Liceo Scientifico e Classico “S. Trinchese”

Modulo 7 ecdl

Navigazione WEB e comunicazione

Sicurezza su internet

Giovedì 27 Gennaio 2011

ore 15.30

Prof Antonio Cazzato

SICUREZZA???

La sicurezza (dal latino "sine cura" senza preoccupazione) può essere definita come "la conoscenza che l'evoluzione di un sistema non produrrà stati indesiderati". **In termini semplici è: sapere che quello che faremo non provocherà dei danni**

"Il problema Internet"
dove nascono i problemi

Solo in Italia Internet rappresenta un bacino di utenza stimato sopra i 25 milioni di utenti

- **1° PROBLEMA: Il mondo digitale (Internet) si rispecchia nel mondo reale**
  - Anche i delinquenti usano Internet
- **2° PROBLEMA: su Internet non vi sono confini territoriali**
- **3° PROBLEMA: Stiamo utilizzando una tecnologia vecchia di 30 anni che non è nata per applicazioni per esempio di E-Commerce o per garantire sicurezza**

Alcuni problemi di sicurezza reali

- Intrusione dalla rete esterna
- furto o manomissione di dati
- sovraccarico di traffico anomalo
- furto di identità e codici segreti
- virus e malware
- spam

Effetti collaterali: perdita di produttività, downtime, consumo di banda, sempre maggiori costi per l'amministrazione

Alcuni problemi di sicurezza reali

Il siciliano Giuseppe Russo arrestato per essersi impossessato via Internet di mille numeri di carta di credito di cittadini USA ed averli adoperati	Grossa fetta di potenziali acquirenti si rifiuta di fare acquisti online a causa di problemi di sicurezza recentemente occorsi
Un canadese di 22 anni condannato a un anno di reclusione per aver violato molti computer dei governi USA e Canada	Stanotte, qualcuno di voi potrebbe…

Minacce nuove – automazione

- Microfurti diventano una fortuna
  - *Limare 1/1000 € da ogni transazione VISA!!!*
- Violazioni quasi senza tracce
  - *Il mio PC ha fatto improvvisamente reboot!!!*

Minacce nuove – distanza

- Non esiste distanza
  - Internet non ha confini naturali
- Ci preoccupano tutti i criminali del mondo
  - *Adolescente inglese viola sistema italiano*
- Leggi versus confini nazionali
  - *Denunce contro… Internet*
  - *Trovarsi in uno stato americano con scarsa cyberlaw e mancanza di estradizione*

Minacce nuove – tecniche diffuse

- Rapidità di propagazione delle tecnologie
  - *Hacker pubblica lo script del proprio attacco*
  - *Scaricato crack slovacco per texteditor*

- Diventare hacker spesso non richiede abilità
  - *Scaricato script per attacco di negazione del servizio (DoS)*
  - *Trovato su Internet parte del codice rubato di Win2K e verificato che…*

Il d.lgs 70/2003: la responsabilità dell'ISP

L'ISP non è responsabile per le informazioni trasmesse attraverso la rete per suo tramite, né della loro memorizzazione automatica temporanea al solo scopo di rendere più efficiente il re-inoltro, né della loro memorizzazione richiesta dal destinatario del servizio.

L'ISP non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite.

Il d.lgs 70/2003: la responsabilità dell'ISP

Però è tenuto ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio.

Sistemi di difesa

- Aggiornamento automatico del sistema operativo
- AntiVirus (sempre aggiornato, protegge da virus, malware, allegati di posta, attacchi durante la navigazione. Non protegge da intrusioni)
- Backdoor Cleaner o cleaner
- Malware scanner, antispyware (http://www.microsoft.com/security/malwareremove/default.mspx, http://www.lavasoftusa.com/software/adaware/)
- Firewall
- Chiusura porte e servizi pericolosi
- Certificati dei siti e sistemi di Crittografia (es. PgP)
- Antispam

Sicurezza della comunicazione

- La sicurezza di una comunicazione coinvolge una molteplicità di aspetti, tra cui assumono un ruolo centrale
  - gli attributi dell'informazione trasferita, tali da caratterizzare in primo luogo la *segretezza* dei messaggi scambiati tra le parti in comunicazione e ulteriormente le loro *integrità* , *autenticità* e *non ripudiabilità;*
  - i provvedimenti di *natura protettiva* atti ad assicurare il conseguimento degli obiettivi suddetti.

Componenti della sicurezza

- **Sono componenti di un messaggio sicuro**
  - la *segretezza*, secondo la quale il messaggio emesso deve essere di significatività informativa per il solo destinatario desiderato, mentre deve essere inintellegibile per tutti gli altri utenti; è ottenuta tramite la cifratura del testo in chiaro e la decifratura del testo cifrato;
  - l'*autenticità*, secondo la quale il ricevente ha garanzia circa l'identità dell'emittente e nei confronti di eventuali impostori;

Componenti della sicurezza

- l'*integrità*, secondo la quale il messaggio perviene al ricevente esattamente nella stessa forma con cui è stato emesso; nel trasferimento non si devono essere verificate variazioni accidentali o maliziose.
- la *non-ripudiabilità*, secondo la quale un ricevente è in grado di dimostrare che un messaggio ricevuto perviene da uno specifico emittente e quest'ultimo non deve essere in grado di negare l'invio del messaggio.

Scopo della crittografia

- La segretezza (confidenzialità) di un messaggio è conseguibile con la *crittografia*, e cioè con la scienza che ha come scopi
  - la trasformazione di un messaggio da un *testo in chiaro* (plaintext) a un *testo cifrato* (ciphertext);
  - la trasformazione in senso contrario,

  in modo da rendere il messaggio sicuro e immune da attacchi accidentali o malintenzionati.

Scopo della crittografia

- La trasformazione di un testo in chiaro in uno cifrato è chiamato *cifratura* e rende il messaggio non intellegibile a persone non autorizzate; tale trasformazione è ottenibile con un *algoritmo di cifratura* .
- La trasformazione inversa è chiamata *decifratura* e consente di passare da un testo intenzionalmente non intellegibile ad uno significativo in termini informativi; tale trasformazione è ottenibile con un *algoritmo di decifratura* .

Scopo della crittografia

- Un *cifrario* è la combinazione di un algoritmo di cifratura e del corrispondente algoritmo di decifratura.
- Un cifrario opera in funzione di una *chiave*.
- Una chiave è un'informazione segreta senza la quale è impossibile (o molto difficile) risalire al testo in chiaro dal testo cifrato.
- Gli algoritmi crittografici sono classificati in
  - metodi a *cifrario simmetrico*;
  - metodi a *cifrario asimmetrico*.

Crittografia a cifrario simmetrico

- Nella crittografia a cifrario simmetrico, la stessa chiave *segreta* è utilizzata, in modo condiviso, dall'emittente per la cifratura e dal ricevente per la decifratura su entrambe le direzioni di trasferimento.

…ma la distribuzione delle chiavi può diventare un'operazione organizzativamente complessa.

Crittografia a cifrario asimmetrico

- Nella crittografia a cifrario asimmetrico sono usate due chiavi: una *pubblica* e l'altra *privata* tra loro correlate;
- la chiave pubblica è usata dall'emittente per *cifrare* il messaggio;
- la chiave privata è usata dal ricevente per *decifrare* il messaggio.
- La chiave pubblica è di dominio pubblico (pur essendo specifica di un ricevente), mentre quella privata è nota solo al ricevente.

Crittografia a cifrario asimmetrico

Un messaggio viene quindi cifrato con la chiave pubblica del destinatario e quest'ultimo è l'unico che potrà leggerlo con la propria chiave privata.

Firma digitale

- Le componenti della sicurezza di un messaggio possono essere ottenute attraverso un metodo chiamato *firma digitale*.
- La firma digitale può essere utilizzata
  - sull'intero messaggio;
  - su un suo estratto (digest).

Firma digitale

- Una firma digitale
  - è l'equivalente elettronico di una firma convenzionale;
  - garantisce l'integrità, l'autenticazione e la non-ripudiabilità;
  - fa uso della crittografia asimmetrica;

Firma digitale

- è funzione anche del messaggio da firmare (può essere duplicata e non c'è distinzione tra quella originale e la copia)

- è separata dal messaggio firmato; quindi il mittente spedisce due messaggi: uno che contiene il documento, l'altro che contiene la firma.

- Per accettare un messaggio firmato digitalmente, il destinatario deve utilizzare un algoritmo di *verifica*, che esamina il messaggio e la firma.

Crittografia

In particolare, la maggior parte dei siti di e-commerce odierni utilizzano livelli di crittografia elevati quali, ad esempio:

- Secure Sockets Layer (SSL).
- Secure Electronic Transaction (SET).

SSL

- SSL (Secure Sockets Layer) è un protocollo progettato dalla Netscape Communications Corporation.

- Questo protocollo utilizza la crittografia per fornire sicurezza nelle comunicazioni su Internet e consentono alle applicazioni client/server di comunicare in modo tale da prevenire il 'tampering' (manomissione) dei dati, la falsificazione e l'intercettazione.

Scopo di SSL

Il protocollo SSL provvede alla sicurezza del collegamento garantendo:

- Autenticazione: l'identità nelle connessioni può essere autenticata usando la crittografia asimmetrica, ovvero a chiave pubblica (RSA, DSS, EL-Gamal). Così ogni client comunica in sicurezza con il corretto server, prevenendo ogni interposizione. È' prevista la certificazione del server e, opzionalmente, quella del client.
- Confidenzialità nella trasmissione dei dati: la crittografia è usata dopo un *handshake* (accordo) iniziale per definire una chiave segreta di sessione. In seguito, per crittografare i dati è usata la crittografia simmetrica (AES,3DES, RC4, ecc.).
- Affidabilità: il livello di trasporto include un controllo dell'integrità del messaggio basato su un apposito MAC (Message Authentication Code) che utilizza funzioni hash sicure (MD5, SHA, RIPEMP-160, ecc). In tal modo si verifica che i dati spediti tra client e server non siano stati alterati durante la trasmissione.

Fasi di SSL

SSL richiede di alcune fasi basilari:

- Negoziazione tra le parti dell‘algoritmo da utilizzare.
- Scambio di chiavi segrete tramite cifratura a chiave pubblica e identificazione tramite l'utilizzo di certificati.
- Cifratura del traffico tra le parti a chiave (segreta) simmetrica.

SSL - HTTPS

- **I protocolli di sicurezza risiedono sotto protocolli applicativi quali HTTP, SMTP e NNTP e sopra il protocollo di trasporto TCP.**
- **SSL può essere utilizzato per aggiungere sicurezza a qualsiasi protocollo che utilizza TCP, ma il suo utilizzo più comune avviene nel protocollo HTTPS.**
- **Il protocollo HTTPS viene utilizzato per aggiungere sicurezza alle pagine del WWW in modo tale da rendere possibili applicazioni quali il commercio elettronico.**
- **Il protocollo SSL utilizza metodi di cifratura a chiave pubblica e utilizza certificati a chiave pubblica per verificare l'identità delle parti coinvolte.**

HTTPS

- L'abbinamento SSL al normale HTTP permette di ottenere un nuovo protocollo: l‘HTTPS.

  Questi garantisce l'invio delle informazioni personali sottoforma di pacchetti criptati. In questo modo, la trasmissione delle informazioni avviene in maniera sicura, prevenendo intrusioni, manomissioni e falsificazioni dei messaggi da parte di terzi. Il protocollo HTTPS garantisce quindi tanto la trasmissione confidenziale dei dati, quanto la loro integrità.

- Ad oggi è sicuramente il sistema più usato, in quanto può essere supportato dai principali browser (Internet Explorer e seguenti, Netscape Navigator ecc.) e non necessita di alcun software specifico o password. Le pagine protette da questo protocollo sono facilmente riconoscibili, in quanto la scritta "https" precede l'indirizzo del sito protetto e le sue pagine vengono contrassegnate da un lucchetto, visualizzabile nella parte inferiore del proprio browser.

HTTPS

- L'HTTPS è un URI (Uniform Resource Identifier) sintatticamente identico allo schema http:// ma con la differenza che gli accessi vengono effettuati sulla porta 443 e che tra il protocollo TCP e HTTP si interpone un livello di crittografia/autenticazione.
- In pratica viene creato un canale di comunicazione criptato tra il client e il server attraverso lo scambio di certificati; una volta stabilito questo canale al suo interno viene utilizzato il protocollo HTTP per la comunicazione.
- Questo tipo di comunicazione garantisce che solamente il client e il server siano in grado di conoscere il contenuto della comunicazione.
- Questo sistema fu progettato dalla Netscape Communications Corporation che si occupa delle autenticazioni e delle comunicazioni crittografate ed è largamente usato nel World Wide Web per situazioni che richiedono particolari esigenze in ambito di sicurezza come per esempio il pagamento di transazioni online. In questo caso SSL garantisce la cifratura dei dati trasmessi e ricevuti su internet.

HTTPS

- Questo protocollo assicura una buona protezione contro attacchi del tipo man in the middle (l'attaccante è in grado di leggere, inserire o modificare a piacere, messaggi tra due parti senza che nessuna delle due sia in grado di sapere se il collegamento sia stato compromesso).
- Per impostare un web server in modo che accetti connessioni di tipo https, l'amministratore deve creare un certificato digitale ovvero un documento elettronico che associa l'identità di una persona ad una chiave pubblica. Questi certificati devono essere rilasciati da un certificate authority o comunque da un sistema che accerta la validità dello stesso in modo da definire la vera identità del possessore (i browser web sono creati in modo da poter verificare la loro validità).
- In particolari situazioni (come per esempio nel caso di aziende con una rete intranet privata) è possibile avere un proprio certificato digitale che si può rilasciare ai propri utenti.
- Questa tecnologia quindi può essere usata anche per permettere un accesso limitato ad un web server. L'amministratore spesso crea dei certificati per ogni utente che vengono caricati nei loro browser contententi informazioni come il relativo nome e indirizzo e-mail in modo tale da permettere al server di riconoscere l'utente nel momento in cui quest'ultimo tenti di riconnettersi senza immettere nome utente e/o password.

SET

- Secure Electronic Transaction (SET) è un protocollo standard per rendere sicure le transazioni con carta di credito su reti insicure e, in particolare, Internet. SET è stato sviluppato da Visa e MasterCard (con il coinvolgimento di altre aziende come GTE, IBM, Microsoft e Netscape) a partire dal 1996.
- Il protocollo impiega un algoritmo di oscuramento che, in effetti, sostituisce con un certificato il numero di carta di credito dell'utente durante le transazioni commerciali. Ciò consente agli imprenditori di accreditare i fondi dalle carte di credito degli utenti senza avere la necessità di conoscere il numero della carta.
- SET fa uso di tecniche crittografiche come i certificati digitali e la crittografia a chiave pubblica per consentire alle parti di identificarsi reciprocamente e scambiare informazioni con sicurezza.

SET

Essenzialmente, SET mette a disposizione tre servizi:

- fornisce un canale di comunicazione sicuro, condiviso da tutte le entità coinvolte nella transazione;
- fornisce fiducia, grazie all'uso di certificati digitali;
- assicura la privacy perchè le informazioni sono a disposizione delle entità in gioco, soltanto dove e quando è necessario.

Altri problemi

- Inizialmente il trasferimento dei dati tra il sito di e-commerce e il cliente avveniva in chiaro. Questo costituiva un possibile problema di sicurezza, soprattutto quando c'era un pagamento con carta di credito.

- Con l'avvento del SSL questo rischio è stato ridotto, ma sono poi comparsi altri problemi quale il Phishing e la comparsa di virus troiani che cercano di rubare informazioni utilizzabili per finalità losche.

Phishing

- Il phishing ("spillaggio (di dati sensibili)", in italiano) è una attività illegale che sfrutta una tecnica di ingegneria sociale (studio del comportamento individuale di una persona al fine di carpire informazioni), ed è utilizzata per ottenere l'accesso a informazioni personali o riservate con la finalità del furto di identità mediante l'utilizzo delle comunicazioni elettroniche, soprattutto messaggi di posta elettronica fasulli o messaggi istantanei, ma anche contatti telefonici.

- Grazie a questi messaggi, l'utente è ingannato e portato a rivelare dati personali, come numero di conto corrente, numero di carta di credito, codici di identificazione, ecc.

Metodologia di attacco

Il processo standard delle metodologie di attacco di spillaggio può riassumersi nelle seguenti fasi:

- l'utente malintenzionato (phisher) spedisce al malcapitato ed ignaro utente un messaggio email che simula, nella grafica e nel contenuto, quello di una istituzione nota al destinatario (per esempio la sua banca, il suo provider web, un sito di aste online a cui è iscritto).
- l'email contiene quasi sempre avvisi di particolari situazioni o problemi verificatesi con il proprio conto corrente/account (ad esempio un addebito enorme, la scadenza dell'account ecc.).
- l'email invita il destinatario a seguire un link, presente nel messaggio, per evitare l'addebito e/o per regolarizzare la sua posizione con l'ente o la società di cui il messaggio simula la grafica e l'impostazione.
- il link fornito, tuttavia, non porta in realtà al sito web ufficiale, ma ad una copia fittizia apparentemente simile al sito ufficiale, situata su un server controllato dal phisher, allo scopo di richiedere ed ottenere dal destinatario dati personali particolari, normalmente con la scusa di una conferma o la necessità di effettuare una autenticazione al sistema; queste informazioni vengono memorizzate dal server gestito dal phisher e quindi finiscono nelle mani del malintenzionato.
- il phisher utilizza questi dati per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

Difesa

- Banche, istituzioni o internet provider non fanno mai richiesta dei dati personali a mezzo di una e-mail. In caso di richiesta di dati personali, numeri di conto, password o carta di credito,è buona norma, prima di cancellare, inoltrarne una copia alle autorità competenti e avvisare la banca o gli altri interessati, in modo che possano prendere ulteriori disposizioni contro il sito falso e informare i propri utenti.
- Per eventuali comunicazioni, i soggetti sopra citati possono utilizzare un account istituzionale accessibile solo dal loro sito, ma non la e-mail personale del cittadino.
- Una preoccupazione frequente degli utenti che subiscono lo spillaggio è capire come ha fatto il malintenzionato a sapere che hanno un conto presso la banca o servizio online indicato nel messaggio-esca. Normalmente, il phisher non conosce se la sua vittima ha un account presso il servizio preso di mira dalla sua azione: si limita ad inviare lo stesso messaggio-esca a un numero molto elevato di indirizzi di email, facendo spamming, nella speranza di raggiungere per caso qualche utente che ha effettivamente un account presso il servizio citato.
- Pertanto non è necessaria alcuna azione difensiva a parte il riconoscimento e la cancellazione dell'email che contiene il tentativo di spillaggio.

Pharming

- Pharming è una tecnica di cracking, utilizzata per ottenere l'accesso ad informazioni personali e riservate, con varie finalità. Grazie a questa tecnica, l'utente è ingannato e portato a rivelare inconsapevolmente a sconosciuti i propri dati sensibili, come numero di conto corrente, nome utente, password, numero di carta di credito etc.

- L'obiettivo finale del pharming è il medesimo del phishing, ovvero indirizzare una vittima verso un server web "clone" appositamente attrezzato per carpire i dati personali della vittima.

Metodologia di attacco

- L'utente malintenzionato opera, con l'ausilio di programmi trojan o tramite altro accesso diretto, una variazione nel personal computer della vittima.
- Ad esempio, nei sistemi basati sul sistema operativo Windows, modificando il file "hosts" presente nella directory "C:\windows\system32\drivers\etc". Qui possono essere inseriti o modificati gli abbinamenti tra il dominio interessato (p.es. paypal.com) e l'indirizzo IP corrispondente a quel dominio. In questo modo la vittima che ha il file hosts modificato, pur digitando il corretto indirizzo URL nel proprio browser, verrà reindirizzata verso un server appositamente predisposto per carpire le informazioni.
- Un altro metodo consiste nel modificare direttamente nel registro di sistema i server DNS predefiniti. In questo modo l'utente, senza rendersene conto, non utilizzerà più i DNS del proprio Internet Service Provider, bensì quelli del cracker, dove ovviamente alcuni abbinamenti fra dominio e indirizzo IP saranno stati alterati.

Difesa

- **Per difendersi dal pharming non esistono ancora dei programmi specifici se non i firewall che tentano di impedire l'accesso al proprio PC da parte di utenti esterni e programmi antivirus che bloccano l'esecuzione di codice malevolo.**
- **Se il sito a cui ci si collega è un sito sicuro prima dell'accesso verrà mostrato un certificato digitale emesso da una autorità di certificazione conosciuta, che riporterà i dati esatti del sito. Questo certificato andrebbe quantomeno letto e non frettolosamente accettato.**
- **In alcuni casi il sito sicuro non appare come tale solo perché la banca utilizza una tecnica di incapsulamento delle pagine a frames che non mostra il lucchetto nell'apposita casellina del browser né l'indirizzo in modalità https.**

Difesa

- Un primo controllo per difendersi dai siti di spillaggio, è quello di visualizzare l'icona, a forma di lucchetto in tutti i browser, che segnala che sì è stabilita una connessione sicura (p. es. SSL). Tale connessione garantisce la riservatezza dei dati, mentre la loro integrità e l'autenticazione della controparte avvengono solo in presenza della firma digitale, che è opzionale e non segnalata.
- Comunque, una connessione SSL potrebbe essere stabilita con certificati non veritieri, tramite una coppia di chiave pubblica e privata valide, note a chi vuole fare phishing, ma che non sono quelle effettive del sito. Ad esempio, il certificato riporta che il sito it.wikipedia.org utilizza una chiave pubblica, che in realtà è quella del phisher. I browser piuttosto che l'utente interessato dovrebbero collegarsi al sito di una certification authority per controllare: la banca dati mostra le chiavi pubbliche e un'identificativo del possessore, come l'indirizzo IP o l'indirizzo del sito.
- Alcuni siti hanno una barra antiphishing specifica che controlla l'autenticità di ogni pagina scaricata dal sito, ad esempio tramite la firma digitale.

Keylogging

- Un'altra tecnica di spillaggio consiste nell'inserimento di applicativi di keylogging. In questo caso, i link possono rimandare al sito originale, non necessariamente a un'imitazione.
- Un keylogger è uno strumento in grado di intercettare tutto ciò che un utente digita sulla tastiera del proprio computer.
- Esistono vari tipi di keylogger:
  - hardware: vengono collegati al cavo di comunicazione tra la tastiera ed il computer o all'interno della tastiera;
  - software: programmi che controllano e salvano la sequenza di tasti che viene digitata da un utente.
- I keylogger hardware sono molto efficaci in quanto la loro installazione è molto semplice e il sistema non è in grado di accorgersi della loro presenza.

Keylogging

- I keylogger software sono semplici programmi che rimangono in esecuzione captando ogni tasto che viene digitato e poi, in alcuni casi, trasmettono tali informazioni ad un computer remoto. Spesso questi sono trasportati ed installati nel computer da worm o trojan ricevuti tramite Internet ed hanno in genere lo scopo di intercettare password e numeri di carte di credito ed inviarle tramite posta elettronica al creatore degli stessi.
- Sempre a livello software, un programma di Keylogging può sovrapporsi fra il browser e il mondo internet. In questo caso intercetta le password, comunque vengano inserite nel proprio PC. La password viene catturata indipendentemente dalla periferica di input (tastiera, mouse, microfono): sia che l'utente la digiti da tastiera, sia che l'abbia salvata in un file di testo prima di collegarsi a Internet, e poi si limiti a fare copia/incolla, in modo da evitarne la digitazione, sia questa venga inserita da un programma di dettatura vocale.
- Anche in caso di connessione sicura (cifrata), se sul computer è presente un keylogger che invia le password in remoto, tali password potranno essere utilizzate dalla persona che le riceve.

Anti-spillaggio

- Esistono, inoltre, programmi specifici come la barra anti-spillaggio di Netcraft e anche liste nere, blacklist (funzionano come un controllo degli accessi a una certa risorsa, usufruibile da tutti, ad eccezione delle entità identificate nella lista), che consentono di avvisare l'utente quando visita un sito probabilmente non autentico.
- Gli utenti di Microsoft Outlook / Outlook Express possono proteggersi anche attraverso il programma gratuito Delphish, un toolbar inserito nel MS Outlook / MS Outlook Express con il quale si possono trovare i link sospetti in un'email.
- Questi programmi e i più comuni browser non si avvalgono di whitelist (nega a priori a tutti gli utenti l'utilizzo del servizio, ad eccezione di coloro che sono inclusi nella lista) contenenti gli indirizzi logici e IP delle pagine di autenticazione di tutti gli istituti di credito, che sarebbe un filtro anti-spillaggio sicuramente utile.

Conclusioni

- Con la diffusione dell'e-commerce si sono diffuse truffe sempre più insidiose che colpiscono principalmente gli acquirenti. I principali casi sono:
  - Vendita di prodotti da siti civetta: al ricevimento del pagamento non viene inviata la merce, o viene solamente simulata la spedizione. Problema presente anche su ebay.
  - Realizzazione di siti clonati con la finalità di rubare informazioni quali il codice della carta di credito.
  - Aziende fallimentari che accumulano ordini, e introiti, senza la possibilità di evaderli.
- La normativa italiana prevede che tutti i siti di commercio elettronico riportino nella home page la partita IVA e la denominazione dell'azienda. I siti più importanti di e-commerce hanno un certificato digitale che consente di verificare l'autenticità del sito visitato.
- Il principale problema dal punto di vista delle aziende è la gestione degli ordini simulati, dove vengono indicate generalità false o non corrette per l'invio dei prodotti. Per ridurre il problema molte aziende accettano solamente pagamenti anticipati.

Bibliografia

- http://it.wikipedia.org/wiki/Commercio_elettronico
- http://it.wikipedia.org/wiki/HTTPS
- http://it.wikipedia.org/wiki/Secure_Sockets_Layer
- http://it.wikipedia.org/wiki/Secure_Electronic_Transaction
- http://it.wikipedia.org/wiki/Phishing
- http://it.wikipedia.org/wiki/Pharming
- http://toolbar.netcraft.com/
- http://www.delphish.com/
- http://www.dsi.unifi.it/~boreale/DIDATTICA/SICUREZZA/ /ReadSR.pdf