Macro the software partner
Aztec hardware & networking
Consulenze Professionali
informano

RETI INFORMATICHE E SICUREZZA

Internet, Virus, Hackers, Sistemi di Protezione

Premessa: quale sicurezza in internet?

Chiunque sia sul punto di avviare una nuova applicazione di e-business, o stia pensando di vendere prodotti via Web, oppure sia in procinto di dare inizio a una collaborazione con partner commerciali tramite INTERNET, si è posto la fatidica domanda: “MA E’ SICURO?”

Avendo a che fare con sistemi informatici, questa probabilmente è la domanda più difficile alla quale dare una risposta. Ci sono troppe variabili in termini di hardware, firmware, sistemi operativi, middleware, applicazioni e reti perché una persona possa tenere adeguatamente conto di tutte le possibilità. In effetti, l’unico sistema veramente sicuro è un sistema spento, ma a quel punto è evidente che quel sistema non serve più a nessuno.

Fortunatamente, le prospettive non sono così deprimenti quanto si potrebbe supporre. Esistono molte vie percorribili per diminuire la probabilità di una perdita di dati. La soluzione sta nel determinare al meglio quali siano gli effettivi rischi e fare il possibile per minimizzarli, confrontando l’aumento del costo della sicurezza con il costo di una potenziale perdita di dati.

Anche se tutti noi vogliamo sapere se i nostri sistemi sono sicuri, il modo migliore di pensare al problema è porlo in termini relativi anziché assoluti. In altre parole, “Il sistema A è più sicuro del sistema B?”, oppure: “Questo sistema è più o meno sicuro di quanto non fosse un tempo?”. Ancora meglio: “Questo sistema è sufficientemente sicuro per il mio modello di business?”.

Queste domande sono il punto di partenza dal quale iniziare a formulare risposte significative.

Reti informatiche e sicurezza

La storia di Internet.

Prima di entrare nello specifico argomento della sicurezza, è bene tracciare un breve excursus storico. Internet nasce, come molte cose nel campo dell'informatica, da esigenze governative-militari. Nello specifico all'inizio degli anni '60 il governo americano tramite l'ARPA Advanced Research Projects Agency avviò lo studio di un progetto che aveva lo scopo di "tutelare" le informazioni in caso di catastrofe naturale o attacco nucleare.

L'idea era di replicare e suddividere queste informazioni tra diversi computer situati a grande distanza ma connessi tra loro. A studiare il progetto furono chiamate quattro università americane, Santa Barbara e Los Angeles (California), Utah, e Stanford.

Nel 1969 L'università di Los Angeles installò il primo server ed in breve tempo i ricercatori si resero conto della grande valenza comunicativa di quello strumento: oltre all'utilizzo militare per cui era stato pensato in origine, in effetti, si prestava con straordinaria efficacia alla condivisione di qualsiasi tipo di informazione.

Il numero di Server connessi tra loro iniziò ad aumentare, nacque INTERNET, la "rete" e si presentò il primo problema: in base a quali regole i server dovevano scambiarsi informazioni? Il primo scoglio fu superato arrivando alla teoria della commutazione in pacchetti. Il dato da spedire doveva essere suddiviso in entità più piccole, i "pacchetti", che contengono l'indirizzo di origine e quello di destinazione analogamente ad una lettera con Mittente e Destinatario sulla busta.

Presto però si presentò il limite di questo protocollo (l'insieme delle regole) perché in origine il progetto era stato ideato per lo scambio di informazioni tra computer e non contemplava la possibilità di scambiare pacchetti generati da satelliti o ponti radio.

Il primo gennaio 1983 il protocollo NCP (Network Control Protocol) venne sostituito con il TCP/IP (Transfer Control Protocol/Internet Protocol). Questo protocollo che è attualmente la base delle comunicazioni in internet, ma più genericamente, tra un computer e l'altro, ha apportato il vantaggio di liberare le comunicazioni da molti vincoli.

I pacchetti trasmessi con il nuovo protocollo possono avere forma e dimensione diversa e possono venire prodotti da qualsiasi tipo di rete.

Essendo nata in ambito universitario, i primi utilizzatori di internet furono scienziati, ricercatori e studenti. Veniva usata soprattutto per trasmettere posta elettronica e accedere a file condivisi. Successivamente nacquero i primi gruppi di discussione (newsgroup) a tema. In questa fase le informazioni erano rappresentate da puro testo.

Nel 1989 Tim Berners-Lee, un fisico europeo del C.E.R.N. (Centro Europeo per la Ricerca Nucleare), propose la creazione di un'interfaccia grafica che permettesse agli scienziati di scambiare dati in forma visuale. Il nome in codice di questa interfaccia fu World Wide Web.

Nel 1990 Steve Jobs con il computer NeXT introdusse qualcosa di molto vicino all'idea di Berners-Lee: un computer che consentiva agli utenti di creare e modificare documenti ipertestuali (cioè composti da testo, immagini, musica) e di trasmetterli tramite internet.

Nel 1992 il C.E.R.N. iniziò a pubblicizzare il W.W.W. e ad incentivare lo sviluppo di server basati su questa tecnologia. Nuovamente sorse la necessità di definire le regole alla base di questo nuovo tipo di comunicazione e questo portò all'introduzione di un protocollo dedicato alla condivisione degli Ipertesti. Così nacque l'H.T.T.P. ovvero Hyper Text Transfer Protocol/ Protocollo di Trasferimento per Ipertesti.

Ma perché la cosa fosse utilizzabile da tutti, oltre a server in grado di lavorare con questa tecnologia era necessario arrivare ad avere anche dei client (cioè computer collegati con il server) in grado di farlo.

Il C.E.R.N. promosse lo studio di questa tecnologia. La svolta fu data dal N.C.S.A. National Center for Supercomputing Applications che con Mosaic pose le basi per tutti i successivi Browser (navigatori), tra cui, in primis, Netscape Navigator e Microsoft internet Explorer.

Un po' di "Numeri"

Per rendersi conto dell'importanza di Internet come strumento di comunicazione basta guardare il tasso di crescita che ha avuto negli anni. Nel 1985 si stimavano 1961 computer Host e qualche decina di migliaia di utenti.

Tre anni dopo, nel 1988, il numero di Host era intorno alle 80.000 unità, con un incremento del 4000%. Facendo un salto in avanti, fino al 1997 il numero di Host presenti sale a 250.000 fino ad arrivare al milione e oltre stimato nel 2002. E' stato calcolato che il tasso di utilizzo aumenta mediamente del 7% al mese e si stimano attualmente più di 500 milioni di utenti.

Internet ha sviluppato le sue potenzialità utilizzando la tecnologia Web. Il Web è costituito da miliardi di documenti ipertestuali che si trovano in migliaia di computer dislocati in più di 150 paesi.

I rischi

Il rischio di base è il furto di informazioni. Per comprendere l'origine di questo rischio bisogna capire le modalità con cui si accede a Internet. Il protocollo TCP/IP che è alla base della comunicazione in internet, identifica ogni computer connesso alla rete tramite un indirizzo, chiamato appunto indirizzo IP.

La connessione a internet avviene tramite un I.S.P. (Internet Service Provider), ovvero un fornitore di collegamento, che, oltre a fornirci l'accesso alla rete ci assegna un indirizzo IP.

Se utilizziamo una connessione telefonica “a tempo” questo indirizzo è valido fino al momento in cui ci scolleghiamo. Al collegamento successivo ne verrà assegnato un altro.

Ci sono poi alcune modalità di connessione (per esempio l’ADSL) che prevedono l’utilizzo di un indirizzo IP statico (che non cambia mai). Solitamente questo tipo di indirizzo è utilizzato da chi ha una connessione internet continua, 24 ore al giorno. In entrambi i casi la sostanza non cambia. Nel momento in cui accediamo ad internet, apriamo il browser ed iniziamo la navigazione, il computer viene identificato da questo indirizzo IP.

Proviamo a pensare al significato di questa cosa. Sono a casa e clicco sull’icona di collegamento ad internet. Il pensiero è “Vado a fare un giro in internet”. Non so se avete fatto caso ai messaggi che appaiono durante la connessione. Uno di questi dice “Proiezione del computer sulla rete”. Qui sta il punto. Il mio computer viene “proiettato” in Internet. Il verbo giusto da usare non è “andare” in internet, ma piuttosto “essere” in internet.

L’assegnazione dell’indirizzo IP fa diventare quel computer una parte di internet. L’essere in Internet permette la condivisione delle informazioni che il computer contiene e ci espone al rischio di furti e intrusioni.

L’altro rischio, solitamente più noto, in cui possiamo incorrere è l’infezione da parte di Virus. Quali sono le conseguenze che derivano da questi due fattori di rischio? Vediamo in termini economici che danni hanno portato.

I dati si riferiscono all’anno 2001 e dicono che in quell’anno, a causa dei virus Code Red e Sircam sono stati sostenuti costi valutati in circa 4 miliardi di dollari. Le perdite economiche derivanti dagli stessi virus sono state stimate in 10 miliardi di dollari. I due virus citati restano comunque molto distanti dal virus Love Bug che nell’anno 2000 ha provocato da solo danni per una decina di miliardi di dollari.

Per quanto riguarda i furti di informazioni o i danni derivati da intrusioni mancano le stime economiche ma, sempre nel 2001, il numero di questi incidenti è cresciuto del 300% rispetto all'anno precedente. Nei primi otto mesi di quell'anno sono stati rilevati 35.000 incidenti.

Gli Hacker

Bene, iniziamo a dare nomi e cognomi alle cose di cui abbiamo parlato. Abbiamo visto che uno dei rischi in cui incorriamo in internet è il furto di dati e l'intrusione. Ma chi è a fare questo tipo di cose ? La domanda ha una risposta scontata: l'uomo nero di internet è l' Hacker. Direi che la prima cosa da fare è definire letteralmente la parola Hacker, tanto per capire di cosa stiamo parlando.

Hack, sostantivo inglese, significa tacca, spacco, fenditura.

To Hack, verbo, significa fare a pezzi, fendere, tagliare con fendenti.

La cosa comincia a prendere significato. L'hacker è colui che fa a pezzi qualcosa.
Proviamo a definire meglio questo concetto e per farlo prendiamo in prestito la definizione data proprio da un hacker:

"L'intenzione reale di un hacker quando penetra in un sistema è molto simile al concetto di un bambino che apre un giocattolo per vedere come funziona. La differenza sta nel fatto che l'hacker tenta di non rompere il giocattolo (oltre al fatto che il giocattolo non e' il suo...)."

L'hacker che ha scritto questa definizione nel suo manifesto si chiama Elf Qrin. Diversi di loro hanno scritto definizioni o dichiarazioni di coscienza. Ho scelto questa perché,

oltre ad essere semplice, non ho dovuto tradurla. Elf Qrin è un hacker, ed è italiano: ciò aggiunge un tassello non marginale alla ricostruzione del quadro.
Quello di cui stiamo parlando non è un fenomeno “americano”, distante da noi, per due motivi:

1) internet appiattisce le distanze.
2) gli hacker sono anche qui.

Parlando di sicurezza mi è stato riportato un consiglio letto in un libro. In pratica l’idea è che per tutelarci bisognerebbe chiudere l’accesso ad internet fuori dall’orario di lavoro. Va bene, ma l’orario di lavoro di chi?. Il nostro o quello dell’hacker australiano che sta provando a entrare nel computer? In internet, infatti, non è solo la distanza ad essere appiattita, lo è anche il tempo.

Ma stavamo parlando di hacker, abbiamo dato una definizione del termine e, a prima vista, questa definizione non calza pienamente con quello che siamo abituati a sentire dai mass-media. Vediamo di capire un po’ di più chi sono questi hacker.

Intanto sono un gruppo in qualche modo organizzato. Hanno un loro codice etico più o meno discutibile e si sono dati una scala gerarchica. E su questa gerarchia dobbiamo ragionare un attimo per capirli un po’ di più.

Al primo livello c’è il LAMER: è una persona che utilizza programmi e strumenti fatti da altri, e che quindi non conosce, per attaccare un computer. E’ pericoloso perché la sua incompetenza mette a rischio le informazioni e i sistemi di cui prende possesso.

Al secondo livello c’è il NEWBIE, la larva. Come dice la parola stessa, rappresenta l’hacker allo stadio larvale, in fase di sviluppo, che sta accumulando conoscenze.
Al terzo livello c’è l’hacker vero e proprio.

Poi c’è l’ELITE degli hacker, i migliori, e vi troviamo due figure: il WIZARD, il mago e il GURU, il santone.

Vi sono infine altre due tipologie di hacker, parallele a quelle sopraelencate: il DARK SIDE HACKER e il MALICIOUS HACKER.

Il primo di questi due personaggi prende il suo nome da Guerre Stellari. Rappresenta il "lato oscuro della forza", l'hacker che per scelta decide di utilizzare le sue conoscenze per scopi illegali. Il MALICIOUS HACKER invece danneggia altri sistemi per stupidità o cattiveria e senza trarne particolari profitti.

Cosa deduciamo da questa gerarchia: che questo "movimento" non è diverso da tanti altri che comunemente conosciamo. E' fatto di persone che hanno conoscenze in un particolare campo e che hanno la facoltà di scegliere se utilizzarle bene o male.

La definizione semplicistica hacker uguale Criminale Informatico non rende giustizia alle reale situazione. Alcuni di loro sono responsabili di crimini, questo è fuori dubbio, ma il movimento hacker nel suo complesso è anche coautore della crescita di Internet.

Sono hacker i programmatori che hanno creato Unix e Linux, lo sono gli ideatori della filosofia Open Source da cui derivano i programmi gratuiti in grado di sostituire quelli a pagamento più diffusi. Sono sempre idee ed esperienze hacker quelle che stanno alla base del movimento letterario CyberPunk, da cui sono nati prima in forma letteraria film come Johnny Mnemonic e Matrix.

Ora che abbiamo chiarito le caratteristiche del nostro uomo nero cerchiamo di capire cosa lo spinge, quali sono le motivazioni che lo portano ad attaccare altri sistemi.

In sostanza, direi che le sue motivazioni sono fondamentalmente 3:

1) si sta divertendo, sta provando nuovi programmi e quindi è un LAMER;
2) gli interessano effettivamente le informazioni di cui siamo in possesso;
3) ha bisogno di utilizzare il nostro sistema.

Le prime due motivazioni sono abbastanza chiare e, soprattutto la seconda, è facile da valutare nella definizione di una politica della sicurezza. Se le informazioni di cui siamo in possesso sono importanti dobbiamo proteggerle.

L'ultima motivazione può risultare più difficile da capire. Gli interessa utilizzare il nostro sistema per fare cosa? Semplice, per attaccarne un altro senza venire scoperto, per nascondere le sue tracce oppure per attaccare con più forza un sistema ben protetto.

Questo tipo di tecnica si chiama ZOMBIE. Come i non morti dei film Horror i computer controllati in questo modo diventano, a nostra insaputa, trampolini di lancio per altri attacchi.

A questo punto potremmo entrare nel merito delle diverse tipologie di attacco che può utilizzare un hacker. Non credo però che sia utile per chiarire che ruolo deve avere la sicurezza nelle aziende. Passiamo invece a parlare dell'altro rischio derivato da Internet: i virus.

Su questa problematica circolano diverse leggende. Si pensa che siano nati con lo scopo di intralciare le attività di aziende concorrenti o che siano gli stessi produttori di antivirus a crearli per continuare a fare soldi. In realtà il responsabile del primo vero virus fu uno studente della Cornell University. Alle 18 del 2 Novembre 1988 lanciò un programma di attacco alla rete. Entro un'ora il virus aveva reso inutilizzabili molti dei principali centri di ricerca. Questo studente, Robert T. Morris è a tutti gli effetti il primo vero hacker di internet.

Potremmo, anche in questo caso, esaminare i sistemi di infezione più usati ma sarebbe solo una faccenda "tecnica" che non ci porta a capire quali sono le misure necessarie per difenderci, mentre è questo lo scopo di questa chiacchierata.

Abbiamo definito quali sono i rischi e quali sono gli attori. Tutto questo come si applica? Come si concretizza nelle aziende?
Facendo un esempio direi che una azienda che si affaccia in Internet può essere paragonata ai pionieri dei film western. La carovana si sposta e trova un punto in cui stabilirsi. Ha una connessione internet o un suo sito. A questo punto valuta i possibili rischi e cerca le adeguate contromisure. Per gli animali feroci accende fuochi notturni, per gli indiani predispone barricate e muri di cinta e guardie che proteggano il perimetro.

Contemporaneamente ci si organizza internamente. Vengono definiti dei ruoli: tu sei una guardia, tu comandi le guardie e così via. Ogni ruolo ha dei privilegi e delle responsabilità e accede a determinate risorse per svolgere la sua mansione.

La politica della sicurezza informatica in azienda segue le stesse modalità: definita la necessità di utilizzare internet e chiariti i rischi che questo comporta dobbiamo capire se abbiamo o no informazioni sensibili e in che modo, a che livello, vogliamo che queste informazioni vengano protette. Da questa valutazione nasce l'esigenza di "barricarci" e la scelta se farlo utilizzando una palizzata in legno o un muro di cemento armato!

Gli strumenti di protezione

Cerchiamo ora di capire quali strumenti abbiamo a disposizione per proteggerci.

Il primo e ormai comune strumento di protezione è il FIREWALL. Il muro di fiamme.

Questo muro si frappone tra la nostra rete interna e Internet limitando le possibilità di accesso. Ne esistono di due tipi, hardware e software. In sostanza posso acquistare una macchina dedicata a questo scopo o posso utilizzare un programma installato sul mio computer che ne garantisca la sicurezza. La differenza sta nel livello di sicurezza e nel costo. Di norma il FIREWALL hardware dà una tutela maggiore.

Il FIREWALL da solo però può non essere sufficiente. Ho detto prima che il FIREWALL limita la possibilità di accesso, la sua funzionalità però deve essere monitorata: in pratica bisogna dotarsi anche di strumenti che permettono di controllare se il FIREWALL sta lavorando correttamente o se esistono possibili varchi. Anche per questo tipo di controllo esistono software specifici e siti internet che offrono la possibilità di verificare se esistono falle utilizzabili per un attacco.

Il lavoro maggiore per la sicurezza però va fatto all'interno della ditta ed ha a che fare con la gestione dei ruoli. In azienda esistono diversi utenti. Possiamo classificarli in base alle loro competenze e decidere di farli accedere solo alle informazioni che effettivamente servono loro per svolgere i compiti assegnati. Vengono quindi dati dei nomi utente e delle password. Sulle password va fatto un lavoro importante.

La definizione di queste chiavi di accesso dovrebbe tenere conto di alcune regole molto semplici ma che danno un risultato immediato in termini di sicurezza:

1) Non vanno usati i nomi o le date di nascita di parenti e amici.
2) Non vanno usati nomi di cose comuni. Una buona password dovrebbe essere lunga più di 6 caratteri e contenere sia lettere che numeri.
3) E' importante nominare un responsabile a cui va delegato il compito di tenere un archivio delle password e di cambiarle periodicamente.

Un hacker può anche entrare nel nostro sistema, ma se abbiamo gestito correttamente questi ruoli e utilizziamo al meglio gli strumenti di LOGIN possiamo complicargli di molto la vita.

Altri strumenti utilissimi per limitare la perdita di informazioni riguardano la posta elettronica. Nella norma tendiamo a spedire messaggi di posta con il testo in chiaro nel corpo. Un semplice strumento da utilizzare per proteggere questi messaggi è la CRITTOGRAFIA. In sostanza si tratta di funzioni matematiche applicate soprattutto al testo in modo da renderlo illeggibile.

Parlando di crittografia, vengono usate le nozioni di CODIFICA quando si utilizza una funzione matematica e una chiave per ottenere un testo cifrato e di DECODIFICA quando la chiave e la funzione vengono applicate sul testo cifrato per riottenere il testo originale di partenza. Per fare un piccolo esempio supponiamo di voler crittografare la frase “USARE INTERNET” utilizzando una semplice formula di scorrimento dell’alfabeto di 3 posizioni (in questo caso la funzione matematica è l’ordine di scorrimento dell’alfabeto e la chiave corrisponde a 3 posizioni). In questo caso la lettera A diventerebbe D, la B diventerebbe E così via.

La nostra frase verrebbe crittografata così :

Testo in chiaro: USARE INTERNET

Testo cifrato: XVDUHCLQWHUQHW

Ovviamente il destinatario del messaggio deve possedere la chiave crittografica adatta per poter leggere in chiaro il testo.

Un altro sistema di protezione e di verifica del proprio livello di sicurezza è rappresentato dagli AUDIT-TRAIL. In sostanza si tratta di una registrazione delle attività che vengono eseguite su un computer. Vediamo di capire i tipi e i vantaggi degli AUDIT-TRAIL:

1. Internet fa in modo che gli audit-trail evidenzino le richieste di accesso a oggetti riservati;
2. Utilizzando AUDIT-TRAIL su screening router e firewall si possono evidenziare attacchi hacker;
3. Il livello di auditing è configurabile a vari livelli:
    a. Computer (bassa precisione)
    b. Directory (media precisione)
    c. Oggetto (massima precisione);

4. La politica di sicurezza aziendale deve includere una regolare manutenzione e analisi degli AUDIT-TRAIL;
5. In caso di violazioni della sicurezza l'auditing è l'unico strumento per capire cosa è stato fatto e come sono riusciti a farlo.

L'impostazione di un auditing interno non offre una protezione a prova di errore, ad esempio, questo sistema, non ci protegge da tecniche come lo "SPOOFING" e gli attacchi da "SNIFFER" in quanto in questi metodi l'hacker non accede direttamente ai dati ma ne controlla il passaggio o vi accede simulando di essere un utente con i privilegi necessari per farlo.

Altro strumento fondamentale di protezione è rappresentato dal corretto utilizzo e aggiornamento degli strumenti con cui lavoriamo normalmente. Per intenderci, il sistema operativo e il browser internet. Entrambi questi strumenti hanno al loro interno una serie di strumenti e di configurazioni che ci permettono di aumentare il livello di sicurezza dei nostri computer. La configurazione ha una connotazione più tecnica, richiede che si conosca bene lo strumento, che si sappia dove mettere le mani.

Il problema aggiornamenti è più attuale. Ad esempio, per comprendere più da vicino il problema, non so se a qualcuno di voi sia capitato qualche guaio nell'utilizzo di Internet intorno alla fine di gennaio. In particolare, credo che molti utenti con caselle di posta in Libero dovrebbero ricordarsi notevoli disagi in quel periodo.

Il tutto a causa di 376 caratteri, raggruppati sotto il nome di SLAMMER o SQ HELL.

Questo virus, questo worm, ha infettato i database SQL Microsoft e in due giorni si è replicato in più di 120.000 sistemi. E non stiamo parlando di computer di casa ma di Server aziendali che teoricamente dovrebbero essere un po' più sicuri di una macchina qualsiasi.

Parlando degli effetti di questi 376 caratteri basta pensare che, oltre a Libero, sono rimasti inutilizzabili per un po' 13.000 sportelli bancomat di Bank Of America e, dalle nostre parti, 14.000 sportelli delle poste. E' andata ancora peggio negli Stati Uniti dove alcuni centralini del 911, l'equivalente del nostro 113, sono stati costretti a passare alle operazioni manuali.
Tutto ciò cosa ha che fare con gli aggiornamenti? Ha molto a che fare perché il funzionamento di Slammer si basa su un baco, su un errore, di Microsoft SQL Server trovato e corretto con un aggiornamento disponibile fin da Luglio 2002. Il problema è che nei sistemi infettati questo aggiornamento non era stato fatto.

Conclusioni

Per concludere riprenderemo una frase dell'introduzione:
"L'unico sistema sicuro è un sistema spento ma a quel punto è evidente che quel sistema non serve più a nessuno."

L'utilizzo di Internet a livello personale e aziendale consente di avere a disposizione strumenti e informazioni che in qualsiasi altro modo richiederebbero tempi lunghissimi per essere presi ed elaborati. Il suo sviluppo ci porta oggi ad avere tecnologie che ci permettono di utilizzare la Videoconferenza, Corsi on-line (E-Learning), ascoltare musica e leggere libri.

Anche il legislatore si sta ponendo domande sull'utilizzo di questa tecnologia e sul suo impatto nel quotidiano: è già stata approvata, ad esempio, la normativa che permetterà l'invio del documento Fattura per e-mail e archiviato in un cd.

Per questi ed altri motivi l'utilizzo di Internet sta diventando più una necessità che una scelta.

Per lavorare in sicurezza cosa possiamo fare, quindi? Le domande da porsi sono due e sono la base di una politica della sicurezza:

1. COSA dobbiamo proteggere? Bisogna, cioè, stabilire quali sono le informazioni, i computer e qualsiasi altro bene in nostro possesso che hanno valore per la mia attività e cosa siamo disposti a fare per assicurargli un adeguato livello di protezione.
2. COME possiamo proteggere i nostri dati? E cioè, quali strumenti abbiamo a disposizione e di quali regole ci possiamo dotare per ottenere sicurezza?

La tecnologia offre numerosissimi strumenti a supporto della sicurezza, ed esiste un'ampia documentazione a cui è possibile attingere per creare una politica della sicurezza aziendale.

Si tratta quindi di scegliere gli strumenti adeguati in termini di affidabilità e costo e questo tenendo presente quale è il nostro obbiettivo, cioè che risposta abbiamo dato alla prima domanda.

Breve Glossario.

ADSL : acronimo dell'inglese *Asymmetrical Digital Subscriber Line*. Tecnologia di modulazione del segnale che consente la trasmissione dati ad alta velocità sul tradizionale doppino di rame delle linee telefoniche. Tra le possibilità offerte dall'ADSL ci sono una velocità di collegamento a Internet 30 volte superiore a quella di una linea ISDN, un suono che avverte dell'arrivo di posta elettronica e, contemporaneamente, la normale prosecuzione delle comunicazioni telefoniche.

Browser : programma che consente di navigare alla ricerca di qualcosa; in particolare, abbinato a un protocollo di comunicazione TCP/IP, permette di richiedere, raggiungere e visualizzare il sistema di pagine e di collegamenti ipertestuali del *World Wide Web*. Il primo browser è stato Mosaic, sviluppato da Marc Andreesen nel 1993. Con il tempo sono apparsi browser sempre più perfezionati e versatili. I browser di ultima generazione sono appositamente progettati per sfruttare al meglio le potenzialità di Internet con i sistemi operativi più avanzati delle grandi aziende informatiche; sono costituiti dall'integrazione di un insieme di programmi di utilità destinati a permettere di spedire e ricevere informazioni, dati, immagini, *files* audio, ecc. e di corrispondere con qualsiasi altro utente Internet mediante una gamma più o meno ricca di risorse. Questi browser sono multisessione e perciò, mentre si è in attesa di collegarsi a un sito o del trasferimento di informazioni da una risorsa, si possono eseguire simultaneamente molte altre attività in rete.

Crittografia : Scrittura segreta, tale cioè che il testo è comprensibile solo a chi conosca la chiave crittografica usata.

Client : componente software del modello di architettura *client-server* impiegato per contattare e ottenere dati da un programma *server* residente su un

elaboratore remoto. Il programma client, installato su un personal computer, gli permette di trasferire dati dai *server* della rete informatica a se stesso.

Client-Server : modello di architettura che prevede per ogni utente di una rete di elaboratori la disponibilità di un programma *client* capace di metterlo in relazione con un programma *server* residente in un elaboratore remoto; il *server* contattato fornisce le indicazioni richieste al *client* che le trasferisce sulla macchina su cui è installato, a disposizione dell'utente. Tutti gli strumenti di Internet destinati alla ricerca si servono di questo modello.

Firewall : Programma che filtra gli accessi esterni a una rete in modo da prevenire gli attacchi degli hackers, gli ingressi indesiderati e per limitare il traffico in entrata e uscita ai soli usi previsti.

Firma digitale: Procedura informatica, basata sull'uso di codici alfanumerici, che sostituisce la classica firma autografa con nome e cognome (così come timbri, sigilli, punzoni o contrassegni) per rendere validi documenti, contratti o pagamenti inviati per via telematica a un altro soggetto che sia attrezzato per riconoscerla. In Italia è stata introdotta dalla legge n. 127 del 15 maggio 1997, sulla semplificazione degli atti amministrativi. Punto fondamentale della procedura è un sistema di doppie "chiavi" che consente al sottoscrittore (attraverso una "chiave privata") e al destinatario (tramite una "chiave pubblica"), rispettivamente di rendere manifesta e di verificare la provenienza e l'integrità del documento. Le "chiavi" sono rilasciate da apposite società di certificazione (previste in un albo tenuto dall'AIPA, l'Autorità Informatica per la Pubblica Amministrazione). Le "chiavi" sono sotto forma di *file* o scheda con *microchip*. Ogni coppia di chiavi identificherà una persona o un ufficio.

Host : computer connesso alla rete capace di ospitare utenti e informazioni.

HTML : acronimo di *Hyper Text Markup Language* (linguaggio per la marcatura di ipertesti). Linguaggio di programmazione con il quale sono scritti tutti i documenti ipertestuali destinati al *World Wide Web* (WWW).

HTTP: Acronimo di *Hyper Text Transport Protocol* (Protocollo per il Trasferimento dell'Ipertesto). E' utilizzato per collegare i Web Server in internet. La sua funzione principale consiste nello stabilire una connessione con un Server Web trasmettendo pagine HTML, e altre tipologie di file presenti su tali pagine, al computer Client. Allo scopo di continuare a gestire il sempre più crescente volume di traffico in internet si prevede che questo protocollo verrà modificato (in parte o del tutto) nei prossimi anni.

ISP : acronimo dell'inglese *Internet Service Provider*, utilizzato per indicare i provider Internet, ossia le strutture aziendali che si occupano di fornire connettività e servizi in Internet.

Login : procedura che permette il collegamento con qualsiasi servizio in linea o relativa all'apertura di una sessione di lavoro in un sistema informatico.

Server : elaboratore cui si collegano le risorse comuni di una rete locale.

TCP/IP : acronimo per *Transmission Control Protocol-Internet Protocol* (Protocollo di controllo della trasmissione-protocollo di interconnessione), protocollo di comunicazione inizialmente sviluppato dal Dipartimento della difesa statunitense per le proprie reti geografiche e successivamente diventato uno standard *de facto* nell'interconnessione tra reti. Il protocollo TCP/IP è, come dice il nome stesso, composto da due parti distinte che svolgono funzioni differenti. Il

protocollo IP ha il compito di trasferire le unità dati in cui viene suddiviso il messaggio, chiamate pacchetti, attraverso una o più reti tra loro interconnesse, effettuando le operazioni di indirizzamento, instradamento, frammentazione e riassemblaggio dei pacchetti. Ciò è reso possibile dall'utilizzo nelle reti IP di un indirizzamento universale, mediante il quale ogni *host* connesso alle reti è individuato da un indirizzo univoco. Il *protocollo TCP,* invece, è stato progettato per integrare le prestazioni di rete fornite dal protocollo IP: esso garantisce che i pacchetti siano effettivamente consegnati al destinatario della comunicazione. Il TCP riceve i dati da trasmettere e li passa al modulo IP, che si preoccupa della trasmissione sulla rete dei singoli pacchetti; il TCP verifica poi che i pacchetti IP siano stati trasferiti correttamente e abbiano raggiunto la destinazione. In caso di mancata consegna di un pacchetto, il TCP mette in atto le procedure di ritrasmissione per recuperare il pacchetto mancante.

Virus : con il termine virus si definisce un programma, inserito all'interno del *software* di un elaboratore all'insaputa degli utenti, caratterizzato dalla capacità di autoreplicarsi e potenzialmente pericoloso perché in grado di produrre effetti nocivi o indesiderati. Il virus in genere è formato da due parti. La prima svolge la funzione di duplicazione e comprende segmenti per l'installazione del virus in memoria, la sua copiatura su disco o l'agganciamento a un archivio o a un qualsiasi *file* eseguibile. La seconda, non necessariamente presente, è quella destinata a provocare danni; in genere comprende una sezione di verifica, destinata ad attivare il virus appunto al verificarsi di una determinata condizione, per esempio allo scadere di una certa ora di un dato giorno, e una sezione che esegue le attività previste. La presenza sempre più insidiosa di virus (si stima che i virus circolanti attualmente siano oltre 10.000, mentre nel 1990 ne erano conosciuti appena una settantina) ha stimolato la produzione di programmi capaci di contrastarne gli effetti, i cosiddetti

programmi vaccino o antivirus. I principali responsabili della produzione e diffusione di virus sono gruppi internazionali ben organizzati, che usano essenzialmente la rete Internet per la circolazione e lo scambio di informazioni di ogni genere.

W.W.W. : *World Wide Web*, è il più diffuso e famoso strumento appartenente al mondo di Internet. Il World Wide Web è basato su una architettura *client-server* e gli utenti possono ottenere le informazioni richieste sia dal *server* con cui sono direttamente collegati sia da una qualsiasi altra macchina della rete in qualunque parte del mondo.