MINISTERO DELL'ECONOMIA
E DELLE FINANZE

DIPARTIMENTO DELL'AMMINISTRAZIONE GENERALE
DEL PERSONALE E DEI SERVIZI DEL TESORO

I Quaderni dell'Innovazione

Manuale utente sull'uso consapevole di Internet

Suggerimenti per proteggersi
dai pericoli della rete durante
la navigazione in Internet

a cura di:

DANIELA BATTISTI
ROBERTA MANCINI
GIORGIO PAGANO
FABIO PAGLIARINI
GIOVANNA SISSA

7

ISTITUTO POLIGRAFICO E ZECCA DELLO STATO

(6015982/101) ROMA, 2004 - ISTITUTO POLIGRAFICO E ZECCA DELLO STATO S.p.A. - S.

Presentazione

E' evidente come in questi ultimi anni uno dei principali obiettivi delle politiche di governo sia quello di sfruttare le numerose opportunità offerte dall'utilizzo di internet e delle nuove tecnologie informatiche.

La politica di e-government non rappresenta solo l'opportunità di usufruire di nuovi strumenti per rendere più agevoli i rapporti tra Pubblica Amministrazione e cittadino, ma l'occasione per considerare un nuovo modo di offrire servizi aumentandone il valore. In questo panorama il Dipartimento si pone da protagonista, con numerose iniziative e progetti volti a realizzare, attraverso l'informatizzazione, l'evoluzione delle modalità di operare della Pubblica Amministrazione.

La strada che si sta percorrendo contempla la necessità che accanto al potenziamento della leva tecnologica, si sviluppi la capacità di sfruttare al meglio lo strumento in termini di competenze e di cultura informatica. Il presente Quaderno della collana risponde a questa esigenza ed è redatto allo scopo di divulgare un uso consapevole dello strumento Internet mettendo a conoscenza gli utenti, in modo semplice ed efficace, dei pericoli della rete.

Giancarlo del Bufalo

Indice

Premessa

L'uso delle tecnologie dell'informazione evolve e si espande sempre più velocemente. Oggigiorno gli utenti che hanno competenze informatiche non sono più un gruppo ristretto e specializzato all'interno di un'organizzazione: i computer infatti sono diventati strumenti di lavoro spesso insostituibili e sempre più diffusi ed il loro utilizzo per scopo privato e non solo lavorativo, è in continuo aumento. Come tale uso diventa sempre più pervasivo, così cresce anche la possibilità di errore o di uso improprio dello strumento. E' necessario quindi adottare misure che garantiscano un ambiente sicuro per gli utenti Internet, che possa proteggere i minori e rispettare allo stesso tempo la privacy e la dignità di tutti. Questo ambiente può essere creato solo attraverso iniziative nazionali, cooperazione internazionale e una maggiore informazione e comprensione del fenomeno.

Seguendo questa linea di pensiero, il Ministro Stanca ha istituito un Comitato Tecnico Interministeriale per l'Uso Consapevole di Internet (Decreto del Presidente del Consiglio dei Ministri del 12 luglio 2002). Il Comitato Tecnico per l'Uso Consapevole di Internet ha lo scopo di definire, monitorare e valutare i risultati di una strategia unitaria di intervento, finalizzata a creare le condizioni necessarie per garantire a tutti gli utenti la capacità e l'effettiva possibilità di usufruire delle comunicazioni elettroniche in maniera piena e consapevole, con particolare riguardo alle categorie di utenti che richiedono una maggiore tutela.

Un uso quanto più sicuro possibile della rete comporta un ampio raggio di azioni congiunte e coordinate riconducibili nelle seguenti aree:

- procedere all'esame degli interventi di settore realizzati o in corso di realizzazione in ambito nazionale, europeo e internazionale;
- proporre le opportune misure di coordinamento fra le diverse iniziative pubbliche eventualmente già intraprese;
- promuovere le opportune sinergie tra il settore pubblico e quello privato;
- raccogliere e valutare le istanze e le sollecitazioni provenienti dagli utenti e dagli operatori;
- individuare e proporre ogni misura necessaria per l'attuazione degli orientamenti comunitari e degli impegni internazionali assunti dall'Italia;
- definire proposte di carattere tecnico per una consapevole ed incisiva partecipazione del Paese alle iniziative comunitarie e internazionali;
- monitorare lo stato di attuazione e valutare i risultati delle linee di intervento definite, segnalando eventuali esigenze di adeguamento tecnico per il più efficace conseguimento dei risultati perseguiti;
- aumentare l'alfabetizzazione Internet intesa come competenze e capacità nell'utilizzare i nuovi servizi di comunicazione e informazione in maniera critica, sicura e vantaggiosa;

- sviluppare una strategia comune di misure di protezione e di azioni positive che garantiscano alle categorie più vulnerabili una corretta e produttiva fruizione della rete;

In quest'ottica sono state avviate, ad opera del Comitato, una serie di iniziative come:

- Valutare la possibilità di sostenere specifici progetti ed iniziative all'interno del nuovo piano *e*Safe e del nuovo programma tematico IST del VI Programma Quadro soprattutto per quello che riguarda il benchmarking dei prodotti di filtro e blocco di contenuti illegali e dannosi;
- promuovere anche attraverso i responsabili informatici della PA un uso responsabile della rete all'interno delle amministrazioni stesse attraverso la redazione di un manuale ad hoc ed avviare un processo di sensibilizzazione per l'utilizzo di firewalls ed altre forme di filtraggio;
- promuovere iniziative basate su un concetto più ampio di «consapevolezza» che non sia limitato al solo aspetto dei minori ma che riguardi in generale la cultura della sicurezza delle reti toccando gli aspetti dell'introduzione dei codici di autoregolamentazione da parte degli ISPs, governance di Internet, DRM (Digital Rights Management), DMCA (Digital Millenium Copyright Act), ecc.
- Organizzare un Safer Internet Day all'interno dell'IST Prize;
- Fare leva sui responsabili dei siti web della P.A. per divulgare il filtro ICRA e procedere all'etichettatura dei contenuti dei propri siti.

Uno dei frutti delle attività del Comitato Tecnico è *Il Manuale utente sull'uso consapevole di Internet* nato dalla collaborazione tra, gli ideatori del progetto del M.I.T., i responsabili dei sistemi informativi del M.E.F, con il supporto tecnico degli esperti della Consip S.p.A.

Scopo del documento è divulgare un insieme di linee guida sull'*uso consapevole delle comunicazioni elettroniche*, ovvero un uso consapevole di Internet, della posta elettronica, mailing list, chat, forum, ove, con il termine *consapevole* si intende informato, cosciente e messo a conoscenza dei pericoli della rete.

Introduzione

La navigazione in Internet consente di raggiungere decine di milioni di siti localizzati ovunque nel mondo. Analogamente a quanto avviene nella realtà anche in Internet è possibile imbattersi in aree dai contenuti illeciti o dannosi. La percezione del pericolo, durante la navigazione in Internet è però diversa da quella del mondo reale e pertanto si rende indispensabile comprendere alcune caratteristiche tecniche dello strumento al fine di renderne più sicuro l'utilizzo, sia per gli adulti che, a maggior ragione, per i minori.

Anche l'uso della posta elettronica, veicolo per il trasporto di messaggi ed allegati potenzialmente pericolosi, va effettuato con cognizione di causa per evitare danni anche gravi al proprio personal computer.

In breve, per un utilizzo consapevole di Internet si deve essere in grado almeno di:

- tutelare la privacy, intesa come protezione della propria identità e delle informazioni personali residenti sul proprio computer;
- inviare informazioni e dati su Internet in modo sicuro e non decifrabile da terzi non autorizzati;
- attivare misure di controllo per impedire l'accesso a siti non idonei alla consultazione da parte di minori;
- porre in sicurezza il proprio computer e le proprie informazioni da intrusioni e danni da parte di malintenzionati che utilizzano Internet in modo criminale.

La conoscenza dei principali pericoli dell'utilizzo di Internet e delle misure di protezione disponibili nei browser per la navigazione e nei programmi per l'utilizzo della posta elettronica, può consentire di sfruttare le enormi potenzialità che il mondo virtuale offre riducendo i rischi della navigazione.

Il presente documento è diviso in due parti: la prima, di carattere generale, la seconda, più tecnica, è costituita da quattro appendici. Nella parte generale si descrivono i concetti base di una navigazione sicura in Internet (sicurezza delle reti, tracciabilità, siti certificati, protezione sui contenuti), nelle appendici si fa riferimento a esempi di configurazione di alcune opzioni su Internet Explorer e su Microsoft Outlook. Si è scelto di riportare degli esempi tecnici riferiti a questo browser e a questo programma per la gestione di posta elettronica, poiché si tratta di alcuni tra i software maggiormente usati dagli utenti. Istruzioni analoghe sono comunque presenti anche su altri browsers e su altri software per la gestione della posta elettronica (Konqurror, Opera, Kmail, Safri, Mail perOSX, Entourage).

1. Una navigazione consapevole

Quando con il nostro computer ci colleghiamo in Internet, abbiamo l'immediata sensazione della vastità della rete, del notevole e molteplice flusso di informazioni in essa disponibile. Il primo quesito che solitamente ci viene in mente è come trovare un modo efficace ed efficiente per orientarci, per essere in grado di reperire rapidamente le informazioni che ci necessitano. Non pensiamo però che una navigazione in Internet possa causare dei danni al nostro computer, che possa essere registrata, osservata, spiata.

Per un uso davvero consapevole di Internet, quindi, è necessario che gli utenti sappiano cosa accade quando effettuano una certa operazione dal loro computer o cosa potrebbe accadere al proprio pc anche a loro insaputa. Una volta resi gli utenti consapevoli dei rischi in cui potrebbero incorrere durante una connessione, sarà loro discrezione effettuare una navigazione che garantisca una certa sicurezza o meno, sia utilizzando Internet dal posto di lavoro che collegandosi da casa. In quest'ultimo caso i suggerimenti riportati potrebbero essere utilizzati per impostare una navigazione sicura soprattutto nel momento in cui Internet fosse utilizzato anche da minori.

Sicurezza delle reti, tracciabilità, siti certificati, protezione sui contenuti: queste sono alcune delle caratteristiche peculiari di Internet. Vediamone brevemente il significato.

«Sicurezza delle reti», parola chiave che in Internet ha diverse sfaccettature: dalla sicurezza degli accessi in Internet collegandosi da casa alla sicurezza degli accessi dal posto di lavoro; dalla sicurezza nei confronti dei tentativi di accesso dall'esterno (ovvero da parte di sconosciuti che tentano di accedere al proprio computer) alla sicurezza della posta elettronica, ecc.

Quando un utente si collega ad Internet dal posto di lavoro utilizza semplicemente un browser (ad esempio Internet Explorer, Netscape, Opera,), senza chiedersi spesso come si stabilisca la connessione fisica. Per un utente che vuole collegarsi ad Internet da casa è invece, necessario sapere cosa serve per effettuare la connessione. In entrambi i casi occorre conoscere quali siano le eventuali tecniche da utilizzare per evitare che un estraneo (un hacker) possa accedere al sistema e danneggiare le proprie «difese», ed usare illecitamente, o persino danneggiare, i dati contenuti nel proprio disco fisso. Inoltre è bene fornire delle indicazioni per eliminare/ridurre la presenza di virus e programmi spia che compiono operazioni sul computer a nostra insaputa.

Qualsiasi utente Internet può essere soggetto a spamming, ovvero ricezione di messaggi di posta elettronica indesiderati, da parte di anonimi o sconosciuti. La conseguenza dello spamming può essere duplice: da una parte il fastidio dell'utente che riceve molte mail indesiderate (molto simili al caso della normale cassetta della posta riempita di messaggi pubblicitari che spesso vengono cestinati senza essere letti), dall'altra il problema del server di posta che, se sovraccaricato di messaggi, potrebbe avere dei problemi e non funzionare più correttamente con conseguente perdita dei messaggi in arrivo.

Altra parola chiave associata alla navigazione in Internet: «tracciabilità». Quando un utente utilizza un browser (Explorer, Netscape, Opera,) per connettersi ad Internet, il programma si porta dietro un insieme di informazioni (ad esempio il tipo di browser e la versione, il dominio di provenienza, l'indirizzo IP, l'ora e la durata della connessione, le pagine visitate) che vengono memorizzate in un file, detto file di log, appartenente al sito che si sta visitando. Il percorso di un utente in Internet è quindi sempre tracciabile. Tale tracciabilità può fermarsi alle informazioni associate al browser o può avvalersi anche dei cookies. Quest'ultimi sono pacchetti di informazioni che la pagina web o il

sito che stiamo visitando trasmettono al nostro computer e viceversa, per controllare quante volte e cosa l'utente stia visitando all'interno del sito stesso. L'utilizzo dei cookies è invisibile per l'utente che, a meno di opportune configurazioni alle opzioni del browser utilizzato, non si rende conto che il suo cammino in Internet è stato «registrato». Le informazioni che si possono prelevare con i cookies non riguardano dati memorizzati sul pc dell'utente né informazioni personali quali indirizzi di posta elettronica o numero di carta di credito, a meno che non siano esplicitamente digitati dall'utente all'interno di appositi spazi.

Esistono tuttavia dei programmi, un tipo particolare di programmi spia, che si installano sul disco rigido del pc nel momento in cui si scarica da Internet una qualche applicazione i quali, a insaputa dell'utente, raccolgono informazioni di dettaglio sulle caratteristiche fisiche della macchina, sulla sua navigazione e sui suoi dati personali (e-mail). Queste informazioni vengono comunicate a società che sfruttano i dati raccolti per profilare l'utente ed inviargli messaggi pubblicitari mirati. Molto spesso i programmi spia utilizzano la tecnologia ActiveX, che consente la condivisione delle informazioni tra diverse applicazioni. A volte i programmi spia possono essere inviati anche come allegati a messaggi di posta elettronica. Occorre dunque fare molta attenzione prima di aprire gli allegati delle e-mail.

«Siti certificati», parola chiave legata alla sicurezza della navigazione. Sul web spesso si inseriscono dati personali, come ad esempio il numero di carta di credito. Per essere sicuri che tali dati arrivino alla giusta destinazione e che non siano intercettati lungo il cammino in Internet, si utilizzano i certificati digitali, ovvero un documento che certifichi la validità e la «bontà» del sito, nonché un tipo di trasmissione dati sicura.

Con il termine «protezione sui contenuti» si intende solitamente la sicurezza sulla tipologia di contenuti, ovvero il fatto di poter raggiungere navigando in Internet siti con contenuti non offensivi, non pornografici, non violenti, ecc.

Anche se Internet, data la sua complessità, va considerata intrinsecamente insicura in tutti i suoi risvolti, è anche vero che basta controllare taluni aspetti tecnici e tenere gli occhi aperti circa le questioni pratiche, informandosi il più possibile per poter contare su ampi margini di sicurezza. Molte proprietà sulla sicurezza possono essere impostate a livello del browser. Tuttavia occorre ricordare che più sono stringenti le impostazioni sulla protezione, meno libertà d'azione si ha su Internet.

2. Sicurezza delle reti

2.1 Accesso da casa via rete telefonica

Per la connessione in Internet è necessario disporre di un PC, di un modem e di una linea telefonica. Un utente che si collega in Internet dalla propria abitazione effettua tale collegamento attraverso un Internet Service Provider (ISP), un'organizzazione o società che fornisce connettività agli utenti.

I vari ISP fungono da intermediari: si effettua infatti una connessione da casa propria verso l'ISP e da qui, utilizzando l'infrastruttura tecnica dell'ISP stesso, ci si collega in Internet in maniera totalmente trasparente per l'utente. Tra gli ISP più comuni abbiamo Tiscali, Tin.it, Libero. Il collegamento avviene componendo il numero di telefono di un ISP; il

modem, che generalmente è interno al PC, trasforma i dati che si vedono sullo schermo in impulsi (che viaggiano sul filo telefonico) e viceversa consentendo agli utenti di vedere gli oggetti su pagine web e di navigare in Internet.

La connessione ad Internet tramite ISP, a meno di non attivare alcuni servizi a pagamento (1), non protegge l'utente dai pericoli della rete che saranno illustrati nei prossimi paragrafi. I principali ISP hanno inserito, nella loro offerta a pagamento, servizi di accesso a Internet "sicuri", che possono fornire antivirus, antispamming, controllo dell'accesso Web per i minori, etc.

Per un utente che si collega da casa tramite ISP si può solo suggerire di utilizzare il buon senso e seguire alcune regole di base:

- Avere installata sempre l'ultima versione dell'antivirus, effettuando aggiornamenti in linea dal sito del produttore dell'antivirus. Un antivirus non aggiornato è un antivirus inutile.
- Munirsi (e mantenere aggiornata) una versione di antivirus avviabile da dischetto o CD-Rom, da usare in caso di compromissione grave del computer (e.g. quando il virus infettante impedisce il normale funzionamento dell'antivirus).
- Utilizzare, oltre all'antivirus, un firewall personale.
- Provvedere periodicamente all'aggiornamento, oltre che dell'antivirus e dell'eventuale firewall, del sistema, del browser e del client di posta elettronica, con particolare attenzione per le patch di sicurezza che vengono pubblicate.
- Utilizzare un antivirus che fornisca anche protezione specifica per la posta e per il download di contenuti da Internet.
- Utilizzare per l'accesso a Internet macchine dotate di sistema operativo più sicuro (Windows 2000 o XP, piuttosto che 95, 98 o Me). Eventualmente sfruttare la possibilità di istallare più sistemi operativi sulla stessa macchina.
- Evitare di utilizzare, per l'acceso a Internet, una macchina su cui sono presenti risorse condivise (directory del disco, stampanti, etc.); eventualmente disattivare la condivisione prima di accedere o, meglio, sfruttare la possibilità di istallare una versione diversa del sistema operativo con una configurazione più sicura.
- Cancellare frequentemente la cache di Internet.
- Diffidare dai file allegati ai messaggi di posta elettronica e comunque non aprirli mai senza prima aver effettuato un controllo.
- Disattivare la visualizzazione automatica del contenuto dei messaggi (e.g. la finestra di anteprima) almeno per la posta in arrivo e diffidare dai mail di origine sconosciuta.
- Controllare con cura i nomi dei file allegati, prestando particolare attenzione alla loro estensione effettiva (che spesso può essere non visualizzata a causa dell'impostazione di default di windows che la sopprime per i tipi registrati) e tenendo presente che non solo le estensioni .exe, .com e .bat corrispondono ad eseguibili (al riguardo può essere utile dare un'occhiata all'elenco dei file considerati pericolosi da Outlook stesso nella versione XP e perciò bloccati).

---

(1) si veda l'appendice 8 su questo tema.

- Utilizzare per la visualizzazione dei messaggi il formato RTF (o, meglio ancora, il TXT), piuttosto che lo HTML che consente una maggiore integrazione di contenuti dinamici ed un più facile sfruttamento delle vulnerabilità di sicurezza.
- Prestare attenzione (sottoporre a scansione dopo aver aggiornato l'antivirus, non aprire gli allegati prima di averli salvati su disco ed accuratamente verificati, etc.) nell'apertura di messaggi inattesi anche se di origine apparentemente nota.
- Diffidare assolutamente di e-mail di origine sconosciuta, specie se l'oggetto è ''invitante''.
- Evitare di usare CD-ROM e dischetti di origine sconosciuta o dubbia.
- Scaricare programmi solo da siti fidati.
- Fare copie di backup dei dati più importanti.
- Evitare di inserire dati riservati (ad esempio numero di carta di credito) su siti sconosciuti o non certificati.
- Evitare la memorizzazione sul computer di dati riservati (e.g. numero di carta di credito), in particolar modo sull'hard disk.
- Per evitare di essere sommersi da e-mail, nelle varie registrazioni sui diversi siti Internet lasciare un riferimento di e-mail che non sia quello principale.
- Cambiare frequentemente la password.
- Evitare la memorizzazione delle password di accesso sul computer, ma digitarle personalmente ogni volta.

2.1 Accesso da sede di lavoro protetta (via firewall) e file di log

Il firewall rappresenta uno strumento di sicurezza, una sorta di schermo, che consente di proteggere il computer dai tentativi di accesso dall'esterno

Generalmente i firewall vengono utilizzati negli ambienti lavorativi. In tali ambienti i computer dei vari dipendenti appartengono ad una rete interna, detta rete aziendale, in cui condividono alcune risorse. I firewall (2) consentono di isolare la rete aziendale dagli eventuali tentativi di intrusione dall'esterno e/o di inibire, se ritenuto necessario, funzionalità di un utente interno verso l'esterno. Esistono comunque diversi tipi di personal firewall che possono essere installati su PC personali e non appartenenti a rete aziendale. (3)

A seconda di come si configura un firewall, quest'ultimo può intercettare e memorizzare in alcuni file, detti file di log, tutti i messaggi, tutte le operazioni che fa un utente (esterno ed interno), ad esempio tutte le pagine web visitate, tutti i file che sono stati scaricati, l'utente che si è collegato, data e tempo di permanenza, browser utilizzato, sistema operativo, indirizzo IP, nome dell'host, ... (4)

---

(2) Oltre al firewall, altri meccanismi di protezione sono dati dai proxy server e dagli IDS (Intrusion Detection System).

(3) L'uso dei personal firewall in ambiente aziendale può creare problemi, specie riguardo all'amministrazione centralizzata delle postazioni di lavoro. Viceversa è molto consigliabile per i sistemi personali mobili (e.g. notebook), che vengono spesso utilizzati in ambienti privi delle protezioni presenti nella rete interna e possono diventare veicolo di infezione per quest'ultima) e sui computer personali utilizzati da casa.

(4) La funzione principale del firewall è il filtraggio del traffico entrante ed uscente sulla base del protocollo utilizzato e degli indirizzi della sorgente e della destinazione. Normalmente un firewall non è in grado effettuare un filtraggio basato sulla semantica dei pacchetti che lo attraversano (può bloccare l'accesso ad un certo indirizzo IP, e.g. ad un web server, ma non ad una certa pagina presente al suo interno, non è in grado di distinguere tra accesso in lettura ed accesso in scrittura, etc.). Per questo tipo di controllo occorre fare ricorso ai proxy, che, essendo specifici per un certo insieme di protocolli, sono in grado di entrare nel merito dello scambio che con tali protocolli avviene.

Osservando i file di log si possono vedere anche gli eventuali tentativi che sono stati fatti dall'esterno per accedere al sistema. (5)

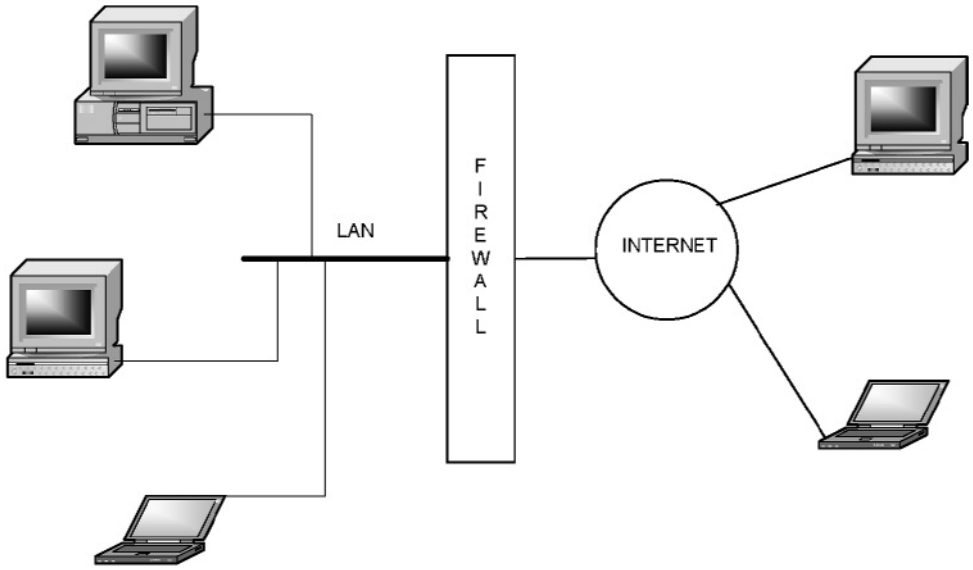

Figura 1: utilizzo del firewall come barriera tra la rete interna ed Internet

2.3 Gli hacker

L'hacker è colui che prova ad accedere ad un sistema esterno per ottenere informazioni riservate, provocare delle interruzioni di servizio, ecc. Le ragioni di tali intrusioni sono solitamente legate ad un vantaggio personale (ad esempio provando ad accedere a sistemi bancari) o a motivi ideologici/politici (ad esempio modificando la homepage di un sito per inviare messaggi politici o religiosi o per dimostrare che l'obiettivo non è invulnerabile).

Solitamente l'hacker non è interessato ad entrare nel computer di un generico utente ma in un grande sistema, cercando di evadere tutti i meccanismi di protezione.

I punti deboli su cui gli hacker insistono particolarmente per accedere ai sistemi esterni sono sistemi operativi ed applicazioni. Dopo aver implementato le contromisure riguardanti le vulnerabilità note dei sistemi (6), il miglior modo per un ente o azienda per

---

(5) Un'analisi completa è solitamente condotta in modo integrato sia sui log dei firewall sia sui log dei server e degli altri apparati di comunicazione coinvolti.

(6) Prima ancora dell'utilizzo dei firewall e degli IDS, è di fondamentale importanza l'implementazione delle contromisure riguardanti le vulnerabilità note dei sistemi. In particolare la tempestiva applicazione delle patch di sicurezza e delle procedure di ''hardening''. I firewall non possono nulla contro i tentativi di intrusione che avvengono accedendo ai servizi normalmente attivi e sfruttando i bug presenti nel software (si consideri il recente esempio del worm SQHell che ha bloccato gli uffici postali italiani e provocato notevoli danni soprattutto in oriente).

Riguardo agli IDS deve essere usata estrema cautela nell'uso di reazioni automatiche (e.g. il blocco del traffico per un certo periodo di tempo) poichè queste possono a loro volta introdurre vulnerabilità nei confronti di altri tipi di attacco, in particolare del tipo DOS.

proteggere il proprio apparato informatico da intrusioni esterne è l'utilizzo del firewall, con conseguente analisi dei file di log per avere informazioni sugli eventuali tentativi di intrusione.

Si riportano comunque di seguito alcuni semplici suggerimenti per i dipendenti del MEF per una navigazione sicura.

Protezione tramite password: la password può essere intercettata durante la sua trasmissione sulla rete, può essere «rubata» dal DB su cui è memorizzata, può essere individuata da un hacker per tentativi.

Il suggerimento è di utilizzare delle password che non siano troppo semplici o troppo corte. Inoltre sarebbe bene cambiare periodicamente le password evitando di memorizzarla sul disco rigido del computer.

Script o programmi di installazione non utilizzati: Il software e i servizi non necessari o datati solitamente non vengono aggiornati. Non è infatti insolito che un utente non sappia esattamente cosa ci sia sul proprio computer. Questi software non aggiornati possono essere vulnerabili. Si suggerisce di rimuovere il software non necessario e disattivare i servizi non necessari.

Vecchie versioni del sistema operativo: molte vulnerabilità a volte dipendono da buchi presenti nei sistemi operativi. Si suggerisce di controllare che la versione di windows installata sia la più recente. Controllare anche la disponibilità di aggiornamenti provvedendo ad istallare nel più breve tempo possibile quelli critici, soprattutto se riguardanti la sicurezza.

2.4 Lo spamming

Nel gergo telematico per «spamming» si intende un insieme di messaggi di posta elettronica che vengono recapitati ad un normale utente senza che questi li abbia chiesti. Nel caso dello spamming, tali messaggi, oltre a riempire la casella di posta, hanno anche un costo per l'utente (tempo per scaricare i messaggi ed utilizzo della rete).

Conoscendo meglio come agiscono gli spammer è possibile intervenire sia come «prevenzione», evitando di fornire sulla rete informazioni utili agli spammer stessi, sia come «cura», adottando dei metodi per filtrare lo spamming.

Uno dei luoghi più fecondi per la raccolta di indirizzi di posta elettronica è dato dalle Newsgroup. In caso di partecipazione ad un Newsgroup, una delle prime abitudini da prendere è quella di apporre nella firma che identifica l'e-mail, delle parole che non c'entrano. Esempio: firmarsi con un indirizzo del tipo 'mitt*ente@mio*indiri*zzo.com' dando istruzioni per 'sistemare' l'indirizzo ('se vuoi rispondere, devi solo eliminare gli asterischi dall'indirizzo...'). Questa tecnica funziona. Gli strumenti automatici, infatti, che cercano indirizzi sulla rete non capiscono tali istruzioni e collezionano l'indirizzo sbagliato 'mitt*ente@mio*indiri*zzo.com' che non riceverà mai l'e-mail.

Si suggerisce estrema cautela nell'iscrizione a newsgroup e alle mailing list: non iscriversi a tutte quelle che si trovano, piuttosto selezionarne alcune, sceglierle con cura e cercare di evitare di dare informazioni personali sulla rete.

Naturalmente gli indirizzi non vengono raccolti solo dalle Newsgroup, ma si possono prendere anche dai siti web. Un indirizzo di e-mail messo a disposizione su un sito serve per essere contattato da un qualsiasi visitatore. Se invece una persona lo utilizza per inviare informazioni o messaggi non richiesti, di carattere commerciale o altro, ecco l'abuso. Non ha importanza che siano messaggi di tipo pubblicitario, politico, eccetera: l'abuso c'è lo stesso.

Qualche volta capita di ricevere un messaggio del tipo: '...ti abbiamo inserito nella nostra mailing list... ...per evitare di ricevere la nostra posta puoi spedire una e-mail a unsubscribe@bla.bla.com...etc...' E' buona norma non rispondere a tali messaggi poiché a volte gli spammer riescono a ottenere un elenco di nomi che afferiscono ad una determinata struttura, conoscono il dominio ma non sanno esattamente la composizione dell'e-mail (se nome.cognome@dominio.it. o n.cognome@dominio.it o n.cognome@dominio.it); vengono dunque fatte una serie di prove e l'eventuale «unsubscribe» dell'utente corrisponde molte volte ad una conferma del proprio indirizzo. Quando arrivano tali messaggi è bene cancellarli ed ignorarli: senza conferma non arriveranno una seconda volta. Comunque osservando attentamente l'intestazione della mail spam che si è ricevuta, si può risalire al provider utilizzato dagli spammer per avvertirlo della e-mail ricevuta. Dovrà essere poi il provider a «schermarsi» da tali spammers.

Quando si invia una mail a più utenti o si fa un forward di una mail che si è ricevuta, è bene cancellare dall'intestazione del messaggio inoltrato ogni eventuale riferimento ai precedenti indirizzi di posta elettronica. Diffondere, anche involontariamente, indirizzi di posta elettronica, altrui, oltre che a violare la legge sulla privacy, dà modo a possibili profittatori di riempire tali caselle con avvisi pubblicitari e proposte commerciali (spamming). Per specificare il destinatario della e-mail ci sono tre caselle:

A: (Destinatario principale)

Cc: (Copia carbone, destinatari per conoscenza)

Bcc: (o Ccn, Copia carbone nascosta)

IMPORTANTE! Se si sta diffondendo un messaggio a molte persone, alcune delle quali non si conoscono tra loro, è meglio non inserire gli indirizzi nel campo **A:** ma inserirli tutti nel campo **Bcc:**. In questo modo ogni destinatario non potrà vedere l'elenco degli indirizzi email e si eviterà di diffondere tali informazioni (NB. Nel caso il vostro programma richieda di inserire un indirizzo nel campo A: inserite semplicemente il vostro indirizzo email).

Con questo piccolo accorgimento è possibile limitare lo spamming di messaggi commerciali, un altro fastidioso fenomeno, ben conosciuto tra gli utenti Internet.

2.5 Posta elettronica, i problemi degli allegati

Quando arrivano dei messaggi di posta elettronica che contengono degli allegati, bisogna avere molta accortezza prima di aprirli, per evitare di scaricare un ActiveX con programmi spia o un virus. Le modalità di protezione che si definiscono a livello del browser valgono anche per la posta elettronica.

Per quello che riguarda i virus degli allegati, esistono dei software specifici che, una volta installati e configurati (nel caso di aziende tali software sono configurati dagli addetti al server di posta, effettuano le seguenti operazioni:

Messaggi in arrivo

- per ogni e-mail ritenuta infetta sarà effettuato un tentativo di ripulitura
- se il tentativo di ripulitura si conclude con successo, la mail verrà consegnata con un messaggio di notifica di avvenuta pulitura

- se il tentativo di ripulitura ha esito negativo, l'allegato sarà cancellato e al destinatario (a volte anche al mittente, dipende da come è configurato l'antivirus) perverrà una notifica di avvenuta eliminazione del file

Messaggi in uscita
- per ogni e-mail ritenuta infetta sarà effettuato un tentativo di ripulitura
- se il tentativo di ripulitura si conclude con successo, la mail verrà consegnata con un messaggio di notifica di avvenuta pulitura
- se il tentativo di ripulitura ha esito negativo, la mail sarà inviata al destinatario senza allegato, e verrai informato che è stato individuato un virus non eliminabile.

3 Tracciabilità e privacy

3.1 Informazioni sui cookies

Quando un utente si collega in Internet e richiede il caricamento di una pagina, si attiva un meccanismo di comunicazione tra il client (la macchina su cui sta lavorando l'utente) ed il server (la macchina su cui risiede il sito). Ad esempio, per una pagina contenente tre immagini ed un file di testo vengono attivate quattro richieste consecutive dal client al server, ognuna completamente indipendente dalle altre. Il server gestisce in modo equivalente quattro richieste provenienti dallo stesso client o da client diversi. A volte è però importante mantenere traccia delle richieste inviate dallo stesso client. Questo può accadere ad esempio quando ci troviamo di fronte ad applicazioni tipo ''negozio elettronico'', dove è necessario conservare una lista di articoli acquistati, oppure quando un utente sceglie delle preferenze per visitare un sito (come lingua, colore,). Per tenere traccia delle operazioni che effettua un utente, ovvero delle chiamate che il server riceve dallo stesso client, si utilizzano i cookies.

Un cookie (letteralmente significa «biscottino») è una stringa di caratteri che viene spedita dal server al browser contenente informazioni relative all'utente e alla sua interazione con il sito. Tale stringa viene memorizzata in un file sulla macchina del client (provate a fare una ricerca del file «cookie» sul vostro PC: potreste restare stupiti nello scoprire da quanti siti internet il rispettivo server ha lasciato un cookie nella vostra macchina!). Tutte le volte che il browser si connette ad un server per richiedere una pagina, valuta anche la possibilità di inviargli un cookie eventualmente ricevuto in precedenza, permettendo così di mantenere le informazioni di stato. I parametri che contraddistinguono un cookie, e che quindi permettono al browser di stabilire se deve inviarlo o meno, sono:

- *data di scadenza*. È possibile fare in modo che un cookie non sia più inviato dopo una certa data;
- *dominio*. Un cookie sarà spedito solo a un certo dominio oppure a un certo host;
- *path*. Il browser invierà il cookie (oppure i cookies) solo quando richiede un URL che inizia con un certo percorso;
- *sicurezza*. Se richiesto, il browser invierà il cookie solo durante le connessioni sicure, quelle normalmente usate per le transazioni commerciali.

Un cookie può contenere **solo** le informazioni fornite dall'utente durante la visita a un sito Web. Ad esempio, un sito non è in grado di ottenere l'indirizzo di posta elettronica di un utente a meno che questi non lo invii al sito inserendolo in un modulo Web. La creazione di un cookie non consente al sito Web l'accesso al resto del computer dell'utente.

Pur essendo uno strumento molto potente che consente di incrementare l'interattività del sito web, i cookies possono essere disattivati in quanto possono rappresentare un abuso della privacy.

Si riportano di seguito i principali rischi dovuti all'utilizzo dei cookies:

- Problemi di sicurezza: dati sensibili (come password, dettagli di carte di credito) che transitano su Internet attraverso connessioni non sicure sono spesso memorizzate in cookies. In teoria il contenuto dei cookies potrebbe essere accessibile da chiunque sia in grado di intercettarli su Internet o da chi tenti di effettuare un accesso remoto sul computer dell'utente. I cookies dovrebbero essere criptati quando contengono dati personali.
- Tracciabilità: i cookies possono essere intercettati da un utente esterno consentendogli di identificare le attività dell'utente.
- Divulgazione di dati personali: un sito che, attraverso la tecnologia dei cookies, raccoglie informazioni personali su un utente Internet può scambiare questi dati con altri siti (ad esempio con business partner o vendendo tali informazioni). Questa condivisione di dati può essere ottenuta facendo in modo che i cookies siano sincronizzati tra diversi gruppi/società. Questo implica che informazioni personali raccolte durante una visita in un sito in cui l'utente ha volontariamente comunicato tali informazioni, possono essere usate da siti in cui tali informazioni non sono mai state fornite o da siti che non sono mai stati visitati (un esempio tipico è dato dallo spamming).
- Controllo limitato dei browser: gli utenti Internet hanno un controllo estremamente limitato sul contenuto e sull'uso dei cookies, poiché in genere tale tecnologia non è direttamente visibile. Alcuni browsers provvedono agli utenti delle opzioni che consentono la disabilitazione dei cookies. Tuttavia questa restrizione può avere come conseguenza il fatto che alcuni siti siano totalmente inaccessibili. Per coloro che decidono di accettare i cookies non ci sono meccanismi di browser che informano l'utente sull'uso che è stato fatto dei cookies o di quali dati sono stati memorizzati con essi.

3.2 Utilizzo inconsapevole dei programmi spia

Un programma spia, o spyware, è un software, generalmente scaricato gratuitamente da Internet, che manda informazioni dal computer dell'utente, senza che l'utente lo sappia, durante la sua navigazione in Internet. Di solito le informazioni inviate riguardano il tipo di navigazione, i siti visitati, le icone più cliccate, piuttosto che informazioni relative al numero di carta di credito. Oltre al fatto che tali informazioni sono trasmesse senza il consenso dell'utente, occorre anche considerare che gli spyware sono solitamente programmi scritti male, che possono contenere diversi errori e che possono causare malfunzionamenti al computer.

Gli spyware possono essere suddivisi in due diverse categorie, surveillance (di sorveglianza) e adware.

I software di sorveglianza memorizzano le sequenze di caratteri, catturano le schermate, Questi programmi sono solitamente usati da corporazioni, investigatori privati, tutori della legge,

L'adware è invece una sorta di cavallo di troia, un software che si installa attraverso un altro software o via controlli ActiveX su Internet. Gli adware memorizzano informazioni sull'utente, possibilmente le password, indirizzi e-mail, la configurazione hardware e software, nome, età, sesso dell'utente, i siti visitati,

Come con gli spam, gli adware utilizzano la CPU, la RAM e le altre risorse del computer dell'utente.

Occorre tener presente però che non tutti gli spyware sono utilizzati a danno degli utenti: esistono anche società serie che collezionano dati sui consumatori per utilizzarli al meglio in un ambiente competitivo, per migliorare i profitti dell'azienda senza danno, o arrecando dei vantaggi anche all'utente.

E' necessario quindi essere in grado di chiudere, o almeno di limitare l'accesso degli spyware ai nostri computer, ed effettuare dei controlli per verificare che i nostri pc non contengano tali software.

Un buon antivirus identifica alcuni adware come virus; è bene quindi tenere sempre aggiornato l'antivirus sulle macchine.

Inoltre, poiché l'installazione di spyware può essere legata all'esecuzione di ActiveX, si illustreranno in appendice le possibili configurazioni di questi sul browser Explorer.

Infine esistono anche dei software, alcuni gratuiti disponibili su Internet ed altri a pagamento, in grado di identificare eventuali componenti degli spyware.

Ovviamente per limitare problemi dovrebbe essere sempre il buonsenso a prevalere, cercando di non scaricare i vari software dai vari siti indiscriminatamente, ma ponendo molta attenzione a quanto il sito sia sicuro e attendibile.

3.3 I controlli ActiveX

Quando si scarica un software da un sito esterno spesso vengono attivati dei controlli ActiveX. ACTIVEX é una tecnologia, rilasciata da Microsoft, ideale per il programmatore che opera in ambito Internet. Come suggerisce il nome, in ambito Internet, ActiveX serve proprio per attivare le pagine html, e renderle in grado non solo di mostrare informazioni ma anche di ricevere input dall'utente, elaborare questo input e magari restituirlo nella forma appropriata, in definitiva dare all'utente una maggiore possibilità di interazione, cercando di rendere la pagina html simile ad una vera e propria applicazione. Benché Internet sia l'ambiente ideale per ActiveX questo non deve far credere che l'uso di tale tecnologia sia limitato ad Internet: anche se certe caratteristiche rendono i componenti ActiveX ideali per l'uso in rete, essi possono essere tranquillamente usati nelle normali applicazioni.

I *controlli ActiveX* sono dei componenti che possono inserirsi nelle pagine Web. Tali controlli, non essendo eseguibili, non possono funzionare da soli, ma devono essere usati all'interno di un altro contenitore, sia esso un eseguibile, una pagina HTML o un documento ActiveX. Quest'ultimo a sua volta ha bisogno di essere ospitato all'interno di un browser che lo supporti o in un raccoglitore di documenti. La conseguenza di ciò è che quando si apre una pagina web basata su tecnologia ActiveX, possono scaricarsi sul nostro computer alcuni file o componenti (7).

---

(7) Tecnologia analoga (e precedente) a quella Microsoft è data dagli Applet Java, che presentano rischi del tutto simili. Grazie alla diffusione della programmazione Java in ambito Web, la probabilità di imbattersi in contenuti attivi di questo tipo è tutt'altro che trascurabile.

3.4 Utilizzo di software per individuare programmi spia

Il controllo degli ActiveX spesso non è sufficiente ad eliminare l'installazione di spyware, poiché non tutti i programmi spia, anche se la maggior parte, si basano sull'uso degli ActiveX. Oltre alle opzioni di controllo sull'uso degli ActiveX è bene utilizzare dei software che consentano di controllare attentamente tutte le componenti del pc e che siano in grado di individuare file sospetti nei registri, nei cookies e nelle varie cartelle. Questi programmi sono detti ad-aware e, a seconda del tipo, possono essere installati sulla propria macchina o possono semplicemente essere eseguiti. Alcuni software rimuovono direttamente i file sospetti; altri software consentono di isolare tali file e la loro eliminazione non è automatica ma a richiesta dell'utente.

I software ad-aware si basano sulla seguente caratteristica: i componenti dei più comuni programmi spia sono noti e sono tali componenti che vengono cercati tra i cookies e nei registri. Ovviamente l'elenco dei programmi spia e dei loro componenti non è fisso ma varia col variare degli spyware. Per questo motivo i software ad-aware necessitano di continui aggiornamenti a seconda dei nuovi spyware e dei nuovi componenti individuati.

Di seguito è riportato l'elenco di alcuni tra i più noti programmi che lanciano spyware:

Add/Remove Plus!, AutoFTP PRO, Crystal FTP, CuteFTP 3.0, CuteFTP 3.0 beta, CuteFTP/Tripod, CuteMX, CutePage, Delphi Component Test, Delphi Tester, Dialer 2000, DigiBand, NewsWatch, DigiCams - The WebCam Viewer, Digital Postman, DirectUpdate, DL-Mail Pro 2000, DNScape, Doorbell 1.18, Download Minder 1.5, FreeImageEditor, FreeIRC, FreeNotePad, FreeSite, FreeWebBrowser, FreeWebMail, FreeZip!, FTPEditor, Go!Zilla, HTML Translator, jIRC, JOC

Alcuni esempi di software ad-aware sono
Ad-aware (*http://www.lavasoft.de/*)
Optout (*http://grc.com/optout.htm*)

4 Siti certificati

4.1 Certificati digitali

Un certificato è un documento che attesta l'identità di un utente o la protezione di un sito. Vediamo un esempio di come un utente internet possa interagire con certificati e transazioni sicure. Connettendosi sul sito della Banca di Roma, dopo aver selezionato Banca telematica e Accesso al servizio, gli utenti vengono avvisati da un messaggio che stanno utilizzando una connessione sicura e si apre una nuova finestra in cui gli utenti devono digitare user-id e password. Questi dati vengono trasmessi cifrati, con una connessione sicura, identificabile dagli utenti per il fatto che in alto nel browser invece di essere scritto http:// si trova https:// e dalla presenza di un lucchettino giallo nella parte in fondo a destra del bordo della finestra (vedi ***Figura 2***: l'indirizzo e il lucchettino sono evidenziati con una freccia)). Solo cliccando sul lucchettino vengono visualizzate tutte le informazioni sul certificato, tra cui il nome dell'autorità certificatrice, la data di emissione e di scadenza del certificato, ecc. La chiave per decodificare il messaggio la conosce solo

la Banca di Roma; quindi, qualora il messaggio venisse intercettato da terzi, non sarebbe interpretabile perché in codice. Questo è il principio su cui si basano molti siti di commercio elettronico su cui viaggiano i numeri di carta di credito.

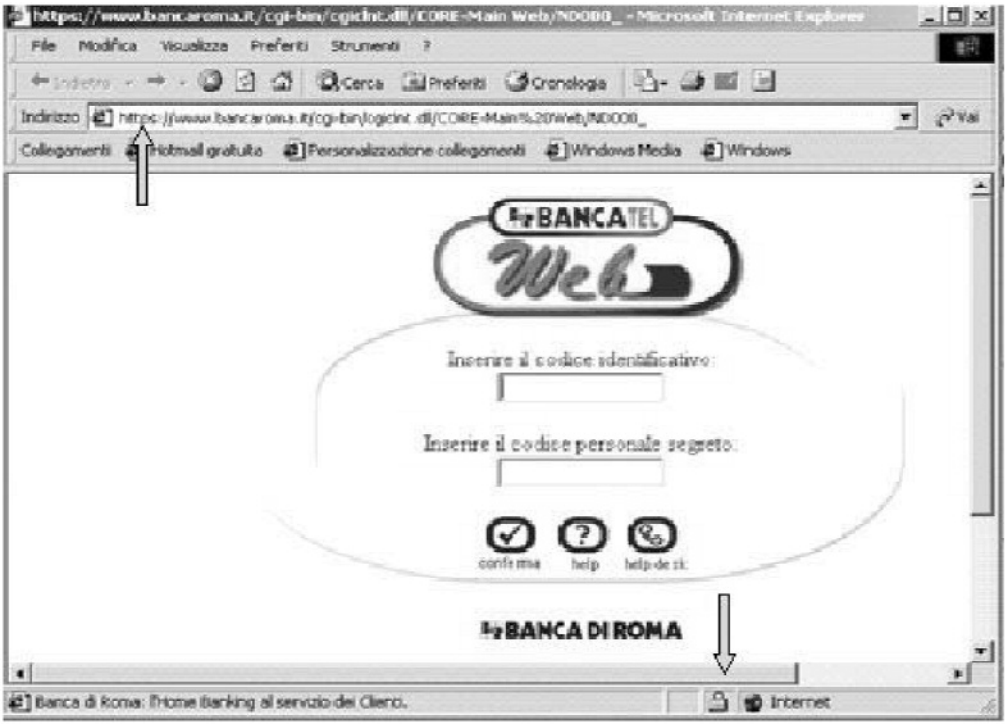

Figura 2: sito digitalmente certificato. Nell'indirizzo in alto a sinistra si può identificare la connessione https; in fondo a destra si può identificare il lucchettino

4.2 Messaggi legati alle connessioni sicure

Di seguito si riportano le immagini di alcune finestre che descrivono l'interazione uomo-macchina nel caso del passaggio da una connessione normale ad una protetta e viceversa.

Figura 3: Visualizzazione di una finestra in cui si avvisa l'utente che si sta andando da una connessione semplice ad una protetta

Si sta tentando di stabilire una connessione protetta con il sito Web. Questo sito Web fornisce una comunicazione protetta e dispone di un certificato valido. Comunicazione protetta significa che le informazioni inviate al sito, quali il nome o il numero di carta di credito, sono crittografate in modo da non poter essere lette o intercettate da altre persone. Il certificato è una dichiarazione che garantisce la protezione di un sito Web. Un certificato contiene informazioni che garantiscono che un sito Web è autentico. In tal modo nessun altro sito può assumere l'identità del sito originale.

Quando si accede a un sito Web protetto, per avvisare l'utente vengono visualizzate questa finestra di dialogo e l'icona di un lucchetto chiuso sulla barra di stato. Quando si esce da un sito protetto, viene visualizzato un messaggio di avviso.

Se si desidera che questa finestra di dialogo venga sempre visualizzata quando si accede a un sito Web protetto, assicurarsi che la casella di controllo Non mostrare l'avviso in futuro sia deselezionata.

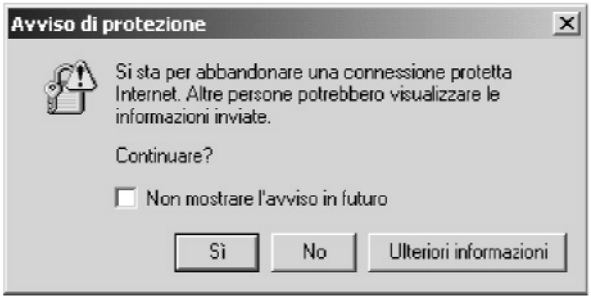

Figura 4 Accesso a un sito Web non protetto da un sito protetto

Il sito Web visualizzato in precedenza era protetto. Un sito Web protetto fornisce una comunicazione protetta e dispone di un certificato valido. Comunicazione protetta significa che le informazioni inviate al sito, quali nome o numero di carta di credito, sono crittografate in modo da non poter essere lette o intercettate da altre persone. Il certificato è una dichiarazione che garantisce la protezione di un sito Web. Un certificato contiene informazioni che garantiscono che un sito Web è autentico. In tal modo nessun altro sito può assumere l'identità del sito originale.

Il sito Web al quale si desidera accedere tuttavia non utilizza un protocollo di protezione e le informazioni inviate e ricevute non saranno protette. Il sito non dispone di un certificato e non è possibile verificarne l'identità.

In base alle informazioni di cui si dispone sul sito Web e sul computer in uso, è possibile decidere se accedere o meno al sito.

Se si ritiene che le informazioni di cui si dispone non siano sufficienti, fare clic su No.

5 Protezione sui contenuti

Con «protezione sui contenuti» si intende solitamente la sicurezza sulla tipologia di contenuti, ovvero il fatto di poter raggiungere navigando in Internet siti con contenuti non offensivi, non pornografici, non violenti, ecc.

A volte navigando in Internet si possono raggiungere dei siti dal contenuto potenzialmente pericoloso, quali siti che contengono immagini o documenti di violenza, guerra, droga, pedofilia, Tali contenuti possono essere particolarmente pericolosi nel caso in cui l'utente si connette da casa ed ha dei bambini che possono utilizzare la rete. Per superare questo problema attualmente Internet offre due alternative:

1) liste di siti pericolosi
2) filtri

Sui vari browser utilizzabili per accedere ad Internet è possibile definire delle liste di siti etichettati come pericolosi e non consentire l'accesso a tali siti.

Oltre alle opzioni sui diversi browser esistono anche dei software a pagamento che forniscono liste di siti pericolosi. Alcune di queste liste possono essere personalizzate dall'amministratore della macchina aggiungendo o eliminando siti; in altri casi ciò non è possibile. Tali liste necessitano di essere aggiornate con una certa frequenza, con ulteriore spesa dovuta all'aggiornamento delle stesse.

In altri casi le liste di siti pericolosi non sono lasciate al gestore delle macchine ma sono gestite direttamente da un provider o da una agenzia esterna: l'utente si collega al provider dell'agenzia e sarà questa a controllare se è possibile accedere o meno al sito internet prescelto. In questi casi il servizio viene pagato dall'utente al provider o all'agenzia. E' da far presente però che l'utilizzo di un'agenzia come «intermediario» per l'accesso ad Internet potrebbe rallentare i tempi di accesso alla rete.

Uno degli esempi di agenzia esterna è rappresentato da Davide, il cui funzionamento si basa sull'esistenza di una lista di siti pericolosi, aggiornati con una certa frequenza. Questo servizio è a pagamento e gli utenti per usufruirne devono collegarsi ad Internet passando per il Pop di Davide.

I filtri si basano sull'utilizzo di alcune parole chiave: il loro compito è quello di impedire la visualizzazione di siti internet che contengono le parole indicate come «pericolose» nel filtro.

I browser più comuni consentono di indicare che livello impostare il filtro stesso relativamente a siti con contenuto di violenza, sesso. Un esempio di filtro è dato da ICRA Internet Content Rating Association.

ICRA è un filtro che, una volta installato su un PC, permette la personalizzazione del tipo di navigazione in Internet consentendo (o restringendo) l'accesso a siti con contenuto di pedofilia, violenza, oscenità, ecc. Si tratta di un filtro utile soprattutto a genitori, scuole. Il filtro non è dinamico né «intelligente», nel senso che non è in grado di distinguere il contenuto dei siti, ma semplicemente legge delle etichette nascoste che vengono messe sulla homepage di alcuni siti internet. L'utilizzo di ICRA è infatti composto di due parti: da una parte l'etichettatura del sito, dall'altra l'installazione del filtro stesso. L'installazione è demandata ai genitori, l'etichettatura ai webmaster.

L'etichettatura consiste in una sorta di autocertificazione. I webmaster dei vari siti internet dovrebbero rispondere ad un questionario (domande del tipo «il sito contiene immagini di nudo? SI/NO») ed inviarlo a ICRA. A questo punto sarà generata un'etichetta che sarà reinviata ai webmaster affinché l'etichetta stessa sia aggiunta al sito Web. L'etichetta non è visibile agli utenti, ma viene letta dal filtro se è stata attivata tale funzione. Facoltativamente, è possibile aggiungere un pulsante con il logo ICRA o un collegamento testuale che indichi che il sito è etichettato.

Ad oggi sul sito internet www.mininnovazione.it, sotto la voce «chi ha paura della rete» è possibile attivare il link per scaricarsi gratuitamente il filtro ICRA.

Per quello che riguarda la mail indesiderata, nei più comuni software per la gestione dell'e-mail sono disponibili delle funzionalità che consentono di etichettare una mail come indesiderata o con contenuto per adulti ed è possibile impostare alcune regole in modo che, riconosciuto il mittente, un suo messaggio venga eliminato appena ricevuto.

6 APPENDICI TECNICHE

Sono di seguito riportati alcuni esempi di configurazioni su Microsoft Outlook 2002 e Microsoft Internet Explorer 5.5. Per versioni diverse di Microsoft Outlook e Internet Explorer i riferimenti potrebbero non corrispondere.

7 Configurazione degli antivirus su Microsoft Outlook 2002

Diversi antivirus (ad esempio McAfee e Norton) mettono a disposizione dei plug-in per Microsoft Outlook in modo da poter impostare, una volta installato l'opportuno antivirus sul proprio computer, alcune proprietà di gestione direttamente su Outlook.

Selezionare dal menu Strumenti la voce «Proprietà di scansione posta»

Figura 5: Proprietà di scansione posta

Qui, sotto l'etichetta Rilevamento, selezionare «Tutti i messaggi nella cartella Posta in arrivo» e «Tutti gli allegati» (vedi ***Figura 5***).

Sotto l'etichetta Azione si trova una tendina che contiene cinque possibili azioni da effettuare al rilevamento di un virus in un allegato. Si suggerisce di settare «Pulisci automaticamente l'allegato infetto» (vedi ***Figura 6***).

Le etichette Avviso e Rapporto servono per impostare un eventuale messaggio al titolare del pc nel caso di virus trovati negli allegati delle mail di cui lui è il destinatario o il mittente.

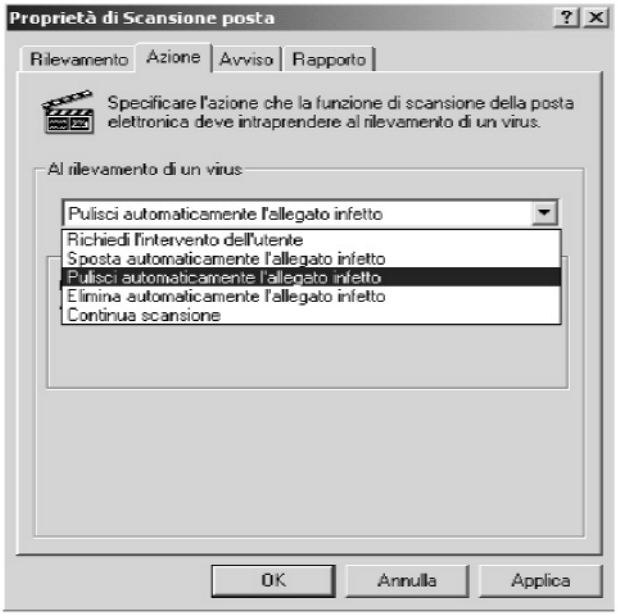

Figura 6: Impostazione dell'azione per la pulizia di allegati infetti

8 Configurazione dei cookies su Internet Explorer 5.5

Dal menu Strumenti selezionare la voce Opzioni Internet. Si aprirà la seguente finestra:

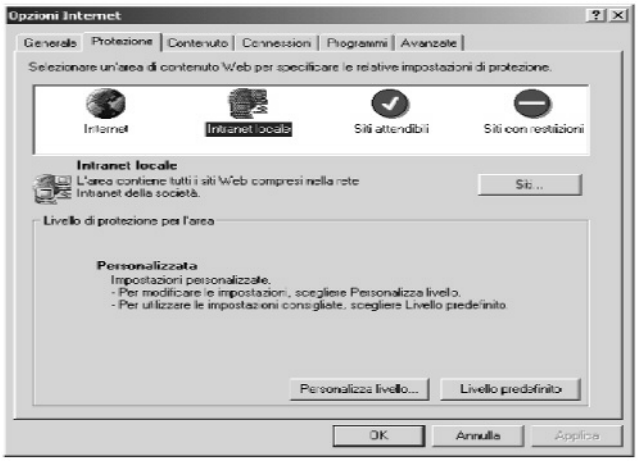

Figura 7: Opzioni di protezione sul browser Internet Explorer

Sotto l'etichetta Protezione è possibile configurare i cookies per i siti Internet e per la intranet. Per non mantenere le impostazioni di default occorre selezionare l'icona relativa ad Internet e poi cliccare sul tasto Personalizza livello. Si aprirà la seguente finestra:

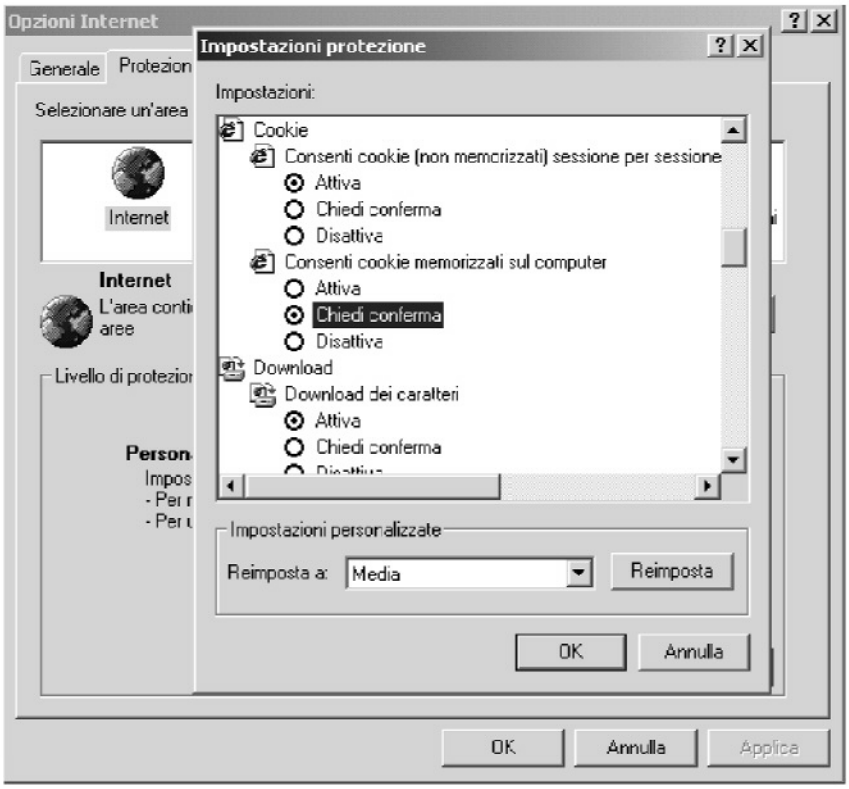

Figura 8: Impostazioni di protezione per i cookies

Ci sono due tipi di cookies che possono essere utilizzati, quelli che non vengono memorizzati sul pc dell'utente e che durano solo la singola sessione, e quelli che vengono memorizzati sul computer. Per default vengono settati entrambi ad Attiva. Per quello che riguarda i cookies che non sono memorizzati, si suggerisce di mantenere l'opzione di default, ovvero Attiva. Invece, per quelli che si memorizzano sul computer poiché, come detto precedentemente, disabilitando i cookies alcuni siti non possono essere visitati, si suggerisce di settare l'opzione Chiedi conferma. In questo caso sarà l'utente che, a seconda del sito che sta visitando, deciderà se consentire o meno di memorizzare i cookies sul proprio pc.

Gli stessi due settaggi dei cookies si trovano anche sulle altre tre voci: intranet, siti attendibili e siti con restrizioni.

Poiché l'intranet si considera sicura, si suggerisce di lasciare la configurazione dei default, ovvero di settare entrambe le opzioni ad Attiva.

Sotto la voce Siti attendibili si trova l'elenco dei siti Internet considerati sicuri. Inizialmente tale lista è vuota e, cliccando sul tasto Siti, si apre la seguente finestra che consente l'inserimento di indirizzi http:

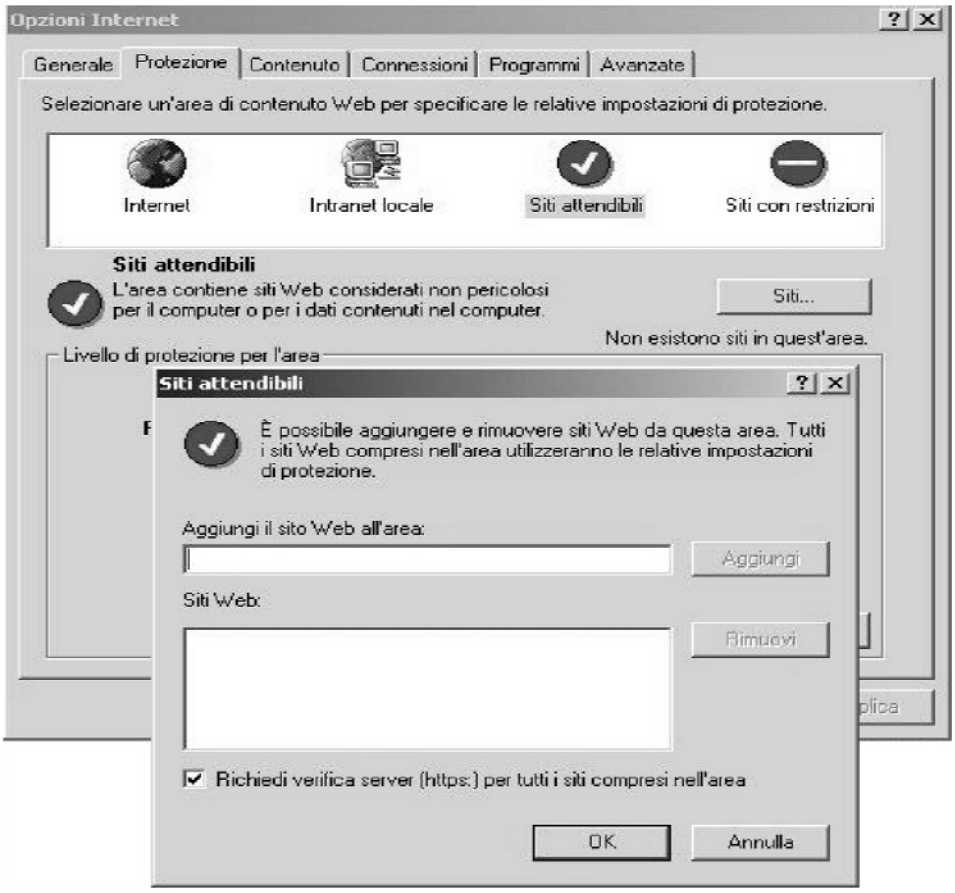

Figura 9: Configurazione dei siti attendibili

Per i siti accessibili, proprio perché considerati sicuri, si suggerisce di settare entrambe le opzioni sui cookies ad Attiva.

L'amministrazione dei siti con restrizioni è analoga a quella dei siti sicuri solo che, trattandosi di siti non sicuri, si suggerisce di settare entrambe le opzioni sui cookies a Disattiva.

9 Configurazione degli ActiveX su Internet Explorer 5.5

I *controlli ActiveX* sono dei componenti che possono inserirsi nelle pagine Web (per essere visualizzati richiedono plug-in o client specifici come Internet Explorer) e permettono un completo accesso alle caratteristiche di Windows ma, non possono essere eseguiti su altre piattaforme. I controlli, non essendo eseguibili, non possono funzionare da soli, ma devono essere usati all'interno di un altro contenitore, sia esso un eseguibile, una pagina HTML o un documento ActiveX. Quest'ultimo a sua volta ha bisogno di essere ospitato all'interno di un browser, che lo supporti, o in un raccoglitore di documenti.

Ci sono alcune opzioni in Internet Explorer, che consentono di decidere come configurare gli ActiveX.

Dal menu Strumenti selezionare la voce Opzioni Internet; selezionare l'icona Internet e poi Personalizza livello. Si aprirà una finestra in cui saranno presenti cinque opzioni relativamente agli ActiveX:

a) esegui controlli e plug-in ActiveX
b) esegui script controlli ActiveX contrassegnati come sicuri
c) inizializza ed esegui script controlli ActiveX non contrassegnati come sicuri
d) scarica controlli ActiveX con firma elettronica
e) scarica controlli ActiveX senza firma elettronica

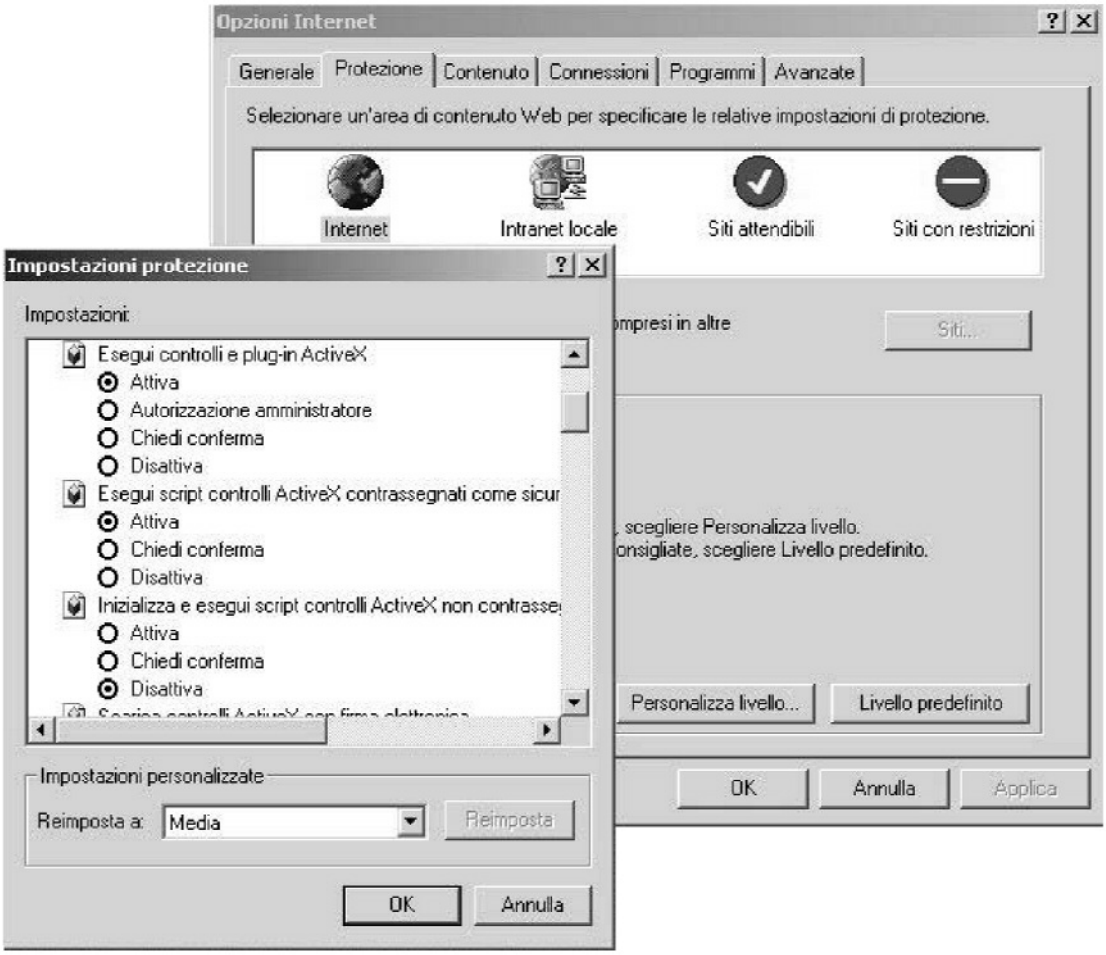

Figura 10: Impostazione di protezione per gli ActiveX

Nel caso dei siti Internet, si suggeriscono le seguenti configurazioni:

a) chiedi conferma
b) attiva
c) disattiva
d) attiva
e) chiedi conferma

Nel caso dei siti intranet e dei siti attendibili, si suggeriscono le seguenti configurazioni:

a) attiva
b) attiva
c) attiva
d) attiva
e) attiva

Nel caso dei siti con restrizione si suggeriscono le seguenti configurazioni:

a) disattiva
b) attiva
c) disattiva
d) disattiva
e) disattiva

10 Configurazione su Explorer 5.5 delle opzioni legate alla navigazione su siti certificati

Su Internet Explorer 5.5, selezionando dal menu Strumenti la voce Opzioni Internet e selezionando l'etichetta Avanzate, si visualizza la finestra riportata in ***Figura 11***.

I valori riportati sono quelli di default. Vediamo la descrizione dei principali attributi:

Avvisa in caso di certificati di siti non validi: Specifica se si desidera essere avvisati nel momento in cui l'indirizzo o URL, presente nel certificato di protezione di un sito Web non è valido.

Avvisa se si passa da modalità protetta a non protetta: Specifica se si desidera essere avvisati quando si passa da siti Web protetti a siti Web non protetti.

Usa SSL 2.0: Specifica che si può scegliere di inviare e ricevere le informazioni protette tramite SSL2 (Secured Sockets Layer Level 2), il protocollo standard per le trasmissioni protette. Tutti i siti Web protetti supportano questo protocollo.

Usa SSL 3.0: Specifica che si può scegliere di inviare e ricevere le informazioni protette tramite SSL3 (Secured Sockets Layer Level 3), un protocollo più sicuro di SSL2. Questo protocollo potrebbe non essere supportato da tutti i siti Web (8)

Usa TLS 1.0: Specificache è possibile inviare e ricevere informazioni protette con TLS (Transport Layer Security), uno standard di protezione aperto simile a SSL3 (Secure Sockets Layer).Anche questo protocollo potrebbe non essere supportato da tutti i siti Web.

Verifica revoca dei certificati del server: Specifica se si desidera verificare che un certificato di sito Internet sia stato revocato prima di accettarlo come valido.

Verifica revoca dei certificati dell'autore: Specifica se, prima di accettare un certificato come valido, si desidera che ne venga controllata la data di scadenza.

---

(8) La differenza più importante con lo SSL2 è il supporto della «client authentication», ossia dell'identificazione anche del soggetto che accede. Affinché ciò sia possibile, è necessario che anche la macchina usata per accedere, o, meglio ancora, l'utente che accede, disponga di un opportuno certificato digitale.

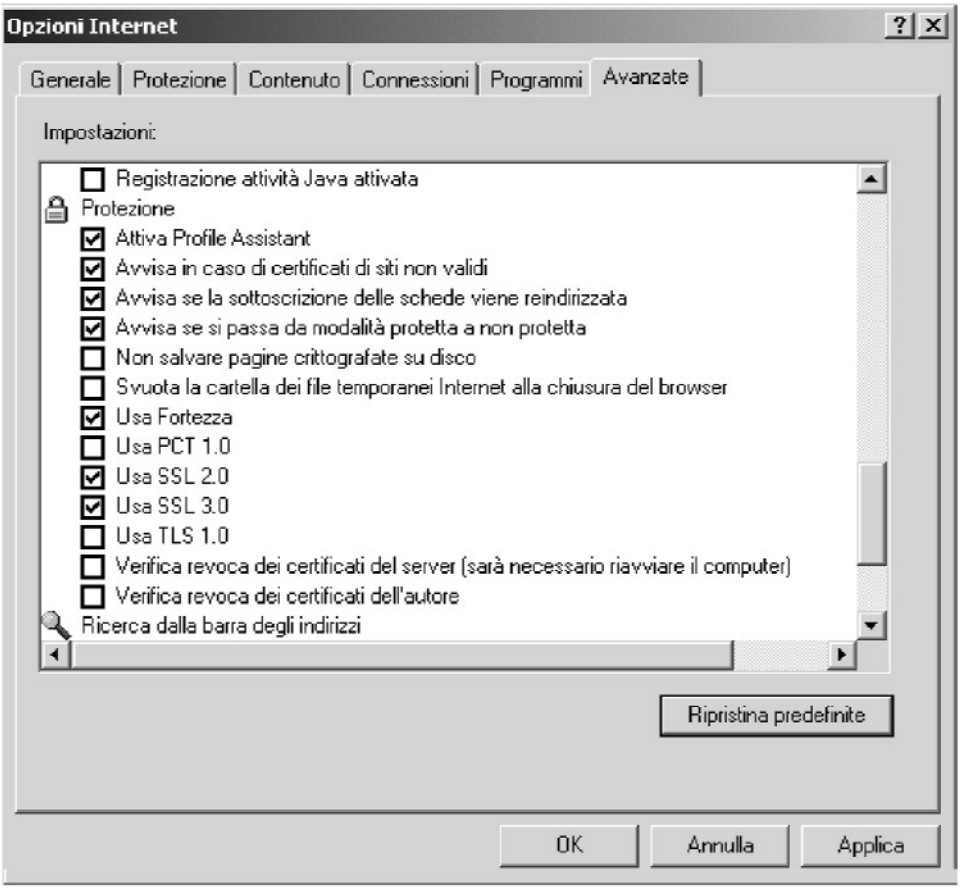

Figura 11: Opzioni Internet relative alla protezione

Per avere informazioni di maggior dettaglio sui certificati, eseguire le seguenti operazioni:

sotto il menu Strumenti selezionare Opzioni Internet e poi Certificati. Si aprirà una finestra (vedi ***Figura 12***) in cui si può selezionare lo scopo del certificato (autenticazione client, posta elettronica protetta, scopi avanzati, tutti). Selezionato lo scopo del certificato si può vedere l'elenco di tutti i certificati personali, quelli di altri utenti, quelli emessi da autorità di certificazione intermedie, quelli emessi da autorità di certificazione attendibili relativamente allo scopo selezionato. Selezionata l'etichetta dei certificati emessi dalle autorità intermedie o dalle autorità attendibili, si ottiene una lista di certificati. Con un doppio click su uno degli elementi della lista si ottengono informazioni sul certificato come quelle riportate in ***Figura 13***.

Esiste un archivio di certificati. Questi possono essere esportati dall'archivio al disco rigido con la funzione Esporta di ***Figura 12*** e possono essere importati dal disco rigido verso l'archivio con la funzione Importa della stessa figura. Ovviamente un certificato per essere importato deve essere stato ricevuto (ad esempio per e-mail) da una Autorità di certificazione dopo che ne è stata fatta richiesta.

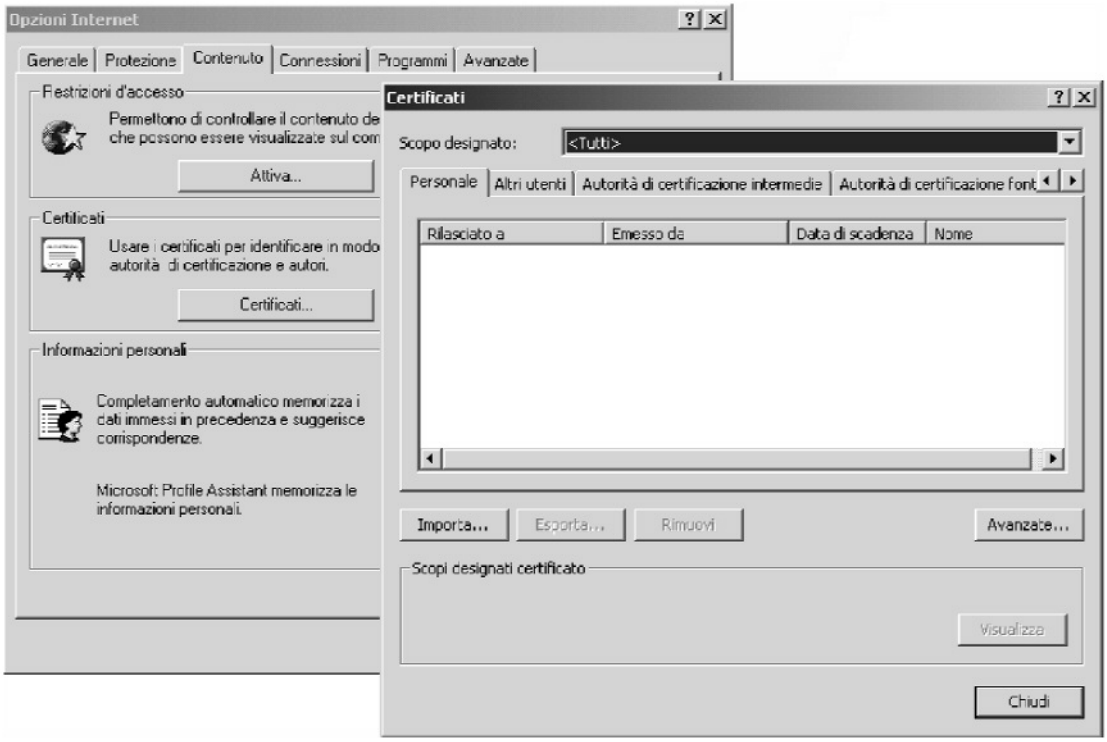

Figura 12: Informazione sui Certificati dalle Opzioni Internet

Figura 13: Informazioni di dettaglio su un certificato

11 Opzioni disponibili su Internet Explorer 5.5 per le restrizioni sui contenuti

All'interno di Internet Explorer selezionare dal menu Strumenti la voce Opzioni Internet; selezionare l'etichetta Contenuto e, sotto Restrizioni d'accesso selezionare la voce Impostazioni. Si aprirà una finestra (vedi ***Figura 14***) in cui, sotto l'etichetta Restrizioni d'accesso compare una sigla RSAC (Recreational Software Advisory Council) e dei parametri (linguaggio, scene di nudo, sesso e violenza). La RSAC (che oggi non esiste più e che dal 1999 è stata sostituita dall'ICRA Internet Content Rating Association) prevede strumenti di base per filtrare la visualizzazione dei siti web in relazione al loro contenuto.

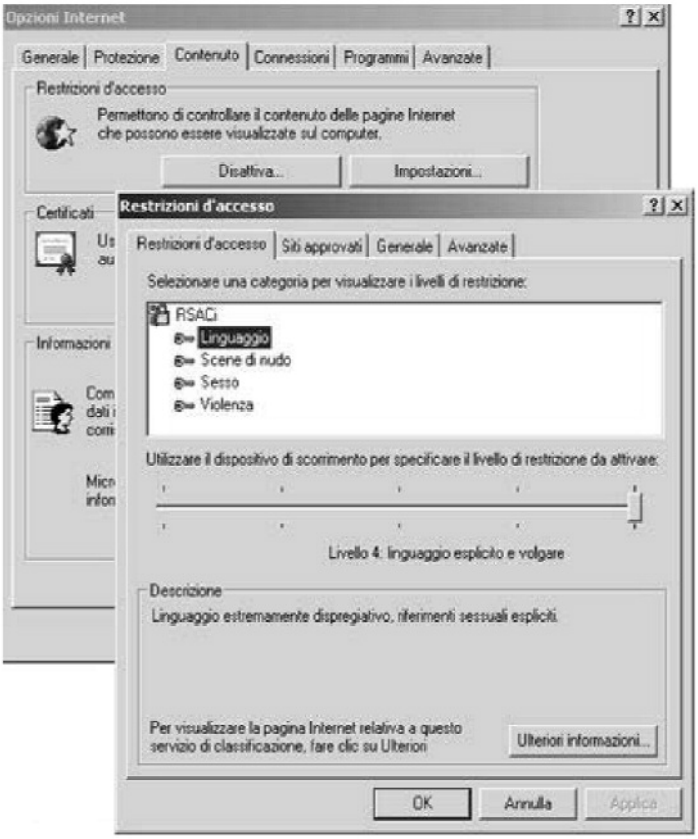

Figura 14: Restrizioni d'accesso

Vediamo come funzionano tali filtri. I responsabili dei contenuti dei siti, a seconda delle risposte che danno ad un questionario, proposto da RSAC/ICRA, associano un valore numerico (che va da 0 a 4) ad un insieme di parametri (per RSAC sono quattro: linguaggio, scene di nudo, sesso e violenza; per l'ICRA sono di più). Il valore 0 rappresenta la situazione ottimale, senza pericoli; il valore 4 indica un sito, il cui contenuto è decisamente solo per adulti. Tali valori e tali parametri possono essere relativi ad un intero sito web, ad un suo ramo o ad una sua pagina e sono inseriti, in maniera del tutto trasparente ai navigatori Internet, sul sito in modo da etichettarlo.

Nella finestra riportata in ***Figura 14*** è possibile impostare i filtri in modo da consentire l'accesso solo a quei siti i cui valori dei parametri siano minori o uguali ai valori scelti. In maniera più semplice, se in tale finestra tutti e quattro i parametri (linguaggio, scene di nudo, sesso e violenza) sono stati impostati a 3, durante la navigazione in Internet sarà possibile accedere solo ai siti in cui i quattro parametri assumano un valore tra 0 e 3.

Selezionando l'etichetta Siti approvati, è possibile inserire un elenco di siti che possono essere sempre acceduti o che non possono essere mai acceduti indipendentemente dal valore dei parametri visti nelle Restrizioni d'accesso. (***Figura 15***)

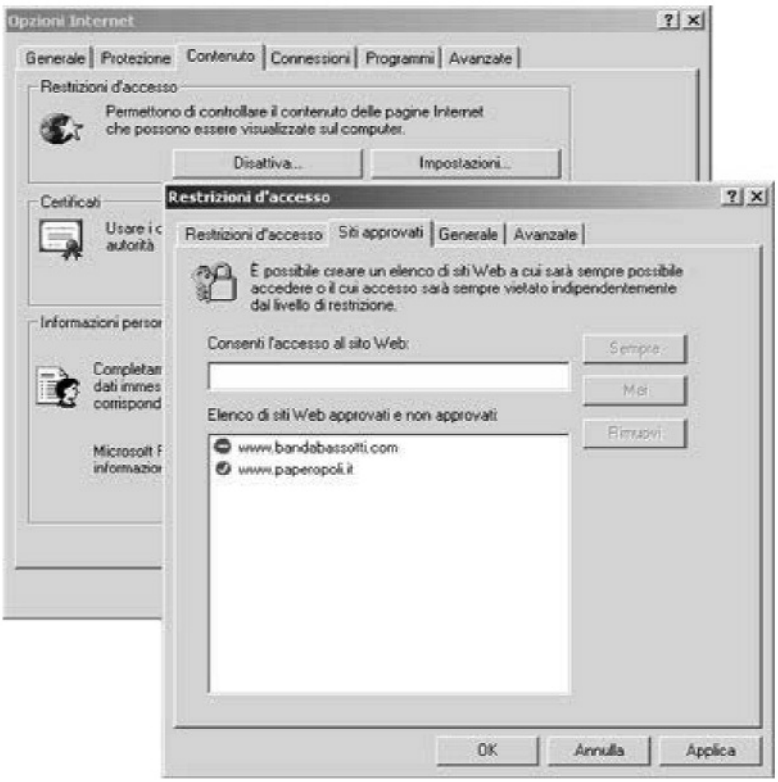

Figura 15: Elenco di siti sempre accessibili o mai accessibili

Selezionando l'etichetta Generale, si accede alla finestra riportata in ***Figura 16***. Se in tale finestra si seleziona l'opzione «Visualizzazione di siti senza descrizione», sarà possibile accedere anche ai siti che non hanno le descrizioni RSAC. In caso contrario, se tale opzione è deselezionata, non sarà possibile accedere a siti che non hanno le descrizioni RSAC. Opzionalmente, solo con la password di supervisore, è possibile visualizzare siti con restrizioni.

Infine, selezionando l'etichetta «Avanzate» (vedi ***Figura 17***), è possibile indicare una agenzia che funga da intermediario: in questo modo l'accesso ad Internet sarà controllato dall'Agenzia scelta e sarà condizionato dai filtri di cui dispone. Ovviamente è da tener presente che l'inserimento di una figura intermedia, che filtri la connessione ad Internet, potrebbe rallentarne il tempo di collegamento.

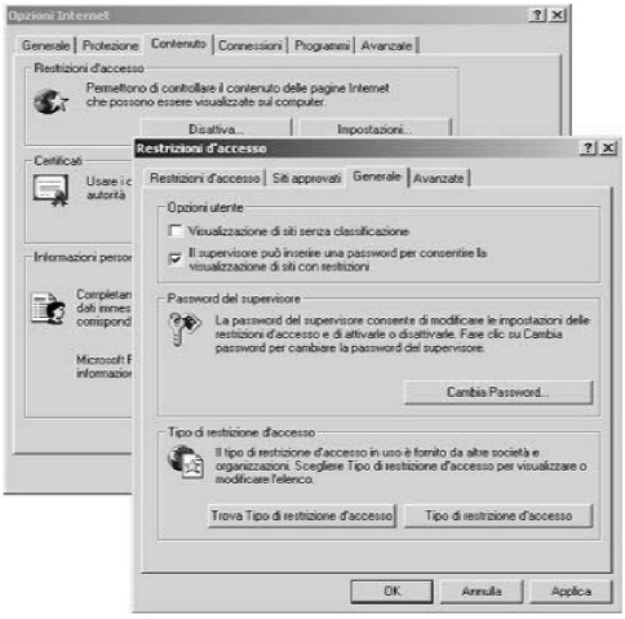

Figura 16: Opzioni di visualizzazione

Figura 17: Utilizzo di Agenzie per le restrizioni d'accesso

12 Posta elettronica: opzioni di protezione per posta indesiderata o per contenuto per adulti

In Microsoft Outlook sono disponibili delle funzionalità, che consentono di etichettare una mail come indesiderata o con contenuto per adulti ed è possibile impostare alcune regole in modo che, riconosciuto il mittente, un suo messaggio venga eliminato appena ricevuto. Si descrivono di seguito le operazioni necessarie per effettuare tale operazione.

Ricevuta una e-mail considerata come indesiderata o con contenuto per adulti, selezionare il messaggio ricevuto, cliccare con il tasto destro del mouse, selezionare la voce «posta indesiderata» e da qui selezionare «Aggiungi all'elenco Mittenti posta indesiderata» o «Aggiungi all'elenco Mittenti contenuto per adulti». La stessa operazione si può effettuare selezionando un messaggio di posta elettronica e selezionando dal menu Azioni la voce «Posta indesiderata».

È possibile inserire indirizzi o domini nell'elenco mittenti dei contenuti per adulti o dei mittenti posta indesiderata anche senza aver ricevuto una e-mail, semplicemente conoscendo indirizzi e domini. Tale operazione si effettua in questo modo: selezionare dal menu «Strumenti» la voce «Organizza» e da qui selezionare la voce «Posta indesiderata». Nella parte superiore della finestra della posta in arrivo si aprirà una finestra in cui è possibile evidenziare con colori diversi i messaggi considerati come posta indesiderata o come contenuto per adulti (vedi ***Figura 18***).

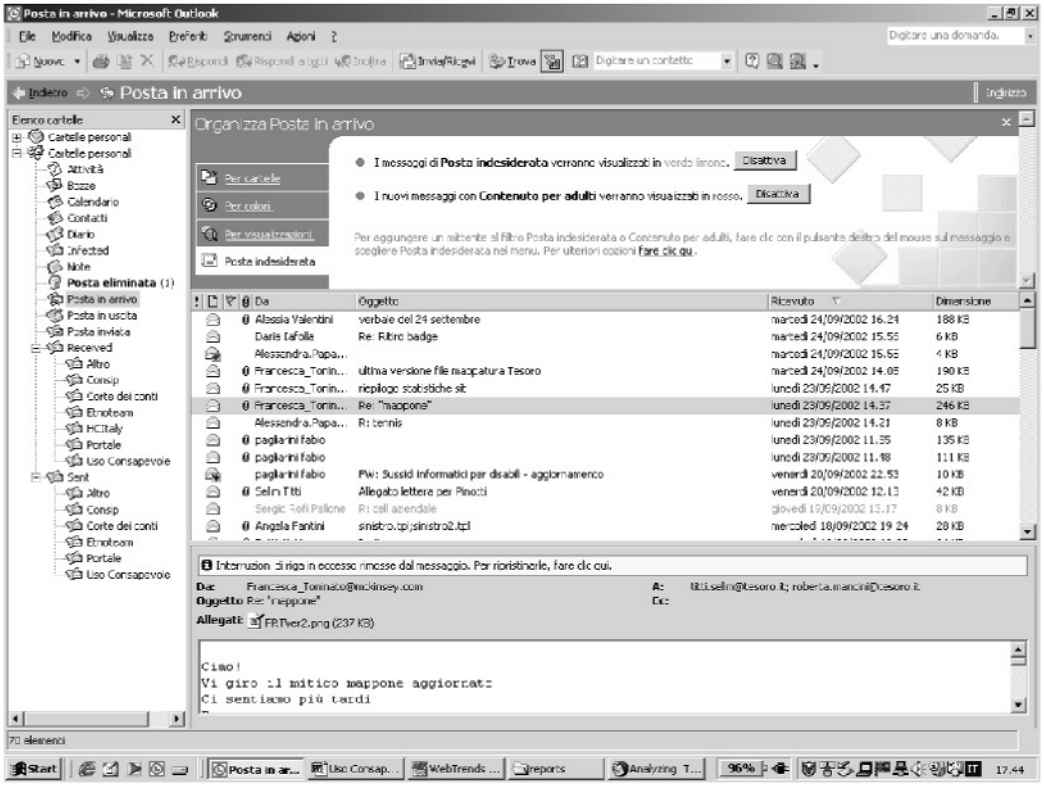

Figura 18: Organizzazione posta in arrivo: posta indesiderata

Selezionando il link «Fare click qui», nella parte superiore della pagina si apre la finestra riportata in ***Figura 19***.

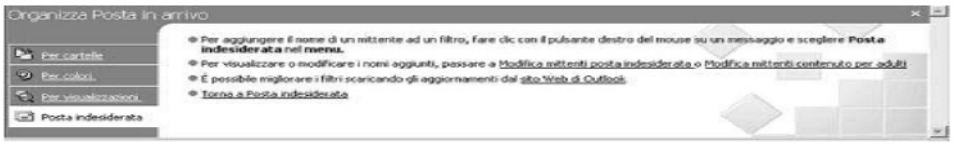

Figura 19: Modifica mittenti posta indesiderata o modifica mittenti contenuto per adulti

Da qui, selezionando il link Modifica mittenti posta indesiderata è possibile inserire indirizzi di e-mail noti, modificare indirizzi esistenti, eliminare indirizzi (vedi ***Figura 20***).

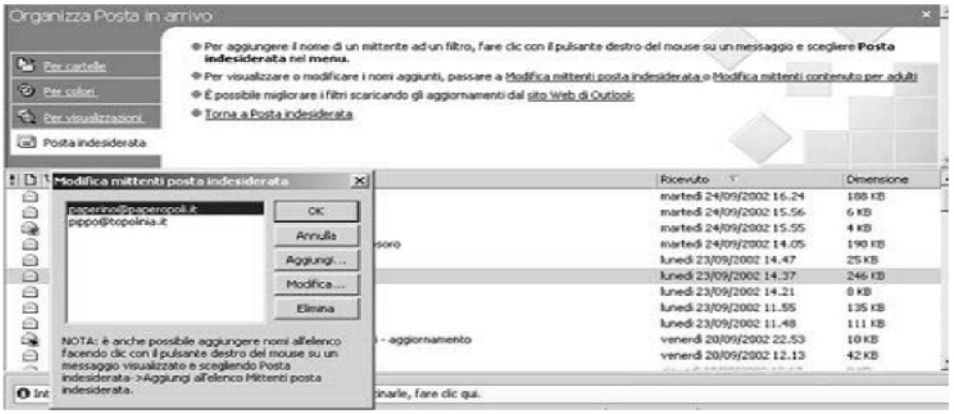

Figura 20: Modifica mittenti posta indesiderata

In particolare, selezionando il tasto Aggiungi, è possibile inserire sia un indirizzo che un dominio (vedi ***Figura 21***).

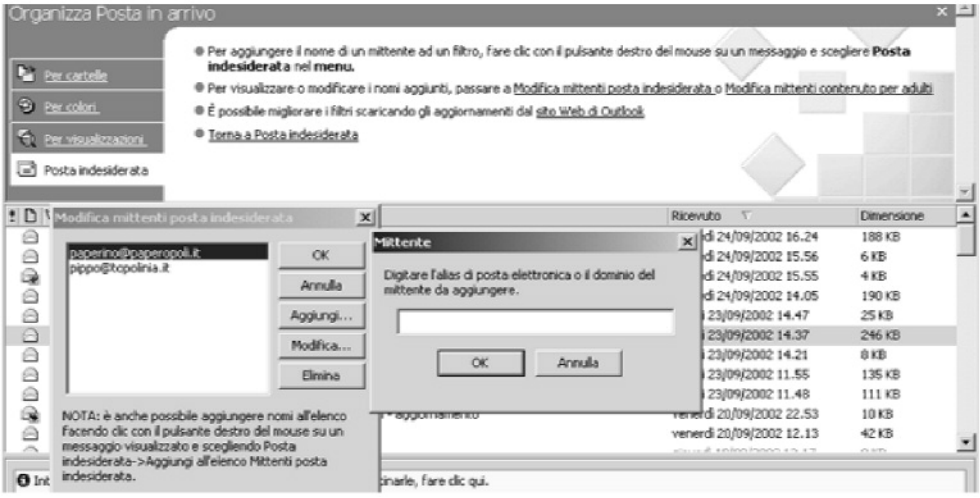

Figura 21: Inserimento nuovo utente o dominio

Analogamente si gestiscono gli indirizzi dei mittenti di contenuti per adulti.

Man mano che si ricevono le e-mail «di disturbo», si può arricchire sempre di più la lista dei mittenti di posta indesiderata e quella dei mittenti di posta per adulti.

A questo punto si può definire una regola per la quale le mail etichettate come indesiderate siano evidenziate di colori diversi, o spostate in un determinato folder, o eliminate,

Vediamo di seguito un esempio di come si imposta una regola per eliminare tali e-mail.

Nella finestra «Organizza posta in arrivo», ottenuta selezionando la voce «Organizza» del menu «Strumenti», selezionare a sinistra «Per cartelle» e poi in alto a destra «Creazione guidata di regole» (vedi ***Figura 22***).

Figura 22: Creazione di regole

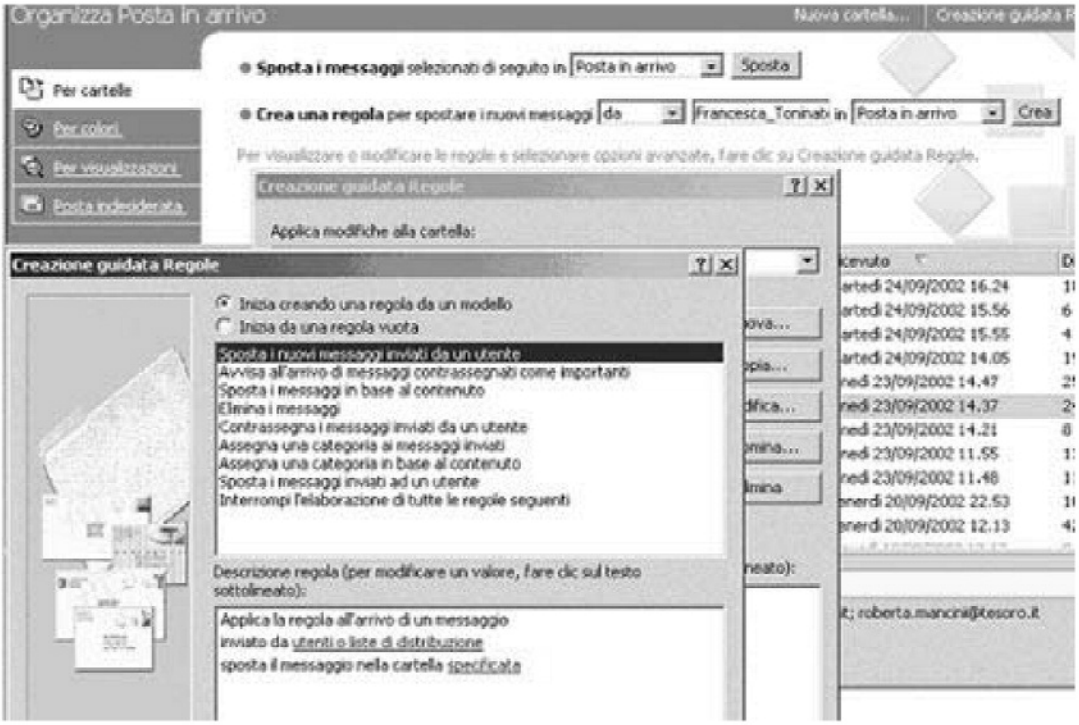

Figura 23: Creazione di una nuova regola

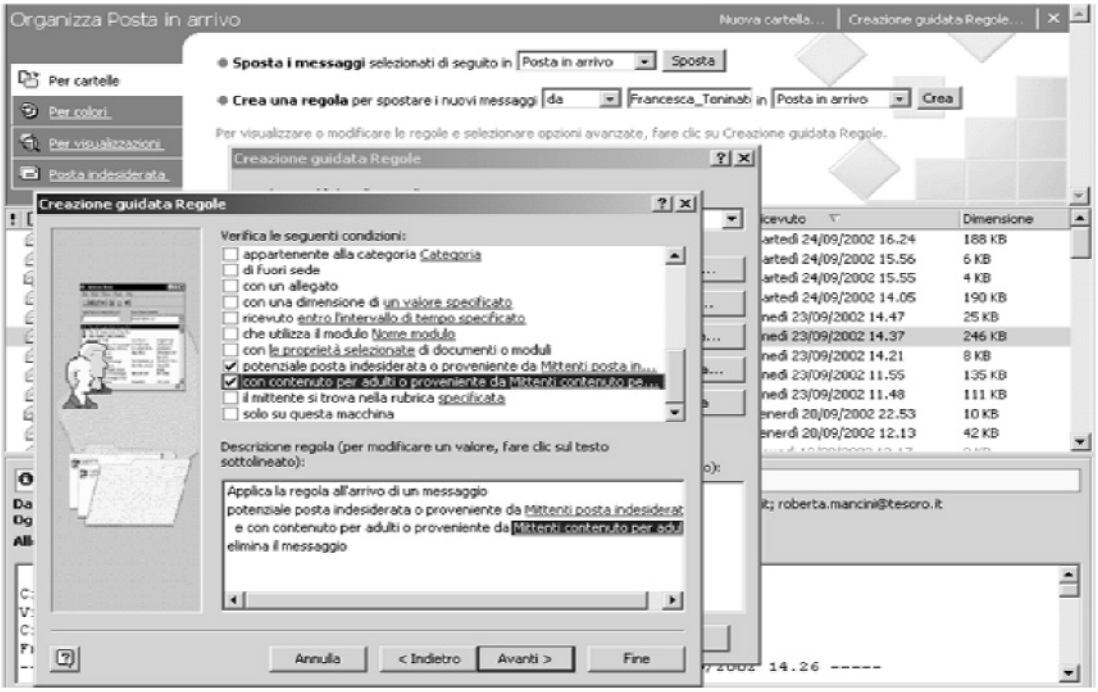

Figura 24: Impostazione delle condizioni

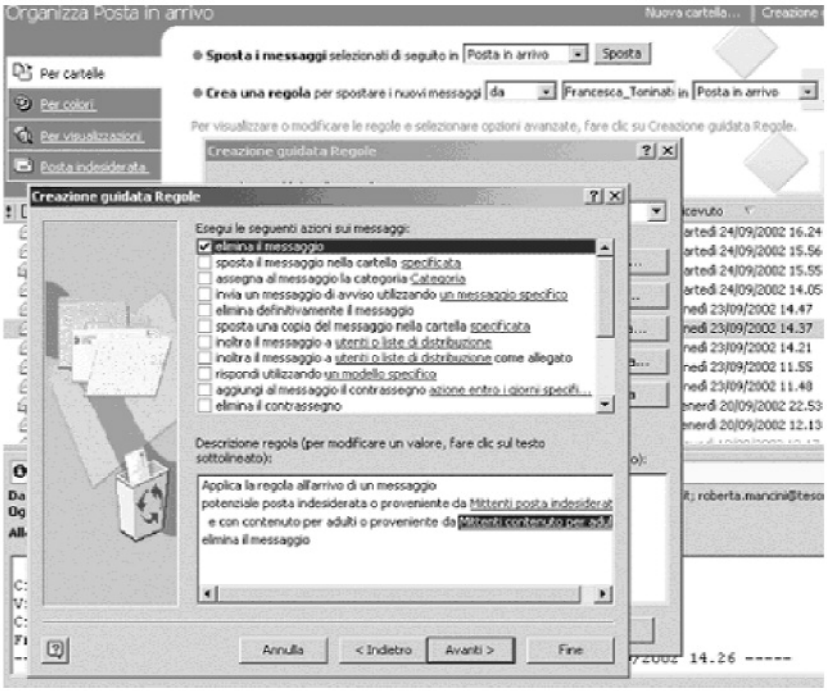

Figura 25: Selezione dell'azione

Selezionare «Inizia creando una regola da un modello» (è un modo facilitato di procedere), «Elimina messaggi» e cliccare «Avanti» (vedi ***Figura 23***). A questo punto occorre impostare delle condizioni. Le due condizioni selezionate richiedono di eliminare le e-mail il cui mittente è nella lista dei mittenti posta indesiderata o contenuto per adulti (vedi ***Figura 24***). Selezionando Avanti, si passa alla schermata successiva, che suggerisce il tipo di operazione. Qui, selezionare la voce «Elimina il messaggio» (vedi ***Figura 25***).

Selezionando Avanti, si arriva in una schermata in cui è possibile inserire delle eccezioni (ad esempio eliminare tutti i messaggi provenienti dal dominio paperopoli.it tranne quelli inviati da paperino@paperopoli.it).

Selezionando Avanti, si accede alla schermata in cui si assegna un nome alla regola (vedi ***Figura 26***). La creazione della regola è così terminata.

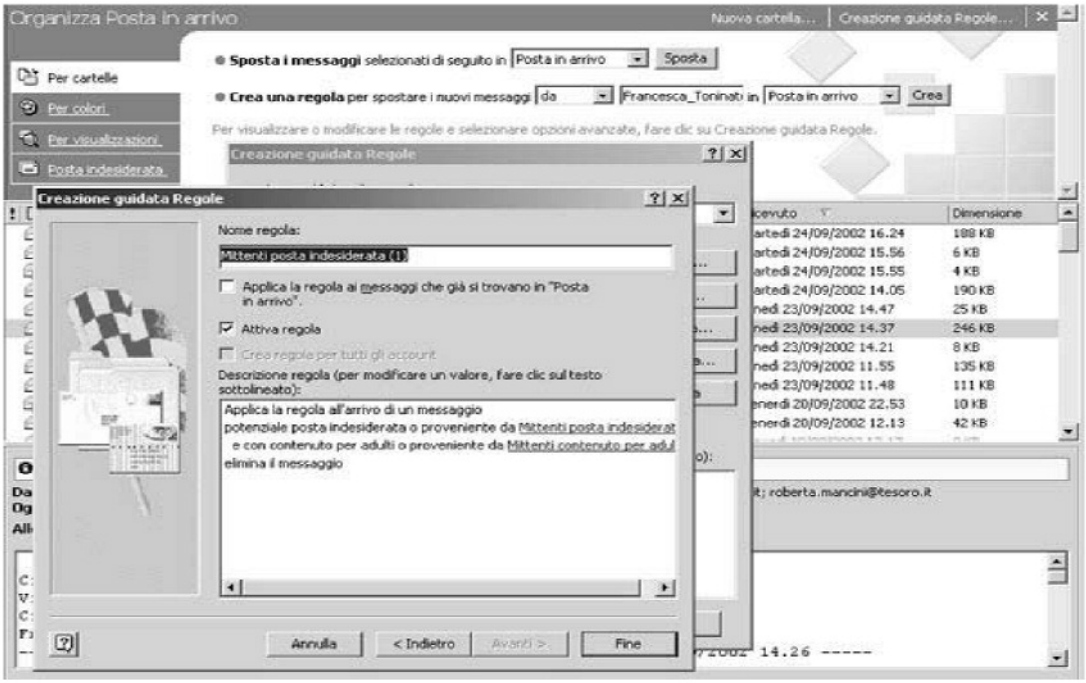

Figura 26: Nome della regola

13 Linux

Sono di seguito riportati alcuni esempi di configurazioni dei browser Konqueror 3.1.1 e Mozilla 1.4 e del client di posta KMail 1.5.1

13.1 Virus & dialers (la frode corre sul web)

I danni causati dai virus e dai dialer sono spesso agevolati dal fatto che l'utente utilizza il PC con pieno accesso a tutte le risorse del sistema, ovvero può installare programmi e accedere ai file importanti del sistema operativo in modalità scrittura (modifi-

care/cancellare). Il problema non è particolarmente grave nel caso di linux, perché, come tutti i sistemi Unix, le funzioni di amministratore di sistema (root) e di utente normale sono rigorosamente separate (i file di sistema importanti sono di proprietà dell'utente root, l'utente normale non vi ha accesso).

La raccomandazione è quella di lavorare, in particolare quando connessi ad internet (navigare, scaricare email ecc.), come utente generico, in questo modo eventuali danni, provocati da virus, saranno limitati ai file a cui l'utente ha il permesso di accesso; lavorare invece come utente privilegiato, ovvero come root, abbassa il livello di sicurezza intrinseca del vostro sistema e permette, potenzialmente, ai virus di causare danni seri quali il danneggiamento dei file dell'utente e/o dell'ambiente di lavoro, costituito dal sistema operativo e dagli applicativi installati sul sistema.

13.2 Configurazione dei cookie su Konqueror 3.1.1

Dal menu Impostazioni, selezionate la voce Configura Konqueror e poi l'icona Cookie, si aprirà la seguente finestra:

Figura 1 Impostazione dei cookie in Konqueror

Sotto l'etichetta Politica, potete stabilire la modalità con cui il browser gestirà i cookie (Accetta, Rifiuta, Chiedi conferma), la politica per ogni singolo dominio, creare una lista di siti attendibili, creare una lista di siti con restrizioni.

Il primo gruppo di opzioni si riferisce a impostazioni che si si applicano a tutti i cookie:

- Accetta solo cookie dal server che li ha originati: alcune pagine web cercano di impostare cookie da server diversi da quello da cui state visualizzando la pagina HTML. Ad esempio vi mostrano annunci pubblicitari che spesso appartengono a un altro server; questi annunci cercano di impostare un cookie con lo scopo di tracciare le pagine che visitate attraverso più siti web. Disabilitare questa opzione significa che solo i cookie provenienti dallo stesso web server, quello a cui vi siete esplicitamente collegati, saranno accettati.
- Accetta automaticamente i cookie di sessione: un uso comune dei cookie è quello di tracciare la vostra navigazione all'interno di un sito durante la sessione corrente; questi cookie vengono cancellati quando abbandonate la sessione di navigazione. Questa pratica può risultare molto utile, p.es., utilizzare il servizio di web mail senza il concetto di sessione, ci costringerebbe a reintrodurre utente e password per ogni messaggio email che desideriamo leggere. Abilitare questa opzione significa che i cookie di sessione sono sempre accettati, anche se avete scelto di non accettare altri tipi di cookie da quel sito web.
- Considera tutti i cookie come cookie di sessione: se questa opzione è abilitata, tutti i cookie vengono considerati di sessione, ovvero non vengono memorizzati quando abbandonate il sito web (la definizione abbandonare il sito web è ambigua, alcuni cookie sopravvivono ancora un pò dopo che avete lasciato il sito web).

La sezione politica predefinita vi permette di impostare un comportamento predefinito valido per tutti i siti web; le opzioni sono mutuamente esclusive:

- Chiedi conferma prima di accettare i cookie: se questa opzione è abilitata, ogni volta che un sito web chiede l'impostazione di un cookie ne sarete avvisati (Figura 2);
- Accetta i cookie come politica predefinita: se questa opzione è selezionata tutti i cookie saranno accettati senza avvisare;
- Rifiuta i cookie come politica predefinita: se questa opzione è impostata tutti i cookie saranno rifiutati senza avvisare.

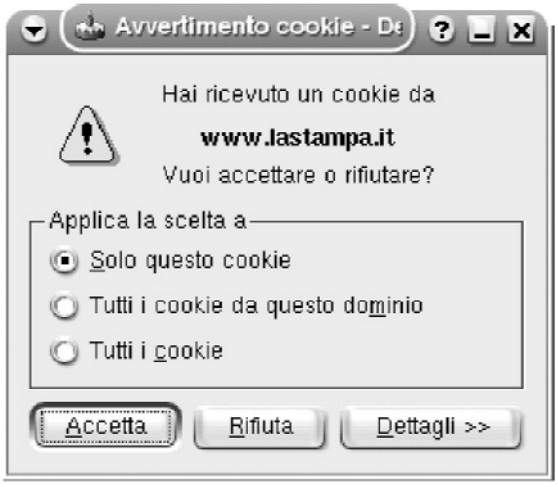

Figura 2 Richiesta di conferma cookie

Nella sezione Politiche specifiche per il dominio potete selezionare un dominio e personalizzare il comportamento del browser nei suoi confronti; avete inoltre a disposizione i bottoni Nuova, per impostare una nuova politica, Cambia, per modificare una politica, Cancella, per eliminare una politica, Elimina tutte, per eliminare tutte le politiche. Per i siti per cui sono state cancellate le politiche si applicheranno le impostazioni predefinite.

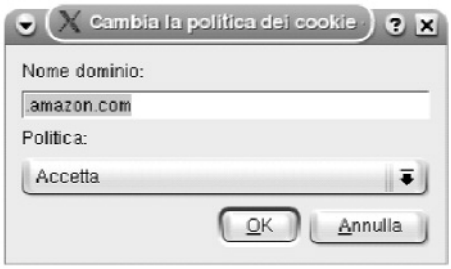

Figura 3 Politica cookie per singolo dominio

Sotto l'etichetta gestione potete visualizzare cosa hanno registrato sul vostro PC i cookie ed, eventualmente, eliminare tutte o parte delle informazioni:

Figura 4 visualizzazione delle informazioni di un cookie

13.3 Configurazione cookie su Mozilla 1.4

Dal menu Edit, selezionate la voce Preferences poi le categorie Privacy & Security e Cookies, si aprirà la seguente finestra:

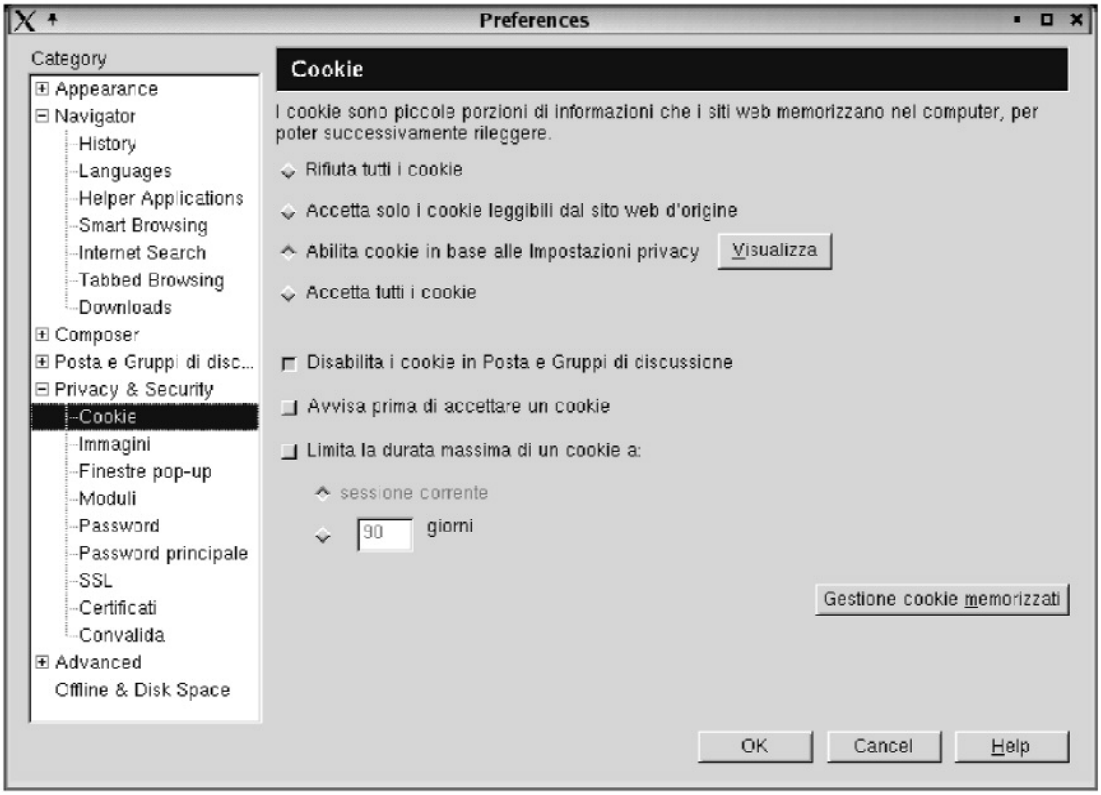

Figura 5 Impostazione dei cookie in Mozilla

Le opzioni proposte assumono i seguenti significati:

- Rifiuta tutti i cookie: in modo automatico il browser rifiuterà tutti i cookie.
- Accetta solo i cookie leggibili dal sito web di origine: produce il rifiuto dei cookie provenienti da riferimenti ad altri siti siti (p. es. Annunci pubblicitari).
- Abilita cookie in base alle impostazioni privacy: permette al vostro browser di agire in conformità alle policy di privacy che alcuni siti web pubblicano e al livello impostato.
- Accetta tutti i cookie: in modo automatico il browser accetterà tutti i cookie.
- Disabilita i cookie in posta e gruppi di discussione: si riferisce all'utilizzo di Mozilla anche per queste due applicazioni.

- Avvisa prima di accettare un cookie: avvisa l'utente ogni volta che un sito web tenta di impostare un cookie; le opzioni disponibili sono Accetta, Rifiuta, Mostra i dettagli (Figura 6).
- Limita la durata massima di un cookie :stabilisce la durata (la vita) del cookie.

Figura 6 Accettare un cookie

- Tramite il bottone Gestione cookie memorizzati potete accedere alla finestra di gestione cookie a livello di sito; in particolare sotto l'etichetta Stored Cookies sono visualizzati i siti a cui appartengono i cookie, il loro nome, il loro eventuale stato e le principali caratteristiche. Potete cancellare i cookie: tutti, tramite il bottone Remove all cookies, o singolarmente, tramite il bottone Remove cookie.

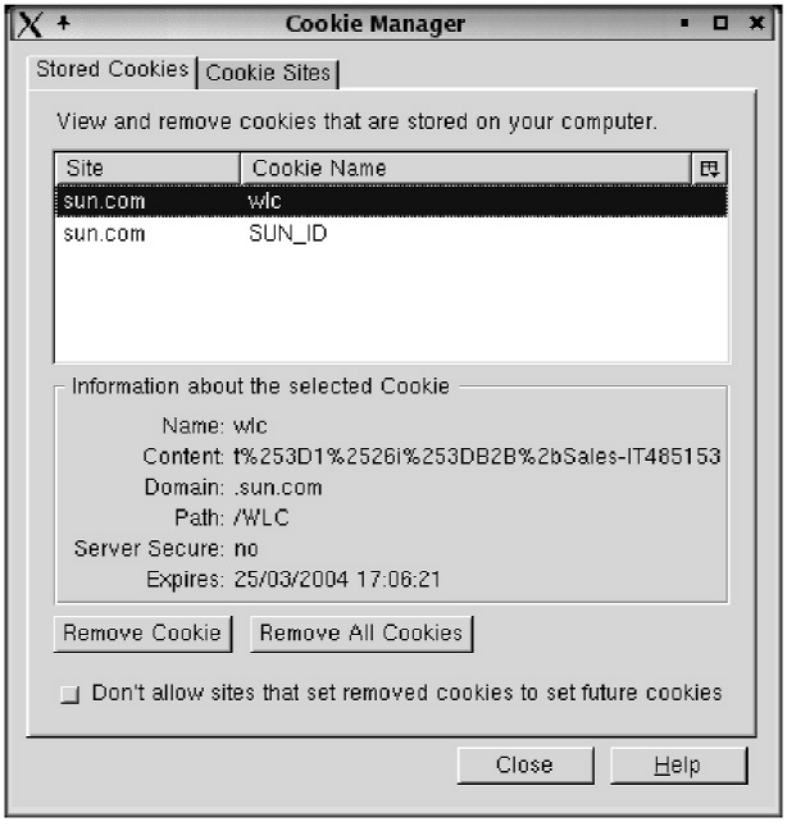

Figura 7 Amministrazione dei cookie

Se l'opzione Avvisa prima di accettare un cookie è selezionata, sarete avvisati ogni volta che un sito tenta di impostare un cookie, avrete, quindi, la possibilità di Accettare o di Rifiutare.

I siti elencati Sotto l'etichetta Cookie sites sono quelli per cui avete formulato una scelta (Accetta o Rifiuta) e potete eventualmente rimuoverli dalla lista.

Le opzioni possibili sono:

Remove site: rimuove dalla lista i siti selezionati;

Remove all sites: rimuove tutti i siti della lista.

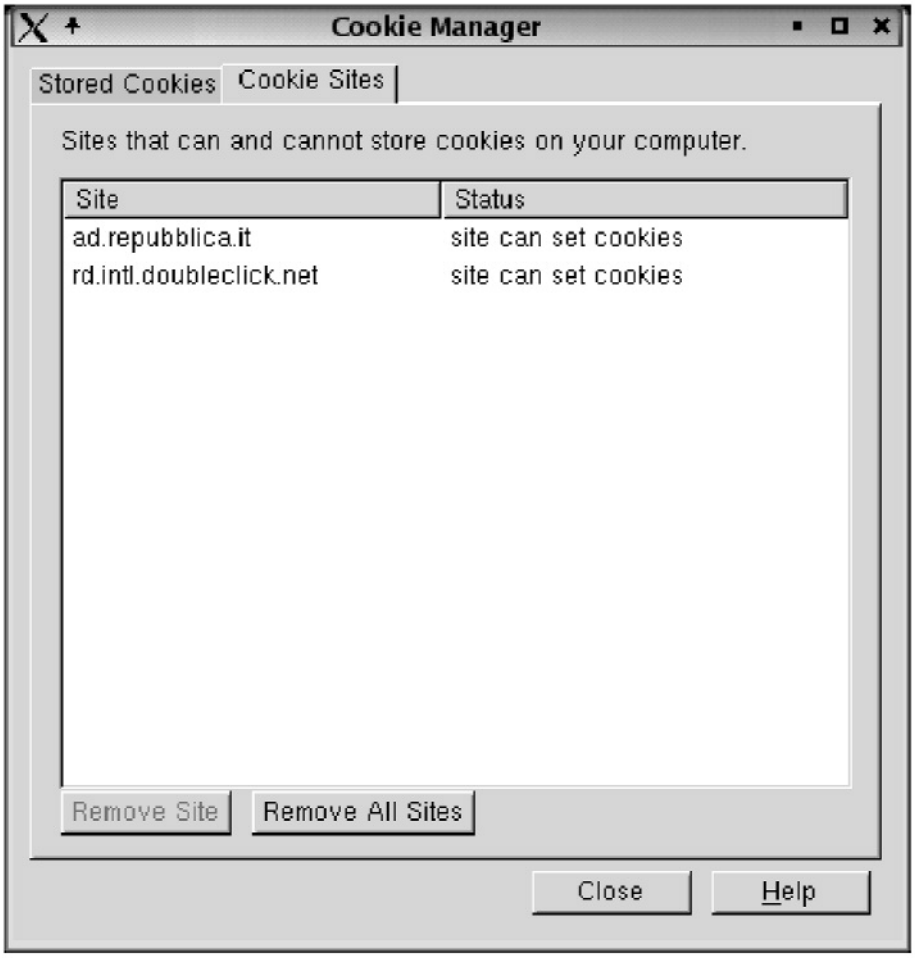

Figura 8 Cookie sites

Il Cookie manager non ricorderà più nulla dei siti rimossi dalla lista. Se l'opzione Avvisa prima di accettare un cookie è attiva, sarete nuovamente avvisati quando un sito web, eliminato dalla lista, richiederà il permesso di scrivere un cookie.

13.4 Configurazione su Konqueror 3.1.1 delle opzioni per la navigazione su siti certificati

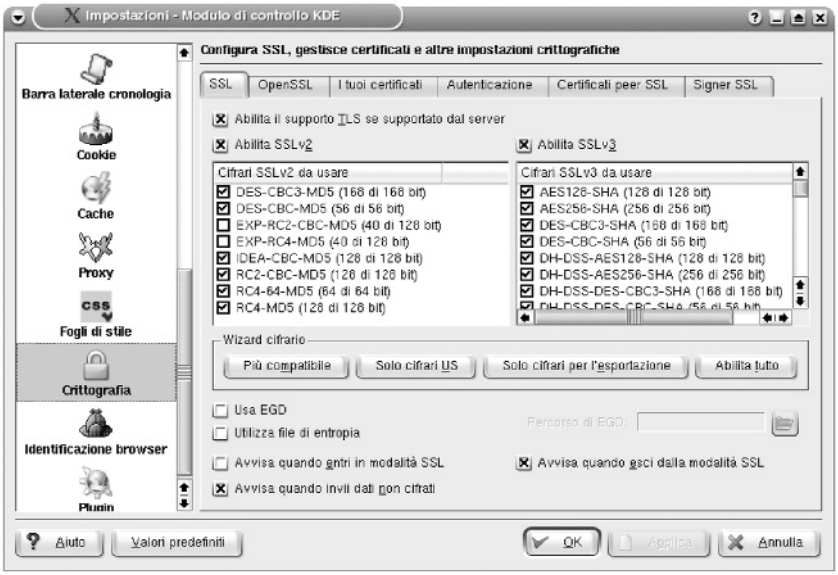

Figura 9 Crittografia

Sotto l'etichetta SSL trovate le opzioni relative alla scelta del protocollo di cifratura da utilizzare:

- Abilita SSL versione 2: specifica che si può scegliere di inviare e ricevere le informazioni protette tramite il protocollo standard per le connessioni protette SSL2 (Secure Sockets Layer Level 2); tutti i siti web protetti supportano questo protocollo.
- Abilita SSL versione 3: specifica che si può scegliere di inviare e ricevere le informazioni protette tramite il protocollo standard per le connessioni protette SSL3 (Secure Sockets Layer Level 3); non tutti i siti web protetti supportano questo protocollo.
- Abilita TLS: specifica che si può scegliere di inviare e ricevere le informazioni protette tramite il protocollo standard per le connessioni protette TLS (Transport Layer Security); non tutti i siti web protetti supportano questo protocollo.

Il resto delle opzioni permette di determinare il metodo di cifratura da utilizzare; cambiate queste impostazioni solo se avete esperienza sull'uso di questi protocolli. Potete inoltre impostare:

- Più compatibile per la compatibilità con la maggior parte dei server;
- Solo cifrari US per selezionare solo cifrari «forti» a 128 bit;
- Solo cifrari per l'esportazione per selezionare solo cifrari «deboli» a 56 bit;

Infine:

- Avvisa quando entri in modalità SSL: se selezionato, vi avvisa tutte le volte che state per entrare in un sito abilitato SSL
- Avvisa quando esci dalla modalità SSL: se selezionato, vi avvisa tutte le volte che state per uscire da un sito abilitato SSL
- Avvisa quando invii dati non cifrati: se selezionato, vi avvisa quando state per inviare dati con cifrati sul web (p.es. i dati di un form)

In generale vi consigliamo di lasciare inalterate le impostazione di default se non avete esperienza.

Sotto l'etichetta OpenSSL potete testare se il browser ha rilevato correttamente le librerie necessarie al buon funzionamento.

Sotto l'etichetta I tuoi certificati la lista mostra gli eventuali vostri certificati, da qui potete amministrarli.

The Authentication Tab

Non ancora documentato

Sotto l'etichetta Certificati per SSL potete visualizzare e amministrare i siti e i certificati che il browser conosce.

13.5 Configurazione di Mozilla1.4 delle opzioni per la navigazione su siti certificati

Dal menu Edit selezionate la voce Preferences poi le categorie Privacy & Security e SSL, si aprirà la seguente finestra:

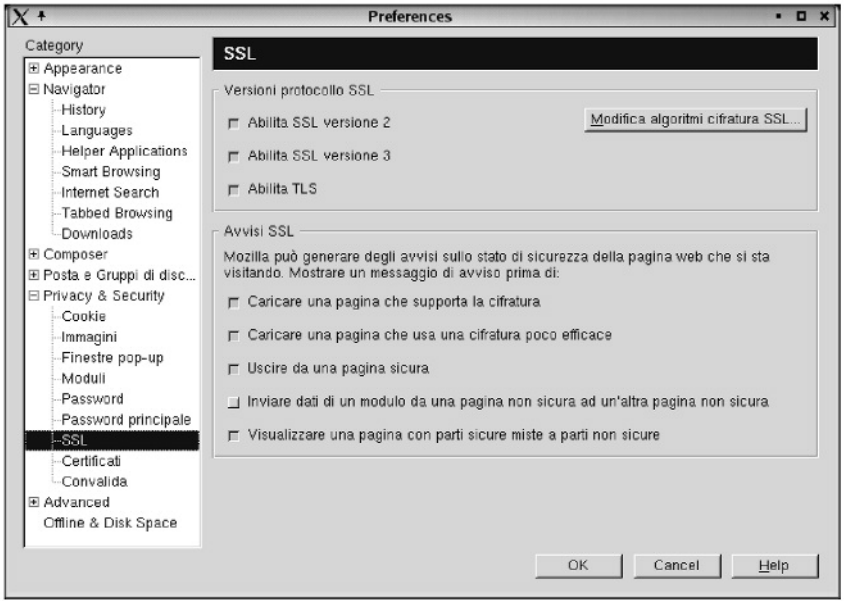

Figura 10 Impostazioni protocolli di sicurezza

I valori riportati sono quelli di default. Nella sezione Versioni protocollo SSL gli attributi hanno il seguente significato:

- AbilitaSSL versione 2: specifica che si può scegliere di inviare e ricevere le informazioni protette tramite il protocollo standard per le connessioni protette SSL2 (Secure Sockets Layer Level 2); tutti i siti web protetti supportano questo protocollo.
- Abilita SSL versione 3 specifica che si può scegliere di inviare e ricevere le informazioni protette tramite il protocollo standard per le connessioni protette SSL3 (Secure Sockets Layer Level 3); non tutti i siti web protetti supportano questo protocollo.

- Enable TLS specifica che si può scegliere di inviare e ricevere le informazioni protette tramite il protocollo standard per le connessioni protette TLS (Transport Layer Security); non tutti i siti web protetti supportano questo protocollo.

Quando il sito web che si sta visitando utilizza una connessione cifrata, l'utente viene avvisato per mezzo dell'icona che si trova nell'angolo basso a sinistra del browser (il lucchetto si chiude). Se la connessione non è cifrata il lucchetto si apre.

Ulteriori avvisi possono essere impostati nella sezione Avvisi SSL, in particolare:

- Caricare una pagina che supporta la cifratura: selezionate questa opzione se volete essere avvisati ogni qualvolta state per visualizzare una pagina che supporta la cifratura.
- Caricare una pagina che offre una cifratura poco efficace: selezionate questa opzione se volete essere avvisati ogni qualvolta state per visualizzare una pagina che supporta un livello di cifratura «debole» (chiavi a 40 bit).
- Uscire da una pagina sicura: selezionate questa opzione per essere avvisati quando lasciate una pagina che supporta la crittografia per una che non la supporta.
- Inviare dati di un modulo da una pagina non sicura ad un'altra pagina non sicura: selezionate questa opzione quando inviate dati su una connessione non sicura. In internet i dati inviati su una connessione non sicura possono essere facilmente intercettati da terzi utenti.
- Visualizzare una pagina con parti sicure miste a parti non sicure: selezionate questa opzione se volete essere avvisati quando visualizzate una pagina che comprende informazioni che non sono cifrate

Tramite la categoria Certificati si accede alla seguente finestra:

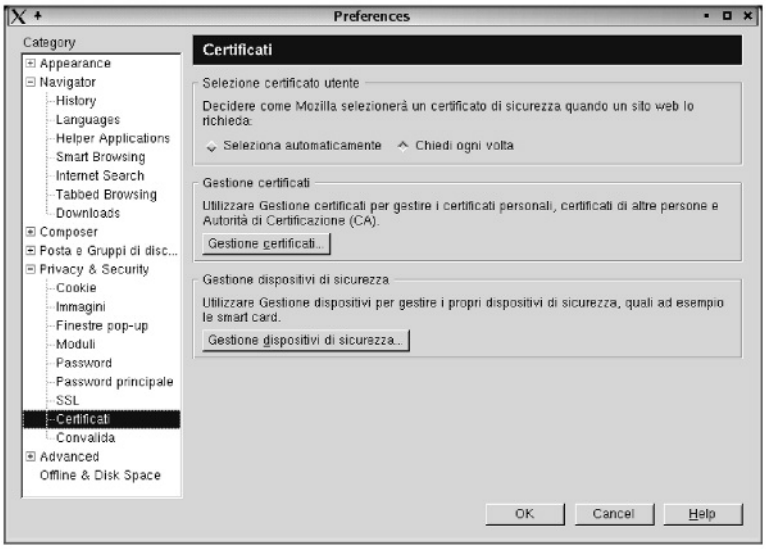

Figura 11 Certificati

Alcuni siti web richiedono la vostra identificazione per mezzo di un certificato. L'opzione che impostate nella sezione "Selezione certificato utente" determina la modalità con cui il browser individua il certificato da presentare al richiedente tra quelli che eventualmente avete su file.

- Seleziona automaticamente: selezionate questa opzione se desiderate che il browser selezioni il certificato senza chiedervelo. Questa è l'impostazione di default.
- Chiedi ogni volta: selezionate questa opzione se volete che il browser vi chieda il certificato ogni qualvolta un sito web lo richiede.

I certificati digitali sono gli equivalenti della carta d'identità, aiutano altre persone ad identificarci, ci aiutano ad identificare gli altri (altre persone, siti web, organizzazioni).

Per esaminare o configurare i certificati che avete su file, utilizzate il bottone Gestione certificati:

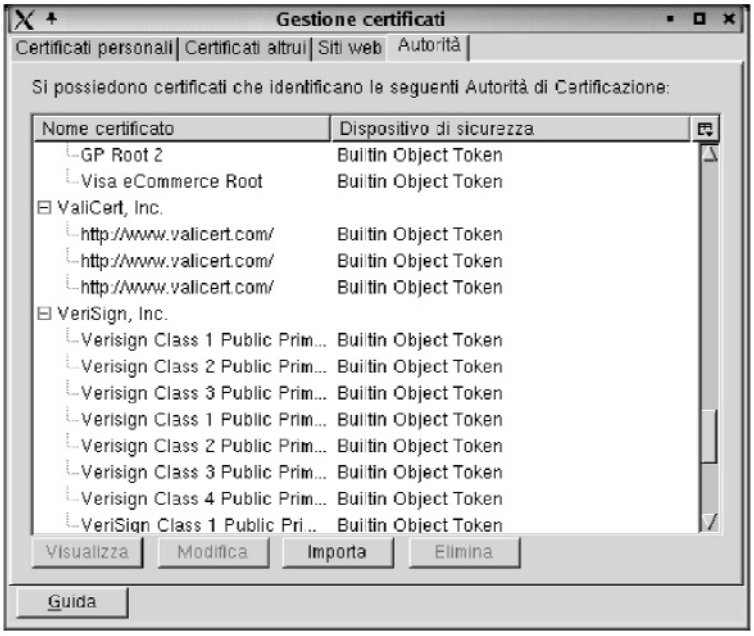

Figura 12 Gestione certificati

Una spiegazione dettagliata della gestione dei certificati esula dagli scopi della presente appendice.

Un dispositivo di sicurezza immagazzina i vostri certificati e può essere hardware e/o software, p.es. una smart card. Il browser che ha la sua sicurezza intrinseca software, può, tuttavia, utilizzare dispositivi addizionali quali p.es. la smart card. Per esaminare e/o configurare i dispositivi addizionali di sicurezza, utilizzate il bottone Gestione dispositivi di sicurezza. Una spiegazione dettagliata esula dagli scopi di questa appendice.

Tramite la categoria Convalida si accede alla seguente finestra:

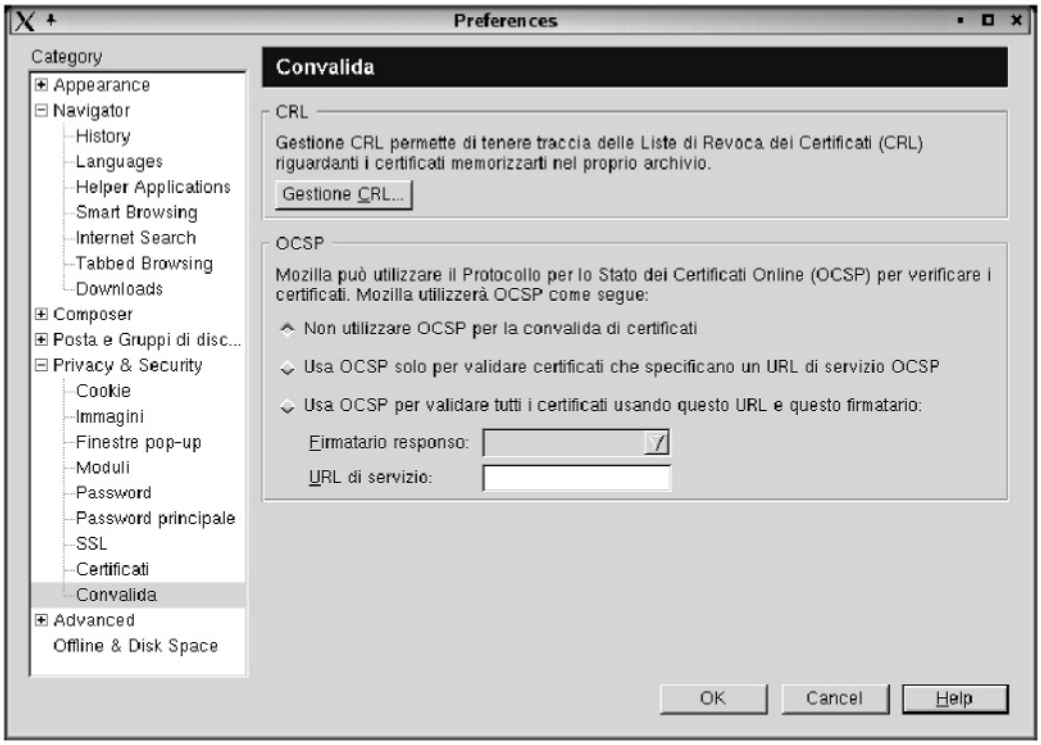

Figura 13 Convalida certificati

Questa sezione descrive come impostare le preferenze di validazione e come controllare la revoca dei certificati. Una lista dei certificati revocati (Certificate Revocation List) viene generata e firmata dall'autorità di certificazione; tale lista può essere scaricata e controllata al fine di verificare la validità dei certificati prima del loro eventuale utilizzo. Utilizzate il bottone Gestione CRL per accedere alla lista degli eventuali certificati revocati memorizzati nel proprio archivio.

Il protocollo on line OCSP (Online Certificate Status Protocol) rende possibile il controllo on line della validità del certificato ogni volta che viene utilizzato. Il processo prevede il controllo di una lista mantenuta aggiornata su uno specifico sito web; il vostro personal computer deve ovviamente essere connesso ad internet.

13.6 Gestioni filtri posta elettronica di KMail1.5.1

I filtri consistono in un modello di ricerca, le cui regole sono utilizzate come criterio per determinare se il filtro stesso debba essere applicato ad un dato messaggio, e in una lista di azioni, che descrivono cosa fare dei messaggi che corrispondono con il modello di ricerca.

Dal Menu Impostazioni, selezionate la voce Configura Filtri, si aprirà la seguente finestra:

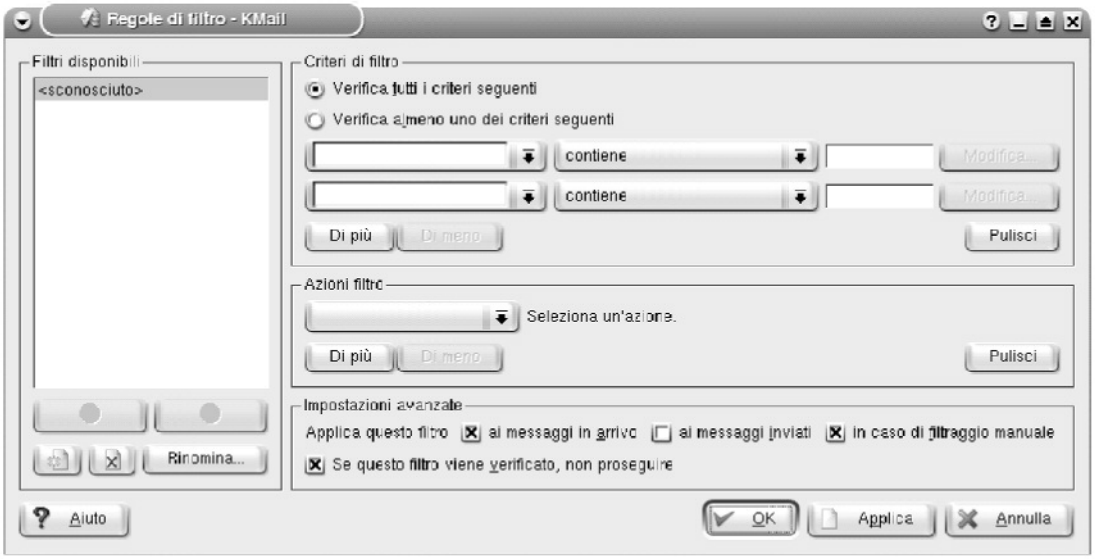

Figura 14 Configurazioni filtri sulla posta «scaricata»

Evidenziamo che i filtri descritti in questa sezione sono applicati dopo che i messaggi sono stati scaricati dal server di posta (POP3). La funzione di Aiuto di KMail vi permette di richiamare il relativo manuale (David Rugge traduzione di Luciano Montanaro) che descrive bene ed in lingua italiana la funzione dei filtri, riportiamo di seguito alcune parti.

I filtri sono valutati uno dopo l'altro, iniziando dal primo della lista dei filtri. Il primo corrispondente al messaggio in esame viene eseguito. Potete richiedere che anche i filtri successivi vengano applicati, ma il comportamento predefinito è di fermarsi dopo l'esecuzione del primo filtro.

Di solito i filtri sono applicati ai messaggi in arrivo, ma possono anche essere applicati ad un messaggio o ad un gruppo di messaggi. Per filtrare i messaggi in modo selettivo, selezionate i messaggi che volete filtrare ed usate la combinazione di tasti Ctrl+J o seleziona Messaggio-›Applica filtri. Questo applicherà tutti i filtri marcati per il filtraggio manuale nella finestra di dialogo relativa ai filtri ai messaggi selezionati.

Creazione rapida dei filtri

Ci sono due metodi per creare un filtro: il metodo rapido è di usare Strumenti-›Crea filtro.... Questo richiamerà una finestra di dialogo e presenterà un nuovo filtro che ha la prima regola del modello di ricerca e la prima azione (come ''sposta nella cartella'' predefiniti). Nella maggior parte dei casi, tutto quello che devi fare è scegliere in quale cartella il messaggio dovrà essere spostato. Ma, ovviamente, puoi modificare il filtro come preferisci.

La cosa interessante di questo metodo è che cercherà in tutti i modi di creare un filtro per le mailing list utilizzando un'intestazione che identifichi univocamente la lista. Se ci riesce, il supposto nome della lista viene presentato nella voce del menu Strumenti-›Crea filtro-›Filtra su ''Mailing-List ''....

Il secondo metodo consiste nella costruzione manuale del filtro da zero, richiamando la finestra di dialogo dei filtri e utilizzando Impostazioni-›Configura filtri. Ulteriori dettagli li potete trovare facendo clic sul bottone AIUTO.

Un'altra possibilità di Kmail è quella di applicare i filtri ai messaggi sul server, ovvero prima che siano scaricati sul vostro PC; dal Menu Impostazioni selezionate la voce Configura filtri POP, si aprirà la seguente finestra:

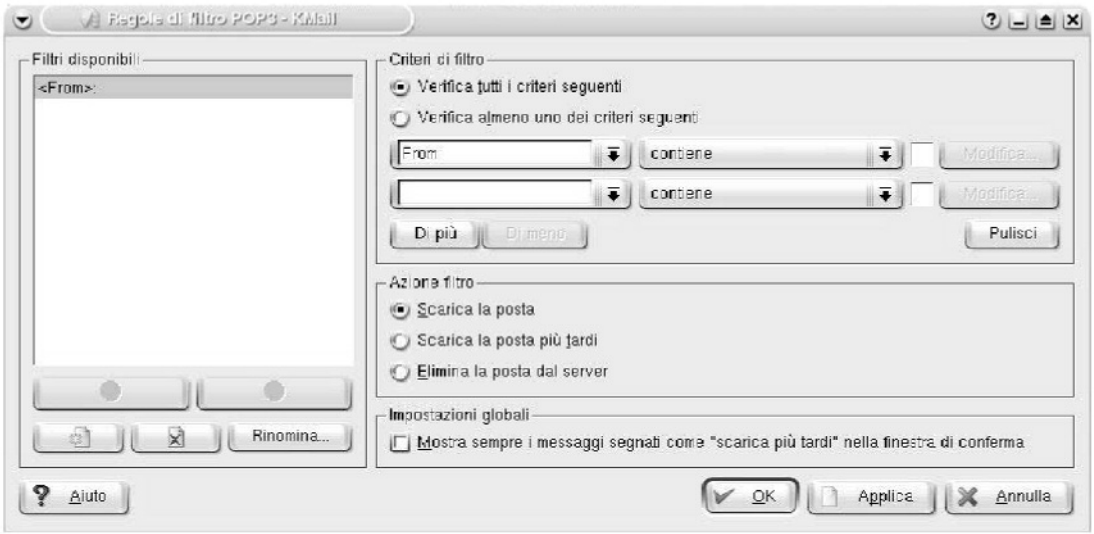

Figura 15 Filtri applicati ai messaggi sul server POP

Potete usare i filtri di download (o filtri POP) per filtrare i messaggi da un server POP, prima che siano scaricati completamente. Potete utilizzarli per impedire a KMail di scaricare messaggi enormi, (e risparmiare tempo), di spamming, con contenuti non adeguati ai minori.

Dalla finestra di dialogo dell'account POP potete abilitare il filtraggio in fase di download marcando la casella Filtra i messaggi se più grandi di. Una volta fatto ciò, potete specificare una dimensione soglia. I messaggi che superano la soglia verranno controllati utilizzando le regole da te definite. Se non corrispondono con nessuna regola di filtraggio, verranno mostrati in una finestra di conferma, e potrete decidere come procedere. La dimensione predefinita per il filtraggio è di 50.000 Byte. Questo è un buon valore, perché non aggiunge troppo carico alla connessione. Tutti i messaggi che vengono controllati da un filtro aumentano il traffico con il server della posta, perché l'intestazione è scaricata due volte. L'azione predefinita è Scarica messaggio per evitare la perdita di messaggi.

Attenzione

Fate attenzione con l'opzione Elimina la posta dal server, visto che non c'è modo di recuperare la posta cancellata dal server.

Per aggiungere regole di filtraggio si procede analogamente al filtraggio dei messaggi. Sul lato sinistro c'è la parte di gestione dei filtri esistenti; sul lato destro ci sono i controlli per la configurazione delle condizioni di attivazione del filtro attualmente selezionato. Usate il pulsante Nuovo per specificare un filtro. Usando Azioni del filtro, potete specificare che azioni eseguire quando un messaggio corrisponde alla regola di filtraggio. Le opzioni disponibili sono:

- Scarica posta: scaricherà i messaggi che corrispondono con la regola di filtraggio, come tutti i messaggi che non superano la dimensione di soglia.
- Scarica la posta più tardi: marcherà i messaggi per scaricarli più tardi. Ciò significa che i messaggi corrispondenti rimarranno sul server POP finché non sceglierai di scaricarli cambiando manualmente l'azione.
- Cancella la posta dal server: cancellerà i messaggi dal server senza scaricarli. Una volta che un messaggio è cancellato dal server, non c'è alcun modo di recuperarlo. State attenti, le regole potrebbero scattare per messaggi che vi interessano. Potete utilizzare questa opzione per cancellare i messaggi di spamming con contenuto non adeguato ai minori, ovvero i cosiddetti messaggi di posta «indesiderata».

L'opzione Mostra sempre in messaggi corrispondenti a «Scarica in seguito», nella finestra di conferma causerà l'apparizione di una finestra di dialogo di conferma durante il controllo della posta se almeno un messaggio era marcato come Scarica in seguito - anche se tutti i messaggi che superano la dimensione di soglia corrispondevano ad una regola. Questa opzione è utile nel caso che ci siano messaggi corrispondenti ad una regola e marcati Scarica in seguito, ma che non si ricevano messaggi di dimensione superiore alla soglia per un lungo periodo. Senza questa opzione, la finestra di conferma non si presenta mai, e non avrai occasione di ricevere i messaggi accodati cambiando a mano l'azione.

Per aggiungere regole di filtraggio si procede analogamente al filtraggio dei messaggi. Sul lato sinistro c'è la parte di gestione dei filtri esistenti. Sul lato destro ci sono i controlli per la configurazione delle condizioni di attivazione del filtro attualmente selezionato. Usate il pulsante Nuovo per specificare un filtro. Usate ''Azioni del filtro si'' per specificare che azioni eseguire quando un messaggio corrisponde alla regola di filtraggio. Ulteriori dettagli li potete ottenere facendo clic sul pulsante AIUTO.

14 Entourage

Sono di seguito riportati alcuni esempi di configurazione dei programmi Entourage (omologo di Outlook per Macintosh) e Microsoft Internet Explorer 5.2.x per Macintosh OS X. La versione per OS 9.x è la 5.0 e non sussistono differenze sostanziali. Le due applicazioni della Microsoft per Macintosh non verranno più supportate e saranno sostituite dal Browser Safari e dall'applicazione per la gestione della posta elettronica Mail prodotte direttamente da Apple. Mail è una delle poche applicazioni a includere i filtri di Bayes insieme con i consueti filtri boleani

Le impostazioni consigliate e le spiegazioni a livello teorico e pratico nelle appendici precedenti fornite per Internet Explorer sono le stesse; in Macintosh cambiano solamente le modalità di rappresentazione e quindi la reperibilità delle singole voci che risultano inserite in altri contesti.

14.1 Configurazione degli antivirus su Entourage

Microsoft ha rilasciato per la versione di Office 2001 e la successiva versione X l'applicazione Entourage, una sorta di replica di Outlook per il mondo Macintosh. In entrambe le versioni e i relativi sistemi operativi Macintosh OS 9.x e X 10.x.x non è necessario configurare le applicazioni di posta elettronica affinché effettuino scansioni

Figura 1 Una finestra di gestione di Entourage X

Questo perché la presenza di virus negli allegati dei messaggi non ha nessun effetto nei sistemi operativi di Macintosh (non vengono danneggiati). I programmi antivirus utilizzabili, Virex e Norton, effettuano il controllo sulla posta in arrivo e in uscita ma non forniscono nessun plug-in aggiuntivo.

14.2 Configurazione delle aree e dei cookie su Internet Explorer

Dal Menu Explorer (Mac OS X) selezionare Preferenze, quindi Protezione. Sotto l'etichetta Protezione è possibile configurare gli avvisi relativi alla sicurezza nella visualizzazione di una pagina web o nella compilazione e invio di un modulo.

Figura 2: Opzioni di protezione sul browser Internet Explorer

Sotto l'etichetta Aree di protezione è possibile: aggiungere o rimuovere un sito dall'area selezionata, inviare una notifica relativa a tutti i potenziali problemi di sicurezza riguardanti i siti Web appartenenti ad una zona selezionata, specificare le impostazioni personalizzate per la zona selezionata.

Figure 2 Aree di Protezione

La finestra Impostazioni Cookie elenca i cookie registrati sul disco rigido e il loro status. È possibile rimuovere il cookie selezionato dall'elenco e dal computer, visualizzarne le proprietà, disabilitarlo e scegliere alla sua ricezione la modalità di gestione desiderata.

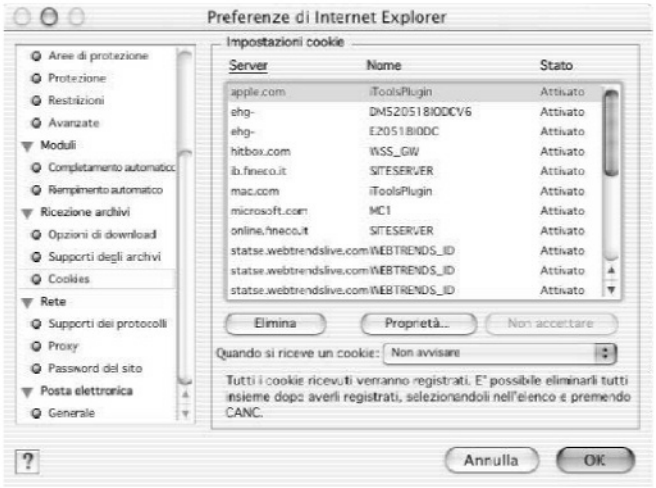

Figure 3 Impostazioni cookie

14.3 Configurazione degli ActiveX su Internet Explorer 5.x

I *controlli ActiveX* sono dei componenti che possono inserirsi nelle pagine Web (per essere visualizzati richiedono plug-in o client specifici come Internet Explorer).

La gestione dei controlli ActiveX e dei plug in si trova in Areee di Protezione › Impostazioni.

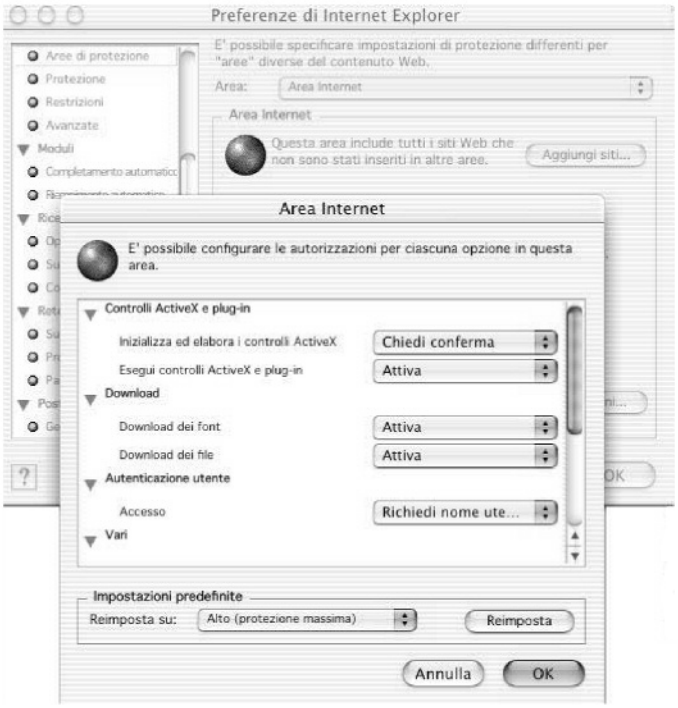

Figure 4 Gestione Controlli ActiveX e plug-in

14.4 Opzioni disponibili su Internet Explorer 5.x per le restrizioni sui contenuti

All'interno di Internet Explorer selezionare dal menu Explorer la voce Preferenze, quindi la sottovoce Restrizioni

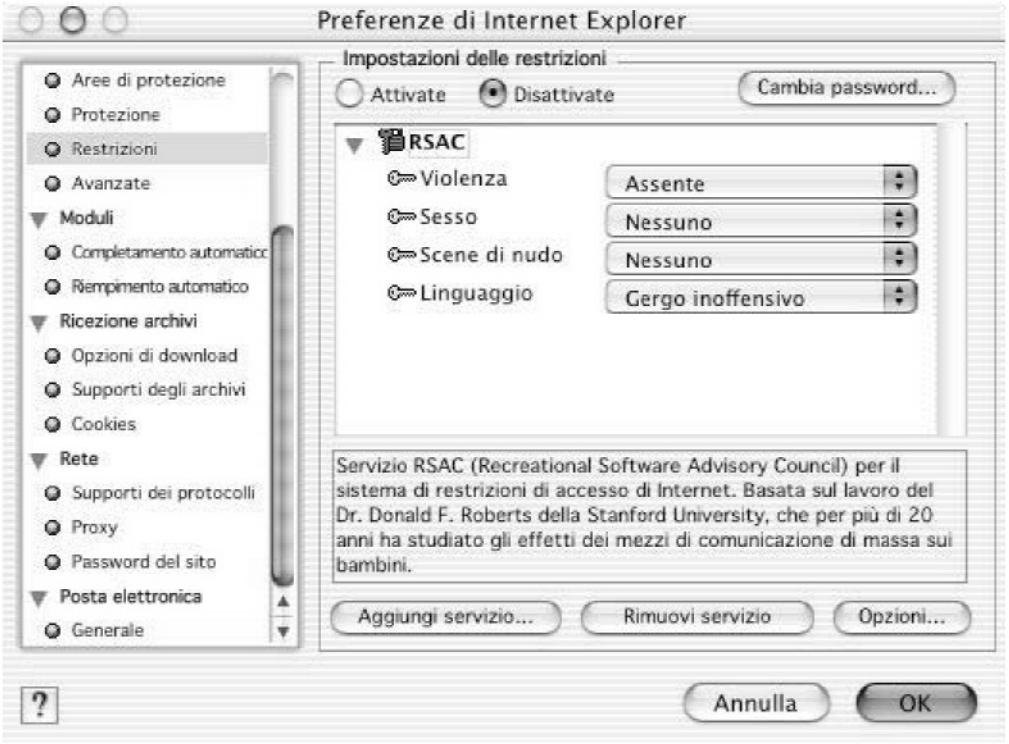

Figure 5 Impostazioni delle restrizioni

14.5 Posta elettronica: opzioni di protezione per posta indesiderata o per contenuto per adulti

Microsoft Entourage X e 2001 presenta il tradizionale filtraggio booleano e il filtraggio Junk Mail (posta Indesiderata, accessibile dal menu Tools›Junk Mail Filter), essenzialmente una piccola raccolta di filtri booleani e di regole a punti che funziona come singola unità nel normale filtraggio della posta del programma. La sensibilità del filtro viene controllata con un cursore.

14.6 Posta elettronica: Mail per OS X

L'applicazione che gira solo sotto il sistema OS X 10.x permette di filtrare i messaggi di posta indesiderata fin dal primo avvio senza nessuna configurazione. Il programma, che, come già detto, utilizza i filtri di Bayes insieme a quelli booleani, è facilissimo da «addestrare».

Dal Menu Mail si sceglie o si verifica che sia selezionata l'opzione Posta Indesiderata › Training; A partire da questo momento il programma provvede automaticamente a trasferire i messaggi di spam nella cartella omonima. Nel caso in cui alcuni messaggi non vengano riconosciuti e spostati, basta indicare, dopo averli selezionati, i messaggi come posta indesiderata, facendo clic sull'icona del pulsante. Nel caso di errore basta posizionarsi nella cartella Posta Indesiderata e selezionare i messaggi «desiderati» (Figura 6 prima icona in alto partendo da destra).

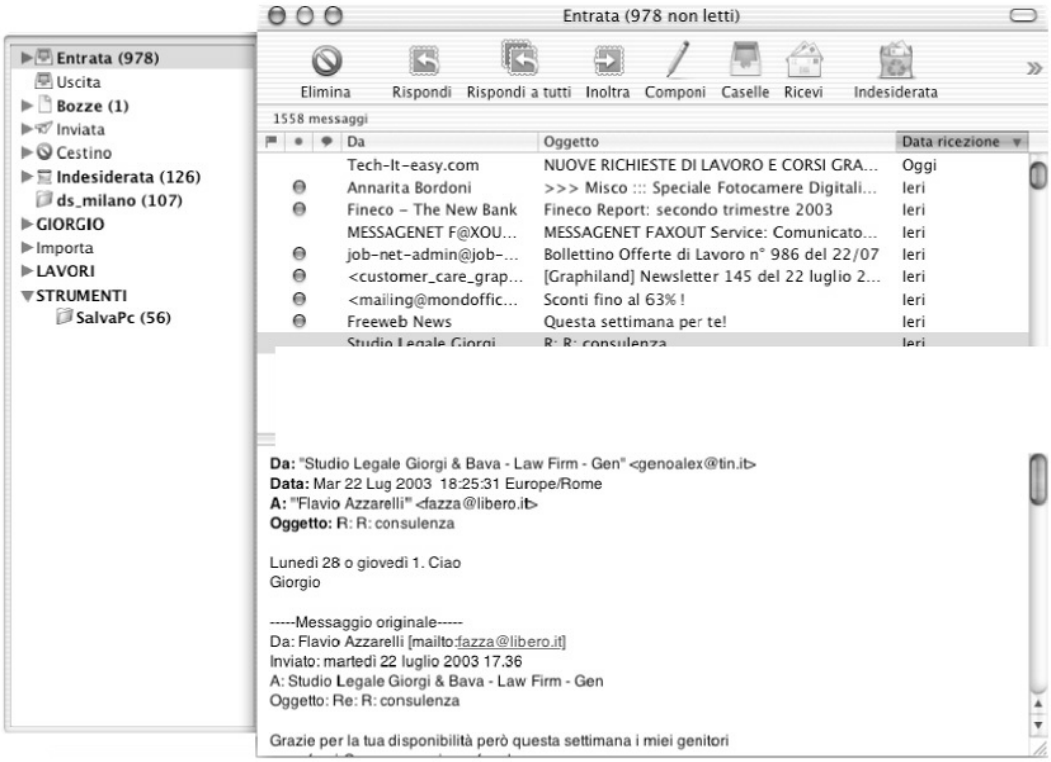

Figure 6 L'applicazione Mail per OS X 10.x

Questa semplicissima operazione permette al programma di autoistruirsi. L'utente in qualsiasi momento potrà decidere di automatizzare completamente l'operazione, selezionando dal Menu Mail›Posta Indesiderata›Automatico. Questa modalità sposta i messaggi sospetti nella casella Posta Indesiderata, utilizzando le informazioni apprese nella fase di Training.

14.7 Navigazione: Safari per OS X

Anche questa applicazione, distribuita gratuitamente sul sito di Appla, necessita di una versione OS X 10.2.x per funzionare. Al primo avvio, se sulla macchina è già installato Internet Explorer ne importa automaticamente i Favoriti. È open source e basato su Konqueror a sua volta un open source. Il programma non ha particolari problematiche di utilizzo. Tra le caratteristiche implementate prevede la presenza di una barra per la ricerca incorporata fornita da Google.

Figure 7 La schermata del browser Safari per MAC OS X 10.2.x

Le impostazioni relative alla sicurezza sono concentrate in un unico pannello; nella versione attuale del browser non sono previsti controlli sulle restrizioni e sulle aree di protezione.

Figure 8 Impostazioni Sicurezza su Safari

15 Windows ed applicativi vari (Opera 7.1 e Eudora (9))

15.1 Configurazione Riservatezza (Cookie)

Dal Menu File selezionate l'opzione Preferenze, poi la categoria Riservatezza, apparirà la seguente finestra:

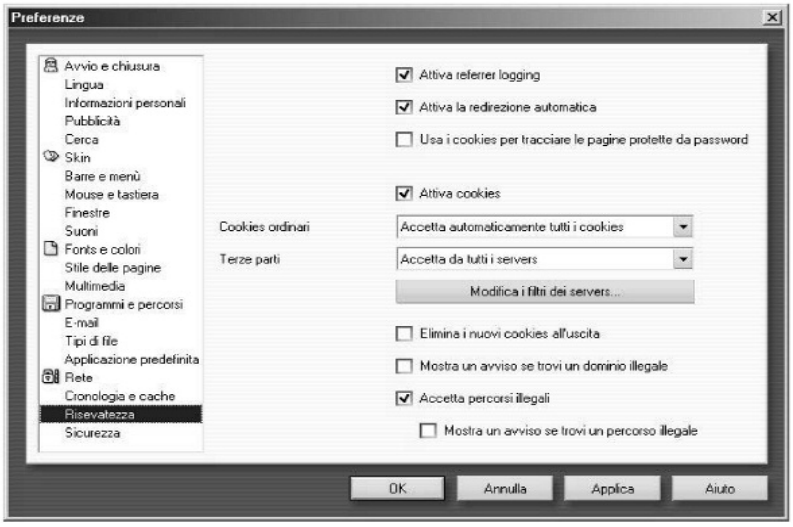

Figura 1 Gestione Riservatezza

Le opzioni configurabili per i cookie sono:

- Accetta automaticamente tutti i cookie: se selezionata, accetta incondizionatamente tutti i cookie;
- Non accettare i cookie: se selezionata, rifiuta incondizionatamente tutti i cookie;
- Accetta solo i cookie dai server selezionati: se selezionata crea una lista di server dai quali si possono accettare i cookie;
- Mostra i cookie ricevuti: se selezionata, mostra ogni cookie alla ricezione chiedendo se accettarlo o meno.

Le opzioni seguenti consentono di rifinire le scelte sopra elencate:

- Accetta da tutti i server: se selezionata, accetta i cookie impostati da qualunque server in qualunque dominio;
- Accetta solo i cookie per il server: se selezionata accetta solo i cookie impostati da un server per se stesso, rifiutando quelli destinati ad altri server nello stesso dominio e a terze parti (vedi sotto);
- Mostra i cookie di terze parti: se selezionata, visualizza i cookie provenienti da altri domini chiedendo se accettarli o meno;
- Non accettare cookie di terze parti: se selezionata, accetta tutti i cookie dallo stesso dominio, ma non quelli da altri domini.

Potete personalizzare la gestione dei cookie a seconda del sito dal quale provengono; ad esempio, si possono accettare tutti quelli inviati da sicuro.esempio.org e rifiutare

(9) Opera ed Eudora sono disponibili su vari Sistemi Operativi (Windows, Linux, MacIntosh)

tutti quelli di nonsicuro.esempio.org.; fate clic sul pulsante ''Modifica i filtri dei server'' e si aprirà la seguente finestra:

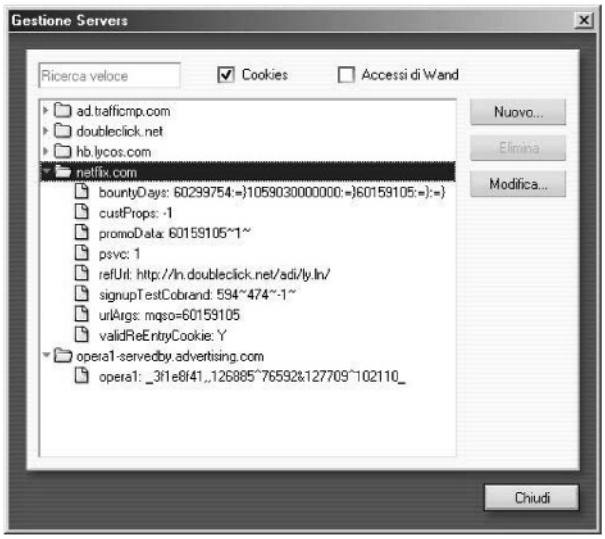

Figura 2 Personalizzazione gestione cookie per dominio

che mostra la lista dei domini; per mezzo dei bottoni Nuovo, Elimina, Modifica potete operare le personalizzazioni.

Figura 3 Gestione proprietà cookie di uno specifico server

Infine le opzioni:

- Elimina i nuovi cookie all'uscita: se selezionata Opera, rimuove tutti i cookies nuovi o modificati alla chiusura del programma;
- Mostra un avviso se trovi un dominio illegale:se selezionata Opera, vi avvisa qualora un server tenti di impostare un cookie il cui dominio non corrisponde col suo;
- Accetta percorsi illegali: se selezionata Opera, vi avvisa qualora un server tenti di impostare un cookie in cui sono presenti errori nei percorsi.

15.2 Configurazione sicurezza

Dal menu File selezionate l'opzione Preferenze, poi la categoria Sicurezza, si aprirà la seguente finestra:

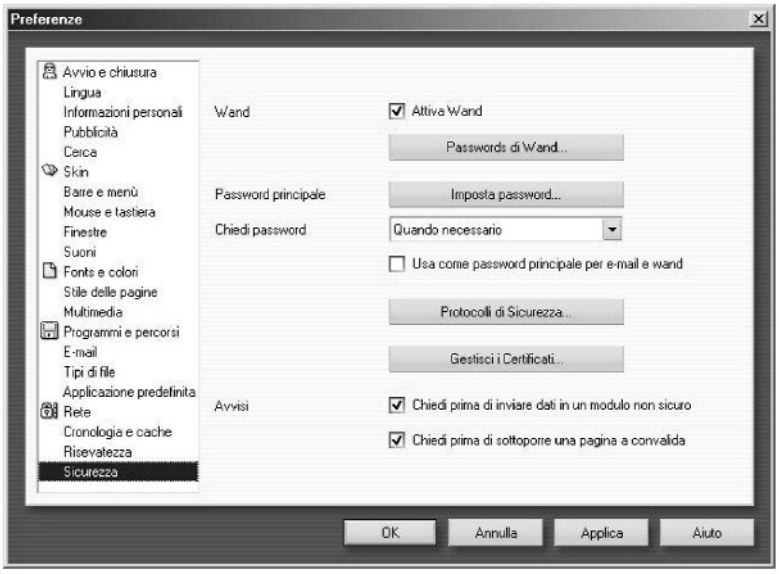

Figura 4 Gestione sicurezza

Potete attivare le opzioni che riguardano i certificati per mezzo dei bottoni:

- Protocolli di sicurezza che permette di definire i protocolli di sicurezza da utilizzare (Figura 5)
- Gestisci i certificati che permette di gestire i certificati (Figura 6)

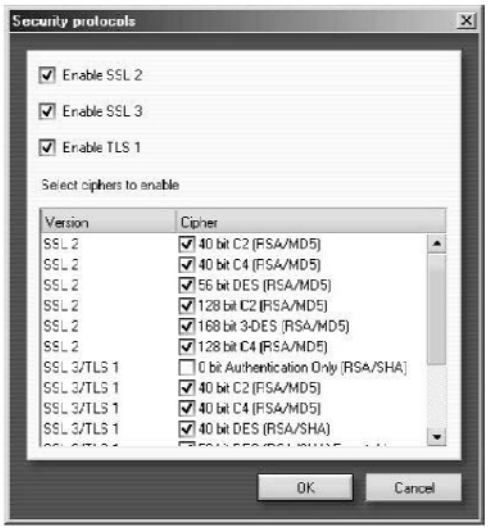

Figura 5 Gestioni protocolli di sicurezza

La spiegazione dei principali protocolli è già stata fornita in altra appendice.

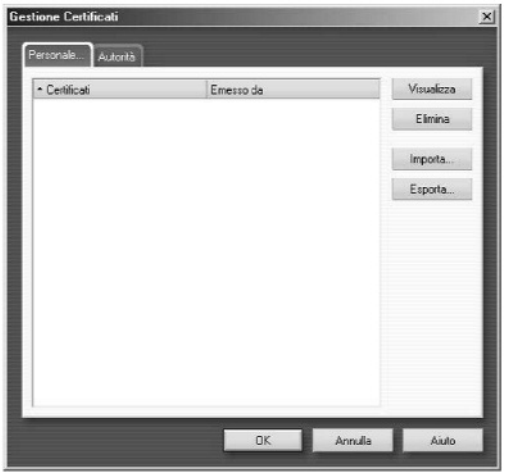

Figura 6 Gestione dei certificati personali

In particolare, sotto l'etichetta Personale trovate l'elenco dei certificati personali che sono impiegati per permettere la vostra identificazione su un sito Web. Questi certificati vengono solitamente installati la prima volta che vengono sottoscritti.

Sono disponibili le seguenti opzioni:

- Importa: importa i certificati esportati da un altro browser o scaricati da Internet;
- Esporta: esporta i certificati per consentire il loro uso in altri browser;
- Elimina: elimina i certificati di cui non vi fidate o che non vi servono;
- Visualizza: visualizza le informazioni relative al certificato selezionato.

Sotto l'etichetta Autorità vi sono le Autorità di Certificazione che servono a riconoscere i siti Web sicuri. La maggior parte dei certificati di Autorità che potrebbero servirvi è distribuita con Opera.

Figura 7 Gestione delle autorità di certificazione

Le opzioni che consentono l'importazione, l'esportazione e l'eliminazione sono essenzialmente le stesse già mostrate per i certificati personali (vedere sopra).

15.3 Eudora

Purtroppo le attuali versioni di eudora per i sistemi operativi Windows e MAC OS non consentono molte operazioni per il blocco dei messaggi di spamming.

Anche se il sistema dei filtri di Eudora è buono, purtroppo non ha incorporato sistemi per la gestione della posta indesiderata. È opportuno, comunque, configurare il programma affinché non esegua contenuti incorportai nei messaggi o negli attachment ricevuti in allegato.

15.4 Configurazione Viewing mail

Nella finestra Options, accessibile dal menu Tools, selezionare a sinistra la sottoscheda Viewing Mail e controllare che non compaia il segno di spunta in corrispondenza della voce ''Allow executables in HTML content''. Questa opzione impedisce che controlli quali Activex, Javascript, VB Script e Java Applets vengano eseguiti.

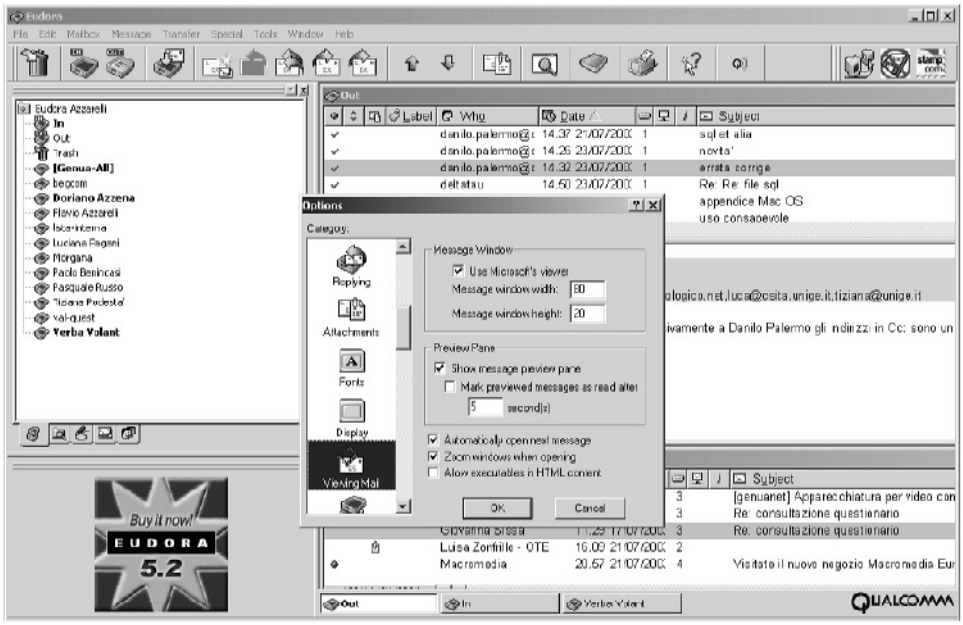

Figura 27 Option

15.5 Mood Watch

Potrebbe essere stato un ottimo metodo per riconoscere ed eliminare lo spamming. Si tratta di un sistema che, analizzando il contenuto del messaggio, individua parole da censurare e le segnala con un valore rappresentato graficamente da un numero di peperoncini da uno a tre. Purtroppo, questi graziosi peperoncini piccanti non possono essere

selezionati tramite il sistema di filtri in dotazione con Eudora, quindi non risultano utili. Inoltre utilizzano un dizionario in lingua inglese non in lingua italiano. Comunque, il sistema segnala sempre i messaggi contententi insulti e altre oscenità.

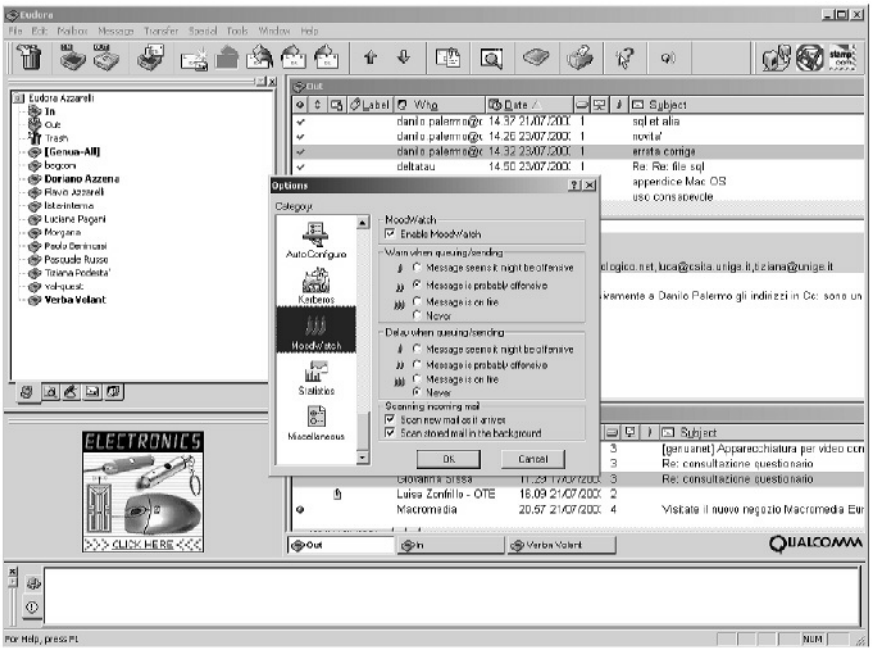

Figura 28 Mood watch