

Come proteggersi dagli attacchi in Rete? **Alcuni consigli su come difendersi**

Internet, grazie alla sua capillare diffusione e al suo ampio utilizzo, offre infinite opportunità di business ad aziende e consumatori, rendendo disponibili le informazioni in modo semplice ed immediato, ma rappresenta anche un potente veicolo in mano ai pirati informatici per sferrare attacchi a chiunque.

Oggi, la fruibilità di informazioni va di pari passo con la disponibilità di strumenti di hacking (strumenti volti ad agevolare le attività dei pirati informatici), al punto che anche una persona inesperta può improvvisarsi hacker.

Diciamo “improvvisarsi” per sottolineare la differenza tra un hacker alle prime armi, come questo, e un vero hacker.

Un hacker esperto, cioè un “vero hacker”, non si ferma all’ uso di strumenti facilmente scaricabili da Internet ma va ben oltre. Sulla base dell’ esperienza acquisita nel tempo sui Sistemi Operativi e di Rete, l’ hacker esperto si spinge al punto di sviluppare lui stesso gli strumenti che userà per sferrare i suoi attacchi.

Internet negli ultimi mesi è diventato molto più pericoloso per gli utenti, a causa di svariati attacchi che utilizzano il Web per lanciarsi e diffondersi nell’intera rete di computer esistenti. Alcuni nuovi exploit che in particolare sfruttano le vulnerabilità dei browser Web, compresi gli attacchi avvenuti a cavallo tra giugno e luglio 2004, evidenziano le sofisticate tecniche che gli hacker hanno sviluppato per prendersi gioco o falsificare i siti Web e come i codici maligni riescano con facilità a sottrarre nomi utente, password e altre informazioni importanti (phishing).

Gli hacker sfruttano le vulnerabilità dei browser Web per introdurre contenuti fasulli, come ad esempio dei moduli falsi per l’inserimento dei dati della propria carta di credito, sfruttando i frame di un sito sicuro. Gli utenti visitano quello che ritengono essere un sito sicuro, come una banca online o un sito di e-commerce e, mentre apparentemente il sito che visitano *sembra* essere attendibile, si tratta in realtà di una contraffazione, rendendo così gli utenti vulnerabili agli hacker che operano ‘dietro le quinte’.

Tipologie di virus e minacce ampiamente diffuse in Rete

Malware. Termine utilizzato per identificare tutti quei programmi, spesso causa di grossi problemi sul “computer-vittima”, che vengono installati sul sistema senza l’autorizzazione dell’utente. Si tratta sempre di programmi nocivi.

Virus. Poiché il confine tra virus in senso stretto e altre tipologie di minacce quali worm, trojan e dialer è divenuto oggi molto sfumato, il termine virus è divenuto sinonimo di “malware”.

Virus polimorfico. Implementa un algoritmo che ne consente la mutazione ad ogni infezione. In questo modo, risulta di più difficile rilevamento da parte dei software antivirus.

Virus di boot. Oggi pressoché scomparsi, questi tipi di virus infettano il settore di avvio di floppy disk e dischi fissi anziché singoli file.

Macrovirus. Infettano documenti Word, Excel, Powerpoint e simili “nascondendosi” all’interno di essi sotto forma di macro nocive.

Worm. Non necessita di legarsi a file eseguibili come i classici virus ma richiede l’intervento dell’utente per infettare il sistema. Quest’ultima barriera è ormai caduta da tempo, poiché gran parte dei worm sfruttano vulnerabilità del sistema operativo (non risolte da parte dell’utente mediante l’applicazione delle patch di sicurezza opportune) per “autoavviarsi”. Come i virus, i worm integrano un payload (la parte contenente il codice dannoso vero e proprio) e sempre più spesso attivano una backdoor o un keylogger aprendo la porta ad altri tipi di attacco provenienti dalla Rete.

Trojan horse o Cavallo di Troia. Versione digitale dello stratagemma utilizzato da Ulisse per entrare in città con i suoi soldati, il trojan “informatico” vuol sembrare all’utente ciò che non è per indurlo a lanciare il programma, in realtà dannoso. I trojan in genere non si diffondono automaticamente come virus e worm e vengono usati per installare backdoor e keylogger sul “computer-vittima”.

Backdoor. Aprono una o più porte “di servizio” che consentono di superare dall’esterno tutte le misure di sicurezza adottate sul sistema. Utilizzate per prendere il controllo di una macchina. Molti virus “moderni” integrano anche una o più backdoor.

Keylogger. Programmi maligni che registrano tutti i tasti premuti da parte dell’utente e ritrasmettono password e dati personali in Rete. Se sul proprio sistema si è rinvenuto un keylogger oppure un virus che integra questa funzionalità, dopo la sua eliminazione è bene provvedere immediatamente alla modifica di tutte le proprie password.

Exploit. Falle di sicurezza presenti nel sistema operativo e nei software in uso. In Rete pullulano i software che consentono di sfruttarle per far danni (aver accesso al sistema, guadagnare diritti amministrativi, rubare password e così via). Una ragione in più per mantenere i software utilizzati (a partire dal sistema operativo) sempre costantemente aggiornati.

Phishing. E' il metodo utilizzato per rubare informazioni personali quali password, numeri di carte di credito, informazioni finanziarie e così via. Si tratta di vere e proprie truffe che utilizzano e-mail e siti web appositamente creati, per spingere l’utente ad inserire dati personali. L’uso di elementi grafici e formule testuali proprie di famosi servizi online (istituti di credito, portali di e-commerce, aziende di telecomunicazioni,...) possono rappresentare la chiave di volta per spingere i più creduloni ad inserire informazioni confidenziali.

I tentativi di frode online sono in continua crescita: il numero dei messaggi di posta elettronica e dei siti web espressamente creati con lo scopo di truffare gli utenti meno attenti, sta raggiungendo dimensioni davvero spaventose.

Il meccanismo è sempre lo stesso: malintenzionati remoti cominciano con l’inviare migliaia di e-mail ad account di posta elettronica di tutto il mondo. All’interno del corpo del messaggio, si spiega che un famoso istituto di credito, un’azienda di servizi online od un portale sul web, hanno la necessità di verificare i vostri dati personali. Si invita quindi l’utente a cliccare su un link (che porta ad un sito web) spingendolo ad inserire username, password o codici di accesso.

I "messaggi-esca" sono solitamente inviati in formato HTML: i truffatori possono così inserire nel messaggio loghi ed altri elementi grafici propri di famosi istituti con l'intento di "abbindolare" l'utente ma, soprattutto, mascherare il falso link.

Ultimamente sono proprio le banche ad essere prese più di mira: una volta che l'utente clicca sul link indicato nell'e-mail truffaldina ed inserisce i dati per l'accesso, ad esempio, al proprio conto online, il malintenzionato può acquisire quei dati e dilapidarlo completamente. Gli istituti di credito maggiormente oggetto di phishing sono quelli statunitensi: sono decine i tentativi di truffa messi in atto grazie all'invio di false e-mail e siti web appositamente sviluppati.

Ma non solo. Anche l'Italia sta divenendo sempre più spesso oggetto di attenzione: gli esempi più critici, registratisi più di recente, sono quelli che hanno coinvolto Poste Italiane, Banca Intesa, Unicredit Banca e molte altre.

Generalmente i truffatori inviano casualmente ad indirizzi e-mail reperiti in Rete (utilizzando la stessa logica e le medesime tecniche adoperate dagli spammer) i loro messaggi-esca. Il messaggio riportato nel corpo del testo tenta di indurre l'utente a cliccare su un falso link camuffato con l'URL del sito web ufficiale della banca italiana, richiedendo poi di introdurre i dati di accesso personali. Per mettere a nudo tutti i tentativi di truffa, è bene disattivare la visualizzazione - all'interno del client di posta elettronica - dei messaggi in formato HTML preferendo sempre il testo puro. In questo modo è immediato accorgersi di come l'indirizzo venga camuffato.

Diffidate sempre di chi vi richiede, via e-mail, la conferma di dati personali. Istituti di credito, siti di e-commerce e così via non richiedono - tramite l'invio di messaggi di posta elettronica - questo tipo di informazioni.

Fate sempre riferimento ai siti web ufficiali e non cliccate mai sui link presenti nelle e-mail di questo tipo.

Pharming (o "DNS poisoning"). E' sempre più diffusa l'abitudine, da parte di molti worm, di modificare il contenuto del file HOSTS di Windows. Tale file permette di associare un particolare URL mnemonico (es. www.google.it) ad uno specifico indirizzo IP: ciò ricorda da vicino il funzionamento del server DNS del provider Internet. Ogni volta che si digita un indirizzo nella barra degli URL del browser, il sistema verifica - prima di tutto - se vi sia un'associazione corrispondente all'interno del file HOSTS. Solo quando questa non viene trovata si passa all'interrogazione del server DNS del provider. La modifica del file HOSTS era prima "prerogativa" di spyware e hijackers: oggi sta divenendo pratica sempre più diffusa anche tra i virus. Potrebbe capitare, quindi, digitando l'URL del motore di ricerca preferito, di un famoso portale e così via, di essere stranamente "proiettati" verso siti web che non si sono assolutamente richiesti. Il file HOSTS può essere memorizzato in locazioni differenti a seconda della specifica versione di Windows che si sta utilizzando. In Windows NT/2000/XP/2003 è in genere salvato nella cartella \SYSTEM32\DRIVERS\ETC mentre in Windows 9x/ME nella cartella d'installazione di Windows. La modifica del file HOSTS di Windows può quindi essere sfruttata per sferrare attacchi "phishing".

Il pharming, invece, è una diversa tipologia di attacco indirizzata in primo luogo ai server DNS. Una volta infettato, il server DNS indirizza i navigatori ad un sito fraudolento malgrado abbiano digitato l'Url corretto nel loro browser.

Il pharming è più difficilmente rilevabile dal momento che il browser non segnala nessuna anomalia lasciando credere all'utente di navigare in un sito legittimo. La maggiore pericolosità del pharming, rispetto al phishing, è che non viene colpito il singolo navigatore, destinatario di una e-mail con un link fraudolento, ma un elevato numero di vittime attaccate nello

stesso istante in cui accedono a un falso dominio.

Siti maligni. Sempre più spesso vengono recapitate, nella nostra casella di posta elettronica, e-mail fraudolente contenenti link a siti web davvero pericolosi. E' possibile incappare in siti web maligni anche semplicemente "navigando" in Rete. Aggressori remoti riempiono questi siti dannosi con script e controlli attivi in grado di eseguire codice nocivo sul personal computer dell'utente. Tutto ciò semplicemente visitando con il browser una pagina creata allo scopo.

Per difendersi da questi attacchi è bene accertarsi di installare con regolarità tutte le patch rilasciate per il sistema operativo e per le applicazioni in uso.

In uno studio effettuato da Symantec e riferito al secondo semestre dello scorso anno, si legge come fossero addirittura più di 1.400 le nuove vulnerabilità di sicurezza (addirittura 54 per settimana!) scoperte nei vari software. Tra queste, più del 97% sono considerate rischiose o molto pericolose (la presenza di queste vulnerabilità può condurre ad attacchi remoti in grado di compromettere completamente il sistema preso di mira). In aggiunta a questo idilliaco scenario, il 70% di esse è stato definito come facilmente sfruttabile da remoto, cosa che estende in modo impressionante il numero dei possibili attacchi.

Un esempio? Websense Security Labs ha lanciato qualche tempo fa l'allarme circa un tentativo di estorsione perpetrato via web. Visitando un sito web maligno con Internet Explorer senza aver applicato tutte le patch di sicurezza Microsoft, ci si potrebbe ritrovare con tutti propri documenti resi assolutamente illeggibili. L'aggressore remoto, quindi, intenta una vera e propria estorsione nei confronti dell'utente: "o acquisti lo speciale software di decodifica o perderai tutto." E' questa la sostanza della minaccia.

Accedendo al sito web dell'aggressore senza aver applicato la patch MS05-023 per Internet Explorer, il browser effettuerà automaticamente il download di un trojan ("download-aag") e provvederà ad eseguirlo sul sistema dell'ignaro utente. A questo punto, il trojan si conatterà ad un altro sito web maligno provvedendo a prelevare ed attivare un software "ad hoc" che codificherà tutti i documenti personali presenti sul disco fisso. Viene quindi mostrato un messaggio con le indicazioni per l'acquisto del software di decodifica (costo: 200 Dollari). L'applicazione tempestiva di patch di sicurezza e l'effettuazione periodica di copie di backup permettono di evitare di incappare in simili problemi.

Trojan "estorsori". Seguendo la stessa scia, informiamo i nostri lettori sulla diffusione di PGPCoder (Gpcode), un malware che - una volta mandato in esecuzione (è possibile ritrovarselo nella casella di posta elettronica) - codifica alcuni file presenti sul disco fisso (per, esempio, tutti quelli con estensione .doc) tentando di estorcere una somma di denaro all'utente che desidera rientrarne in possesso. Alcuni produttori di software antivirus (ad esempio, F-Secure), essendo l'algoritmo di codifica usato fortunatamente molto semplice, hanno prontamente fornito i tool per operare una decodifica.

"Typosquatting". E' noto come molti malintenzionati registrino nomi a dominio simili a quelli di famosi siti web con lo scopo di "catturare" tutti quegli utenti che digitino erroneamente l'URL nella barra degli indirizzi del browser. Esistono però siti web con nomi molto simili a quelli di famosi portali ed apprezzate realtà "internettiane" che contengono ogni sorta di nefandezza. Il caso più famoso è quello di un sito web che imitava l'indirizzo www.google.com a meno di una lettera. Basta quindi digitare erroneamente l'indirizzo proprio del famoso motore di ricerca, aggiungendo una lettera in più (la "k"), per ritrovarsi all'interno di un sito pieno zeppo di componenti nocivi di ogni genere: una volta aperto con il browser, il sito sfrutta una vasta gamma di vulnerabilità note del sistema operativo e dei browser per cercare di installare sul personal computer del malcapitato spyware e malware di ogni tipo. Domini Internet

con materiale pericoloso che ricalcano da vicino URL di famosi portali nascono però ogni giorno: l'installazione di un buon "personal firewall", di un software antivirus aggiornato e l'applicazione delle patch di sicurezza per sistema operativo e browser sono sempre l'arma migliore per evitare problemi!

Spamming. detto anche "fare spam", è l'invio di grandi quantità di messaggi elettronici non richiesti (generalmente commerciali). Può essere messo in atto attraverso qualunque media, ma il più usato è Internet, attraverso l'e-mail.

Spyware. Software indesiderato che esegue specifiche attività sul computer, solitamente senza il vostro consenso. Questo termine è spesso associato ad un software che visualizza annunci pubblicitari (adware) o software che identifica informazioni personali o riservate.

Denial of Service. Rendere un servizio non disponibile al pubblico. Può essere messo in atto sottoforma di:

- **Killer Packet:** invio di pacchetti malevoli che causano il blocco o il riavvio della macchina
 - ✓ *Ping of Death:* invio di ping di dimensioni eccessive
 - ✓ *Teardrop:* invio di pacchetti frammentati con offset sovrapposti, la ricostruzione del pacchetto originario causa il riavvio della macchina
 - ✓ *Land:* pacchetti con ip_sorgente=ip_destinazione e flag SYN blocca lo stack TCP/IP Microsoft.
- **SYN Flood:** invio massiccio di un flusso di pacchetti SYN con indirizzo sorgente spoofato, provoca la saturazione della pila delle connessioni half-open dello stack TCP/IP della vittima, che non può accettare nuove connessioni. Nella variante DDoS l'invio massiccio di pacchetti non proviene da una singola macchina ma da una serie di computer asserviti all'assalitore tramite l'uso di backdoor o virus/worm.
- **Smurf:** è un attacco che sfrutta la presenza di un moltiplicatore, tipicamente un router che consente l'invio in broadcast di pacchetti. L'attaccante manda ad esempio un ICMP Echo Request in broadcast, tramite il moltiplicatore, ad una serie di macchine. L'Echo Request ha l'indirizzo sorgente spoofato contenente l'IP della vittima, così le macchine che lo ricevono inviano un ICMP Echo Reply in massa alla macchina bersaglio.

Sniffing. Lettura abusiva di pacchetti che transitano in Rete. Può essere fatto sottoforma di:

- **ARP Spoofing:** sfrutta il protocollo ARP e in particolare la cache ARP. Siccome il protocollo ARP è *stateless*, si possono mandare pacchetti ARP reply non richiesti e appositamente contraffatti, che associano un IP ad un MAC diverso da quello legittimo. In questa maniera, per effettuare lo sniffing di tutto il traffico originato da una data macchina è sufficiente "avvelenare" le tabelle ARP della macchina nella entry corrispondente al gateway. Così tutto il traffico (diretto al Gateway) passerà attraverso la macchina attaccante.
- **MAC Flooding:** gli switch di rete hanno la capacità di memorizzare nelle proprie tabelle interne diversi indirizzi MAC corrispondenti alle varie interfacce, così da poter indirizzare i pacchetti rapidamente. Queste tabelle ovviamente hanno una dimensione finita (circa 128k indirizzi). Una volta riempita la cache ARP dello switch, esso non potendo più indirizzare nuovo MAC, per evitare di perdere pacchetti, entra in uno stato di *failopen mode*, in cui si comporta come un hub inoltrando tutti i pacchetti sui vari segmenti di rete, rendendo lo sniffing molto semplice.

- **STP exploit:** sfrutta il protocollo STP. Siccome l' albero STP viene costruito mediante pacchetti di tipo BPDU (bridge protocol data unit) non autenticati, chiunque si può fingere il nodo privilegiato "root switch" attraverso cui passano i pacchetti.
- **ICMP redirect:** sfrutta il protocollo ICMP, una volta sniffato un pacchetto ICMP originale, e registrati i bit dell' header, è possibile spoofare un falso pacchetto di risposta, indicando una strada più breve verso un dato host, che passa – ovviamente – per la macchina attaccante.

Spoofing. Falsificazione dell' indirizzo per fingersi qualcun altro. Esistono diverse tipologie di attacco di spoofing:

- **IP Spoofing:** la tecnica dell' IP Spoofing prevede la creazione di pacchetti IP modificati ad hoc in cui la parte di header che contiene l' indirizzo IP sorgente viene alterata, inserendo un IP diverso da quello legittimo. In questa maniera, ovviamente, non si riceverà alcuna risposta ai propri messaggi (*blind spoofing*).

Per risolvere il problema del *blind spoofing* si possono attuare due strategie:

- Uso di una macchina all' interno della stessa rete del bersaglio per compiere sniffing e raccogliere la risposta
- Uso di source routing per imporre un percorso di ritorno che passa per la macchina attaccante.

Nel protocollo TCP, oltretutto, è richiesta la presenza di un numero di sequenza, che si incrementa via via durante una connessione a partire da un numero pseudo-casuale generato all' inizio della connessione. Se l' host è all' interno della stessa rete di mittente o destinatario è possibile per esso osservare i numeri di sequenza, e intromettersi correttamente nella comunicazione, altrimenti deve in qualche modo (altre macchine asservite..) procurarsi il sequence number per poter mettere in atto l' attacco.

- **DNS Spoofing:** si può intercettare una richiesta DNS e rispondere con un pacchetto UDP spoofato (fingendosi il server DNS) e indirizzando verso un IP diverso da quello legittimo. Si può anche inserire in un server DNS una voce alterata sfruttando il meccanismo ricorsivo dei server DNS, intercettando la richiesta di un server "recursive" e spoofando la risposta di un server "authoritative".
- **DHCP poisoning:** procedura identica al DNS poisoning, che consente, a fronte dell' intercettazione di una richiesta DHCP, di fornire ad una macchina un IP, un DNS e un gateway predefinito.

HIJACKING. Intermediari non autorizzati prendono il controllo del canale di comunicazione:

- **Man in the middle:** è una tipologia di attacchi in cui l' aggressore riesce ad intercettare, modificare e inviare messaggi tra due nodi, senza che essi siano consci dell' intercettazione. Un esempio di questo genere è il TCP session hijacking, cioè l' inserimento in una connessione TCP attiva. L' aggressore effettua lo sniffing dei pacchetti, registrando i numeri di sequenza dei pacchetti TCP. Una volta bloccato uno dei due, mediante flood o DOS, l' aggressore può fingersi l' endpoint bloccato mediante IP spoofing e spingere l' altro host a rivelare informazioni riservate.

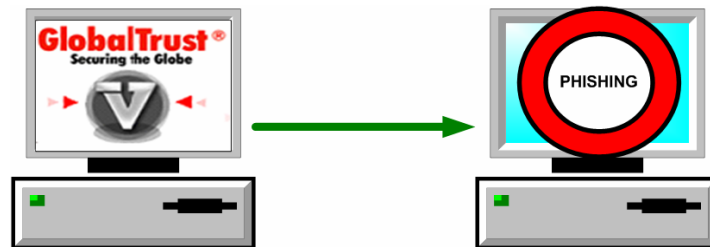
COME CI SI PUÒ DIFENDERE?

Elenchiamo alcuni buoni consigli che ciascun utente dovrebbe adottare:

- durante la navigazione su Web, in modo tale da sapere realmente l' identità e la legittimità dei siti visitati;
- per proteggere documenti sensibili, inviati in Rete o presenti sul PC, da accessi non autorizzati;
- per proteggere il proprio PC da worms, cavalli di troia, spyware e spam;
- per proteggere l' intera infrastruttura di rete aziendale.

1) VERIFICARE LA LEGITTIMITÀ DI UN SITO WEB CHE SI STA VISITANDO O AL QUALE DOBBIAMO FORNIRE DATI PERSONALI

È possibile verificare la legittimità di un sito Web utilizzando un nuovo Tool gratuito presente sul mercato: Globaltrust Verification Engine (VE) .



Con VE installato, basta posizionare il mouse sopra il logo presente all' interno di un qualsiasi sito Web che si sta visitando, e, se il logo viene riconosciuto legittimo, viene visualizzato un "indicatore di fiducia" visibile sotto forma di bordo verde.

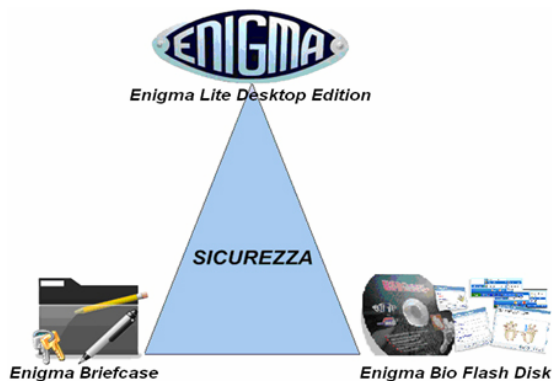
[Per scaricare gratuitamente il tool e la guida d' uso associata](#)

2) PROTEGGERE DOCUMENTI E DATI SENSIBILI DA ACCESSI NON AUTORIZZATI

I meccanismi di sicurezza *specifici* sono:

- **la crittografia**, per la *confidenzialità dei dati*;
- **la firma digitale**, per il *non ripudio dei messaggi*.
- **Utilizzo di certificati digitali e algoritmi crittografici** per effettuare le due operazioni sopra elencate

Le soluzioni offerte da **GlobalTrust** sono:



La suite **GlobalTrust Enigma** offre la gestione completa ed integrata di tutte le attività inerenti alla protezione e alla firma digitale dei documenti personali e/o aziendali, siano essi residenti su supporti o file system locali o su complessi sistemi di storage centralizzati.

FUNZIONALITÀ DI ENIGMA LITE DESKTOP EDITION



Per maggiori informazioni sul prodotto, vai sul sito della Globaltrust.

FUNZIONALITÀ DI ENIGMA BRIEFCASE



Per maggiori informazioni sul prodotto, vai sul sito della Globaltrust.

FUNZIONALITÀ DI ENIGMA BIO FLASH DISK



Registrazione di una o più impronte digitali per accedere al contenuto protetto del token USB



Impostazione di una password per accedere al contenuto protetto del token USB



Memorizzazione di (userID e password personali) utilizzati per accedere ad un' area riservata di uno o più siti web

Blocco/Sblocco del PC non appena "Enigma Bio Flash disk" viene scollegato/collegato dalla/alla porta USB.

Gestione sicura di più account di posta elettronica

Gestione di un volume criptato presente sul token.

Per maggiori informazioni sul prodotto, vai sul sito della [Globaltrust](http://www.globaltrust.it) .

Certificati Digitali

Che cos' è il certificato digitale

Il certificato digitale è un documento elettronico (file) utilizzato per identificare con esattezza l' identità di una persona o un' entità. Nel mondo informatico esso rappresenta ciò che la carta d' identità costituisce nella vita reale.

Come quest' ultima, infatti, esso ha una validità temporale limitata e viene rilasciato da una terza parte di fiducia:

- Autorità emittente
- Autorità di certificazione (CA-Certification Authority)



Qual è la funzione dell' Autorità di Certificazione?

Una Autorità di Certificazione rilascia i certificati a chi ne fa richiesta dopo averne attestato l'identità.

Svolge il ruolo di garante dell'identità di chi usa il certificato da lei rilasciato, così come le autorità di pubblica sicurezza (prefettura, comune, ecc...) che emettono documenti di identificazione quali il passaporto o la carta d'identità.

Chiunque può verificare la validità di un certificato, in quanto le C.A. devono mantenere un pubblico registro dei certificati emessi e una Lista dei Certificati Revocati (Certification Revocation List) disponibile per la verifica per via telematica da parte di tutti gli utenti.

Solitamente vengono emessi certificati per identificare:

- **L' Autorità di certificazione:** a tal fine, i certificati dovrebbero essere precaricati nei browser, cosicché sia possibile riconoscere, come validi, tutti i certificati emessi da quella CA. È consigliabile controllare la lista dei certificati delle CA presenti sul vostro browser, sia esso Microsoft Internet Explorer, Netscape Navigator o altro;
- **Un sito:** in questo caso si parla di **Certificati SSL Web Server**. Essi garantiscono che il server che sta rispondendo corrisponde al dominio certificato. Questo tipo di certificati viene usato in genere per effettuare:

- login sicuri per le Intranet

- login sicuri per siti Web
 - Form di registrazione sicuri
 - Invio di informazioni dei clienti
 - Invio di informazioni di pagamento
 - Prova dell' identità di un business on-line.
- **Un soggetto:** il certificato contiene informazioni quali nome, cognome, indirizzo, e-mail, ecc...; esso può essere utilizzato per garantire la provenienza di una e-mail, per usufruire di servizi personali, ecc.
 - **Un software:** Il certificato garantisce la provenienza del software. Questo utilizzo è importante specialmente se il prodotto viene distribuito in Rete.

Come ottenere un certificato

I certificati digitali delle più diffuse autorità di certificazione, sono solitamente pre-caricati nei browser; oppure sono scaricabili da Internet.

Quando servono per stabilire l' identità di un utente di solito vengono consegnati direttamente all'interessato utilizzando come dispositivo di memorizzazione un dischetto, una chiave USB oppure una smart card (supporto dotato di microchip, usato per memorizzare i dati dell' utente in modo cifrato). Essa rappresenta, oggi, il supporto con più alto grado di sicurezza.

Campi di applicazione:

- Quando vengono forniti o si utilizzano servizi on-line come pagamenti e consultazione di dati riservati.
- Quando si scambiano messaggi di posta elettronica: il mittente che compare su una e-mail non ci assicura riguardo all'identità di chi ha spedito veramente quel messaggio.
- Quando vogliamo verificare la validità di documenti in formato elettronico scaricati da internet o vogliamo garantire l'autenticità di documenti da noi pubblicati.

Per maggiori informazioni sui certificati rilasciati dalla [Globaltrust](#).

Sono disponibili anche diverse soluzioni pensate appositamente per [l'e-business](#)

3) MAGGIOR CONTROLLO SUGLI ACCESSI A DATI SENSIBILI E GESTIONE SICURA DELLE IDENTITÀ

Le aziende devono estendere l'accesso alle proprie risorse sensibili ad un numero sempre crescente di impiegati, di soci, di fornitori e di clienti. Risulta, quindi estremamente importante gestire questo numero sempre maggiore di identità e le responsabilità legate alla loro amministrazione.

Non solo la loro gestione ma anche il pericolo legato al loro furto è una problematica da considerare attentamente.

Un furto di identità è, infatti, causa di enormi perdite dirette e di immagine nelle aziende per non parlare poi dell'aumento della sfiducia degli utenti nei servizi offerti dalle aziende.

Le principali soluzioni offerte dalla Globaltrust sono:



[Entrust IdentityGuard™](#)



[Globaltrust Secure Identity™](#)

Per maggiori informazioni a riguardo visita il sito della [Globaltrust](#).

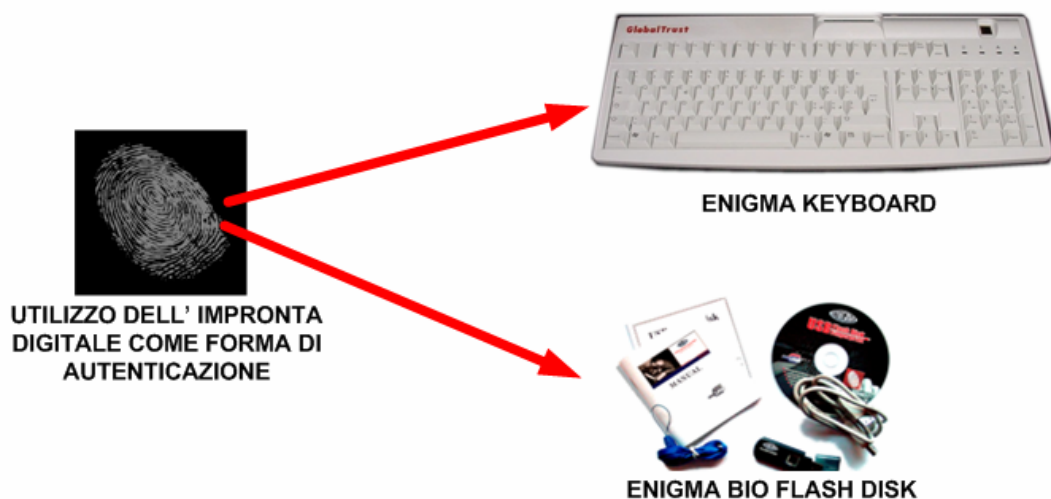
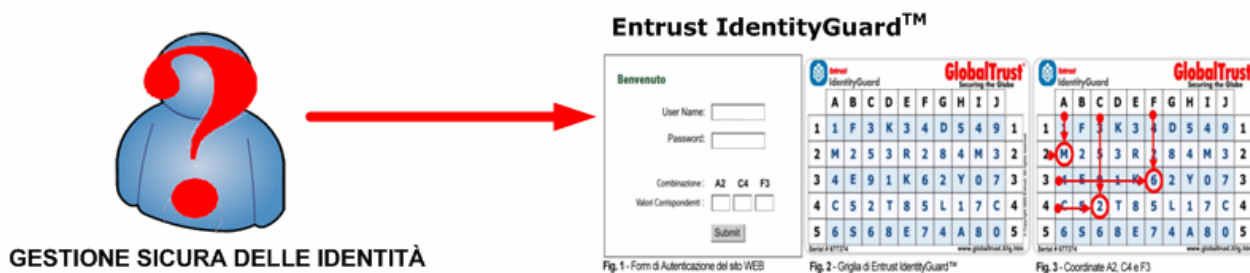
4) UTILIZZARE FORME DI AUTENTICAZIONE/PROTEZIONE PIÙ FORTI DI UNA SEMPLICE PASSWORD

In quasi tutte le interazioni tra gli utenti e i sistemi informativi vengono utilizzate password, frasi identificative o codici di sicurezza. La maggior parte delle forme di autenticazione, come la maggior parte delle protezioni per file e dati, si basa su password fornite dall'utente. Dal momento che gli accessi correttamente autenticati spesso non vengono registrati, o anche se vengono registrati non lo sono in modo da fornire alcun segnale di allarme, una password compromessa rappresenta un'opportunità potenziale di esplorare un sistema dall'interno senza essere identificati. Un aggressore avrebbe accesso completo a qualsiasi risorsa disponibile per quell'utente e sarebbe molto vicino ad essere in grado di accedere ad altri account, a macchine vicine e forse anche ad ottenere privilegi di amministrazione. Nonostante questi pericoli, gli account con password deboli o addirittura senza password rimangono estremamente diffusi e le società con una buona policy sull'utilizzo delle password ancora troppo rare.

Le più comuni vulnerabilità delle password sono dovute a:

- Account utente senza password o con password deboli.
- A prescindere dalla robustezza delle password, spesso gli utenti non le proteggono adeguatamente.
- Il Sistema Operativo o il software applicativo creano account di amministrazione con password deboli o privi di password.
- Gli algoritmi di hashing delle password sono noti e spesso gli hash vengono memorizzati in modo da essere accessibili a chiunque.

Le soluzioni proposte da Globaltrust a riguardo sono:



5) PROTEGGERE IL PROPRIO PC CON GLI ATTUALI STRUMENTI SOFTWARE DI SICUREZZA.

In particolare:

- Proteggiamo il nostro PC con buoni strumenti di sicurezza, un buon antivirus e un valido antispyware ma teniamoli costantemente aggiornati. Ricordiamoci di attivare anche le funzioni di scansione in tempo reale (real-time scan) di entrambi.
- Installiamo e configuriamo un buon personal firewall e, perché no, anche strumenti per crittografare i dati per noi più critici.
- Ricordiamoci di controllare tutti i file che riceviamo o spediamo facendoli verificare dall'antivirus. Per far ciò è sufficiente configurare correttamente il proprio antivirus.
- Eseguiamo costantemente la scansione dei dispositivi del nostro PC (dischi fissi, compact disc e dischetti), per verificare la presenza di virus, worm, spyware. L'ideale è attivare la scansione automatica da parte dei software antivirus e antispyware, magari all'avvio del sistema operativo.

- Facciamo regolarmente il salvataggio (BACKUP) dei nostri dati (almeno quelli più critici).
- Aggiorniamo il software di base (sistema operativo, browser di navigazione Internet, posta elettronica e così via) come da suggerimento dei fornitori: facciamo cioè il cosiddetto "patch update".
- Non installiamo software superfluo o di dubbia provenienza. Attenzione quindi al software freeware. È buona norma verificare che il software che si sta scaricando sia firmato digitalmente, in modo tale da ricondurci alla legittima provenienza.
- Facciamo attenzione alle applicazioni quali ActiveX, JavaScript e Visual Basic Scripting configurando correttamente il browser e quando possibile teniamole disattivate.
- Non apriamo mai allegati di dubbia provenienza: verifichiamo prima che l'antivirus abbia fatto il suo dovere!
- Facciamo attenzione ai servizi offerti in rete: molti sono specchietti per le allodole e ricordiamoci sempre che navigando in Internet seminiamo tracce del nostro passaggio!
- Poniamo attenzione ai link diretti a banche o negozi forniti da sconosciuti: possono essere falsi e portarci ad un sito truffa.
- Facciamo attenzione alla posta in formato HTML, potrebbe contenere delle insidie.
- Facciamo "pulizia" del nostro PC cancellando regolarmente file inutili (es. cookies, file temporanei, ecc).

6) RENDERE SICURA LA PROPRIA RETE FISICA AZIENDALE ATTRAVERSO APPARATI HARDWARE E PROCEDURE DI SICUREZZA.

APPARATI HARDWARE

- **FIREWALL**

Sistema di controllo degli accessi, verifica tutto il traffico che lo attraversa:

- controllo dei pacchetti IP (*IP filtering*)
- mascheramento degli indirizzi (NAT)
- blocco di pacchetti pericolosi

Un firewall non fa altro che implementare delle regole, se queste sono sbagliate o scritte male il suo lavoro è inefficiente, se non dannoso.

Dove può essere applicato un Firewall:

- **a livello di rete (Network layer)**. In questo caso effettua operazioni di:

- **Packet Filtering:** effettua un filtraggio dei pacchetti uno ad uno basandosi solo sull' header, non è quindi in grado di tener traccia di sessioni e connessioni. Con questo metodo si può negare l' accesso a determinati range di indirizzi, oppure chiudere certi servizi e protocolli, o consentire accesso solo a determinate coppia **sorgente.ip:port/destinazione.ip:port**. Siccome per questo lavoro è necessario conoscere soltanto l' header dei pacchetti, l' opera di packet filter può essere svolta da un router avanzato, noto come *screening router*.
- **Stateful Packet Filtering:** effettua lo stesso filtraggio di un packet filter, ma in più tiene conto dello **stato della comunicazione**, riproducendo la macchina a stati del TCP. Può quindi verificare la correttezza dei pacchetti, che adesso devono corrispondere ad una specifica richiesta (SYN-ACK), verificare i numeri di sequenza. In questa maniera, pacchetti provenienti dall' esterno vengono autorizzati solo se riconosciuti parte di una comunicazione effettivamente cominciata dall' interno. Può operare ispezioni anche a livello applicativo, riconoscere e controllare sessioni FTP e http, ma soprattutto può funzionare come NAT (Network Address Translation). Effettua una deframmentazione per difendere dagli attacchi che la sfruttano. Come già detto riconosce le sessioni TCP e – non con la stessa efficacia – quelle UDP.
- ❖ Riconoscimento sessione TCP: verifica di corrispondenza IP-sorgente/IP-destinazione, correttezza dei numeri di sequenza, controllo sui flag.
- ❖ Riconoscimento sessione UDP: viene considerata risposta ad un pacchetto UDP, un altro pacchetto UDP che giunge al mittente entro un timeout configurabile.

Altra capacità dei firewall SPF è quella di PAT (Port Address Translation), cioè consentire la condivisione di un singolo indirizzo IP tra più macchine, indirizzando una o l' altra tramite la porta.

- **a livello di applicazione (application layer)**. In questo caso si parla di :

- **Circuit level firewall:** effettua un *relay* delle connessioni TCP, il client si connette al firewall, il quale si connette al server; il firewall instaura un circuito virtuale per conto del client. Così facendo può verificare la legittimità di tutti i dati e delle connessioni tenendo conto di IP-sorgente/IP-destinazione, numeri di sequenza, ETH-ingresso/ETH-uscita. Non viene controllato il payload che si forwarda al client, non effettua controllo di autenticazione, e spesso richiede la modifica delle applicazioni per il suo corretto funzionamento.
- **Application proxy firewall:** funge da intermediario come nel caso precedente, ma effettua un controllo sui pacchetti anche a livello applicativo. Vengono usati per fornire un sottoinsieme delle funzionalità offerte da un server. Questo può difendere sia gli utenti interni che accedono a server remoti, che i server stessi (reverse proxy). Questo tipo di firewall può dare problemi di prestazioni, dato che il flusso applicativo viene ricostruito due volte: in ricezione il server proxy verifica la correttezza della richiesta e la inoltra, quando il client ha elaborato una risposta, prima di lasciarla passare all' esterno, il proxy la controlla.

- **DMZ, Architettura a due zone**

Lo scenario attuale delle reti aziendali prevede la necessità di garantire traffico

- dall' interno verso l' interno (dai client ai server interni)
- dall' esterno verso l' interno (visite ed accessi da Internet ai server aziendali)
- dall' interno verso l' esterno (navigazione web, e-mail)
- dai server di front—end a quelli di back-end (web Server che ricerca dati in un DBMS)

Per questo si è creata una zona ibrida, la Zona DeMilitarizzata (DMZ). Gli utenti Internet, dall' esterno, possono accedere solo alla DMZ, nella quale risiedono i server aziendali “sacrificabili”, nel senso che non erogano servizi critici per l' azienda.

In questo scenario può però essere necessario garantire ad un utente esterno, tramite Internet, l' accesso alla zona interna e sicura della rete aziendale, passando indisturbato attraverso la DMZ. Allo stesso modo può essere necessario collegare reti interne di due sedi distaccate di un' azienda in tutta sicurezza. Per consentire ciò sono nate le **Virtual Private Network (VPN)** e cioè tunnel criptati attraverso la rete pubblica.

Ci sono due possibili politiche per le VPN:

- **tutto il traffico nel tunnel:** una richiesta dell' utente esterno verso Internet viene soddisfatta dall' interno della rete aziendale e incanalata all' interno del tunnel, aumentando il traffico di rete e l' occupazione di CPU per la criptazione.
- **Split tunneling:** le richieste internet dell' utente esterno vengono evase direttamente, senza passare attraverso il tunnel VPN. Questa soluzione è più semplice, più economica, ma rende vulnerabile il sistema: si può attaccare la macchina esterna attraverso Internet e mettere a rischio la VPN.

L' implementazione di una VPN può avvenire tramite IPSec o per via tunnel SSH/SSL.

PROCEDURE DI SICUREZZA

La sicurezza sui diversi livelli di accesso di un utente si basa su domande del tipo “Who are you?” e “What can you do?”.

Altra filosofia sfruttata per aumentare il grado di sicurezza sugli accessi è:

- **Intrusion Detection System:** la filosofia degli IDS sta nella domanda “Why are you doing this?”, vuole cioè cercare i fallimenti degli altri meccanismi di sicurezza, identificando le tracce lasciate dalle azioni di un attaccante. Per fare ciò si possono utilizzare due politiche:
 - **Anomaly Detection:** analisi a *posteriori*, identifica le deviazioni dal comportamento normale, analizzato per via statistica, e riporta gli scostamenti. Va quindi definito in qualche modo il comportamento standard, e una soglia di tolleranza, oltre la quale il sistema fa scattare un allarme. In questo modo è teoricamente possibile rilevare ogni tipo di intrusione; ogni comportamento anomalo – però – anche se non pericoloso, potrebbe essere percepito come tale. Problematiche classiche di questa modalità sono i soggetti da misurare e la soglia di allarme.
 - **Misuse Detection:** analisi a *priori*, in base ad un database di attacchi conosciuti, confronta i log di sistema con schemi di violazione noti. Serve un formalismo per definire i comportamenti malevoli, il sistema può quindi riconoscere

solo gli attacchi noti, e il linguaggio usato per definire i pattern di attacco può non essere abbastanza espressivo. D'altro canto in questo caso l'identificazione è inequivocabile e può far scattare reazioni apposite. Il problema principale di questo approccio è la difficoltà di gestire e tenere aggiornato il database dei pattern e la possibilità di sviare il sistema tramite, ad esempio, il cambiamento di encoding.

A seconda dell'oggetto dell'ispezione, si può ulteriormente distinguere

- ***IDS host based***, che operano su una singola macchina
- ***IDS network base***, che analizzano il traffico su determinati segmenti di rete.

SNORT

Snort è un *IDS network based e misure based*, è un *packet sniffer* che basa il riconoscimento degli attacchi su regole.

I pacchetti vengono prima analizzati da un preprocessore, poi passano ad un detection plugin che cerca eventuali tracce note; un output plugin effettua analisi e trasforma i dati raccolti.