati su quelle vulnerabilità

WEB/MAIL CONTENT FILTERING

Si tratta dei sistemi per il controllo dell'utilizzo aziendale dei servizi Internet, delle politiche di corretto uso del servizio di posta elettronica e per il filtraggio di traffico E-mail. Mediante lo strumento di content filtering si effettua una cernita

fra i siti a cui si può accedere o meno: il servizio in genere si basa su una lista di indirizzi Internet e quindi di Url a cui non è possibile accedere. Questa lista è divisa per categorie ed ogni categoria è attivabile singolarmente. A fronte di un tentativo di accesso di un utente verso uno dei siti presenti nel content filtering, in genere la connessione viene bloccata.

XML

Xml è l'acronimo di eXtensible Markup Language, ovvero linguaggio di codifica estensibile, per codificare testo e dati allo scopo di elaborare i contenuti con il minimo intervento e scambiarli attraverso differenti periferiche hardware, sistemi operativi e applicazioni. Xml offre un metodo standard per rappresentare testo e dati in un formato che permette di scambiarli attraverso piattaforme, lingue e applicazioni. Un esempio di linguaggio definito con Xml è il Wml (Wireless Markup Language) usato per creare le pagine Internet visualizzabili sui telefonini Wap, oppure altri come il Cml (Chemical Markup Language) o il MathMl (Mathematical Markup Language). Secondo Andersen Consulting entro il 2003 il 30% delle transazioni B2B saranno effettuate in Xml, anche perché non necessita di ingenti investimenti, è alla portata delle Pmi, è "orientato all'interoperabilità semplice, non necessita di particolari skill, l'adozione in ambienti di lavoro è graduale e indolore mantiene la compatibilità con l'esistente, non è invasivo ma consente una graduale evoluzione verso sistemi aperti e più facilmente mantenibili".