Linee guida sulla sicurezza

Indice

Perché proteggere un Computer?

Ogni volta che guidiamo un'automobile ci preoccupiamo di allacciare le cinture di sicurezza, evitiamo di guidare contromano, ci fermiamo quando il semaforo è rosso, suoniamo il clacson per segnalare la nostra presenza a un guidatore un po' distratto che sta uscendo da un posteggio... Poi quando arriviamo, ci preoccupiamo di posteggiarla in un posteggio regolare, possibilmente custodito, di rimuovere le chiavi dal quadro, di chiudere le porte, di inserire l'antifurto (a volte anche due, non si sa mai...) e di non lasciare oggetti di valore in macchina. Per sicurezza abbiamo fatto l'assicurazione contro furto, incendio... In poche parole proteggiamo noi stessi e la nostra auto da incidenti, furti e quant'altro.

E il nostro computer? Ci siamo mai preoccupiate di proteggere il nostro computer? Che rischi corriamo? Quali danni possiamo avere?

Ma no, il computer è al sicuro a casa o in ufficio, e poi è vecchio, non ha un gran valore economico; ma è proprio vero?

Il computer è molto di più di un insieme di componenti (memoria, disco fisso, processo...) e di licenze software (sistema operativo, elaboratore di immagini):

- tramite il mio sito web, faccio conoscere la mia azienda
- per discutere un nuovo contratto utilizzo la posta elettronica
- accedo alle informazioni sugli alberghi per le vacanze
- gestisco il mio conto corrente
- acquisto e vendo su internet
- gestisco tutta la contabilità dell'azienda
- e poi ho memorizzato le foto delle vacanze...

Dunque, proteggere un computer vuol dire non solo proteggere il suo hardware e le sue licenze software ma soprattutto proteggere i dati contenuti sulla macchina.

Si subisce un danno se l'informazione è in qualche modo difettosa o non disponibile oppure se è rivelata a persone non autorizzate.

Assicurare la protezione di un sistema informatico significa preservare le sue risorse dall'uso non autorizzato e salvaguardare le informazioni in esso contenute da letture o manipolazioni non autorizzate, accidentali o deliberate.

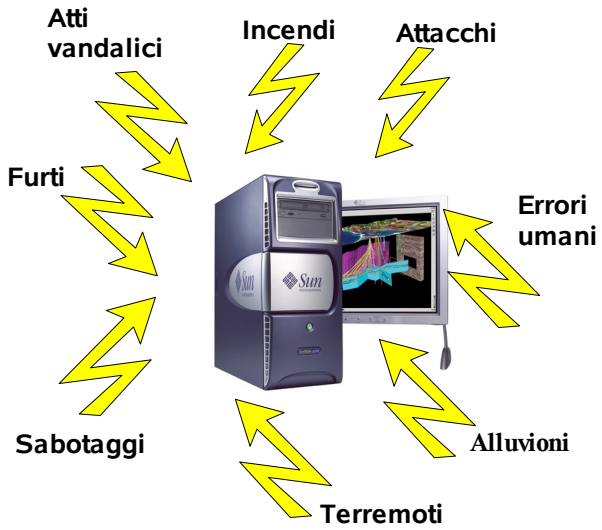
Cosa proteggere?

Il mio computer personale o il sistema informatico della mia aziendale è una risorsa preziosa, da proteggere; ma quali sono le componenti da proteggere? Facile, TUTTE:

- i PC e i server aziendali
- le periferiche (stampanti, fax, dischi esterni...)
- il software installato
- i supporti di memorizzazione (CD, DVD, cassette, dischetti, dischi USB, penne USB...)
- la rete (cavi, apparati di rete...)
- le connessioni di rete (modem, modem ADSL, accesso ad Internet, linee telefoniche dedicati...)
- i dati e i file presenti sui sistemi....

Proteggerlo, ma da che cosa?

Quali sono i rischi? Da che parte arrivano?



Esiste uno specifico settore della sicurezza che si occupa di determinare quelle che sono i fattori di rischio di un sistema informatico e delle organizzazioni che possiedono tali sistemi. Sono stati identificati i seguenti rischi:

- rischi provenienti da disastri naturali
- rischi di fuoco,
- rischi di acqua,
- rischi di sabotaggio,
- rischi di interruzione di servizio,

- rischi di interruzione del sistema di condizionamento,
- rischi di perdita di apparecchiature hardware essenziali,
- rischi di caduta di tensione.

Una minaccia è un'agente ostile che, mediante una specifica tecnica e metodologia oppure un evento casuale, produce un effetto indesiderato su un elemento del sistema.

Riferendosi alle minacce cui è esposto un sistema informatico, si opera una distinzione fra:

- **minaccia non dolosa (o accidentale)**

  Una minaccia è considerata non dolosa quando non esiste un'esplicita volontà di provocare danno. In questa classe rientrano tutti i disastri attribuibili a catastrofi naturali, a fattori accidentali, errori o bug hardware o software, errori involontari commessi dall'uomo.

- **minaccia dolosa (o intenzionale).**

  Una minacce è considerata dolose o intenzionali quando è attuata da una o più persone ed ha un fine doloso, cioè se esiste un'esplicita volontà di provocare un danno o di ottenere un vantaggio illecito.

É possibile suddividere ulteriormente in minacce interne ed esterne al sistema informatico, a seconda se esse sono perpetrate da un entità interna o all'esterna all'ambiente.

Sistemi sotto attacco

Abbiamo visto come un qualsiasi computer è costantemente minacciato. Cerchiamo ora di capire a quale tipo di minaccia è sottoposto.

Un sistema è sicuro se riesce a garantire i seguenti tre obiettivi:

- **disponibilità**
  I proprietari e i legittimi clienti di una risorsa informatica (dato, servizio, programma o componente hardware) possono accedere liberamente alla risorsa, senza ostacoli, rallentamenti od interruzioni.
- **riservatezza**
  Solo i proprietari e i legittimi clienti di una risorsa informatica possono accedere alla risorsa e conoscere il suo contenuto.
- **integrità**
  I proprietari e i legittimi clienti possono accedere a risorse che erogano correttamente il loro servizio e forniscono contenuti esatti.

La lotta fra chi attacca e chi difende un sistema informatico consiste nella lotta per la distruzione o la protezione di uno dei tre obiettivi: un sistema è sotto attacco se qualcuno minaccia la disponibilità, la riservatezza o l'integrità dei dati o del sistemi.

La disponibilità, la riservatezza e l'integrità di un dato o di un sistema possono essere compromesse da un attacco deliberato o da un incidente casuale.

Attaccare deliberatamente un sistema

Gli attacchi deliberati sono un insieme di azioni finalizzate ad interrompere l'erogazione di un servizio (compromissione della disponibilità), ad alterare le informazioni contenute (compromissione dell'integrazione), ad accedere a informazioni protette (compromissione della riservatezza) e ad impossessarsi di una risorsa o di un sistema.

Un hacker (= pirata informatico) quanto attacca un sistema punta ad ottenere:

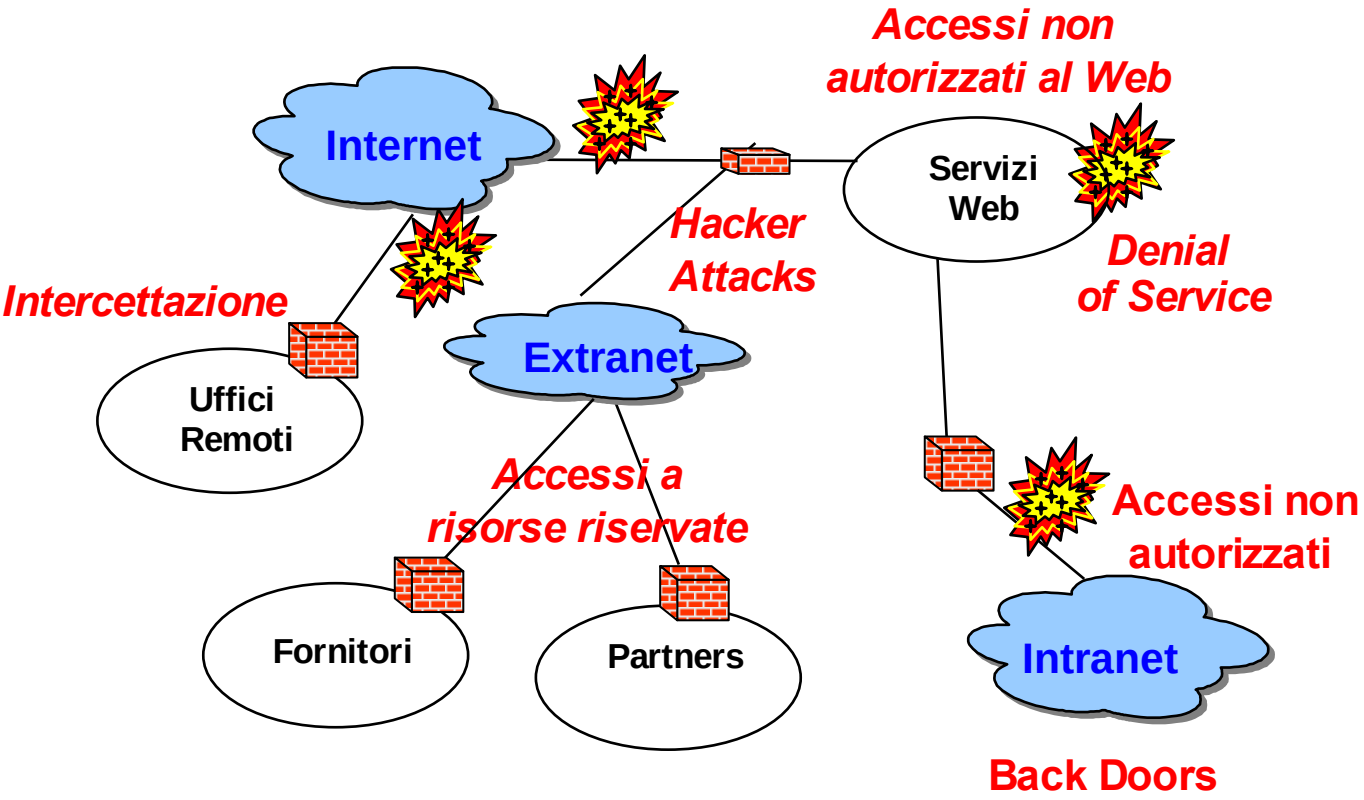
- **una componente fisica**

  Le componenti fisiche sono i calcolatori, gli apparati di reti, le periferiche, i cavi, la connessione alle reti esterne, l'allacciamento con la rete elettrica.

- **una componente logica**

  Le componenti logiche sono il software, i dati e tutte le informazioni trattate nell'ambiente.

Un hacker che vuole attaccare un sistema può percorrere molte strade differenti; proviamo ora ad illustrare le principali.



Attacchi fisici

Gli attacchi fisici sono tutti gli attacchi portati alle componenti fisiche dei sistemi.

Il furto è un attacco di tipo fisico. Dischi USB, nastri, CD, DVD, documentazione in formato cartaceo, portatili, agende - più in generale tutti gli oggetti piccoli - sono i più esposti ai furti, sia perché possono essere facilmente nascosti, sia perché vengono più frequentemente portati fuori dagli uffici. Il furto di oggetti più grossi (server, apparati di reti...) sono un attacco più raro ma comportano un danno molto maggiore.

Il furto compromette la riservatezza, la disponibilità e la riservatezza del sistema informativo.

Un attacco simile al furto è la duplicazione non autorizzata: fotocopiare documentazione in formato cartaceo, duplicare un CD, un DVD o il contenuto di un hard-disk USB... Esso è particolarmente insidioso perché solitamente non lascia tracce e quindi è molto difficile scoprirlo.

Questo attacco compromette la riservatezza dei dati.

Un ultimo tipo di attacco fisico è il danneggiamento o vandalismo in cui le risorse informatiche sono distrutte, manomesse od alterate. Esempi di questo tipo di attacco possono essere la rottura di cavi o di componenti hardware, l'incendio o l'allagamento di una sala macchina...

Questi attacchi compromettono l'integrità e la disponibilità di un servizio ma non la sua riservatezza.

Per proteggere i nostri sistemi da attacchi fisici, possiamo adottare gli stessi accorgimenti che adottiamo per proteggere ogni altro nostro bene (dall'automobile a portafoglio).

Intercettazioni

Le intercettazioni sono attacchi finalizzati ad ottenere illegalmente le informazioni scambiate tra i sistemi.

C'è molta più gente che ascolta di quanto sembra...

Durante una conversazione fra due persone (sia essa una telefonata o due parole scambiate in “privato”) le persone se non rilevano la presenza di una terza persona tendono a considerare la conversazione con riservata e sicura. Una persona male intenzionata può invece ascoltare indisturbato la conversazione (intercettando la telefonata oppure ascoltando da dietro il buco della serratura). Analogamente intercettare sulla rete una comunicazione tra due calcolatori senza essere scoperto è molto più facile di quanto non sembri.

Le tecniche più comuni per eseguire questi tipi di intercettazione sono:

- analisi del traffico in transito sulla rete (sniffingg);

- impersonificazione di un apparato, sistema o utente (spoofing);
- utilizzo di un programma di emulazione di un servizio per ottenere informazioni riservate (ad esempio un programma di emulazione dell'interfaccia

Gli attacchi di tipo sniffing sono particolarmente insidiosi perché si limitano ad ascoltare il traffico in transito sulla rete senza alterarlo. È molto difficile individuare un ascoltatore poiché esso non modifica il traffico e quindi non lascia tracce sulla rete. Risulta fondamentale prevenire le intercettazioni.

Questi attacchi possono sfruttare debolezze intrinseche dei sistemi e dei protocolli oppure configurazioni non adeguate. Le intercettazioni violano la riservatezza dei dati e, nei casi di spoofing e emulazione, possono violare anche l'integrità dei dati.

Le contromisure tipiche per questi attacchi sono:

- sistemare gli apparati di rete e i cavi di connessione in luoghi sicuri
- suddividere le rete in più sottoreti e definire regole precise per il passaggio di informazioni tra le varie sottoreti
- limitare i diritti di installazione dei software sui sistemi
- controllare i punti di accesso alla rete per i portatili ed eventualmente provvedere ad un sistema di autenticazione degli stessi
- **prevedere comunicazioni crittate che rendono inservibili qualunque informazioni catturata sulla rete**

Intrusione

L'intrusione su un sistema permette all'attaccante di impossessarsi della macchina e di compromettere l'integrità, la privacy e la disponibilità di un servizio.

Una persona che si introduce illegalmente nell'abitazione di un'altra persona può avere diverse motivazioni: può essere un ladro, può essere un vandalo che si diverte a distruggere la proprietà altrui o può essere un concorrente che vuole fotografare le carte relative a un progetto aziendale segreto. Analogamente un hacker può introdursi sul sistema per svariate ragioni e al variare di esse può lasciare tracce più o meno evidenti del suo passaggio.

Se non sono stati adottati strumenti particolarmente robusti di autenticazione, il punto di accesso più comune a un sistema, o a un'applicazione, è carpire la password di un ignaro utente ed accedere al

sistema identificandosi come la vittima. Un hacker può impossessarsi della password ascoltando il traffico di rete e leggendo i dati di autenticazione in transito in chiaro sulla rete (intercettazione) oppure può dedurla partendo da informazioni note sulla persona (nome, data di nascita, indirizzo, cantante preferito...).

Le contromisure tipiche per questi attacchi sono:

- **crittare le sessioni di autenticazione;**
- **utilizzare sistemi robusti di autenticazione;**
- definire regole per la scelta di password sicure;
- bloccare una login dopo un certo numero di tentativi falliti di accesso.

Tralasciando l'intrusione tramite password ottenuta illecitamente, un pirata può accedere al sistema usando tecniche più raffinate. In questi casi gli attaccanti possono sfruttare bachi dei programmi, configurazioni sbagliate o servizi lasciati inavvertitamente aperti...

Per individuare i punti possibili di accesso al sistema, i pirati ricercano le porte TCP e UDP aperte sui sistemi e i servizi attivi dietro a queste (“probing del sistema”).

Le contromisure tipiche per questi attacchi sono:

- configurare i programmi in modo accurato e coerente con i consigli fornite dal produttore;
- disattivare e rimuovere di tutto il software inutilizzato;
- effettuare l'hardening e la minimizzazione dei sistemi e delle applicazioni;
- restringere le politiche di accesso dei firewall;
- aggiornare periodico patch e hot fix.

Al variare delle intenzioni dell'hacker si possono avere di volta in volta delle violazioni della riservatezza, dell'integrità o della disponibilità dei dati.

Attacchi di deduzione

Gli attacchi di deduzione sono condotti ottenendo informazioni riservate sui sistemi incrociando dati provenienti da fonti differenti, lecite e illecite.

Alcune informazioni possono essere ottenute in maniera lecita, come i nomi delle macchine che erogano i servizi o il software installato sulle macchine. Altre informazioni sono fornite da altri attacchi portati al sistema, dalla scansione della rete, al probing o alle intercettazioni.

Quest’attacco analizza le informazioni pubbliche integrandole con quelle ottenute con mezzi illeciti al fine di individuare elementi utili sulla struttura dell'ambiente informatico e sui suoi punti deboli. Queste informazioni possono poi essere utilizzate per successivi attacchi.

Per esempio, un hacker può utilizzare i dati forniti dal comando di sistema "finger", per individuare gli utenti presenti sul sistema, e formulare delle ipotesi sulle loro password tramite i loro dati personali pubblicati su un'altro sito.

Per evitare questi tipi di attacchi bisogna valutare quali informazioni possono essere rese disponibili agli utenti, rimuovendo qualunque dato sensibile non necessario. Strumenti di Intrusion Detection e di correlazione degli eventi possono evidenziare un insieme di operazioni che prese singolarmente risultano essere ragionevoli ma che eseguite insieme indicano un attacco in corso.

Tramite gli attacchi di tipo deduzione un pirata può compromettere la riservatezza delle informazioni.

Virus

I virus sono programmi autoreplicanti che si propagano sulla rete. Essi si riproducono degradando le prestazioni dei sistemi ed eseguono operazioni non lecite manomettendo dati e sabotando i sistemi. Nella classificazione dei virus sono considerati i

- il tipo di danno che comportano (variazione della data e dell'ora, modifica delle configurazioni dei sistemi, modifica e cancellazione dei file presenti nei sistemi, diffusione di file e informazioni…)
- modalità di infezione, cioè lo strumento che utilizzano per propagarsi (allegati di posta elettronica, macro-virus nascosti nei file di documentazione, virus presenti in pagine web...)
- modalità di mimetizzazione, cioè la capacità di nascondersi e non farsi individuare.

I virus compromettono l'integrità e la disponibilità dei servizi; alcuni virus minacciano anche la riservatezza dei dati.

Il sistema privilegiato per proteggere gli ambienti dai virus è l'utilizzo di anti-virus integrato con un aggiornamento periodico delle patch e degli hot fix e un'adeguata politica di sicurezza.

Back door

Un ladro che svaligia una casa non ha alcun interesse a ritornarci, rischia solo di essere scoperto mentre una spia dell'azienda concorrente ha interesse a ritornare più volte per accedere i documenti portati a casa dell'ignara vittima. Per questa ragione la spia cercherà, una volta entrato di farsi copia del mazzo di chiavi di casa per poter ritornare indisturbato. Analogamente molti hacker una volta entrati su un sistema tendono ad installare degli accessi riservati al sistema per poter tornare

indisturbato sulla macchina. Questi punti di accesso nascosto si

In caso di intrusione, l'analisi delle configurazione, dei file e del software, che va sotto il nome di analisi forense, permette di rilevare le porte nascoste introdotte e il software modificato dal pirata. Permettendo un libero accesso ai sistemi, tramite le Back Door un intruso può compromettere l'integrità, la riservatezza e la disponibilità dei sistemi.

Denial Of Service

I Denial of Service o “interruzioni di servizio” sono attacchi finalizzati ad impedire l'erogazione di un servizio da parte di un sistema. Essi non violano l'integrità o la riservatezza dei dati, ma rendono i servizi non disponibili ai legittimi utenti.

Comunemente questi attacchi tentano di saturare la banda inviando pacchetti che si propagano a catena.

Una corretta configurazione della rete e dei sistemi riduce il numero di possibili servizi sfruttati negli attacchi di tipo “Denial of Service”. Inoltre una corrette configurazione di firewall, gateway e apparati di rete permette di bloccare l'inutile propagazione dei pacchetti.

Social Engineering

Il "Social Engineering" cerca di carpire, con l'inganno o con la corruzione, informazioni utili dai dipendenti di un'azienda.

Il fattore umano risulta spesso essere l'anello più debole di un'architettura di sicurezza. Quando tutte le altre strade risultano inutili un pirata riesce ad ottenere molte informazioni riservate proprio grazie a questo tipo di attacco.

I modi tramite cui un pirata può carpire informazioni sono diverse.

- **Corruzione**
  La corruzione di un dipendente è un classico esempio di questi tipi di attacchi. Le persone potenzialmente più vulnerabili sono quelle che accedono a informazioni molto riservate ma ricoprono un ruolo “secondario” nell'azienda e male retribuito.
- **Ricatto**

  Questo sistema risulta più economico del precedente ma di più difficile attuazione. Può risultare molti difficile ottenere informazioni riservate su una persona utili per ricattarla.

- **Inganno**

  Un modo efficace ed economico di carpire le informazioni è sfruttare la buona fede e la disponibilità delle persone. Per realizzare questo tipo di attacco si contatta (di solito telefonicamente) un impiegato impersonando un superiore, o un altro collega, e richiedendogli informazioni riservate sull'azienda. Il pirata assume un tono e un atteggiamento minaccioso per intimorire la persona con cui sta comunicando ("...non sai con chi stai parlando....", "...queste informazioni servono per un importantissimo meeting organizzato al massimo livello aziendale...", "...dovrò informare Mr. Tizio che solo la sua divisione si è rifiutata di fornire queste informazioni....", "...il tuo rifiuto produrrà danni per l'Azienda e conseguenze disciplinari per te...").

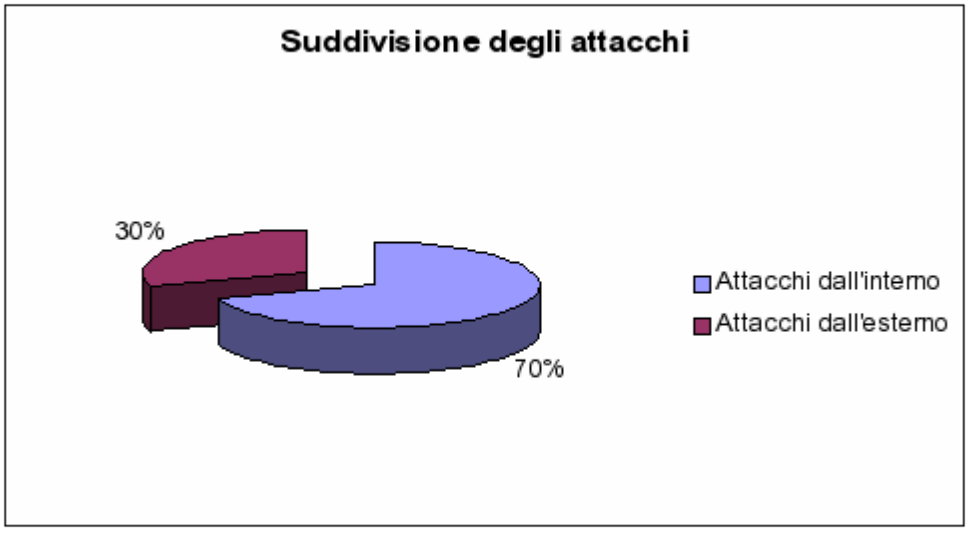
  

  Un'adeguata formazione del personale e un piano per la segnalazione degli incidenti può fare molto per ridurre il fattore umano. È infatti più difficile ingannare un dipendente adeguatamente formato e in grado di distinguere le richieste lecite da quelle illecite.

Tramite gli attacchi di tipo Social Engineering, un pirata può compromettere la riservatezza delle informazioni. Se il pirata è particolarmente bravo può anche compromettere la disponibilità e l'integrità dei sistemi e dei dati.

Gli attacchi possono venire dall'esterno, se sono condotti da una persona estranea all'ambiente, oppure dall'interno, se sono condotti da un dipendente, un socio, un collaboratore, un fornitore, un cliente, un partner. Gli attacchi interni sono molto più diffusi di quelli dall'esterno.

Il grafico riassume la distribuzione degli attacchi
fra interni ed esterni negli anni 2000-2001 (fonte CSI/FBI).



Crimini informatici

Gli attacchi deliberati ai sistemi informatici, oltre ad essere immorali, sono illegali. I reati informatici sono stati introdotti dalla legge n.547 del 23 dicembre 1993 "*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*".

Riportiamo un estratto del testo della legge con la descrizione dei reati informatici.

Art. 1 *1. All'art. 392 del codice penale, dopo il secondo comma è aggiunto il seguente:*

"Si ha, altresì, violenza sulle cose allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico".

Art. 2 *1. L'art. 420 del codice penale è sostituito dal seguente:*

*"Art. 420. - (**Attentato a impianti di pubblica utilità**).-Chiunque commette un fatto diretto a danneggiare o distruggere impianti di pubblica utilità è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a quattro anni.*

La pena di cui al primo comma si applica anche a chi commette un fatto diretto a danneggiare o distruggere sistemi informatici o telematici di pubblica utilità, ovvero dati, informazioni o programmi in essi contenuti o a essi pertinenti.

Se dal fatto deriva la distruzione o il danneggiamento dell'impianto o del sistema, dei dati, delle informazioni o dei programmi ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema, la pena è della reclusione da tre a otto anni".

Art. 3 *1. Dopo l'art. 491 del codice penale è inserito il seguente:*

*"Art. 491-bis. - (**Documenti informatici**).- Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente agli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli".*

Art. 4 *1. Dopo l'articolo 615-bis del codice penale sono inseriti i seguenti:*

*"Art. 615-ter. - (**Accesso abusivo a un sistema informatico o telematico**). - Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.*

La pena è della reclusione da uno a cinque anni:

I) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in essi contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici d'interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

*Art.615-quater. - (**Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici**). Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a un anno e con la multa sino a lire 10 milioni.*

La pena è della reclusione da uno a due anni e della multa da lire 10 milioni a 20 milioni se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617-quater.

*Art. 615-quinquies. - (**Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico**). -Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi un esso contenuti o a esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a lire 20 milioni".*

Art. 5 *1. Nell'art. 616 del codice penale, il quarto comma è sostituito dal seguente:*

"Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza".

Art. 6 *1. Dopo l'art. 617-ter del codice penale sono inseriti i seguenti:*

*"Art. 617-quater. - (**Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche**). - Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.*

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo d'informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri e con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;

3) da chi esercita anche abusivamente la professione di un investigatore privato.

*Art. 617-quinquies. - (**Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche**) .- Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.*

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617-quater.

*Art. 617 sexies. - (**Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche**). - Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro armi.*

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma del l'art. 617-quater".

...

Art. 9 *1.Dopo l'art. 635 del codice penale è inserito il seguente:*

*"Art. 635-bis. - (**Danneggiamento di sistemi informatici e telematici**). - Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.*

Se ricorre una o più delle circostanze di cui al secondo comma dell'art. 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni".

Art. 10 *1. Dopo l'art. 640 bis del codice penale è inserito il seguente:*

*"Art. 640-ter. - (**Frode informatica**). - Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità sui dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire 100 mila a 2 milioni.*

La pena è della reclusione da uno a cinque anni e della multa da lire 600 mila a 3 milioni se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'art. 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante".

Eventi accidentali

Affianco agli attacchi portati deliberatamente ai sistemi, l'integrità, la riservatezza o la disponibilità di un sistema può essere compromessa da un guasto (rottura hardware o errore software) oppure da un errore umano (cancellazione di un file sbagliato, l'inserimento di un dato sbagliato...) o da una calamità naturale (alluvione, terremoto, uragano...). Pur essendo eventi accidentali (avvenuti senza malizia da parte di nessuno), essi possono provocare grossi danni di sicurezza. Per questa ragione le misure di sicurezza adottate devono prevedere la gestione non solo di attacchi informatici ma anche di errori accidentali.

Gli errori umani costituiscono infatti la causa principale per la perdita accidentale dei dati. Per proteggere i sistemi da questi rischi possiamo prevedere delle interfacce mirate per facilitare la gestione dei dati e ridurre gli errori di incongruenza e limitare l'accesso degli utenti solo all'aria di loro competenza. In sintesi riduciamo il rischio di errori accidentali limitando l'insieme di operazioni fornite agli utenti e controllando la validità dei dati immessi.

Accanto a questi incidenti ci sono eventi legati all'ambiente in cui si trovano le macchine: rottura degli impianti di condizionamento, interruzione della corrente elettrica o rotture delle tubature dell'acqua. Ci sono infine calamità naturali come incendi, terremoti o alluvioni.

Un adeguato piano di salvataggio dei dati e di ripristino dei sistemi, permette di recuperare i danni provocati ai sistemi. Proprio per far fronte agli eventi più disastrosi una buona regola è di conservare una copia dei file di sistemi e dei dati in una sede distinta (possibilmente in un'altra città).

Contromisure

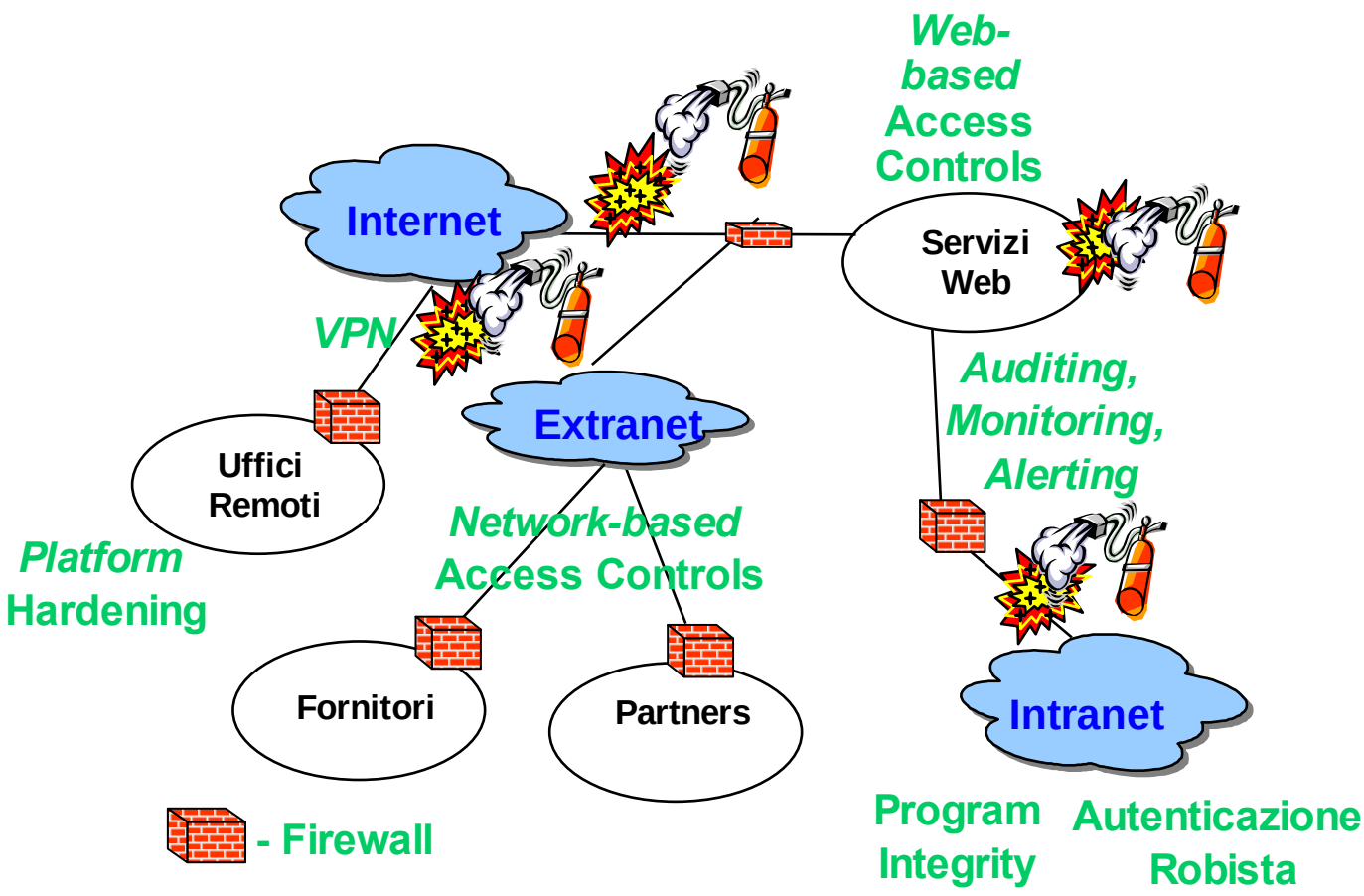
I capitoli successivi illustreranno dettagliatamente le contromisure che si possono adottare contro attacchi alla sicurezza ed errori accidentali.

Prima di esaminare in dettaglio se singole azioni, evidenziamo che esse si distinguono in:

- **azioni preventive**
- **azioni correttive.**

Le prime sono finalizzate a ridurre i rischi di violazioni delle sicurezza; le seconde sono finalizzare a individuare gli attacchi e a porre rimedio ai danni provocati.

Le contromisure possono essere di tipo logico se agiscono a livello di software e di flusso di dati o di tipo fisico se agiscono sugli apparati fisici (calcolatori, cavi, apparati di rete o periferiche) e di accessi fisici agli ambienti.


Web-based Access Controls
Internet
Servizi Web
VPN
Extranet
Auditing, Monitoring, Alerting
Uffici Remoti
Network-based Access Controls
Platform Hardening
Fornitori
Partners
Intranet
- Firewall
Program Integrity
Autenticazione Robista

Come quantificare i rischi?

Se dobbiamo spedire una collana del valore di 100.000 Euro allora troveremo vantaggioso ingaggiare una società di trasporto valori per una spesa di 100 Euro. Se invece spediamo un libro del valore di 10 Euro, la società di trasporto valori fornisce ancora un servizio interessante? Ovviamente no. Nel secondo caso l'investimento per la protezione del libro è superiore al rischio di danno derivante dalla sua perdita.

Analogamente nel campo informatico, prima stimiamo i rischi connessi all'ambiente informatico e poi decidiamo l'investimento per la sua protezione. Per proteggere adeguatamente i propri beni senza uno spreco di risorse economiche, valutiamo il beneficio (come riduzione del rischio) e il costo di tutte le contromisure e scegliamo solo le contromisure il cui beneficio è superiore al costo.

Analisi del rischio

L'analisi del rischio identifica e quantifica i rischi connessi all'ambiente informatico e le vulnerabilità che li causano. In campo finanziario il rischio connesso ad un bene è pari al prodotto tra il costo derivante da un evento non desiderato e la probabilità del verificarsi dell'evento stesso.

Prima di tutto identifichiamo e cataloghiamo i nostri beni informatici.

- **Dati e informazioni.**

  Questa categoria raccoglie tutte le informazioni trattate dall'ambiente informatico: i file personali, il contenuto dei database, i siti web, le informazioni archiviate sui Media, i dati inseriti negli applicativi, la posta elettronica, le informazioni in transito sulla rete...

- **Documentazione.**

  Questa categoria raccoglie la documentazione in formato cartaceo ed elettronica: i manuali, la documentazione dei progetti, il disegno della rete, il suo piano di indirizzamento, la politica di sicurezza, i report sulle attività di manutenzione...

- **Hardware.**

  Questa categoria raccoglie calcolatori, terminali, tastiere, dischi, memoria, apparati di rete, cavi, alimentatori della corrente, stampanti, fotocopiatrici, fax...

- **Software.**

  Questa categoria raccoglie sistemi operativi, applicativi, script, file di configurazioni, codici sorgente, programmi per il controllo dell'ambiente, tool per l'amministrazione...

- **Supporti multimediali.**

  Questa categoria raccoglie i Media: carta, dischetti, nastri, CD, DVD, palmari, cassette....

- **Licenze.**

  Questa categoria raccoglie le licenze dei Software, le bolle di consegna dell'Hardware e i contratti di manutenzione.

- **Persone.**

  Nel caso di enti o società, questa categoria raccoglie il personale aziendale, con la propria esperienza e formazione professionale.

- **Reputazione, immagine e prestigio.**

  La reputazione di una persona o di un'aziendale è molto importante.

  Un danno alla sua immagine spesso è maggiore di un danno a un suo bene materiale, poiché riconquistare il prestigio perso richiede grosso investimento e tempi lunghi.

Per ogni bene da proteggere l'analisi del rischio definisce i costi derivanti da eventi non desiderati e le loro probabilità di accadere.

Per stabilire i costi l'analisi identifica, per ogni bene, i suoi requisiti di sicurezza. I requisiti più comuni sono la disponibilità, l'integrità e la riservatezza. A questi si affiancano, volta per volta, requisiti specifici come la sicurezza fisica, il non ripudio, specifici requisiti di legge... L'analisi individua le minacce o eventi indesiderati che possono portare alla perdita di totale o parziale di uno di questi requisiti. Esempi tipici di minacce sono il furto, l'interruzione di servizio, gli atti vandalici, le calamità naturali, gli accessi non autorizzati... Per ognuna di questi possibili eventi indesiderati, l'analisi stima la probabilità del verificarsi dell'evento e l'impatto sui requisiti di sicurezza e quindi il suo costo.

Esistono tool e metodologie che affiancano e guidano la fase di analisi del rischio, definendo le tematiche da analizzare e i parametri da considerare. Questi strumenti forniscono la struttura e le indicazioni delle componenti dell'ambiente da considerare, le potenziali vulnerabilità associate alle varie componenti. Tuttavia la quantificazione del rischio è a carico dell'analista.

Le difese informatiche: Politiche e Meccanismi

Nei precedenti capitoli abbiamo visto che un sistema informati è esposti a molti rischi. Cerchiamo ora di capire quali difese possiamo mettere in campo per proteggere i computer e le reti. Parleremo quindi di:

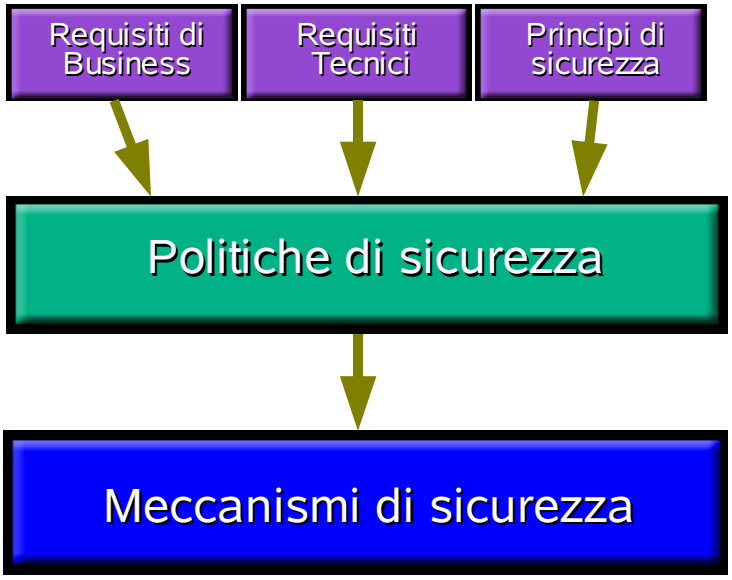
- **Politiche di Sicurezza**

  Le politiche di sicurezza sono delle linee guida ad alto livello che devono essere seguite nel progetto, nell'implementazione e nella gestione dell'ambiente informatico.

  Quindi le politiche decidono cosa sarà fatto.

- **Meccanismi di Sicurezza**

  I meccanismi di sicurezza sono l'insieme di funzioni che realizzano la politica di sicurezza. Quindi i meccanismi decidono come sarà fatto.



È fondamentale separare le Politiche di Sicurezza dai Meccanismi per aumentare la flessibilità delle soluzioni adottate e semplificare la loro gestione. Ad esempio se cambiamo il software antivirus con un altro prodotto, se la politica di sicurezza è ben distinta dai meccanismi utilizzati allora il cambio dell'antivirus comporta un aggiornamento minimo delle politiche; d'altra parte se la politica di sicurezza è strettamente collegata ai meccanismi implementati allora al variare dell'antivirus corrisponde una revisione sistematica della politica. Le Politiche di Sicurezza sono soggette a frequenti cambiamenti, ad esempio al variare delle legislazioni vigenti, quindi più i meccanismi di implementazione sono generali e indipendenti minori sono i cambiamenti richiesti a seguito di una modifica della politica.

Nella definizione della politica di sicurezza bisogna innanzi tutto valutare l'ambiente informatico ed evidenziate i requisiti di sicurezza generali che il sistema dovrà possedere. Per garantire questi requisiti e per contrastare le minacce, andremo ad agire in tre momenti distinti:

- **Prevenzione**:

  "Meglio prevenire che curare..."

  Basandosi su questa logica, definiremo nella politica di sicurezza tutte le regole necessarie per proteggere i nostri sistemi da attacchi o da incidenti e metteremo in campo tutti i meccanismi necessari per realizzare le politiche di sicurezza.

- **Controllo**:

  Controlleremo periodicamente tutti i sistemi ricercando attacchi o guasti e interverremo, in caso di necessità, per gestire e risolvere gli eventuali problemi rilevati. Se rileviamo un attacco in corso riusciremo più facilmente ad identificare gli hacker e a procedere legalmente contro di loro.

- **Ripristino**:

  Se gli strumenti di prevenzione e controllo non riescono a contrastare un attacco, risulta fondamentale avere la possibilità di ripristinare le informazioni e i servizi nel minor tempo possibile. Quindi dovremo prevedere a priori il salvataggio periodico di tutte le informazioni e le procedure per il ripristino dei dati e dei servizi.

Come valutare il livello di sicurezza di un sistema informatico

Per valutare le caratteristiche di sicurezza di un sistema informatico, bisogna valutare qual è il suo livello di trustworthiness.

Trustworthiness è la misura in cui l'utente può affidare al sistema informazioni di valore e contare su di esso perché per garantire l'integrità, la riservatezza e la disponibilità delle informazioni gestite.

La trustworthiness copre i seguenti aspetti.

- **Accessibilità:** le informazioni devono essere accessibili unicamente agli utenti aventi diritto
- **Disponibilità:** le informazioni devono essere il più possibile disponibili anche a fronte di malfunzionamenti.
- **Continuità:** i sistemi che erogano i servizi non devono causare discontinuità del servizio.
- **Integrità:** l'informazione deve essere protetta contro la modifica accidentale o deliberata.
- **Tempismo:** i tempi di ripristino a fronte di malfunzionamenti accidentali o dolosi devono essere minimi.


Disponibilità
Confidenzialità
Trustworthiness
Integrità
Accedibilità
Tempismo

Politica di sicurezza: cos'è?

Consideriamo,ad esempio, i proprietari di due villette vicine e che partono entrambi per le vacanze.

La prima persona ha fatto installare un sistema di antifurto ultimo modello per la propria villetta e vetri antisfondamento alle finestre, ma poi parte dimenticandosi di inserire l'antifurto, lasciando le chiavi di casa nascoste sotto un vaso di fiori di fianco alla porta (non si sa mai che perda la mia coppia di chiavi) e lasciando la finestra della sala socchiusa (vetro e persiane) per evitare che si formi troppo umidità per le piante.

La seconda persona ha installato un sistema di antifurto ormai vecchio di alcuni anni, ma lo fa revisionare periodicamente. Prima di partire cambia le pile dell'antifurto con pile nuove, chiude tutte le finestre e le persiane, inserisce l'antifurto, chiude a chiave la casa e si porta via una seconda copia delle chiavi di casa per precauzione.

Il secondo proprietario ha protetto meglio la propria casa prima di partire perché ha saputo usare gli strumenti a disposizione per la protezione della propria casa. Dunque per proteggere un qualsiasi nostra proprietà, sia essa una casa o un sistema informatico, non basta possedere degli strumenti o meccanismi di protezione ma è necessario avere regole di comportamento per rendere questi strumenti efficaci.

Una “Politica di Sicurezza” è l'insieme organico delle regole formali per il corretto utilizzo degli strumenti a protezione di un proprio bene.

La “Politica di Sicurezza Informatica” è l'insieme organico delle regole formali che definiscono la modalità di gestione degli strumenti informatici e dei dati dell'azienda o dell'ente in esame.

Il suo **obiettivo** è quello di garantire il **trustworthiness** del sistema informatico: cioè l'accessibilità, la disponibilità, la continuità, l'integrità e il tempismo del sistema informatico.

Il suo **scopo** primario è formare gli utenti e il personale sui requisiti essenziali per garantire la sicurezza dell'ambiente informatico e illustrare le tecniche, le tecnologie e gli strumenti per realizzare tali requisiti.

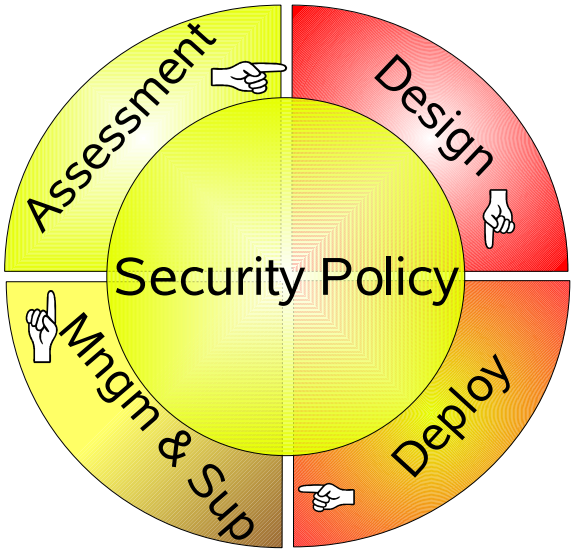
La struttura base di una buona politica di sicurezza informatica illustra:

- I principi e gli obiettivi di sicurezza.
- Le regole di sicurezza aziendale.
- Le attività consentite e quelle proibite.
- Le procedure operativo o modalità per applicare la politica all'ambiente.
- L'indicazione delle responsabilità dei singoli.

Consigliamo di definire una “Politica di Sicurezza” flessibile, comprensibile, realistica, consistente

e applicabile al contesto aziendale o personale. Il suo successo dipende notevolmente dalla sua flessibilità, cioè dalla sua capacità di definire le regole chiavi per realizzare la sicurezza informatica indipendentemente dai sistemi e/o dal software.

Per non perdere la propria efficacia, la Politica di Sicurezza richiede di essere aggiornata nel tempo, tenendo presente l'evolversi da una parte delle tecniche di attacco e dall'altra delle esigenze di sicurezza dell'ambiente.



Documentazione

Per condividere la Politica di Sicurezza informatica, suggeriamo di formalizzarla in un documento contenente:

- la definizione degli obiettivi
- i principi, gli standard e le regole da osservare
- le procedure operative per la gestione dell'ambiente informatico
- le procedure operative per il salvataggio dei dati
- le procedure da adottare in caso di guasto, malfunzionamento o sabotaggio
- la definizione delle responsabilità degli individui
- i riferimenti ai documenti che possono supportare ed integrare la Politica di Sicurezza

DPS (Documento programmatico sulla sicurezza)

Chiunque gestisce dati personali e sensibili altrui è tenuto a produrre un "documento programmatico sulla sicurezza" (DPS) in cui descrive le misure adottate per proteggere l'accesso ai dati sensibili.

Questo documento, aggiornato ogni anno entro il 31 Marzo di ogni anno, descrive:

- le tipologie di dati sono trattati,
- i sistemi coinvolti nel trattamento di questi dati,
- le misure di sicurezza in essere e da adottare per proteggere questi dati,
- gli strumenti tecnologici utilizzati,
- gli interventi formativi per aggiornare il personale aziendale.

Una stesura completa e dettagliata del DPS, oltre ad essere un obbligo di legge (D.Lgs. n. 196 del 30 giungo 2003), fornisce un'adeguata analisi dei rischi a cui è esposto il sistema e delle possibili contromisure. Il DPS può essere quindi visto non come un costo per l'azienda ma come un'opportunità e un buon punto di partenza per la definizione di una Politica della Sicurezza Informatica.

Per garantire un adeguato livello di sicurezza dei dati, non è sufficiente un DPS esaustivo, ma è necessario poi realizzare tutte le nuove misure descritte e seguire le costantemente tutte le procedure definite.

I requisiti di legge inerenti al DPS

Per il trattamento di dati personali e sensibili, il Decreto Legislativo n. 196 del 30 giugno 2003, "*Codice in Materia di protezione dei dati personali*", fornisce i requisiti di legge sulla definizione del documento programmatico sulla sicurezza, sulle istruzioni da fornire agli utenti e sui controlli periodici da effettuare...

L'articolo 34 e l'appendice B di questa legge forniscono indicazioni precise sul DPS e sulle politiche da adottare informatica richiesti dalla legislazione vigente.

Art. 34 Trattamenti con strumenti elettronici

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

1. *autenticazione informatica;*
2. *adozione di procedure di gestione delle credenziali di autenticazione;*
3. *utilizzazione di un sistema di autorizzazione;*
4. *aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;*
5. *protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;*
6. *adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;*

7. *tenuta di un aggiornato documento programmatico sulla sicurezza;*
8. *adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.*

Appendice B

Art. 4 *Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.*

...

Art. 10 *Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.*

...

Art. 14 *Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.*

Art. 15 *Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.*

Art. 16 *I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.*

Art.17 *Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.*

Art. 18 *Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.*

Art. 19 *Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:*

1. *l'elenco dei trattamenti di dati personali;*
2. *la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;*
3. *l'analisi dei rischi che incombono sui dati;*
4. *le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;*
5. *descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;*
6. *la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;*
7. *la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;*
8. *per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.*

...

Art 21 *Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.*

Art. 22 *I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.*

Art. 23 *Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.*

Art. 24 *Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi*

all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

I miei sistemi informatici sono a posto con la legge?

La continua evoluzione del settore informatico comporta un continuo aggiornamento delle legislazioni legate al settore informatico. Negli ultimi anni, per contrastare l'aumento dei crimini informatici e del danno prodotto all'economia, sono stati introdotti requisiti minimi di legge che devono essere adottati da chi gestisce sistemi informativi e da chi tratta dati personali altrui.

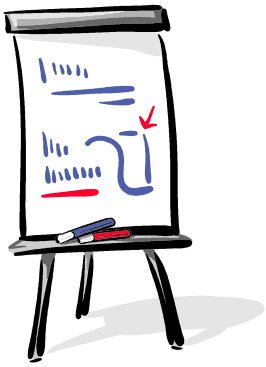
Con questi cambiamenti legislativi non è più sufficiente che una persona non danneggi deliberatamente i sistemi altrui per essere a posto con la legge. Essa deve anche adottare delle misure minime di protezione (stabilite dalla legge) per proteggere i propri sistemi da accessi illeciti e impedire che i criminali li utilizzano per attaccare altri sistemi.

È quindi importante che i gestori dei sistemi informativi si mantengano sempre aggiornati in campo legislativo...

Un riferimento, soprattutto per gli enti pubblici, in campo di legislazioni informatiche è il CNIPA (Centro Nazionale per Informatica nella Pubblica Amministrazione). Questa authority è responsabile della definizione delle linee guida e la stesura delle regole tecniche di attuazione per l'uso dell'informatica nella Pubblica Amministrazione.

Consigliamo, in fine, una stretta collaborazione tra la divisione dei sistemi informativi e l'ufficio legale. Quest'ultimo, in particolare, deve segnalare tempestivamente ogni nuova legge applicabile all'ambiente informatico ai gruppi dei sistemi informativi.

Come realizzare progetti sicuri?



Nei progetti vengono comunemente usate informazioni riservate sia dell'azienda sia di eventuali clienti o partner. Per questa ragione i progetti, se non gestiti correttamente possono diventare dei buchi di sicurezza. In questo capitolo presentiamo il ciclo di vita dei progetti, focalizzando l'attenzioni sulle relative problematiche di sicurezza e sulle contromisure da adottare.

Sicurezza nel ciclo di vita dei progetti

Illustriamo brevemente le principali fasi di vita di un progetto e requisiti di sicurezza specifici.

1. **Definizione e pianificazione**

   In questa fase individuiamo le nuove esigenze, studiamo le cause e le motivazioni dei nuovi bisogno e analizziamo le componenti del sistema coinvolte. Confrontiamo alcune possibili soluzioni, corredate da uno studio sugli impatti di ciascuna sul sistema e scegliamo la soluzione più appropriata.

   I principali requisiti di sicurezza di questa fase sono:

   - individuare gli elementi critici da proteggere
   - identificare i requisiti di sicurezza degli elementi critici
   - identificare i requisiti di legge relativi agli argomenti trattati dai progetto
   - scegliere i partecipanti al progetto e verificare le loro conoscenze
   - per progetti complessi, definire le responsabilità di ciascuna persona

2. **Sviluppo e acquisizione.**

   In questa fase studiamo come realizzare praticamente la soluzione scelta, disegnandola e scegliendo le sue componenti. Procediamo all'acquisto e/o allo sviluppo delle sue componenti.
   In questa fase è essenziale individuare, richiedere e includere i requisiti di sicurezza nella realizzazione della nuova soluzione. Realizzare prima un sistema e poi studiare gli accorgimenti per garantire la sua sicurezza è sempre più costoso. Gli interventi a posteriori a volte portano a soluzioni di compromesso che limitano sia le potenzialità del sistema che il livello di sicurezza dello stesso.

   La sicurezza di una soluzione è pari alla sicurezza del suo anello più debole: ogni singola componente insieme alla sua integrazione con il sistema deve soddisfare tutti i i requisiti di sicurezza richiesti.

3. **Implementazione.**

   In questa fase vengono installate, configurate e testate le nuove componenti e la loro integrazione con le componenti esistenti.

   Fra i vari test consigliamo di dare sempre un'adeguata importanza **ai test sulla sicurezza del**

sistema. Quando la soluzione ha superato felicemente tutti i test, il nuovo sistema o processo viene inserito nell'infrastruttura esistente.

Consigliamo di **formare gli utenti** sul funzionamento della soluzione e sui suoi requisiti di sicurezza poiché un loro errore potrebbe sempre compromettere la sicurezza del nuovo servizio.

4. **La fase operativa e di manutenzione.**

   In questa fase il sistema eroga il suo servizio ai clienti.

   Esso è sottoposto alle operazioni di manutenzione ordinaria (come l'aggiornamento degli utenti) e straordinaria (come l'aggiornamento ad una versione successive o la sostituzione di una componente guasta).

   I principali requisiti di sicurezza di questa fase sono:

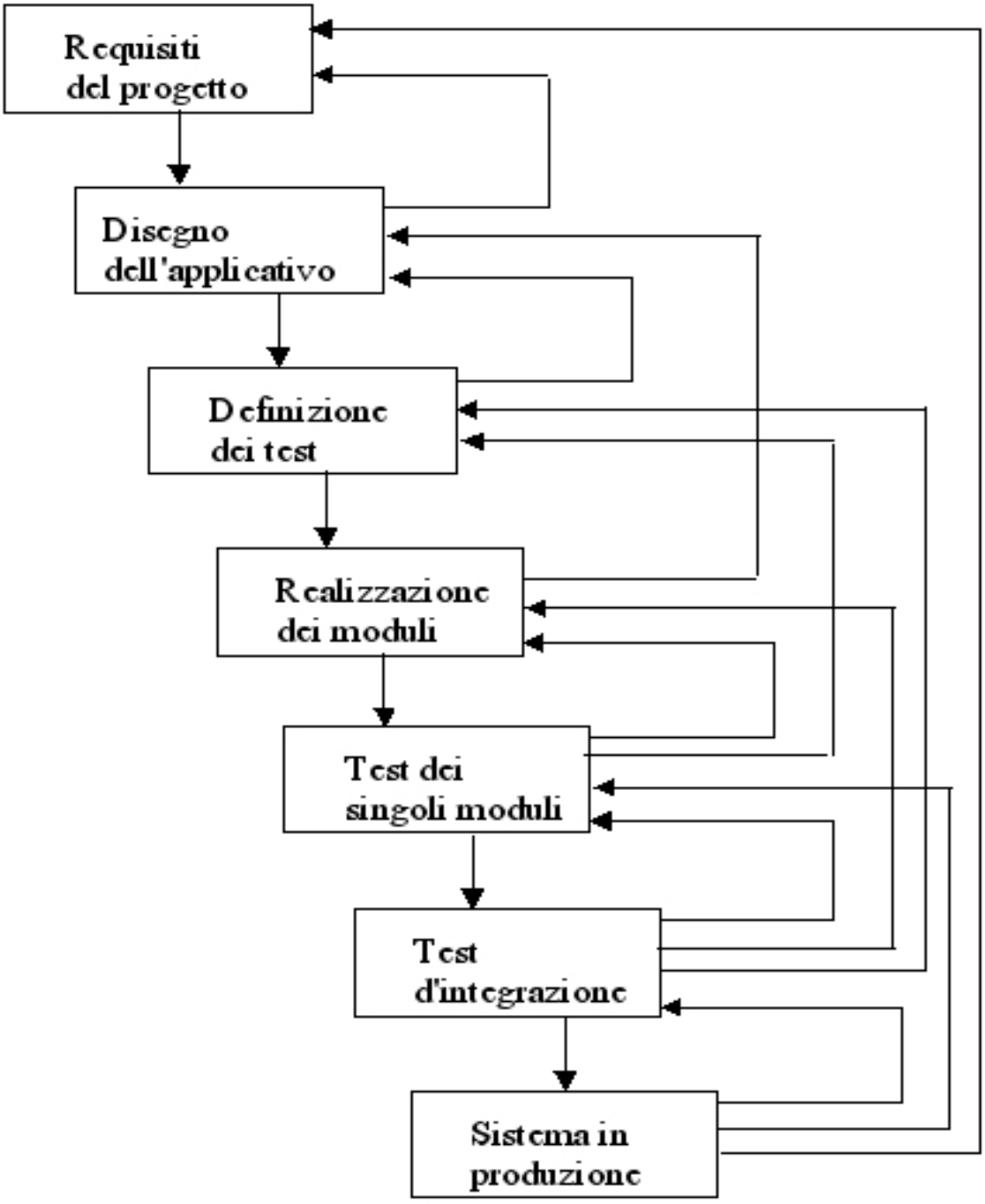
   - aggiornare periodicamente il sistema
   - aggiornare i permessi di accesso al sistema
   - formare i nuovi utenti
   - archiviare e conservare opportunamente i dati trattati
   - prevedere un piano per la gestione degli incidenti e per il ripristino del servizio

5. **Dismissione.**

   Per tutti i sistemi esiste un momento della loro vita in cui non servono più perché diventati inutili o obsoleti e quindi vengono dismessi.

   In questa fase è essenziale stabilire come proteggere i dati presenti nell'hardware (dischi, sistemi, documentazione in formato cartaceo) da dismettere.

Questi cinque passi generali devono poi essere contestualizzati in base al tipo di progetto in esame. A titolo di esempio il seguenti grafico illustra tutti i passi necessari per realizzare e portare in produzione un programma costituito da diversi moduli.


Requisiti del progetto
Disegno dell'applicativo
Definizione dei test
Realizzazione dei moduli
Test dei singoli moduli
Test d'integrazione
Sistema in produzione

Chi è chi?

Come distinguere i buoni dai cattivi?

Questa è una delle domande fondamentali per chiunque si occupi di sicurezza! Cerchiamo dunque dei metodi per distinguere le persone che possono accedere ad una risorsa da quelle che non possono accedere. La metodologia più comunemente utilizzata per distinguere gli accessi leciti dai tentativi di accesso da parte di male intenzionati è suddivisa in tre fasi:

- **Identificazione**
  Un utente fornisce la propria identità: chi sono?
- **Autenticazione**
  Un utente fornisce una o più prove per dimostrare la propria identità: ti dimostro che sono proprio io!
- **Autorizzazione**
  In base alla identità fornita e verificata, vengono definiti i permessi associati all'utente: dove posso andare?

Identificazione

Come primo passo, cataloghiamo le tipologie di persone che accedono alle informazioni e li suddividiamo in gruppi omogenei (dipendenti, partner, clienti....). Al variare del tipo di informazioni e di servizi a cui accedono i componenti di gruppo, definiamo se è necessario identificarli singolarmente.

Ad esempio i potenziali clienti, che consultano il sito dell'azienda per conoscere i suoi prodotti, sono una tipologia di utenze che non richiede di essere identificata. Mentre partner e clienti, che ordinano prodotti e servizi sul sito, richiedono di essere identificati singolarmente.

Un utente potrebbe appartenere a più gruppi, per esempio potrebbe essere sia un fornitore che un cliente.

Se prevediamo di identificare e autenticare le persone, raccomandiamo di fornire un identificativo personale (=**utenza**), a cui associare uno o più gruppi. In molti contesti, l'**identificativo personale** al posto di quello di gruppo, oltre ad aumentare la sicurezza del processo, è un requisito di legge. Due persone che trattano dati sensibili altrui non possono avere lo stesso identificativo neanche in periodi differenti (Decreto Legislativo n 196 del 30 giugno 2003).

Gli amministratori dell'ambiente sono chiamati ad aggiornare frequentemente l'elenco delle persone autorizzate ad accedere ai sistemi, creando nuove utenze, modificando le caratteristiche delle utenze e eliminando quelle non più usate. La definizione di procedure lineari migliora la gestione delle utenze ed riduce il rischio di errori. La definizione di **profili** semplifica la creazione di un nuovo utente e riduce il rischio di assegnargli privilegi diversi da quelli usati nell'esercizio delle sue funzioni.

Autenticazione

Una persona che accede ad un sistema dichiara la propria identità e fornisce credenziali per dimostrarla. Il processo di dimostrazione della propria identità si chiama autenticazione.

In questo capitolo presentiamo brevemente i principali tipi di autenticazione degli utenti finali e degli amministratori utilizzati in campo informatico. Al variare del servizio richiesto, del tipo di dati consultati e del canale usato per accedere al sistema sceglieremo lo strumento di autenticazione più idoneo.

Autenticazione statica: password

La password è una sequenza statica di caratteri scelti dall'utente data al sistema per autenticarsi. Una soluzione simile alla password è quella dei PIN o codice identificativo. In questo caso il codice di autenticazione è scelto dal sistema e fornito all'utente.

L'autenticazione tramite password o PIN è realizzabile facilmente, con costi molto limitati, via software. Essa permette una notevole scalabilità ed è accettata con molta facilità dagli utenti. Questi vantaggi hanno reso **la password il mezzo più diffuso di autenticazione.** Tuttavia la password presenta numerosi svantaggi e statisticamente è la componente più attaccata con successo dai pirati.

I principali problemi legati alla password sono:

- **Segretezza della password**

  Molti utenti tendono a scrivere le proprie password su foglietti di carta che spesso abbandonano in giro o attaccano sul terminale stesso. Un malintenzionato può, in questi casi, leggere semplicemente la password ed accedere ai sistemi.

- **Invio della password**

  Se la password è inviata in chiaro sulla rete, allora è facilmente leggibile da chiunque ascolti la rete. Una volte catturate le credenziali di un utente legittimo, il malintenzionato può usarle per accedere ai sistemi. Le trasmissioni della sessione di autenticazione richiedono quindi di viaggiare su un canale crittato.

  Analogamente, per non essere letta da altre persone, la password digitata non deve comparire sullo schermo.

- **La conservazione della password sul sistema**

  Si consiglia di memorizzare la password in formato codificato e su un file accessibile dal solo sistema e, al più, dall'amministratore di sistema.

  L'algoritmo di crittografia della password deve essere monodirezionale. È cioè possibile ricavare, a partire dalla password fornita dall'utente, la password codificata per confrontarla con quella archiviata. L'algoritmo non deve invece permettere di ricavare la password in chiaro a partire dalla password codificata.

- **La password di una nuova utenza**

  La password di ciascun account personale deve essere strettamente personale. Molti sistemi possono essere configurati per imporre ad un nuovo utente di cambiare la propria password durante il primo accesso al sistema. In caso contrario è una buona regola inviare l'utente a cambiare la password fornita dall'amministratore nel più breve tempo possibile.

  Nel caso di una utenza abilitata ad accedere a dati personali di altre persone, la legge richiede di aggiornare la password di default al primo accesso (come riportato nell'allegato B della legge 196/2003), anche se il tool non lo impone.

- **L'aggiornamento della password**

  La password deve essere cambiata periodicamente.

  Se l'utente tratta dati personali essa deve essere cambiata almeno ogni sei mesi, se tratta dati sensibili e giudiziari essa deve essere cambiata almeno ogni tre mesi.

- **La scelta di una password debole**

  Studi statistici hanno mostrato che circa la metà degli utenti usa come password nome, cognome, soprannome, data o luogo di nascita proprio, dei propri parenti o dei propri animali.

  Un altro trenta per cento delle persone utilizza nomi di personaggi famosi dello sport, della televisione, del cinema, della musica e dei cartoni animati.

  Un altro undici per cento scegli parole ispirate ai propri hobby e alle proprie passioni. Tutte le password di queste categorie costituiscono password deboli facilmente prevedibili ed indovinabili da chi conosce l'utente.

  Esistono poi alcune parole comuni usate molto frequentemente come password. Per questo motivo, esse risultano particolarmente deboli. Esempi di queste parole sono password, public, private, root, admin, administrator, amministratore, abc123, 11111111, 12345678, passwd, pippo, pluto, secret e sex.

  Gli attacchi di tipo vocabolario, effettuati tramite tool automatici, individuano le password con parole di senso compiuto. Essi infatti provano ad accedere ai sistemi fornendo come password permutazioni delle informazioni sull'utente (inclusa l'utenza) e le parole presenti in un proprio "vocabolario" combinate eventualmente con una o due cifre.

  Questi "vocabolari" sono di solito la fusione tra il vocabolario l'inglese, quello della lingua locale (ad esempio italiano) e le stringhe di caratteri più comuni.

  Questi strumenti rendono deboli qualsiasi password che contiene parole di senso compiuto.

Regole per la scelta di una password non debole

Per proteggere i propri account, suggeriamo di scegliere una password:

- lunga almeno 8 caratteri.
- **priva di parole o frasi**
- composta sia da lettere maiuscole che da lettere minuscole
- con al più due caratteri uguali in successione
- priva di dati personali come iniziali, la data di nascita, l'indirizzo (anche anagrammati) ...
- con almeno una cifra
- con almeno un simbolo

  I simboli speciali come la punteggiatura rendono la password più sicura. Tuttavia ci possono essere dei problemi di incompatibilità tra le tastiere di lingue diverse che contengono caratteri speciali diversi. Se prevediamo di accedere da sistemi con tastiere associate a lingue diverse dalla propria allora scegliamo solo i caratteri più comuni presenti su quasi tutte le tastiere (ad esempio , . : ; / \ | + - * @) evitando quelli caratteristici di un paese (ad esempio le lettere accentato o £).
- priva del carattere spazio

  La scrittura di questo carattere è facilmente identificabile da chiunque spii l'utente che inserisce la password.

Autenticazione robuste

Se un malintenzionato legge la password sulla rete oppure sul server in cui l'utente vuole accedere, allora esso potrà utilizzare queste informazioni per entrare sul sistema spacciandosi per l'utente legittimo. Le tecniche di autenticazione robusta (strong authentication) risolvono questo problema: le informazioni fornite durante una sessione di autenticazione di questo tipo non possono essere usate per un successivo accesso al sistema.

Illustriamo le principali tecniche di autenticazione robusta, spiegando come il contenuto della sessione di autenticazione varia di volta in volta.

- **One-time password**

  Con questo termine si intendono tutti i sistemi di autenticazione che prevedono un elenco di password, ciascuna usabile per una sola sessione. In pratica il sistema crea un elenco di password. L'utente consuma una password ogni volta che la usa. Il grosso problema di questo strumento è la conservazione dell'elenco di password da usare.

  Per evitare di salvare tutte password sul server, si scelgono le password basandosi su una funzione matematica monodirezionale. Tramite queste funzioni data una qualsiasi password dell'elenco possiamo ricavare quella precedente ma non la successiva. Queste funzioni matematiche si chiamano one-way-function.

Il server archivia la password dell'ultima sessione. Quando riceve una nuova password, il sistema ricava la precedente tramite la funzione scelta e la confronta con quella conservata.

- **Token card**

  Le token card sono delle piccole calcolatrici elettroniche che generano il codice di identificazione per una data sessione tramite la combinazione di un codice personale dell'utente (PIN) e un numeri variabile fornito dal sistema.

  Questo sistema è più facile da gestire, soprattutto per l'utente. In questo caso egli deve solo conservare la token card e ricordarsi un PIN. Gli utenti accettano facilmente tali strumenti di autenticazione. Essendo un oggetto fisico, le persone prestano una maggior attenzione alla sua conservazione e alla sua protezione. Tuttavia risulta più costoso poiché l'installazione e la configurazione di questo strumento di autenticazione è più onerosa rispetto alla password. Deve essere inoltre acquistato una token card per ogni utente.

- **Certificati digitali**

  I certificati digitale si basano sulla crittografia a chiave pubblica descritta nel capitolo dedicato all'argomento. I certificati digitali contengono i dati dell'utente proprietario e la sua chiave pubblica. Un utente, in possesso di una coppia di chiavi e del relativo certificato digitale, per autenticarsi firma un dato fornito dal sistema. La firma è autenticata tramite i dati forniti dal certificato.

  Il dato da firmare è prodotto in maniera casuale dal sistema. Ogni sessione di autenticazione risulta quindi diversa dalla precedente.

  Per archiviare la chiave privata con cui firmare i messaggi, possiamo salvare i dati su un supporto Hardware, chiamato Smart Card, oppure demandare la gestione al proprietario. Quest'ultima soluzione non richiede costi aggiuntivi. Tutta la responsabilità della gestione, conservazione e utilizzo della chiave segreta è demandata all'utente. La chiave è conservata sul PC dell'utente seppur in formato crittato con un codice di accesso. Una compromissione del sistema può provocare l'accesso alla chiave segreta e quindi la compromissione del sistema di autenticazione.

- **Smart card**

  Le smart card sono apparati hardware che archiviano la chiave privata di un utente. Esse eseguono al loro interno le operazioni crittografiche di codifica e firma. Questa soluzione elimina i problemi di archiviazione ed uso delle chiavi segrete.

  Essa è d'altra parte più costosa poiché richiede l'acquisto di una Smart Card per ogni utente e di uno Smart Card Reader (periferica per la lettura di una card da parte di un sistema) per ogni postazione di lavoro.

Autenticazione biometrica

Quando incontriamo un amico per strada lo riconosciamo, poiché conosciamo il suo volto, l'aspetto fisico, la sua voce... Quotidianamente identifichiamo e autentichiamo le persone che incontriamo tramite le loro caratteristiche fisiche. Perché i sistemi informatici non possono fare altrettanto?

Attualmente esistono soluzioni commerciali sull'identificazione fisica o biometrica delle persone. Questi metodi forniscono un livello di sicurezza elevato: l'unicità di alcune caratteristiche fisiche

delle persone e la notevole difficoltà di riprodurle rendono questi sistemi di autenticazione difficilmente attaccabili. L'applicazione dell'autenticazione biometrica presenta tuttavia diverse controindicazioni: un costo elevato per realizzare l'infrastruttura (costo che varia sensibilmente dal tipo di misurazione), difficoltà di gestire gli accessi da remoto, diffidenza da parte degli utenti...

Quali caratteristiche fisiche mi distinguono facilmente dagli altri? Quali sono facilmente misurabili? Le principali caratteristiche misurate dai sistemi di autenticazione biometrica sono:

- **L'impronta digitale del polpastrello e della mano.**

  Questo è il metodo più diffuso e meno costoso.

- **La retina.**

  La scansione della retina viene effettuata inviando una luce sull'occhio e quindi sulla retina ed analizzando il riflesso proveniente dalla retina. Gli utenti accettano malvolentieri questo metodo, poiché devono appoggiare l'apparecchio di misurazione sull'occhio.

- **L'iride.**

  Gli apparati di scansione dell'iride non richiedono il contatto fisico tra l'occhio e lo strumento di rilevamento. L'iride tende a rimanere più stabile nel tempo rispetto agli altri parametri. D'altra parte le apparecchiature di scansione dell'iride risultano più costose.

- **Caratteristica tridimensionale della mano e/o del viso.**

  Questi tipi di scansione rilevano la geometria tridimensionale della mano o della faccia. Rispetto ai metodi precedenti è più facile trovare due persone con la stessa struttura della mano. L'aspetto della loro faccia tende a cambiare nel corso del tempo.

- **La firma calligrafica.**

  Questo metodo rileva, tramite penne ottiche, la velocità, la pressione, lo stile e la direzione della penna durante l'operazione di firma. Questi strumenti sono più precisi del solo confronto della firma calligrafica. Tuttavia risultano costosi, molto lenti e meno affidabili degli altri metodi di autenticazione biometrica.

Autenticazione continua

L'autenticazione continua si pone l'obiettivo di combattere gli attacchi basati sulla cattura della sessione. In questi attacchi l'hacker cattura i dati e si impadronisce della sessione creata dall'utente dopo che questo si è autenticato.

I sistemi di autenticazione continua prevedono di verificare l'identità dell'utente, ogni volta che questo esegue una operazione. Il modo tipico per realizzare questi tipo di autenticazione è quello di firmare ogni informazione che viene spedita dall'utente al sistema. Il sistema verifica continuamente l'identità del mittente poiché verifica la firma di ogni messaggio.

Qual è la soluzione più sicura?

Il sistema ottimale di autenticazione richiede di identificare una persona tramite la combinazione di:

- **qualcosa che uno ha**

  Una persona è identificata tramite il possesso di uno oggetto fisico (ad esempio smart card, token card...).

- **qualcosa che uno sa**

  Un utente è identificato in base alla conoscenza di una informazione segreta (ad esempio, una password, una chiave crittografica segreta, un PIN...).

- **qualcosa che uno è**

  Un utente è identificato da un suo tratto fisico peculiare (le impronte digitale, l'immagine dell'iride...).

Aumentando il livello di sicurezza dell'autenticazione aumenta contemporaneamente il costo per realizzarla e l'impatto sulla persona da identificare. Consigliamo di valutare, caso per caso, qual è la soluzione più consona all'ambiente, considerando:

- i requisiti di sicurezza del sistema;
- i requisiti di sicurezza dei dati trattati;
- il canale tramite cui si accede al sistema;
- la tipologia di persone da identificare (dipendenti, clienti, fornitori...)

Requisiti di legge per il trattamento dei dati personali

I seguenti articoli dell'appendice B del Decreto Legislativo n. 196 del 30 giugno 2003, "*Codice in Materia di protezione dei dati personali*", forniscono indicazioni precise sui sistemi di autenticazione informatica richiesti per il trattamento di dati personali.

Art. 1 *Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.*

Art. 2 *Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.*

Art. 3 *Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.*

Art. 4 *Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente*

custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

Art. 5 *La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.*

...

Art. 7 *Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.*

Autorizzazione

Mi sono identificato e ho dimostrato la mia identità, ora dove posso andare? A questa domanda risponde la fase di autorizzazione. Essa associa ad ogni utente l'elenco delle operazioni permesse e proibite. In base ai diritti forniti dal processo di autorizzazione, quando l'utente inoltra una richiesta ad un servizio essa verrà rigettata oppure accettata oppure parzialmente accettata.

Intuiamo facilmente come sia fondamentale associare a ciascun utente il corretto profilo di permessi.

Se creiamo un profili specifico per ogni singolo utente, allora il loro numero potrebbe crescere fino a valori difficilmente gestibili. La soluzione è individuare classi omogenee di utenti (i gruppi definiti in fase di identificazione) e associare a ciascun gruppo i relativi diritti di accesso.

Chi accede a cosa?

I profili di accesso alle risorse possono essere definiti secondo una di queste due opposte regoli base:

- **"tutti gli accessi sono proibiti, se non espressamente permessi"**
- **"tutti gli accessi sono permessi, se non espressamente proibiti"**

Una soluzione che adotta la prima filosofia - chiamata anche **need-to-know** - avrà le seguenti caratteristiche:

- Riduce il rischio di accessi casuali/involontari a dati riservati da parte di persone che non trattano questi dati.
- Riduce l'accesso alle risorse aziendali per uso personale da parte dei dipendenti.
- Aumenta il rischio che un dipendente si trovi rallentato o, addirittura, bloccato nello svolgimento del proprio lavoro per mancanza di permessi.

- I profili possono essere molto complessi, se le attività da permettere sono superiori a quelle da proibire.

Questa filosofia è particolarmente adatta per la definizione dei profili dei gruppi costituiti da clienti, partner esterni, fornitori...

Una soluzione che adotta la seconda filosofia avrà le seguenti caratteristiche:

- Aumenta il rischio di accessi casuali/involontari a dati riservati da parte di persone che non trattano questi dati.
- Aumenta il rischio alla modifica o al danneggiamento (volontario o accidentale) dei dati trattati.
- Gratifica i dipendenti che possono facilmente recuperare tutte le informazioni richieste per lo svolgimento del proprio lavoro e che si sentono stimati ed apprezzati dall'azienda.
- Favorisce l'accesso alle risorse aziendali per uso personale da parte dei dipendenti.
- I profili possono essere molto complessi, se le attività da proibire sono superiori a quelle da permettere.

Al variare del cotesto di business aziendale, del tipo di informazioni trattate e di eventuali vincoli legislativi. Ogni azienda o ente valuterà quale filosofia adottare.

Requisiti di legge per il trattamento dei dati personali

I seguenti articoli dell'appendice B del Decreto Legislativo n. 196 del 30 giungo 2003, "*Codice in Materia di protezione dei dati personali*", forniscono indicazioni precise sui sistemi di autenticazione informatica richiesti dalla legislazione vigente.

Art. 6 *Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.*

...

Art. 8 *Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.*

...

Art. 10 *Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti*

incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

...

Art. 12 *Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.*

Art. 13 *I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.*

Art. 14 *Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.*

Art. 15 *Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.*

Single Sign on

Un commerciale ogni mattina quando si siede sulla sua scrivania, inserisce una prima password e accede al suo computer, inserisce una seconda password e accede alla sua casella di posta, inserisce una terza password sul browser e ottiene l'accesso ad internet, inserisce una quarta password ed accede al configuratore per inserire gli ordini dei clienti, inserisce una quinta password ed accede al tool per emettere le fatture... Aiuto! Qquesta password è quella del configuratore o del tool per emettere le fatture. Se una persona deve ricordarsi molte password, comincerà a scegliere password facile e comincerà a seminare la scrivania di bigliettini con il loro valore.

Una soluzione a questo problema è un sistema di **Unified User Management**. Esso è un sistema centralizzato che contiene i dati per identificare e autenticare gli utenti. Quando un qualunque sistema riceve una richiesta di autenticazione invia questi dati a Unified User Management e riceve da esso il risultato della verifica delle credenziali. Con questa architettura una persona di deve ricordare solamente una password. I Directory server sono la soluzione più diffusa di Unified User Management.

Con questa soluzione l'impiegato ogni mattina si deve ricordare una sola password, ma la deve comunque inserire molte volte, con una bella perdita di tempo e pazienza... Che bello sarebbe inserirla una sola volta! È possibile con un'architettura di **Single Sign on**.

Con quest'ultima soluzione un utente si identifica una volta sola all'inizio della sessione di lavoro e può accedere a tutti gli altri servizi senza ulteriori autenticazioni. Il sistema di **Single Sign-on** riconosce la persona all'inizio dell'attività e gli garantisce l'accesso a tutte le risorse previste dal suo profilo con un processo trasparente per l'utente.

Questa architettura è particolarmente esposta ad attacchi in cui l'hacker cattura la sessione di un utente e accede ai servizi passandosi per quest'ultimo. La realizzazione di un sistema di Single Sign-on richiede quindi particolare attenzione per evitare questi attacchi.

Directory Server

Il Directory Server è un archivio che fornisce una lista di informazioni sugli oggetti memorizzati.

Un esempio di Directory Server è l'elenco telefonico che fornisce informazioni sui numeri di telefono, indirizzo etc. di un elenco di abbonati, disposti in ordine alfabetico.

I Directory Server sono dunque un tipo particolare di Database. Essi si distinguono dagli altri tipi di Database perché sono ottimizzati per operazioni di ricerca e di lettura. Nelle operazioni di scrittura, in particolare di inserimento di una nuova voce, i database tradizionali risultano essere più veloci dei Directory. I Directory sono quindi particolarmente adatti a conservare informazioni relativamente statiche nel tempo. Nel caso dell'elenco telefonico, le operazioni di ricerca di un numero telefonico sono enormemente maggiori delle operazioni di inserimento di un nuovo abbonato.

L'applicazione più importante dei Directory è l'archiviazione dell'elenco delle utenze, dei loro dati di autenticazione e dei loro profili autorizzativi. Le operazioni di creazione e rimozione di un utente sono molto più rari rispetto alle operazioni di lettura dei dati degli utenti per la loro autenticazione. In molti Directory Server vengono integrate funzioni per la profilatura degli utenti, per la gestione delle password e degli altri strumenti di autenticazione e per la definizione dei loro permessi di autorizzazione.

Supponiamo di volere che i nostri dipendenti siano in grado di consultare, sul Directory server, le informazioni sui colleghi del proprio dipartimento ma non di altri dipartimenti oppure di leggere gli indirizzi e-mail dei colleghi ma non il loro indirizzo di casa. Da questi esempi si evince che i Directory server devono fornire uno strumento flessibile per la definizione delle più svariate politiche di accesso ai dati.

In molti Directory la consultazione delle informazione è regolamentata tramite Access Control List (ACL). Possiamo definire, tramite le ACL, regole sui diritti di accesso agli oggetti o agli attributi del directory. Molti directory riescono ad implementare ACL ad un elevato livello di granularità arrivando definire ACL applicabili a un singolo oggetto.

I Directory server sono strumenti particolarmente adatti per implementare lo “Unified User Management” e, in combinazione con strumenti di Gestione delle Identità, il “Single Sign On”

(SSO).

In una architettura di “Unified User Management” o di “Single Sign-On” le varie componenti interrogano il Directory server tramite il protocollo standard chiamato LDAP (Light Directory Access Protocol). Se interrogato tramite protocollo LDAP, il Directory server si protegge da accessi illeciti e da tentativi di manomissione dei dati adottando le seguenti contromisure.

- Verifica delle credenzialità di un utente o di un server.

  I Directory hanno di solito a disposizione diversi tipologie di autenticazione per le diverse esigenze.
- Usa meccanismi di controllo dei dati inviati e ricevuti per evitare alterazioni durante la trasmissione.
- Invia i dati su un canale crittato per proteggere informazioni spedite.
- Consulta le ACL.

Siamo sicuri del servizi richiesti?

Abbiamo presentato i metodi usati dai servizi per identificare gli utenti. Ma un povero utente come può determinare se sta consultando il servizio richiesto o un impostore? Come verifica l'identità di un sito prima di inserire la propria carta di credito per un acquisto?Quando scarica un Applet, un ActiveX come determina la fonte e l'integrità del codice?

I certificati digitali sono la risposta a molte di queste domande. Un server può dimostrare la propria identità a un cliente inviandogli un messaggio firmato accompagnato dal proprio certificato rilasciato da un'entità universalmente riconosciuta. Molti web server usano il protocollo SSL per creare un canale crittato e per dimostrare la propria identità.

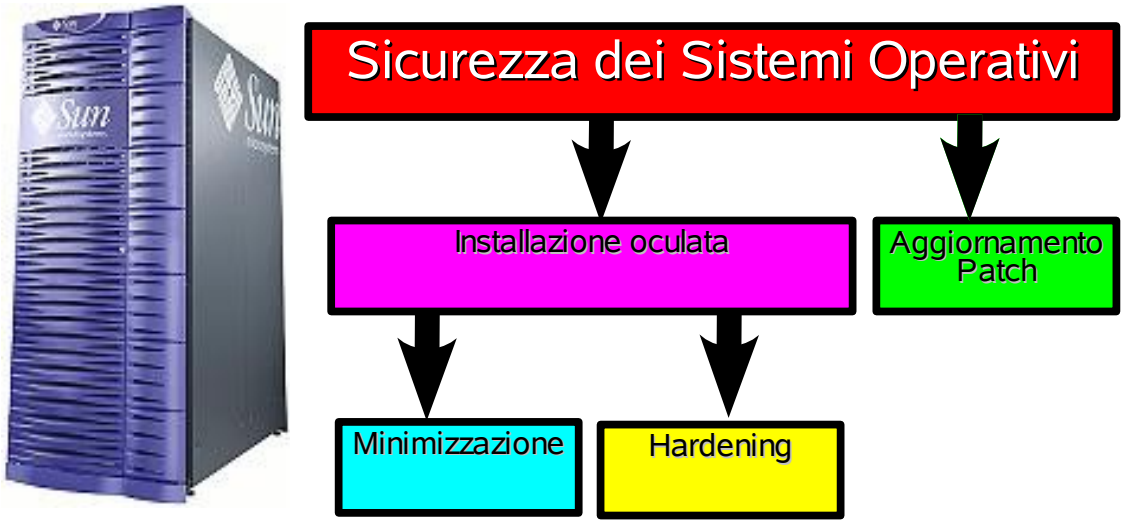
Se un utente scarica un codice informatico (ad esempio, Applet o ActiveX) firmato da una persona o un'organizzazione fidata, allora verifica la firma del messaggio ed esegue il programma in relativa tranquillità. Altrimenti l'unica soluzione è analizzare tutto il codice sorgente alla ricerca di codice malevole.

Sicurezza dei sistemi e degli applicativi

Le misure di protezione che una persona adotta per proteggere la casa e quanto contiene sono differenti da quelle adottate per proteggere una banca e le sue casseforti o da quelle adottate per proteggere una base militare e i suoi depositi di armi. Al variare del valore dell'oggetto da difendere (i propri beni, i soldi e i gioielli depositati in banca o le armi) una persona valuta l'investimento (in tempo, risorse e denaro) ragionevole per la sua protezione.

Analogamente l'investimento effettuato per proteggere un sistema dipende dai servizi erogati dal sistema, dai dati trattati, dai danni derivanti da una sua compromissione, dall'ambiente in cui è inserito...

Questo capitolo presenta dei criteri generali per aumentare il livello di sicurezza dei sistemi adattabili a tutte le situazioni, cosi come, nell'esempio precedente, un antifurto potrebbe essere una soluzione adatta per la casa, per la banca e per base militare...



Installare e ridurre

Chi ben comincia è a metà dell'opera... quindi una buona installazione può aumentare di molto il livello della sicurezza del sistema.

I Sistemi Operativi e gli Applicativi sono spesso dei prodotti molto complessi che contengo al loro interno molte funzionalità e molti servizi. Iniziamo a studiare quali componenti ci servono. Ad esempio, un programma di elaborazione delle immagini sarà molto utilizzato su un PC di casa mentre sarà completamente inutile su un sistema per la gestione dei conto correnti di una banca.

L'installazione standard della maggior parte dei Sistemi Operativi e degli Applicativi carica sul sistema tutte funzionalità contenute nel prodotto. Optando invece per una **installazione personalizzata** possiamo scegliere quali parti del prodotto installare. I programmi di installazione controllano le dipendenze dei prodotti scelti con altre componenti. Essi aggiungono le librerie e i

moduli richiesti dalle componenti selezionate. Con l'installazione personalizzata possiamo inoltre verificare che le componenti di sicurezza fornite dal Sistema Operativo o dall'Applicativo siano installati.

Molti produttori forniscono documentazioni precise su come aumentare la sicurezza del prodotto in fase di installazione e di configurazione. Seguirle vuol dire rendere il nostro sistema più sicuro.

Minimizzazione

A volte i sistemi installati hanno molti pacchetti inutili perché essi non permettono una rimozione così granulare dei pacchetti in fase di installazione o perché sono stati installati in una modalità standard.

In questi casi interveniamo a rimuovere a mano tutti i pacchetti inutili dal sistema già attivo, tramite l'operazione di minimizzazione.

La minimizzazione è la rimozione di pacchetti o features dal sistema in modo da disegnarlo attorno al servizio che deve offrire.

Se interveniamo a posteriori alla eliminazione dei pacchetti, dobbiamo prestare particolarmente attenzione alle dipendenze con altre componenti e con altri applicativi. Non tutti i sistemi operativi e gli applicativi sono capaci, in fase di rimozione, di individuare componenti e/o applicativi chi richiedono per il loro funzionamento il pacchetto da rimuovere.

Hardening

Durante la configurazione del Software, procediamo ad attivare tutti gli strumenti di sicurezza con cui proteggeremo il nostro sistema. Questo processo prende il nome di hardening.

L'hardening è la configurazione del Sistema Operativo o dell'Applicativo finalizzata ad ottenere il migliore livello di sicurezza possibile coerentemente con i servizi erogati, in modo da proteggerlo da attività illecite locali o remote.

Le modifiche effettuate dall'hardening spaziano dalla rimozione dei servizi di rete non utilizzati alla disabilitazione dell'esecuzione di codice presente sullo stack dati, dalla configurazione dei parametri per la gestione delle password alla protezione dei file system.

Produttori di Software ed enti sulla sicurezza rilasciano procedure precise e puntuali sull'hardening di Sistemi Operativi, in funzione dei servizi erogati. Consigliamo di seguire queste documentazioni come linee guida delle attività di hardening.

L'hardening non è certamente una soluzione di security universale; tuttavia è sicuramente un valido freno per utenti locali "maliziosi" ed un ottimo contributo al miglioramento della sicurezza della sua sottorete.

Aggiornare, aggiornare e ancora aggiornare...

Ho installato un sistema sicuro e ho attivato tutti gli strumenti per proteggerlo, allora sono a posto! Purtroppo no! La sicurezza è un processo continuo... perché sempre nuove sono le minacce.

Nuovi errori e nuove vulnerabilità vengono scoperte quotidianamente. Per ogni nuovo baco scoperto, i produttori di Sistemi Operativi e di Applicativi rilasciano tempestivamente un aggiornamento del software per eliminarlo. Queste correzioni vengono chiamate con nomi diverse da produttore differenti: aggiornamenti, "security patches", "hot fix"....

Un elemento essenziale della sicurezza è quindi aggiornare periodicamente il sistema e gli applicativi.

Spesso gli amministratori tendono a pensare "sistema che funziona, non si cambia" o "applica la patch solo se esiste un problema". A causa del continuo crescere del numero di crimini informatici questi atteggiamenti risultano perdenti. La filosofia giusta è un approccio pro-attivo ossia: "applicare le patches prima che qualcuno comprometta il sistema". Per aiutare gli amministratori nell'aggiornamento dei sistemi, molti produttori di software rilasciano notifiche, chiamate Advisory, sui nuovi attacchi accompagniati dall'indicazione della patch da applicare.

Requisiti di legge per il trattamento dei dati personali

I seguenti articoli dell'appendice B del Decreto Legislativo n. 196 del 30 giungo 2003, "*Codice in Materia di protezione dei dati personali*", forniscono indicazioni precise sui requisiti relativi alla gestione dei sistemi e degli applicativi.

Art. 9 *Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.*

...

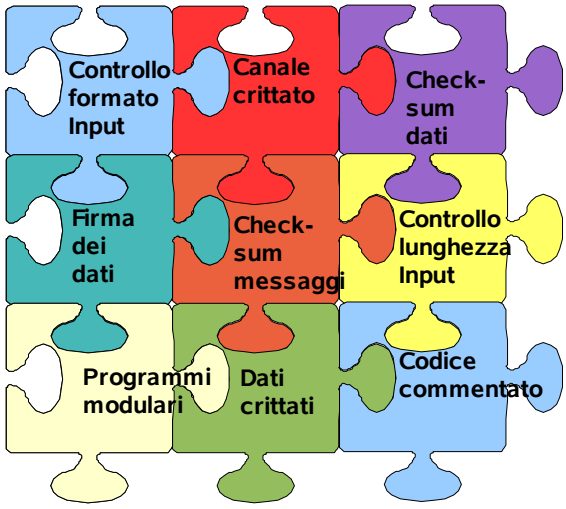
Art. 16 *I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.*

Art. 17 *Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.*

Codici robusti

Quando scegliamo un'automobile verifichiamo la qualità del prodotto: consideriamo la qualità dei materiali scelti, delle saldature, la presenza di barre laterali, dell'ABS... Analogamente quando scegliamo o realizziamo del software un elemento importate è la sua qualità. Un buon codice è un codice robusto e quindi sicuro.

Proviamo ad individuare alcuni elementi da valutare per determinare quanto un codice è sicuro.



Un primo problema è verificare se i dati inviati o archiviati siano stati alterati. La soluzione è associare ai dati check-sum (bit di controllo). Se un dato viene alterato allora se calcolo il check-sum ottengo un valore differente da quello archiviato. Un sistema più evoluto di controllo dell'integrità dei dati è la firma digitale. In quest'ultimo caso oltre all'integrità posso garantire il non-ripudio dei dati conservati.

Se il codice impiega un canale crittografico allora garantisce la riservatezza delle informazioni inviate. Se il codice archivia i dati in formato crittografato allora garantisce la riservatezza delle informazioni salvate.

La sicurezza di un applicativo dipende notevolmente dalla qualità della scrittura del suo codice.

Un codice è robusto e quindi sicuro se fa quello che deve fare e non fa quello che non deve fare.

La qualità degli applicativi compare normalmente nella gestione di una richiesta non prevista o di un dato non conforme. Se il codice è robusto allora riconosce la richiesta come non appartenente alle operazioni consentite, non la esegue e segnala adeguatamente l'errore. Se invece non è in grado di riconoscere richieste errate, allora il codice esegue operazioni illecite e compromette l'integrità dei propri dati. La robustezza di un codice dipende quindi dalla sua capacità di controllare le informazioni fornite dagli utenti.

Prima di tutto deve controllare la lunghezza dei dati inseriti. Molti sistemi non sono in grado di accorgersi se il dato inserito è più lungo di quello previsto. Questi sistemi scrivono in memoria il dato, come se fosse corretto. Questo riempie tutta l'area di memoria ad esso destinato e fuoriesce sovrascrivendo le aree di memoria contigua. Questo evento si chiama “buffer overflow” ed è alla base di molti attacchi informatici. Se l'applicativo gestisce dati più grossi del previsto allora è immune da attacchi di questo tipo.

Un codice robusto deve verificare la coerenza dei dati immessi. Ad esempio il campo relativo ad una nazione deve contenere il nome di una nazione realmente esistente. Il programma deve essere in grado di verificare la bontà di questo dato. Se esso risulta errato allora il programma deve bloccare l'operazione come illecita, proteggendo la propria banca dati da alterazioni e incongruenze.

Un codice robusto deve inoltre gestire la presenza di caratteri speciali all'interno di una stringa dati. Alcuni attacchi usano questi caratteri speciali per mandare in errore il programma.

Ricordiamo infine che una struttura modulare dell'applicativo, semplifica la scrittura e il test dello stesso e riduce il rischio di errori nel codice.

Content Filtering

Se il codice usato per l'erogazione di un servizio non è robusto, in particolare non è in grado di verificare la correttezza dei dati in input, come posso proteggere il mio servizio? Se le pagine del mio sito sono aggiornate molto frequentemente, come posso proteggermi da eventuali errori di codice?

La scelta di un codice robusto è sempre la soluzione migliore. Quando essa non è possibile posso introdurre un strato di protezione tra il mio servizio e la rete circostante. Questo strato si chiama “Content Filtering”. Esso intercetta tutte le richieste indirizzate al sito insicuro e verifica il loro formato. Se le richieste effettuate e i dati forniti sono corretti il Content Filtering le inoltra al sito sottostante, altrimenti le rigetta segnalando un errore al cliente.

Proprietà intellettuale dei programmi informatici

Quando compriamo o vendiamo una autovettura dobbiamo registrare il passaggio di proprietà presso il registro della motorizzazione.

E nel caso di un programma informatico? Abbiamo qualche obbligo di legge?

Possiamo considerare quattro categorie di programmi.

- Programma sviluppato da noi.

  Possiamo usare liberamente i programmi che abbiamo sviluppato.

  Se vogliamo invece rivendere a terzi questo programma, dobbiamo prima registrare la proprietà intellettuale dello stesso e poi rilasciare una licenza d'uso del prodotto.

- Prodotto commerciale.

  Dobbiamo acquistare un licenza dal produttore prima di installarlo sul nostro sistema. Alcuni prodotti commerciali vincolano la licenza ad un particolare modello di macchina o ad una famiglia di server.

- Programma free.

  Possiamo usare liberamente i programmi distribuiti senza vincoli dal loro sviluppatore.

- Prodotto opensource.

  I programmi opensource hanno una loro licenza che stabilisce le condizioni per l'installazione e la modifica. Prima di installare questi programmi dobbiamo verificare se il nostro ambiente possiede i requisiti richiesti.

  Ad esempio alcuni programmi sono gratuiti solo per uso personale. Se vogliamo installarli all'interno di un'azienda dobbiamo acquistare la relativa licenza.

Legislazione sul diritto d'Autore

La proprietà intellettuale dei programmi informatici è protetta dalla legislazione sul diritto d'autore. La legge di riferimento sul diritto d'autore è la legge n.663 del 22 aprile 1941 aggiornata più volte (l'ultimo aggiornamento è stato effettuato dalla legge n.128 del 22 maggio 2004).

Presentiamo un estratto di questa legge per introdurre le problematiche sul diritto d'autore.

Art. 64-bis Fatte salve le disposizioni dei successivi articoli 64-ter e 64-quater, i diritti esclusivi conferiti dalla presente legge sui programmi per elaboratore comprendono il diritto di effettuare o autorizzare:

a) la riproduzione, permanente o temporanea, totale o parziale, del programma per elaboratore con qualsiasi mezzo o in qualsiasi forma. Nella misura in cui operazioni

quali il caricamento, la visualizzazione, l'esecuzione, la trasmissione o la memorizzazione del programma per elaboratore richiedano una riproduzione, anche tali operazioni sono soggette all'autorizzazione del titolare dei diritti;

b) la traduzione, l'adattamento, la trasformazione e ogni altra modificazione del programma per elaboratore, nonché la riproduzione dell'opera che ne risulti, senza pregiudizio dei diritti di chi modifica il programma;

c) qualsiasi forma di distribuzione al pubblico, compresa la locazione, del programma per elaboratore originale o di copie dello stesso. La prima vendita di una copia del programma nella comunità economica europea da parte del titolare dei diritti, o con il suo consenso, esaurisce il diritto di distribuzione di detta copia all'interno della comunità, ad eccezione del diritto di controllare l'ulteriore locazione del programma o di una copia dello stesso.

Art. 64-ter 1. Salvo patto contrario, non sono soggette all'autorizzazione del titolare dei diritti le attività indicate nell'art. 64-bis, lettere a) e b), allorché tali attività sono necessarie per l'uso del programma per elaboratore conformemente alla sua destinazione da parte del legittimo acquirente, inclusa la correzione degli errori.

2. Non può essere impedito per contratto, a chi ha il diritto di usare una copia del programma per elaboratore di effettuare una copia di riserva del programma, qualora tale copia sia necessaria per l'uso.

3. Chi ha il diritto di usare una copia del programma per elaboratore può, senza l'autorizzazione del titolare dei diritti, osservare, studiare o sottoporre a prova il funzionamento del programma, allo scopo di determinare le idee ed i principi su cui è basato ogni elemento del programma stesso, qualora egli compia tali atti durante operazioni di caricamento, visualizzazione, esecuzione, trasmissione o memorizzazione del programma che egli ha il diritto di eseguire. Le clausole contrattuali pattuite in violazione del presente comma e del comma 2 sono nulle.

...

Art. 171-bis Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da lire cinque milioni a lire trenta milioni. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a lire trenta milioni se il fatto è di rilevante gravità.

I miei dati sono riservati? Critto tutto

Questo capitolo illustra come la crittografia funziona e come può essere usata per garantire la riservatezza dei dati.

Crittografia: che cos'è?

Se una pattuglia militare in esplorazione dietro le linee nemiche deve far pervenire un messaggio al suo commando allora affiderà il messaggio ad un portalettere che attraverserà le linee nemiche. Il portalettere non saprà a priori se riuscirà a consegnare il messaggio o se questo verrà intercettato dal nemico. Per non fornire un vantaggio al nemico è fondamentale scrivere il messaggio in un formato tale da risultare leggibile dai propri superiori e illeggibile dal nemico.

La crittografia è la scienza che studia come alterare il messaggio per renderlo leggibile dal solo legittimo destinatario.

Un algoritmo crittografico illustra il procedimento per trasformare un messaggio in chiaro in un messaggio codificato e il procedimento per ritrasformare il messaggio codificato in un messaggio in chiaro.

Anticamente i sistemi crittografici si basavano sulla segretezza dell'algoritmo di trasmissione. Nei tempi moderni si preferisce basare i sistemi crittografici su algoritmi noti e sulla segretezza di un elemento aggiuntivo chiamato “chiave di cifratura”. Gli algoritmi utilizzate negli ambienti informatici si dividono in due categorie in base al diverso utilizzo delle chiavi di cifratura: algoritmi a chiave privata e algoritmi a chiave pubblica.

Crittografia a chiave privata

Gli algoritmi a chiave privata usano la stessa chiave sia in fase di codifica del messaggio che in fase di decodifica. Il mittente e il destinatario condividono quindi la stessa chiave di codifica.

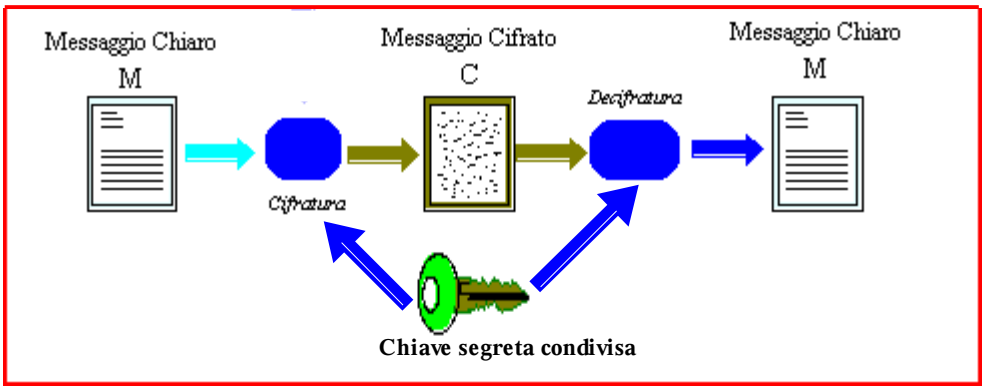
Quando Giovanni deve mandare un messaggio a Mario recupera la chiave segreta condivisa con Mario e codifica il messaggio utilizzando tale chiave. Mario riceve il messaggio codificato da Giovanni, recupera la chiave segreta condivisa con Giovanni e decodifica il messaggio utilizzando tale chiave. Se Stefano intercetta il messaggio inviato da Giovanni a Mario allora non è grado di decifrarlo poiché non conosce la chiave condivisa tra mittente e destinatario. L'unica cosa che resta a Stefano per cercare di decifrare il messaggio è provare tutte le chiavi possibili. Il test di tutte le chiavi si chiama “brute force attach”.

Consideriamo ora un gruppo composto da n persone. Se ogni persona deve poter comunicare in modo riservato con ciascuna delle altre persone allora ogni persona dovrà conservare una chiave per ogni altra persona (n-1). Il numero di chiavi totali sarà quindi parti a n*(n-1)/2 .

Un primo problema è legato alla crescita quadratica del numero di chiavi da gestire al crescere del

numero di persone.

Un secondo problema è la distribuzione della chiave. Se una persona intercetta e conosce la chiave di un'altra coppia di persone allora essa può leggere e alterare tutte le comunicazioni tra le due parti in causa.



Fra i algoritmi crittografici a chiave pubblica o simmetrici ricordiamo:

- **DES** con chiave lunga 40/52 bit
- Triple DES con chiave lunga 128 bit
- **AES** con chiave lunga 128/192/256
- Twofish chiave a lunghezza variabile
- **Blowfish**
- IDEA con chiave lunga 112 o 168 bit
- RC2, RC4 e RC5 chiave a lunghezza variabile

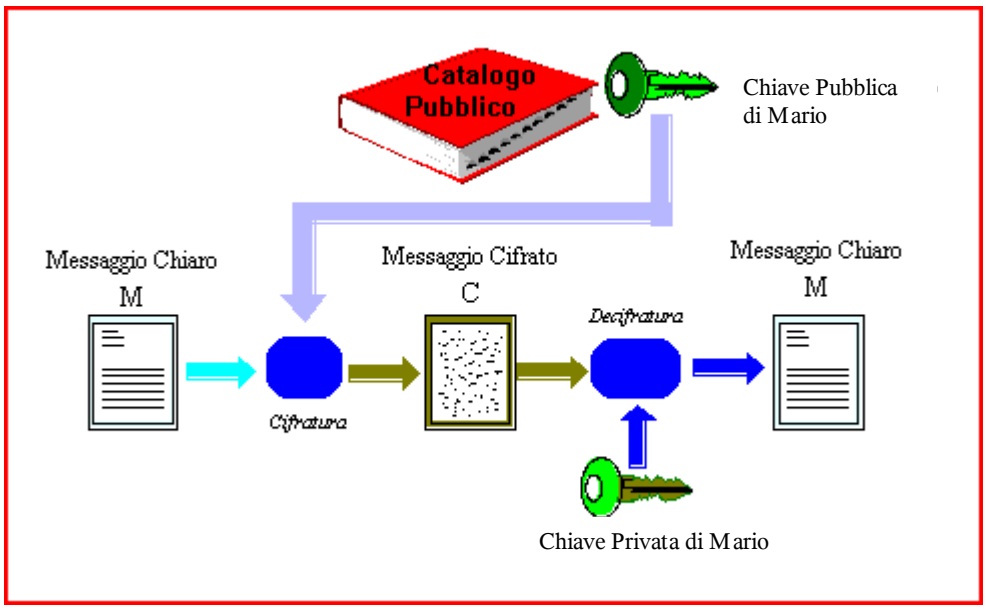
Crittografia a chiave pubblica

Nel passaggio da applicazioni militari della crittografia ad applicazioni civile in campo informatico il numero di chiavi da gestire e distribuire è cresciuto enormemente. Gli ambienti informatici avevano grossi problemi a trovare un modo di distribuire tutte quelle chiavi segrete in modo sicuro. La risposta a tutti questi problemi è venuta da un nuovi tipo di crittografia: quella a chiave pubblica.

Il primo algoritmo a chiave pubblica o asimmetrica è stato inventato nel 1975 da Whitfield Diffie e Martin Hellman.

Nella crittografia a chiave pubblica ogni persona possiede due chiavi:la chiave pubblica e la chiave privata. Se Mario vuole ricevere messaggi riservati genera una coppia di chiavi, diffonde la propria chiave pubblica e mantiene segreta la propria chiave privata. Quando Giovanni deve mandare un messaggio a Mario legge la chiave pubblicata di Mario e codifica il messaggio utilizzando tale

chiave. Mario riceve il messaggio codificato da Giovanni, utilizza la propria la chiave privata per decodificare il messaggio. Se Mario vuole rispondere a Giovanni allora legge la chiave pubblica di Giovanni e la utilizza per codificare il messaggio. Quando riceve il messaggio Giovanni lo decodifica con la propria chiave privata. Se Stefano intercetta i due messaggi allora la sola conoscenza delle chiavi pubbliche di Giovanni e Mario non è sufficiente per decifrarli.



Ogni utente ha due chiavi e quindi il numero delle chiavi cresce come il doppio delle chiavi degli utenti. In un sistema con n utenti il numero delle chiavi nei sistemi a chiave pubblica (2n) è molto inferiore rispetto ai sistemi a chiave simmetrica ($n^2/2$). Questi algoritmi non richiedono di distribuire le chiavi in segreto. Questi algoritmi risultano tuttavia essere più lenti degli algoritmi a chiave privata.

Il più famoso algoritmo a chiave pubblica è **RSA**. Altri algoritmi sono DSA e gli algoritmi basati sulle Curve Ellittiche.

Hash Function

Una “one way hash function” è una funzione matematica che trasforma una stringa di bit di lunghezza variabile (o messaggio) in una stringa univoca di caratteri di lunghezza fissa (riassunto).

Queste funzioni sono monodirezionali cioè le operazioni matematiche per ricercare il messaggio dal suo riassunto richiedono risorse di calcolo attualmente non disponibili. È quindi computazionalmente impossibile trovare un messaggio che produca un riassunto prevedibile. È inoltre computazionalmente difficile trovare due differenti messaggi che producano uno stesso riassunto.

Le hash function sono impiegate per verificare l'integrità dei dati. Esse sono più affidabile dei sistemi di check-sum tradizionali. Queste funzioni sono inoltre usate per ottimizza le operazioni di

firma digitale.

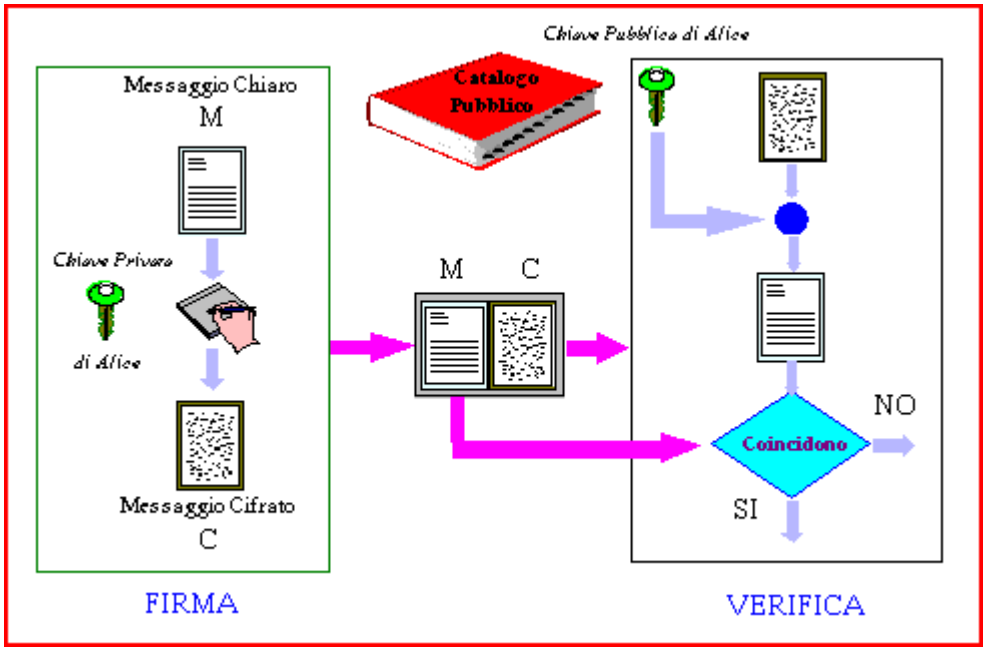
Le principali funzioni hash sono: Message Digest 5 (**MD5**) che produce un output a 128 bit e Secure Hash Algorithm (**SHA-1**) che produce un output a 160 bit.

Firma digitale

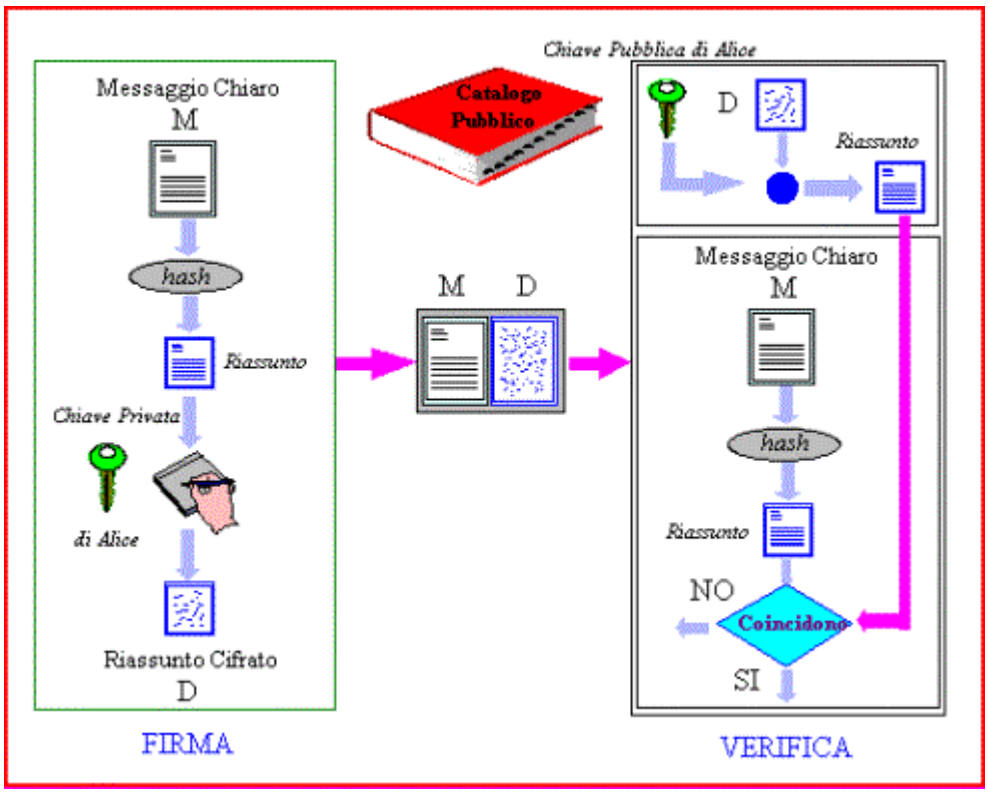
Se Alice manda una lettera ad Alessandro, per dimostrare l'autenticità della stessa appone la sua firma.

In campo informatico è possibile firmare un documento? Quali strumenti ho a disposizione per garantire l'autenticità di un dato?

La crittografia a chiave pubblica fornisce una soluzione a questi problemi: la firma digitale. Nel caso della firma gli algoritmi funzionano esattamente nel metodo inverso rispetto agli algoritmi di codifica. La chiave segreta serve per firmare il messaggio e la chiave pubblica serve per verificare la firma. In questo caso tutti possono verificare la firma, ma solo il proprietario della chiave segreta può firmare.



Se Alice vuole inviare un messaggio ad Alessandro firmandolo allora codifica il messaggio con la propria chiave privata ed invia ad Alessandro il messaggio in chiaro e quello crittato (firma). Alessandro riceve il messaggio in chiaro più la firma. Decodifica con la chiave pubblica di Alice la firma e lo confronta con il messaggio in chiaro. Se i due messaggi risultano uguali allora la firma è autentica.



Con questo schema il messaggio firmato è lungo come il messaggio in chiaro, raddoppiando i bit da trasmettere. Per ridurre le dimensioni del messaggio, il mittente può firmare un riassunto del messaggio. Per generare il riassunto viene usata una funzione hash.

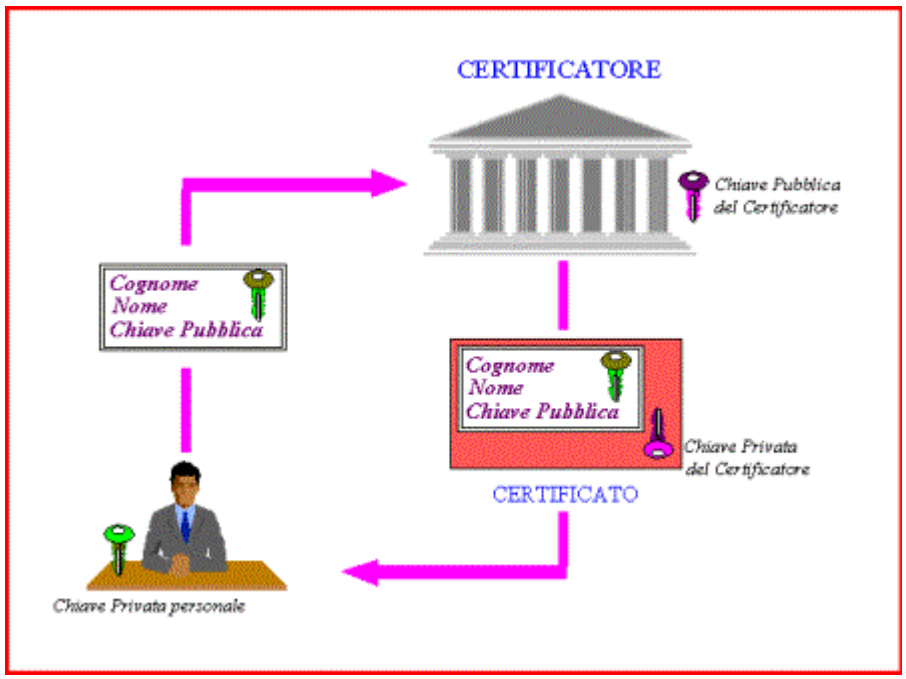
Certificati digitali

Se Stefano diffonde la propria chiave pubblica come se fosse quella di Mario allora è in grado di leggere tutti i messaggio crittati inviati a Mario e a falsificare la firma di Mario.

Negli algoritmi a chiave pubblica, la sicurezza della distribuzione delle chiavi ricopre quindi un ruolo importante.

Per riconoscere l'identità del proprietario di una chiave è stato introdotto il concetto di certificato. Il certificato è il corrispondente elettronico della carda d'Identità. Esso fornisce i dati anagrafici della persona per la sua identificazione. Come la carta d'Identità riporta la firma della persona per eventuali operazioni di confronto così il Certificato digitale riporta la chiave pubblica per verificare la firma digitale. Una persona fisica può richiedere un certificato per firmare i messaggi o ricevere comunicazioni codificate. È possibile richiedere un certificato anche per un servizio informatico. In questo caso il certificato è rilasciato dal servizio ai suoi clienti per dimostrare la sua identità e creare connessioni protette con il proprio cliente.

Il certificato è emesso da un ente certificatore (Certification Authority) riconosciuto. Questo ente garantisce la bontà del certificato così come il comune garantisce la correttezza dei dati riportati nella Carta d'Identità. Come nel caso della carta d'identità, il certificato vale in un preciso intervallo di tempo, cioè ha una data di emissione e una di scadenza. Dopo la data di scadenza la correlazione tra chiave pubblica e persona fisica non è garantita. Alla scadenza naturale del certificato, il proprietario può chiedere all'ente certificatore o il rinnovo del certificato, estendendo l'intervallo di validità, o l'emissione di un nuovo certificato associato ad una nuova coppia di chiavi.



A seguito del furto o dello smarrimento della carta d'identità, una persona denuncia il fatto alla polizia. Essa registra nei suoi sistemi che quel documento non è più valido. Analogamente se la riservatezza di una chiave segreta è compromessa allora il proprietario deve segnalare tempestivamente l'evento all'ente certificato. Quest'ultimo aggiorna i suoi archivi dichiarando il certificato come revocato. Esso rilascia periodicamente una lista (chiamata Certification Revocation List) con l'elenco dei certificati revocati prima della loro scadenza naturale.

Ma un documento firmato elettronicamente ha lo stesso valore di uno con una firma calligrafica? Chi garantisce legalmente l'associazione tra una persona e il suo certificato? Una firma elettronica ha valore legale equivalente a quella calligrafica solo se il certificato associato è stato emesso da un ente certificato riconosciuto dallo stato italiano.

Ogni certificato contiene:

- la chiave pubblica dell'entità
- le informazioni dell'entità (l'indirizzo di posta elettronica dell'entità o l'indirizzo del sito

web oppure il nome e cognome della persona)

- le indicazioni del tipo di certificato
- la data di emissione e la data di scadenza dello stesso
- i dati relativi all'ente certificatore

L'ente certificatore firma il certificato con la propria chiave segreta, dopo aver verificato l'identità della persona o del sistema.

Lo standard di riferimento per il formato dei certificati è X509 v3.

Infrastruttura a chiave pubblica

L'infrastruttura che fornisce un insieme di servizi di sicurezza per la creazione gestione delle chiave pubblica e dei certificati si chiama **Public Key Infrastructure (PKI)** ed è composta da:

- **Registration Authority**,

  La Registration Authority verifica l'identità della persona o il processo che richiede l'emissione di un nuovo certificato o la revoca di un certificato.

  Se il livello di sicurezza del certificato da emettere richiede una identificazione fisica della persona, allora questa si reca presso gli appositi sportelli dell'ente certificatore e si identifica tramite un documento. Il personale dell'ente compila l'apposito modulo della Registration Authority confermando l'identificazione fisica della persona in questione.

  Nel caso di una richiesta elettronica, la Registration Authority verifica il legame tra l'entità (ad esempio indirizzo di posta elettronica) e la chiave. Essa contatta la Certification Authority e chiede l'emissione del certificato. In architetture semplici la Registration Authority può essere integrata all'interno della Certification Authority.

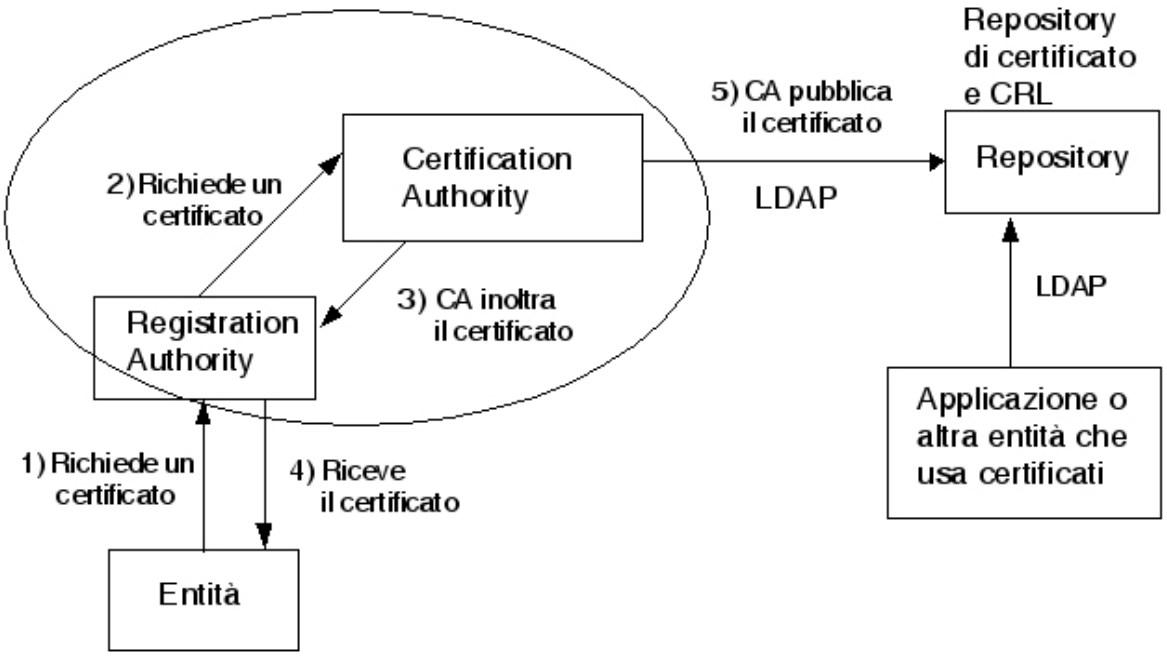
- **Certification Authority**

  La Certification Authority è il cuore dell'infrastruttura. Essa genera il certificato con il formato richiesto e li firma con la propria chiave privata. Gli attributi di un certificato di un utente sono differenti di quelli di un web server. Per verificare il valore di un certificato è essenziale avere le chiavi pubbliche delle Certification Authority. Molti browser contengono al proprio interno le chiavi pubbliche dei principali enti certificatori. Le Certification Authority più piccole, non presenti nei Browser fanno certificare la propria chiave da una Certification Authority più importante, che a sua volta può farsi certificare da un'altra. In questo modo si certificano le chiavi delle Certification Authority a partire da quelle più grandi. Le Certification Authority emettono inoltre le Certification Revocation List (CRL) con l'elenco dei certificati revocati. I certificati che appaiono in questa lista non hanno più valore. Molte sono le cause che possono portare alla revoca di un certificato. Le più comuni sono il furto o lo smarrimento della chiave privata.

- **Repository**

  Nel repository vengono archiviati i certificati e le CRL emessi e resi consultabili da tutti gli utenti. Spesso i Repository sono Directory Server accessibili tramite protocollo LDAP.

Flusso logico di un richiesta di un certificato ad una Certification Authority



- **Time Stamping Authority.**

  Questa componente opzionale dell'architettura associa univocamente una data e un orario ad una operazione di firma emettendo un francobollo temporale.

  Avendo una datazione certa di una firma, una persona può dimostrare che le chiavi e i certificati associati a tale firma erano valide.

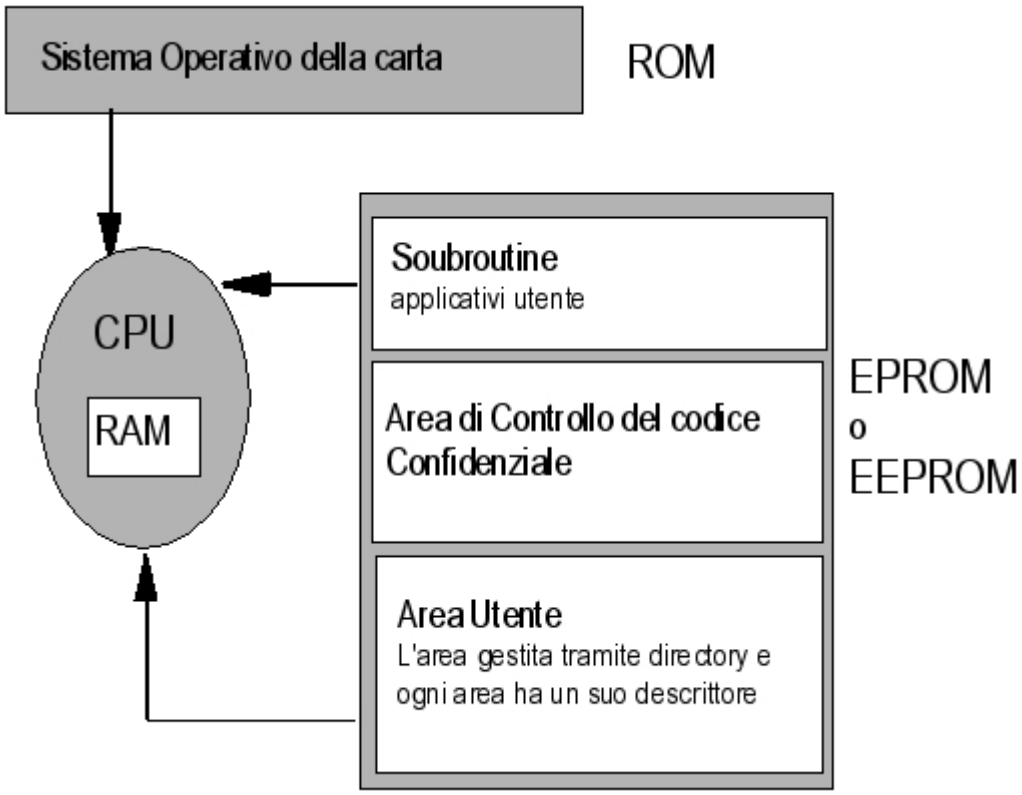
Smart Card

Una volta realizzata un'infrastruttura a chiave pubblica (PKI), ci poniamo il problema di come avere sempre con noi il nostro Certificato. Le Smart Card sono una soluzione di questo problema.

Una Smart Card è una carta che contiene la chiave segreta del possessore e il relativo certificato digitale ed esegue al suo interno le operazioni di codifica e decodifica. Con questa soluzione la chiave segreta non esce dalla Card e quindi è meno esposta ad attacchi. Di contro dobbiamo tuttavia prevedere di installare un lettore di Smart Card su ogni sistema su cui vogliamo utilizzare i servizi crittografici offerti dalla carta.

Per accedere ai servizi erogati dalla carta il possessore si identifica tramite un PIN o, più genericamente, tramite un codice segreto. L'accesso alla chiave privata è protetto tramite “qualcosa che la persona ha” (Smart Card) e “qualcosa che la persona sa” (PIN).

Struttura interna di una Smart Card



Crittografia nella posta elettronica

Se inviamo una lettere con un contenuto sensibile, allora la firmiamo per garantire la sua autenticità e la infiliamo in una busta chiusa per garantire la sua riservatezza.

Come possiamo firmare e imbustare una lettera elettronica? Con la crittografia dei messaggi e la firma digitale!

La codifica di un messaggio permette di scambiare informazioni riservate proteggendole da accessi indesiderati. Se un intruso o un disturbo del canale altera un messaggio, allora il destinatario quando verifica l'autenticità firma digitale scarta il messaggio come un falso. Se un impostore invia un messaggio firmato con la chiave sbagliata, allora il destinatario quando verifica l'autenticità firma digitale scarta il messaggio come un falso. La firma digitale certifica l'identità del mittente, verifica l'integrità del messaggio e garantisce la non repudiabilità del messaggio.

Legislazione sulla firma digitale

Una società pubblica o privata per emettere certificati conformi alla normativa italiana ed europea deve chiedere l'accredito presso il CNIPA. Il CNIPA (Centro Nazionale per l'informazione nella Pubblica Amministrazione) verifica che l'infrastruttura tecnologica e le procedure organizzative della società rispettino i requisiti di legge per l'emissione di un certificato a valore legale. Se il nuovo ente certificatore supera l'esame esso viene aggiunto all'elenco dei certificato accreditati. Questo elenco è disponibile sul sito del CNIPA.

Riportiamo le principali leggi in materia di firma digitale ed enti certificatori:

- Decreto Legislativo n.82 del 7 marzo 2005 "*Codice dell'amministrazione digitale* "
- Decreto Legislativo n.159 del 4 aprile 2006 con integrazione del decreto legislativo n.82 del 7 marzo 2005
- Decreto Legislativo n.10 del 23 gennaio 2002 "*Recepimento della direttiva 1999/93/CE sulla firma elettronica"*
- Decreto del Presidente del consiglio dei ministri del 13 gennaio 2004 *"Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici"*
- Direttiva n.93 del 13 dicembre 1999 del Parlamento europeo e del Consiglio con il quadro comunitario per le firme elettroniche.

Consigliamo la lettura di tali leggi e la consultazione del sito del CNIPA con le sue direttive sull'argomento.

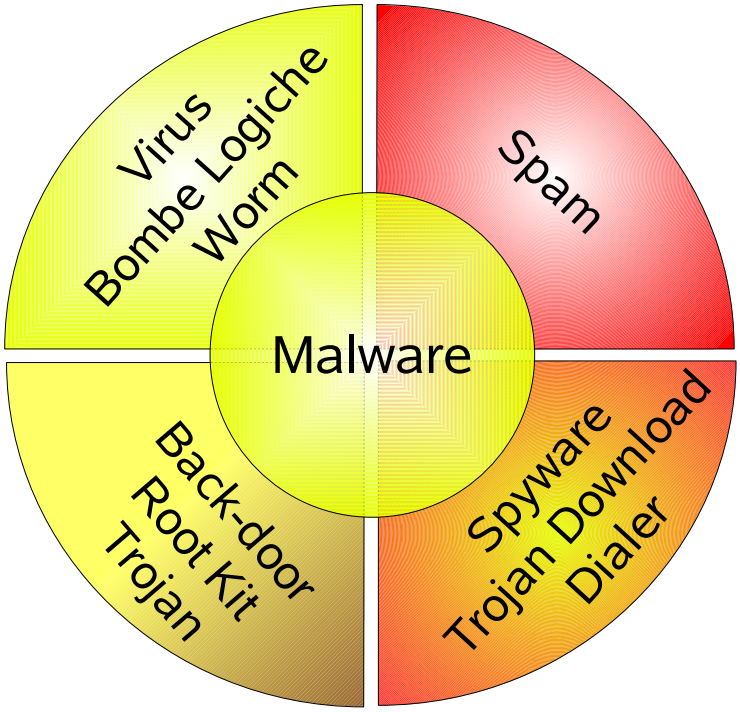
Riportiamo l'elenco delle principali leggi in materia di posta elettronica.

- Decreto Legislativo n.82 del 7 marzo 2005 "*Codice dell'amministrazione digitale"*
- Decreto Legislativo n.159 del 4 aprile 2006 con integrazione del decreto legislativo n.82 del 7 marzo 2005
- Direttiva emanata il 27 novembre 2003 dal Ministro dell'Innovazione e le Tecnologie e dal Ministro per la Funzione Pubblica *"Impiego della posta elettronica nelle pubbliche amministrazioni"*
- Decreto del Presidente della Repubblica n.68 del 11 febbraio 2005 *"Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3"*

Chi ha infettato il mio Computer?

"Aiuto... il mio PC ha preso un virus!" Ma cosa sono i virus? E gli Spyware? Come possiamo proteggerci?

Affianco a pirati in carne ed ossa, i calcolatori sono continuamente attaccati da alcuni programmi il cui scopo è diffondersi sulla rete causando danni ai sistemi colpiti e/o procurando un illecito guadagno al loro inventore. Questi programmi sono genericamente chiamati "Malware" (Malicious Software). Il più importante sottogruppo di "Malware" è costituito dai Virus. Affianco a questa minaccia tradizionale stanno emergendo nuove forme di attacco più insidiose.



Virus

I virus sono programmi autoreplicanti che, una volta eseguito, copiano il proprio codice all'interno di altri programmi del sistema infettato e cercano di propagarsi ad altri sistemi.

Così come in campo biologico, anche in campo informatico esistono molti tipo di virus.

Esistono moltissimi virus in circolazione. Nuovi virus sono creati e diffusi ogni giorno. E' comunque difficile contare e classificare i nuovi virus poiché spesso un nuovo virus è costituito da una piccola modifica di un virus preesistente. I virus si distinguono tra di loro in base alla componente del sistema infettata, alla modalità di infettare il sistema e al tipo di danno provocato.

La velocità di diffusione e la difficoltà di individuare il creatore rendono i virus il tipo più diffuso di attacco al mondo. La sicurezza dei sistemi passa quindi da una adeguata strategia antivirus.

Storicamente i virus utilizzavano molte tecniche per diffondersi: nascondendosi nei file trasferiti da un sistema ad un altro, infettando i dischetti... Oggi con l'avvento di Internet, i virus si diffondono prevalentemente sulla rete. I virus amano particolarmente nascondersi all'interno di messaggio di posta anche se non disdegnano a volte di attaccare i sistemi sfruttando una vulnerabilità nota. Ad esempio se apro un'allegato di posta che contiene un virus, questo infetta il server di posta del mio sistema, legge la rubrica e invia un messaggio contenente il virus a tutti gli indirizzi trovati. La maggior parte dei virus attacca un solo sistema operativo.

Alcuni virus infettano tutti i file, in qualche modo eseguibili, presenti sul sistema, altri solo i file con una particolare caratteristica (quelli di una certa lunghezza, quelli di un certo formato, quelli modificati in una certa data...). Nel primo caso l'obiettivo del virus è quello di propagarsi nel più breve tempo possibile. Nel secondo caso l'obiettivo è quello di infettare il sistema lasciando il minor numero di tracce possibili. In questo caso il virus riuscirà a passare inosservato più facilmente poiché avrà lasciato meno tracce sul sistema.

Alcuni virus sono dotati di meccanismi per mascherare la propria presenza. Particolarmente insidiosi sono i virus che infettano gli antivirus rendendoli incapaci di rilevarli. Per proteggere il calcolatore da questi virus l'antivirus deve rilevare il virus prima di essere infettato. Per questo motivo l'antivirus dovrebbe essere sempre attivo sul sistema e controllare tutti i nuovi file (in particolare i messaggi di posta e le pagine web).

Continuandosi a riprodursi i virus assorbono le risorse di sistema e intasano la rete, riducendo le prestazioni dell'ambiente. Non contenti di consumare le risorse dell'ambiente, la maggior parte dei virus sono programmati per danneggiare i sistemi. Il danno prodotto può essere di diversa natura: dall'alterazione di file e dati alla diffusione di informazioni (per esempio l'invio per posta elettronica dei propri file riservati), dalla cancellazione del file system alla visualizzazione a video di immagine, dall'alterazione delle funzionalità di sistema alla modifica del comportamento di una periferica.

La serietà della minaccia di un virus dipende dalla sua capacità di diffondersi e dal danno provocato sui sistemi infettati.

La velocità di diffusione e la difficoltà di individuare il creatore rendono i virus il tipo più diffuso di attacco al mondo. La sicurezza dei sistemi passa quindi da una adeguata strategia antivirus.

Una categoria particolarmente insidiosa di virus sono le “**bombe logiche**”. Esse si propagano in molti sistemi della rete in modo silenzioso, infettando il maggior numero di sistemi senza procurare apparentemente nessun danno allo stesso. Una volta diffusi al verificarsi di un evento predefinito, solitamente o ad una cerca data o in seguito di un evento esterno, tutte le istanze del virus “esplodono”, cioè si attivano ed attaccano i sistemi. Ritardando l'attacco ai sistemi, il virus aumenta considerevolmente il numero di sistemi infettati prima di essere scoperto.

Una categoria di “Malware” molto simile ai virus è costituita da **worm**. A differenza dei virus, i worm sono dei programmi autonomi e riproducono se stessi all'infinito senza infettare gli altri file di sistema. L'obiettivo più comune di questi programmi è intasare i sistemi e creare un "Denial of Service".

Non solo Virus...

Come in biologia affianco ai virus esistono altre minacce per la salute di una persona, come batteri, funghi, tossine..., così in campo informativo affianco ai tradizionali virus si stanno diffondendo altre forme di software malevolo. Lo scopo principale dei virus è quello di distruggere ed arrecare danno ai sistemi infettati, mentre lo scopo principale di questi nuovi di software malevolo è quello di carpire informazioni riservate ed ricavare un guadagno economico illecito. Questi software malevoli esegue comandi “non autorizzati” all'insaputa del possessore del calcolatore per fornire un beneficio economico al produttore del software e tentano sempre di mascherare la loro presenza.

Questi programmi spesso non si propagano autonomamente. I loro creatori sono quindi costretti a nasconderli all'interno di altri software disponibili su Internet o all'interno di ignari siti web. Una persona che scarica e installa il software interessato, installa inavvertitamente il “malware” e compromettendo la sicurezza del proprio sistema. Un altra persona interroga al sito web di un albergo, compromesso dal pirata, per vedere la disponibilità di una camera e si trova installato sul proprio sistema uno programma spia.

Fra i vari tipi di Malware ricordiamo in particolare:

- **Spyware**

  Gli spiyware sono software che raccolgono informazioni sull'utente e le sue abitudini. Le informazioni illecitamente ottenute vengono poi utilizzate per attività di spamming oppure per la clonazione di carte di credito...

- **Dialer**

  I Dialer sono un tipo particolare di spyware che modificano, in maniera silenziosa, il numero di telefono delle connessione modem o ADSL redirigerlo su un altro numero più costoso e ottenendo un illecito guadagno.

- **Back-door**

  Le porte di servizio installano un'accesso illecita al sistema. Le Back-door sono spesso lasciate sui sistemi dagli intrusi per garantirsi un punto di accesso nascosto sul sistema

- **Root Kit**

  I Root Kit forniscono una raccolta di script e file di configurazione che aiutano gli hacker a mascherare la loro presenza su un sistema. Spesso essi contengono una versione alterata dei principali comandi di sistema. Questi comandi alterati nascondono le Back-door installate e i programmi lanciati dall'intruso.

- **Trojan**

  I cavalli di Troia sono un tipo particolare di Back-door. In questo caso la Back-door è nascosta all'interno di un programmo utile diffuso gratuitamente sulla rete.

- **Trojan downloader**

  Questa categoria particolare di cavalli di Troia provvedono a scaricare i file significati su un'altro sistema, normalmente un'altra macchina precedentemente compromessa dal pirata. Egli può quindi leggere tranquillamente i file ottenuto alla ricerca di informazioni da usare per i suoi scopi illeciti.

Antivirus

Virus, worm, spyware e trojan sono una minaccia costante per i nostri sistemi. Abbiamo però un'arma per proteggerci: gli antivirus.

Gli antivirus controllano i file di un sistema, i messaggi di posta in arrivo, le periferiche di sistema e quant'altro alla ricerca di virus. Questa operazione di controllo si chiama scansione. Come la polizia cerca di individuare un ladro dalle impronte digitali lasciate sul luogo del crimine, così gli antivirus cercano di riconoscere i virus tramite la loro firma. Questa firma è rilevabile all'interno dei file infettati o della e-mail con il virus. La firma è una sequenza di bit contenente i comandi che caratterizzano il comportamento del virus e lo distingue da un programma lecito. Alla scoperta di un nuovo virus, i produttori di antivirus individuano la sua firma, cioè un segmento di codice caratteristico di questo virus, e la rendono scaricabile dagli antivirus. Una volta individuati i virus, l'antivirus li isola e cerca di eliminarli.

Esiste sempre un intervallo di tempo tra la diffusione del virus e la diffusione la sua firma agli antivirus. Durante questo periodo gli antivirus risultano impotenti contro questa minaccia.

Questo periodo può essere particolarmente lungo nel caso di bombe logiche, poiché questi virus si diffondono in maniera silenziosa e poi scoppiano tutti insieme.

Altrettanto pericolosi sono i virus che si diffondono molto rapidamente e che riesco a fare molti danni nel breve intervallo di tempo tra la sua diffusione e quella della sua firma.

Per rendere il nostro antivirus uno strumento di difesa realmente efficace, ricordiamoci di:

- lasciare l'antivirus sempre attivo per controllare tutti i file scaricati dalla rete, contenuti nella posta o importanti da un disco esterno, individuando i virus prima che contagino del sistema;
- aggiornare frequentemente l'antivirus con le nuove firme rilasciate dal produttore.
- eseguire periodicamente la scansione dei dischi interni infatti il sistema potrebbe essere stato infettato da un virus individuabile solo con l'ultimo aggiornamento.

Possiamo inoltre adottare piccoli accorgimenti per ridurre i rischi di un'infezione del nostro calcolatore.

Se riceviamo un messaggio di posta sospetto, contattiamo il mittente per chiedere chiarimenti prima di aprire il messaggio stesso e soprattutto i suoi allegati. Ad esempio, se riceviamo una mail con il titolo "I LOVE YOU" dal nostro capo, probabilmente è un virus. Possiamo eliminare questi messaggi con relativi virus prima ancora di aprirli solo se il nostro client di posta apre un messaggio e i suoi allegati solo dopo esplicito ordine dell'utente.

Se disattiviamo l'esecuzione automatica di script, applet, programmi o comandi presenti in una pagina web evitiamo di installare involontariamente spyware o altri malware, visitando semplicemente un sito web infettato.

Spam

Immaginate di essere in montagna e di vedere partire una valanga. Prima si stacca un po' di neve, poi aumenta, aumenta ancora fino a quando non vi sommerge completamente. È la stessa sensazione di chi è vittima di un'azione di spamming. La propria casella di posta riceverà una valanga di messaggi pubblicitari non richiesti fino a renderla inservibile.

Ma torniamo un passo indietro. Come hanno ottenuto il mio indirizzo di posta? Leggendolo in una discussione su una mailing list a cui avevo scritto o sul mio sito web o provando a caso delle combinazioni plausibili di indirizzi... Il metodo privilegiato rimane tuttavia l'utilizzo di **spyware**. In questo caso è sufficiente che il mio indirizzo fosse presente nell'agenda di un sistema compromesso.

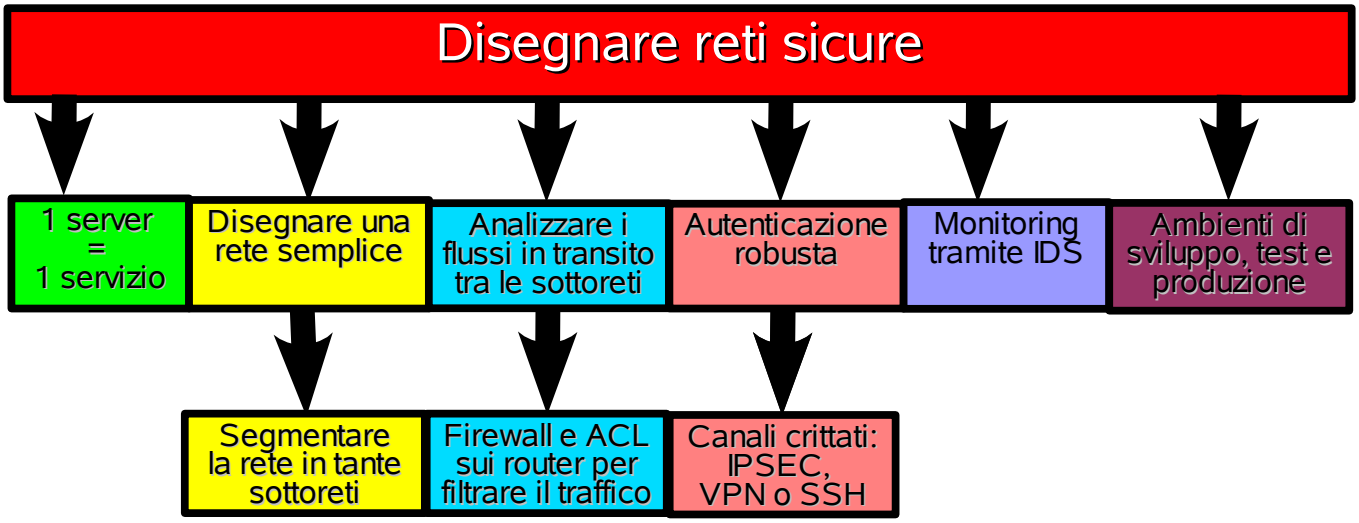
Se evitiamo di diffondere inutilmente il nostro indirizzo di posta possiamo ridurre il rischio di ricevere spam ma non eliminarlo.

Per mantenere la nostra casella di posta pulita dallo spam l'unica vera soluzione è quella di installare dei filtri antispam. Il loro funzionamento è simile a quello degli antivirus: controllano la posta ed eliminano i messaggi di spam.

Come disegno una rete informatica sicura?

Se creare un ambiente che gestisce più servizi, quale disegno adotto? È meglio una rete piatta o dividerla in più sottoreti? Quanti servizi ospito su ciascun server? Da dove gli amministro? Come posso proteggerla?

Pur non avendo la pretesa di rispondere a tutti queste domande, presentiamo alcune considerazioni su come aumentare la sicurezza del mio ambiente informatico in fase di progettazione.



Un server un servizio.

Le società e gli enti erogano diversi servizi tramite la rete. Ognuno di questi servizi ha le sue caratteristiche, i suoi dati, i suoi requisiti tecnici, le sue problematiche di sicurezza e il suo bacino di utenza.

Se un sistema ospita più servizi, allora deve garantire le funzionalità richieste da tutti i servizi e deve essere raggiunto dalle utenze di tutti i servizi. Se un pirata compromette un servizio, e il computer su cui risiede, avrà accesso a tutti gli altri servizi della macchina. Se si ha un servizio per server, quando un hacker compromette una macchina compromette un solo servizio. Distribuendo i servizi (soprattutto quelli critici) su diversi sistemi è possibile implementare politiche di accesso più articolate. Inoltre i sistemi possono essere personalizzati proprio per ottimizzare i requisiti di sicurezza di quello specifico servizio. Associando ad ogni servizio una propria macchina, i servizi possono essere posizionati in sezioni differenti della rete. Ad esempio, supponiamo di installare sulla stessa macchina il server di posta e applicativo aziendale per la richiesta delle ferie. Il servizio di posta richiede di accedere ad Internet per inviare e ricevere e-mail quindi il server risulta connesso da Internet. Se un pirata attacca il servizio di posta da Internet, riesce a compromette non solo questo servizio ma anche quello di richiesta ferie. Se invece installiamo i due servizi su due sistemi differenti, il sistema per la richiesta ferie sarà raggiungibile solo da locale e quindi un pirata da Internet non potrà raggiungere ed attaccare questo servizio.

Qualora non sia possibile suddividere i servizi su più sistemi, strumenti come le zone e il chroot permettono di creare ambienti separati sulla stessa macchina, ognuno dedicato ad un singolo servizio.

Una rete divisa in tante parti

Se la rete è molto piccola e ospita un numero limitato di servizi allora più essere piatta, cioè tutti raggiungono tutti. In questo caso il server si prende interamente carico di discriminare tra gli accessi leciti e quelli illeciti. In un'azienda o in un ente un po' più grande, divisioni diverse usufruiscono di servizi diversi. Per aumentare la sicurezza dei sistemi e per ridurre il rischio connesso ad accessi non autorizzati, può essere spesso molto vantaggioso suddividere la rete in varie sottoreti e regolamentare il traffico tra due distinte sottoreti. Se la rete è adeguatamente segmentata, è più facile posizionare sistemi per la verifica del flusso logico dei dati, filtrando l'accesso alle risorse critiche.

Architettura della rete

Distribuiti i servizi sui vari sistemi, questi devono essere inseriti all'interno della rete. Individuate le componenti con cui un servizio interagisce, scegliamo il punto della rete più adatto in cui inserirlo.

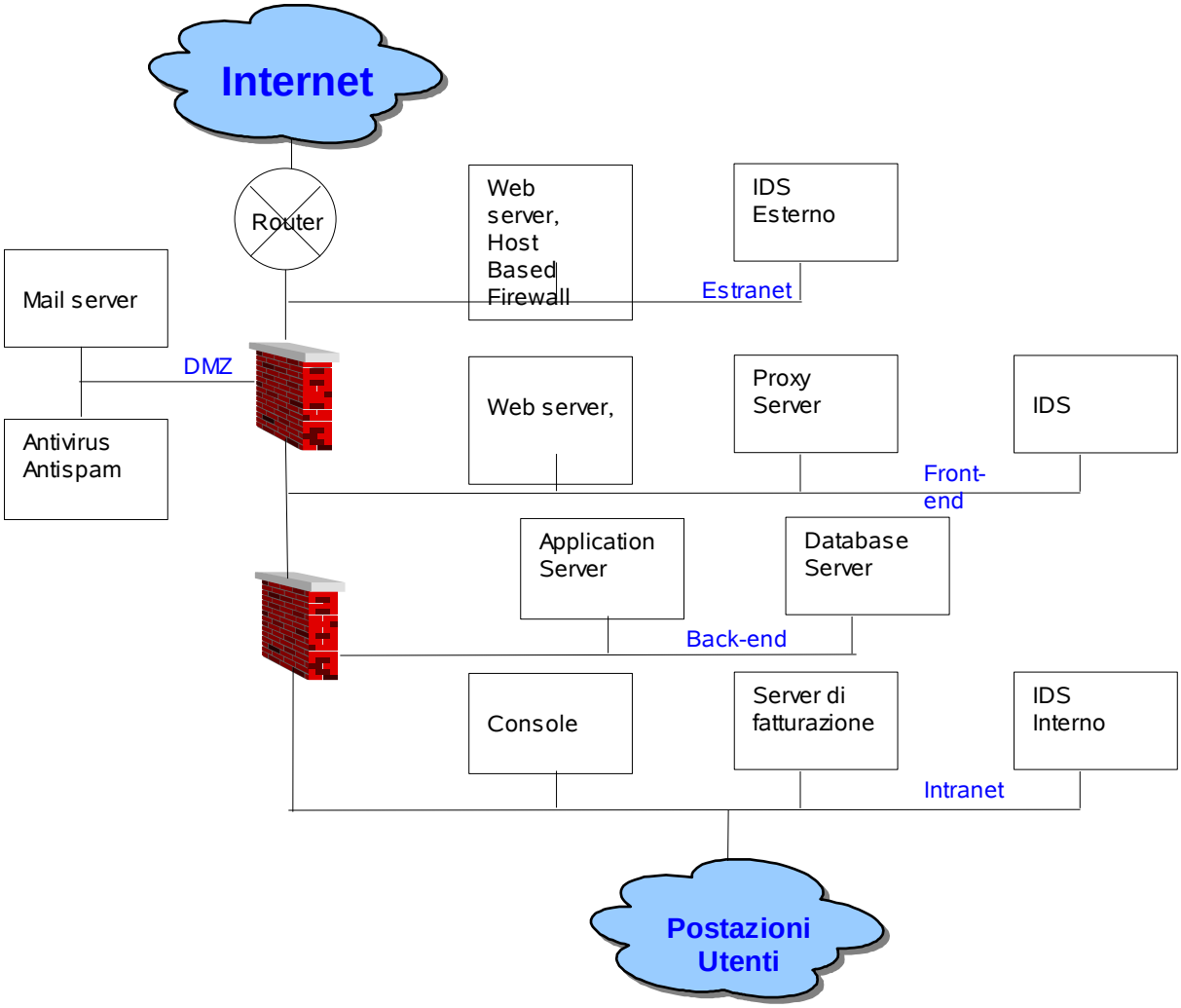
I servizi esposti su Internet (ad esempio DNS server, server di posta, sito web...) vanno posizionati in una sottorete (di solito chiamata zona demilitarizzata o DMZ) separata dal resto dell'ambiente da un Firewall. Se un pirata compromette un server della DMZ non riesce a raggiungere i servizi posizionati nella rete interna dell'azienda. Nelle grosse aziendali la rete di DMZ può essere suddivisa in più reti distinte per servizi distinti.

“Se non puoi disegnare una rete allora non puoi realizzarla!”. Se la struttura della rete è irregolare e poco schematica allora è difficile realizzarla senza commettere errori e senza introdurre buchi di sicurezza. Il disegno di una rete deve essere quindi il più semplice e regolare possibile. Più la rete è complessa ed irregolare più gli amministratori avranno difficoltà a gestirla e mantenerla. Analogamente le sottoreti e le componenti di sicurezza adottate devono essere omogenee o compatibili per garantire una loro migliore integrazione e quindi una risposta uniforme e compatta contro gli attacchi.

Una volta disegnata la rete scegliamo gli apparati di rete più appropriati (switch, router, gateway...) per gestire il traffico. Valutiamo le connessioni tra la diverse sottoreti, soprattutto quelle con l'esterno, e inseriamo gli opportuni Firewall di protezione. E' importante proteggere tutti i punti di connessione da remoto.

Si aggiungono alla rete gli strumenti di controllo e protezione dei servizi: i Proxy server, gli Intrusion Detection System (IDS), i prodotti per la gestione della rete...

Presentiamo un esempio di rete segmentata e protetta da Firewall e IDS.



Il flusso dei dati

Ultimo elemento è individuare il flusso dei dati tra le varie sottoreti e con il mondo esterno. Conoscendo approfonditamente il traffico tra i vari sistemi è molto più facile configurare le regole dei Firewall, dei router e degli IDS.

L'analisi dei flussi e delle reti attraversate dai dati ci permette di evidenziare le comunicazioni critiche da proteggere tramite connessioni codificate e quindi sicure.

Le tecniche più diffuse per creare un canale sicuro sono:

- IPSEC
- SSL
- le Virtual Private Network o VPN.

Questi tre protocolli sono descritti nel capito dedicato alla crittografia.

Controllare gli accessi alla rete

I sistemi informatici sono stati pensati per condividere le risorse e i servizi presenti sulle varie macchine. Il percorso per accedere ad un determinato servizio o applicativo può essere locale o remoto, cioè si può cercare il codice sulla propria macchina o su altre macchine. Il problema quando si richiede un servizio ad un'altra macchina è quello di verificare la reale identità di chi fornisce il servizio; in altre parole il problema è garantire il percorso attraverso la rete.

Il percorso attraverso la rete viene garantito se gli apparati di rete indirizzano correttamente i pacchetti e se alla rete possono connettersi solo le macchine autorizzate. Gli apparati di rete (router, switch ed hub) costituiscono quindi un elemento di potenziale vulnerabilità.

L'accesso a router e switch deve essere protetto da password, che devono essere scelte e protette esattamente come sono scelte e protette le password di sistema. Devono essere previste delle ACL per determinare i diritti di accesso e di modifica delle tabelle. Le tabelle di indirizzamento di switch e router devono essere definite staticamente, in modo da impedire ad un mal intenzionato di modificare il percorso del pacchetti.

Il controllo degli accessi e dei pacchetti in transito tra le varie reti è un elemento essenziale nell'integrazione tra le varie sottoreti. Possono essere previsti dei filtri a livello di router o di firewall per controllare e limitare il traffico in transito tra due reti. Per accessi da reti esterne al sistema (Internet o reti di partner) si può prevedere un sistema di autenticazione dell'utente sugli apparati di difesa perimetrale (Firewall o router). Si può provvedere inoltre a proteggere ulteriormente le comunicazioni con l'esterno tramite canali crittati realizzati dagli stessi protocolli o tramite VPN.

Gli utenti che accedono al sistema informatico dall'esterno sono particolarmente vulnerabili. Per questo motivo si raccomandano sistemi di autenticazione forte per queste tipologie di utenze, come tocken card, crittografia, protocollo di domanda e risposta.

La connessione tra due sottoreti aziendali posizionate in due sedi diverse viene realizzata tramite o una linea dedicata o una qualsiasi linea pubblica (ad esempio Internet).

In una linea dedicata i due estremi della linea sono definiti staticamente e non possono essere cambiati. Inoltre contratti specifici con le società di telecomunicazioni permettono di definire la banda di trasmissione. Questa soluzione è vantaggiosa per tutte le connessioni permanenti tra due sedi. L'uso di una normale linea pubblica risulta abbatte i costi di gestione, ma aumenta i rischi connessi all'uso.

Utilizzando una linea pubblica, i due nodi terminali della linea si devono identificare tra loro per garantire che le due reti connesse siano quelle attese. In questo caso la reciproca autenticazione avviene automaticamente a livello di apparati di rete. Comunemente si usano dei firewall capaci di identificarsi tra loro e di creare una VPN tra le due reti.

Sviluppo, test e produzione

Quando vogliamo fornire un nuovo servizio per prima cosa lo sviluppiamo, poi lo testiamo per controllare il risultato e quindi lo eroghiamo mettendolo in produzione.

In ognuna di queste fasi l'interazione con l'ambiente circostante è diversa. Suggeriamo di separare in tre reti differenti, l'ambienti di sviluppo, di test e di produzione.

- **Ambiente di sviluppo**

  L'ambiente di sviluppo è un ambiente molto instabile dove sistemi e software sono in continua evoluzione. Gli sviluppatori possono cambiare frequentemente le configurazioni di sistema e provare soluzioni differenti. Non tutte le componenti sono già sviluppate e attive. In attesa del loro sviluppo i progettisti spesso usano soluzioni momentanee meno sicure. Ad esempio in attesa di abilitare un canale crittografico tra due componenti, le comunicazioni avvengono provvisoriamente in chiaro.

  In ambiente di sviluppo sono presenti software come compilatori, editori di testi e programmi di debug non presenti negli altri ambienti.

  Gli applicativi in fase di sviluppo risultano quindi più vulnerabili della loro versione finale, sia per la presenza di bachi individuati e rimossi in fase di test sia perché in certe fasi del loro sviluppo sono presenti alcune funzionalità ma non i relativi controlli di sicurezza.

- **Ambiente di test**

  Nell'ambiente di test o collaudo i progettisti controllano e testano i prodotti, le patch e gli aggiornamenti prima di installarli nell'ambiente di produzione. I test servono per individuare eventuali problemi senza causare un interruzione del servizio erogato. Esso ha una configurazione analoga a quella dell'ambiente di produzione.

- **Ambiente di produzione**

  L'ambiente di produzione ospita il servizio che viene effettivamente erogato. L'accesso a questo ambiente dovrebbe essere limitato ai soli amministratori.

Firewall: la prima barriera di protezione

Una banca per proteggere l'accesso alle sue filiali installa metal detector e porte antisfondamento, abilita un sistema di telecamere a circuito chiuso e si dota di guardie giurate all'ingresso. Per controllare l'accesso ad una base, i militare presidiano armati il cancello e verificano l'identità di tutte le persone che vogliono entrare.

Nel caso di una rete informatica, come facciamo a proteggere i punti di accesso? Riusciamo a controllare chi entra? Come ci proteggiamo da attacchi provenienti dall'esterno?

I Firewall sono la risposta a molte di queste domande. Essi proteggono i punti di accesso al nostro ambiente poiché controllare il traffico in transito ed eliminano tutti i flussi non autorizzati.

Esistono molti tipologie di Firewall, ma esse possono essere raggruppate in due macrocategorie:

- **Network Base Firewall**

  Questi Firewall sono componenti autonome di rete che proteggono le reti informatiche dal traffico esterno analizzando e scremando tutto il traffico in transito tra due o più reti.

- **Host Base Firewall**

  Questi Firewall sono dedicati alla protezione di un singolo sistema su cui risiedono e controllano tutto il traffico da e per se stesso.

Come ogni componenti di rete, anche i Firewall sono potenzialmente vulnerabili. Essendo la linea di difesa più esterna, essi subiscono il maggior numero di tentativi di attacco o di aggiramento. La sua configurazione e la sua messa in sicurezza costituiscono quindi un elemento cardine della difesa delle infrastrutture informatiche.

Delegare tuttavia la sicurezza dei sistemi ai soli Firewall tuttavia è molto pericoloso poiché gli attacchi possono partire dall'interno dell'azienda oppure possono sfruttare una vulnerabilità di un servizio erogato.

Le ultime generazioni integrano i servizi tradizionali erogati dai Firewall con altre funzionalità, come antivirus e VPN, e collaborano con altri strumenti di sicurezza come gli Intrusion Detection System.

Network Base Firewall

I Firewall Network Base sono componenti di rete autonome preposte a gestire e filtrare il traffico in transito tra due o più reti. Essi svolgono la funzione di un router infatti indirizzano i pacchetti tra le varie reti. I Firewall utilizzano diverse strategie per discriminare i pacchetti autorizzati da quelli illeciti. La scelta del Firewall è condizionata dalla strategia difensiva adottata.

Proviamo a presentare i principali criteri di cernita dei pacchetti adottati dai Firewall:

- **Packet filtering Firewall**

  Essi rappresentano la prima categoria di Firewall sviluppata. Essi controllano l'indirizzo sorgente, l'indirizzo destinatario e la porta destinataria di un pacchetto, e li confrontano con le proprie regole. Le regole predefinite indicano al Firewall qual è la corretta gestione del pacchetto in esame. Per mandare ciascun pacchetto ricevuto al servizio corretto, un sistema associa ad ogni servizio una porta (cioè un numero) e discrimina i pacchetti in funzione della porta destinataria associata. Per facilitare la comunicazione tra i vari ambienti sono stati definiti degli standard per associare su tutti i sistema la stessa porta per gli stessi servizi informatici. Quando un cliente crea una nuova connessione ad un servizio, il server apre una nuova porta dedicata alla sessione in corso. Il numero di questa nuova porta è compreso tra 1024 e 16384. Per questa ragione nei Firewall di tipo Packet filtering devono essere sempre lasciate aperte le porte presenti in questo intervallo.

  Questi Firewall verifica inoltre la corrette corrispondenza tra l'indirizzo di un pacchetto e l'interfaccia di rete di provenienza. I Packet filtering Firewall sono semplici da configurare. Essi riescono a gestire velocemente un elevato traffico di rete. Di contro non riescono a controllare e filtrare particolari comandi di un protocollo e non rilevano la presenza di virus o codice malevole.

- **ACL dei Router**

  Molti router di nuova generazione riescono a filtrare i pacchetti comportandosi come un Packet filtering Firewall. Questa funzionalità è realizzata tramite le ACL (Access Control List). Il Firewall installato su un router, cioè su un hardware dedicato, è più veloce e gestisce più interfacce ma può essere integrato con un numero bassissimo di funzionalità. Questi Router possono essere un valido primo livello di protezione per limitare la propagazione di pacchetti.

- **Stateful Inspection Firewall**

  Gli Stateful inspection Firewall sono una evoluzione dei Packet filtering Firewall. A differenza dei loro predecessori, questi Firewall sono in grado di gestire le sessioni e in particolare le porte aperte per ogni connessione. Essi quindi non richiedono di aprire sul Firewall tutte le porte superiori alla 1024. Questo tipo di Firewall possiede infatti una tabella contenente lo stato di tutte le connessioni stabilite tra i sistemi esterni e quelli interni.

- **Dedicated Proxy Server**

  I Dedicated Proxy Server sono Firewall dedicati a controllare le connessioni di uno specifico protocollo e quindi a uno specifico servizio. Essi possono fare dei controlli molto più estesi sul protocollo in esame. Possono essere configurati per lasciar passare i comandi solo se appartengono ad un sottoinsieme configurato dall'amministratore. Verificano le informazioni inviati ed eliminano i pacchetti contenenti dati in un formato errato o illecito. Questo tipo di Firewall ha anche l'abilità di richiedere un'autenticazione di tutti gli utenti di rete (tramite userid e password, token, autenticazione dell'indirizzo del calcolatore, autenticazione biometrica, etc.).

  Genera solitamente un log più dettagliato rispetto ai precedenti due tipi di Firewall. Analizzando in profondità i protocolli, questi Firewall non riescono a gestire nuovi tipi di

applicativi e impiegano più tempo a processare ogni singolo pacchetto. I Proxy Server per regolamentare la consultazione di pagine web sono l'esempio più comune di questo tipo di Firewall. Per proteggere gli ambienti informatici si affiancano spesso i Proxy Server dedicati ai servizi più critici ai Firewall tradizionali.

- **Application Proxy Gateway Firewall**

  Application Proxy Gateway Firewall sono dei Firewall che integrano un Statefull Inspection Firewall con Proxy agent dedicati ai servizi più rilevanti o più diffusi. Ciascun Application Proxy Agent gestisce un particolare applicativo o protocollo (HTTP, FTP, LDAP...).

I Firewall moderni erogano servizi aggiuntivi inclusi NAT (Network Address Translation), PAT (Port Address Translation) DHCP (Dynamic Host Configuration Protocol), VPN (Virtual Private Network), antivirus o filtri a livello applicativo.

Firewall Host Based

Gli Host Based Firewall proteggono un singolo sistema da attacchi esterni. Esso più essere usato per proteggere server particolarmente vulnerabili all'interno della rete locale o per proteggere i portatili.

Uno svantaggio nell'impiego di questi tipi di Firewall è il seguente: per ogni sistema deve essere installato un Firewall dedicato ed amministrato separatamente. Se il numero dei server cresce oltre un certo numero risulta più semplice ed economico creare una sottorete dedicata con un Firewall a protezione della rete.

I computer portatili sono, come dice la loro parola, mobili quindi non è possibile demandare la loro protezione ad apparati di rete poiché possono essere collegati su qualunque rete. I portatili insieme ai computer di casa direttamente connessi con Internet sono i principali candidati su cui installare gli Host Based Firewall.

Consideriamo il caso di un impiegato che si connette all'ufficio da casa passando per Internet e consulta dei dati riservati. Se un pirata compromette il PC di casa di questa persona allora ottiene le informazioni riservate.

I Firewall destinati a queste postazioni, chiamati anche Personal Firewall, erogano anche altri servizi come

- strumenti avanzati di autenticazione dell'utente
- VPN client per collegarsi al proprio ufficio su un canale crittato
- antivirus
- strumenti per registrare e tracciare tutti il traffico effettuato

La gestione di questi Firewall può essere centralizzata. Quando un portatile si collega con la rete aziendale, il Firewall scarica la versione aggiornata delle policy dalla console centralizzata e gestita dagli amministratori.

Come avviene per gli antivirus, i personal Firewall devono essere attivi e non semplicemente installati per fornire una protezione efficace.

Dove stanno di casa i Firewall?

I Firewall servono a proteggere i nostri accessi verso l'esterno quindi dovrebbero essere installa su ogni connessione con l'esterno. Le connessioni dall'esterno non sono solo le connessioni con Internet ma anche quelle con partner, fornitori e clienti. Molti attacchi mirati ad una rete ben protetta sono oggi effettuati passando tramite le rete di terze parti. Se un'azienda non protegge queste connessioni risulta vulnerabile contro questi tipi di attacchi. Per reti grosse e complesse, possiamo prevedere l'installazione di un Firewall a protezione di sottoreti particolarmente sensibili.

I Firewall possono essere inseriti in molti modi all'interno della nostra architettura. Presentiamo i tre schemi più utilizzati.

- **Il Firewall perimetrale.**

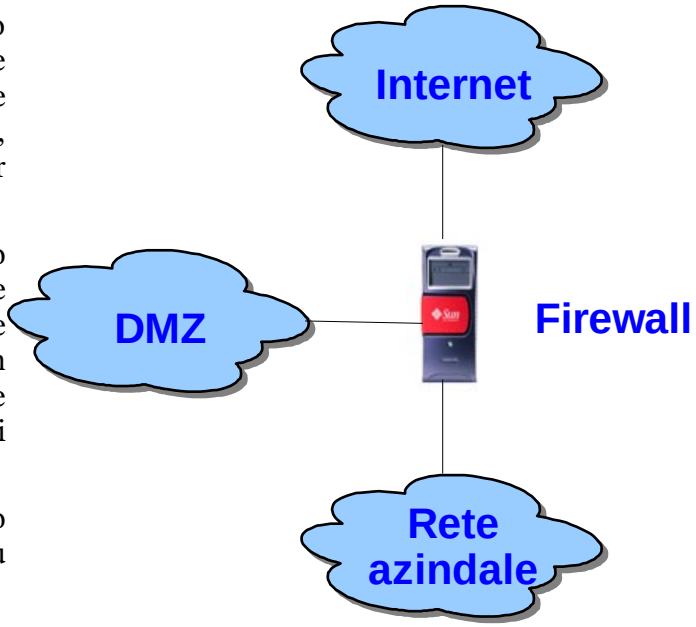
Il Firewall collega la rete locale con la rete esterna e protegge le macchine aziendali da hacker esterni. In questo schema tutte le macchine aziendali sono posizionate sulla stessa rete dietro il Firewall.

- **Firewall con la rete DMZ (zona demilitarizzata).**

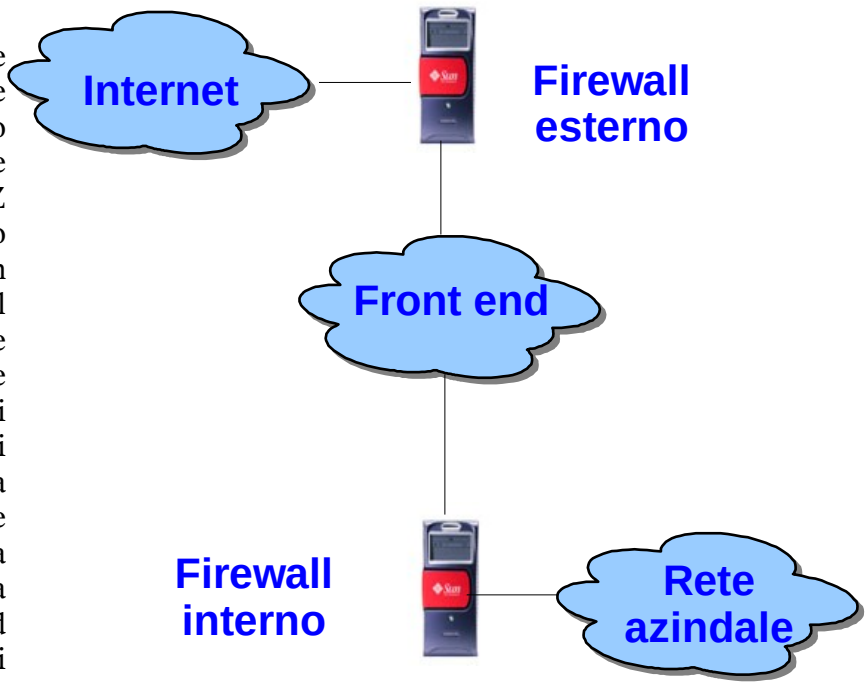
Il Firewall collega anche in questo caso la rete locale con la rete esterna. Esso collega queste due reti con una terza, chiamata DMZ, che ospita un gruppo di server particolarmente sensibili.

Con questa architettura creiamo un ambiente protetto per queste macchine. Contemporaneamente un hacker che compromette un server sulla DMZ deve passare comunque dal firewall prima di raggiungere la rete interna.

In architetture complesse posso dividere i server in due o più DMZ.



- **Firewall su due livelli.**



Questa struttura prevede l'utilizzo di due Firewall. Il primo Firewall collega la rete esterna con la rete DMZ (chiamata in questa caso anche Front-End). In secondo Firewall collega questa rete intermedia con la rete interna. In ambienti molto complessi possiamo prevedere una rete suddivisa in tre livelli. In questo caso la rete esterna è collegata con la rete di Front-End che ospita i servizi consultati da Internet (come i Web server). Questa è collegata ad una seconda rete rete chiamata Back-End che ospita i servizi più critici (Application Server, DataBase Server) consultati dai sistemi di Front-End.

La rete di Front-End o di Back-End è collegata tramite il Firewall alla rete interna dell'azienda.

I Firewall di tipo Packet filtering possono essere disponibili su alcuni sistemi operativi come Linux o Solaris, per controllare il calcolatore invece di una rete. Il vantaggio di questa soluzione è che il server risulta ben protetto, come se fosse posizionato dietro il Firewall su una rete separata, senza richiedere la creazione di un sottorete dedicata.

Canali crittografici

Per proteggere lo scambio di informazioni tra due sistemi sulla rete, possiamo codificare i dati (come abbiamo già affrontato nel capitolo “I miei dati sono riservati? Critto tutto”) e poi inviarli oppure possiamo creare un canale crittografico e trasmettere i dati su questo canale. In questo capitolo presentiamo le soluzioni può diffuse per la creazione di un canale crittografico.

- **VPN**

  Le VPN (Virtual Private Network) sono delle reti virtuali sicure costruite sopra dei canali non sicuri. Esse costruiscono un canale virtuale tra due componenti e garantiscono la riservatezza delle informazioni scambiate, l'integrità dei messaggi e la mutua autenticazione.

  Un esempio tipico di applicazioni VPN è la creazione di un canale sicuro per connettere tra loro due sedi di un'azienda o un portatile con la rete aziendale passando per Internet. Un'azienda non ha controllo su Internet (o più in generale su una rete esterna) quindi considera la comunicazione esposta a rischi. Per proteggerla costruisce uno strato di rete aggiuntivo (VPN) sopra la rete pubblica. Questo strato aggiuntivo critta tutti i pacchetti prima di inviarli a un livello più basso. La rete pubblica scambia questo strato con un normale servizio TCP e quindi lo gestisce correttamente senza ulteriori modifiche. Le VPN possono essere costituite tramite software appositamente installato su macchine e/o su apparati di rete. I Firewall sono i candidati ideali a svolgere le funzioni di VPN concentrator. Molti Firewall possono infatti creare canali crittografici con chi si trova all'esterno della rete (sedi periferiche, portatili, partner...) e controllare le comunicazioni con l'interno della rete.

- **SSL**

  SSL (Secure Socket Layer) è un protocollo standard di rete per la creazione di un canale crittografico utilizzato da un applicativi. Esso si posiziona tra il livello TCP e gli applicativi, come le VPN. Essendo uno standard, SSL è il candidato ideale per gestire le sessioni crittate dei servizi standard (web, DNS, connessioni ai server di posta...). SSL usa la crittografia a chiave pubblica per la fase preliminare di mutua autenticazione e di scambio di una chiave simmetrica. Usa poi un chiave simmetrica di sessione per creare un canale crittografico su cui scambiarsi i dati.

  Gli algoritmi simmetrici disponibili per le sessioni SSL sono IDEA, DES, 3-DES, RC2, RC4, Fortezza. Gli algoritmi asimmetrici disponibili per le sessioni SSL sono RSA, DSA, Fortezza, Diffie-Hellman.

- **IPSEC**

  Il protocollo IPSEC nasce come un ampliamento del protocolli IP, introducendo alcuni servizi supplementari. In particolare aggiunge la cifratura delle informazioni e dei pacchetti in transito, l'autenticazione del mittente e l'integrità dei dati. La cifratura del pacchetti protegge le comunicazioni dal rischio di intercettazione e di perdita della riservatezza del contenuto. Alle informazioni tradizionali sul pacchetto, il protocollo IPSEC permette di aggiungere alcune informazioni supplementari per la verifica dell'identità del mittente. Infine IPSEC prevede dei meccanismi e delle informazioni aggiuntive per controllare l'integrità dei dati trasmessi.

Rispetto alle VPN e a SSL questa soluzione ha il vantaggio di essere completamente trasparente verso gli applicativi. Essi non sono in grado di distinguere se il messaggio viaggia su una rete IP o IPSEC. D'altra parte le connessioni IPSEC richiedono di configurare tutti gli apparati di rete per autorizzare il transito del traffico IPSEC, mentre VPN e SSL non richiedevano modifiche sulla rete. Inoltre IPSEC codifica tutto il traffico, incluso le comunicazioni che potrebbero viaggiare in chiaro.

Sicurezza dei Media

"Ho perso i CD con su le foto del mare", "non trovo più la chiavette con su tutta documentazione del nuovo progetto", "mi hanno rubato il palmare con su i dati della mia carta di credito"...

Un CD che ho comprato ad 1 euro, vale un euro? Qual è il valore reale di un media?

I media dei calcolatori sono tutti gli strumenti finalizzati a contenere, memorizzare e trasportare le informazioni, come dischi, cassette, nastri, CD o stampanti. Il valore di un media è pari al valore del supporto fisico più il valore delle informazioni conservate.

Compromettere il media equivale ad impossessarsi delle informazioni critiche del sistema. I media contenenti informazioni sensibili devono essere protetti in modo analogo al metodo di protezione dei sistemi che elaborano tali informazioni. Le cassette, i dischetti, i nastri, CD, DVD hard-disk esterni, chiavette USB e i fogli di carta, una volta riempiti con i dati e rimossi dagli appositi apparati, (lettori di DVD e CD, porte USB, stampanti, fax...) devono essere conservati in luoghi sicuri e dismessi con processi sicuri, come la formattazione del dischetto o triturare i fogli di carta sensibili.

Requisiti di legge per il trattamento dei dati personali

I seguenti articoli dell'appendice B del Decreto Legislativo n. 196 del 30 giungo 2003, "*Codice in Materia di protezione dei dati personali*", forniscono indicazioni precise sui requisiti relativi alla gestione dei Media contenenti dati sensibili.

Art 21 *Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.*

Art. 22 *I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.*

Come verifico il livello di sicurezza

Prima di immettere sul mercato un nuovo modello di autovetture, la casa produttrice effettua dei crash test. Questi test simulano diversi tipi di incidenti stradali e verificano i danni riportati dalle vetture. Essi dimostrano se le dotazioni di sicurezza della macchina sono davvero efficaci in caso di incidente.

Ritornando all'ambiente informatico, possiamo analogamente testare come i nostri sistemi si comportano sotto attacco? Si, posso simulare il comportamento di un intruso. I penetration test sono delle prove di intrusione effettuate da specialisti di sicurezza. Analogamente ai “crash test” queste prove servono a verificano la robustezza della soluzione e a individuare l'anello debole.

Cos'è un penetration test?

Un “penetration test” è una simulazione di un attacco informatico.

Una società che vuole verificare il livello di sicurezza di un ambiente commissiona l'attività di “penetration test” a un gruppo di esperti di sicurezza informatico. Questo gruppo può essere interno od esterno all'azienda. L'importante è scegliere persone che non sono state coinvolte nella progettazione delle misure di sicurezza. Chi progetta un'architettura non è un buon candidato a verificarla.

Il “penetration test” ricerca le potenziali vulnerabilità del sistema permettendo di rimuoverle. Vengono continuamente scoperte nuove vulnerabilità e nuovi tipi di attacco. Una verifica periodica del sistema permette di eliminare le vulnerabilità e le criticità associate ai nuovi tipi di attacco.

E' importante ricordare che la sicurezza del network è pari alla sicurezza del suo anello più debole. Testeremo l'intero sistema per trovare quell'anello debole e per rinforzarlo nel modo più opportuno.

Quale approccio seguire?

Quando una persona sceglie un'automobile, segue alcuni parametri di scelta che risultano essere strettamente personali. Una auto piccola per girare in città o una grossa per portare molto bagaglio. Una macchina adatta ad andare sullo sterrato oppure una comoda per lunghi viaggi in autostrada. Una berlina o una monovolume...

Analogamente per scegliere le modalità di esecuzione dei “penetration test” un'azienda o un ente deve prima di tutto capire gli obiettivi che vuole raggiungere.

Per prima cosa, i gestori dei sistemi devono scegliere l'approccio da seguire. Vogliono fare delle simulazioni il più aderente possibile al comportamento di un intruso esterno? Vogliono cercare il maggior numero possibile di vulnerabilità dei sistemi? Vogliono porsi nel caso peggiore: un intruso che conosce l'ambiente?

Il primo approccio ai test, chiamato “**Black Hat**”, ha lo scopo di capire quanto tempo e quanto lavoro deve fare un generico hacker per entrare sui sistemi. Negli attacchi “Black Hat” nessuna

informazione preliminare è fornita al Black Hat Team, in particolare:

- Il Team non riceve nessuna informazione sulla tipologia della rete. Nel caso in cui si voglia effettuare i test solo su una parte della rete, il Team riceve le informazioni necessarie a delimitare la sottorete ma nessuna informazione su come è strutturata all'interno la sottorete in esame.
- Il Team non riceve nessuna informazione sul tipo e la configurazione dei sistemi, dei Firewall e degli apparati di rete.
- Il Team non riceve nessuna informazione sugli applicativi e sui dati trattati.
- Al Team non è fornito nessun accesso aggiuntivo ai sistemi.

In sintesi possiamo dire che i test "Black Hat" si avvicina di più ad un attacco reale, perché si avvale dell'attacco al “buio” solitamente sfrutta una sola vulnerabilità per dimostrare in quanto tempo è possibile violare la rete. Spesso nei test “Black Hat” il Team cerca di effettuare tutti i test in maniera silenziosa , senza far scattare gli allarmi degli IDS o dei Firewall. In questo modo seguono completamente il comportamento di un intruso. Questi attacchi silenziosi servono per verificare l'efficacia degli allarmi.

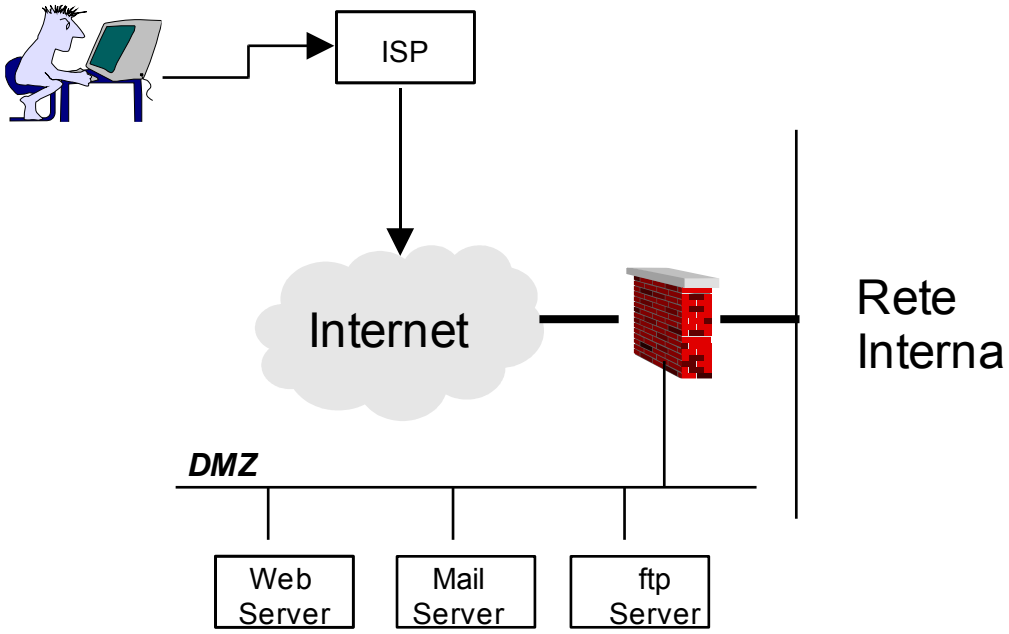
L'approccio opposto è chiamato **“White Hat”**. Il "White Hat" è orientato a verificare la sicurezza dei sistemi tramite un'analisi approfondita a 360 gradi. Essa esamina tutti i punti deboli e ricerca tutte le vulnerabilità dell'ambiente. La fase di “attacco” viene preceduta ed accompagnata da interviste, raccolta dati sui sistemi e sugli apparati di rete e analisi della documentazione. Il White Hat Team deve ricevere dall'organizzazione tutte le informazioni necessarie a capire dove ci possono essere eventuali vulnerabilità (Network Plan, Flussi informativi, Documentazione dei servizi, Firewall Policy...).

Il White Hat Team parte da una posizione privilegiata rispetto ad un generico intruso. I “White Hat” test simulano le intrusioni portate da questi attaccanti privilegiati (dipendente, partner, fornitore, cliente...).

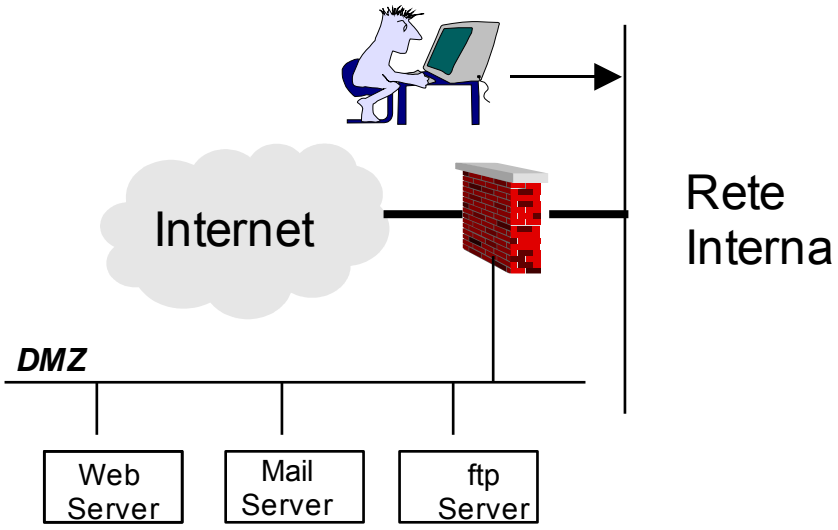
Avendo come obiettivo primario la ricerca delle criticità di sicurezza, in questo tipo di test i White Hat Team, di solito, attaccano a tappeto l'ambiente, facendo scattare gli allarmi di sicurezza.

Scelta la filosofia, i gestori del sistema si trovano davanti ad un secondo dilemma. Da dove provengono le minacce ai sistemi? Da dove devono partire i Penetration test? Dall'interno o dall'esterno? In poche parole i gestori devono scegliere se il punto di partenza degli attacchi deve essere posizionato su Internet o sulla intranet aziendale. Con postazioni d'attacco posizione davanti ai Firewall (su Internet), i test individuano i servizi raggiungibili da Internet e le loro vulnerabilità. I test da Internet sono più adatti all'approccio Black Hat. Con postazioni d'attacco posizione dietro ai Firewall (sulla intranet locale), i test individuano tutti i servizi erogati e le loro vulnerabilità. I test dalla intranet sono più adatti all'approccio White Hat. Alcuni Penetration Test prevedono di effettuare attacchi sia da Internet che dalla intranet.

Un esempio di Probing remoto (da Internet)

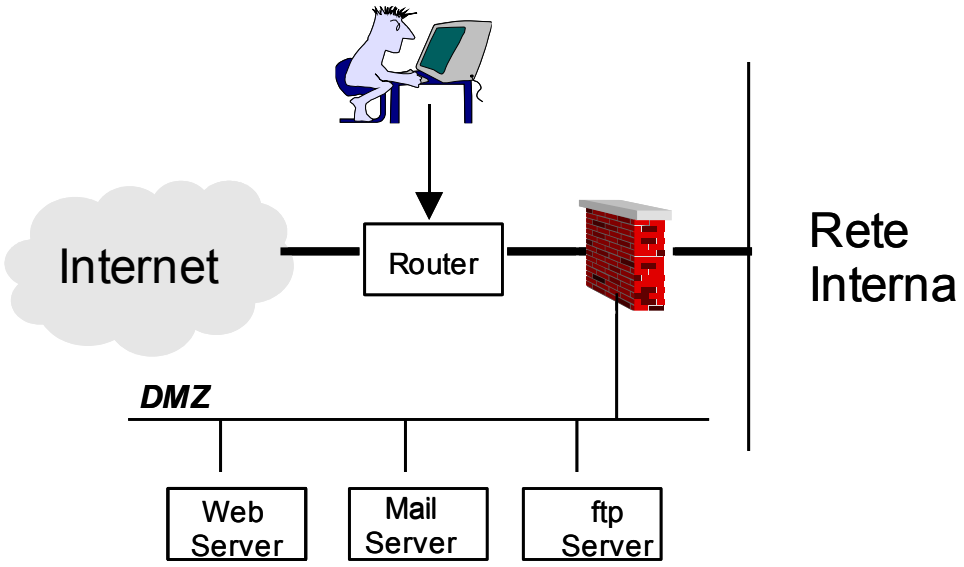


Un esempio di Probing locale (dalla intranet)



Spesso si vuole evitare il transito su Internet delle informazioni raccolte senza perdere i vantaggi di un probing dall'esterno. In questo caso il Team si posiziona all'esterno del firewall ma prima della connessione verso Internet.

Un esempio di Probing esterno senza transito di dati su Internet.



Il terzo elemento da valutare nella scelta di un Penetration Test è la modalità di esecuzione dei test:

- **Test manuale**

  Nei test manuale gli esperti di sicurezza analizzano i servizi disponibili sulla rete. Sulla base delle informazioni raccolte definiscono script ad hoc per provare ad attaccare i servizi individuati. Il test manuale consente una maggiore flessibilità infatti esso segue percorsi diversi a seconda dei risultati ottenuti in ciascuna prova. Si ha sempre sotto controllo la situazione.

  Di contro, i test manuali richiedono un maggior investimento in termini di tempo e risorse.

- **Test automatico**

  Nei test automatici gli esperti eseguono programmi di scansione e ricerca vulnerabilità. Questi test sono più veloci ma meno flessibile e più impreciso. Essi infatti si limitano a controllare un insieme di vulnerabilità note. Generano spesso falsi positivi.

Durante i Penetration test gli esperti di sicurezza usano spesso un approccio misto: prima eseguono i tool automatici per fare una panoramica sulle vulnerabilità dei sistema e poi provano a violare il sistema con test mirati, circoscritti dai risultati forniti dai tool.

Quali test effettuare?

Le autovetture sono sottoposte a diversi crash-test. Ad esempio, il test dell'Alce serve a verificare la tenuta di strada in presenza di brusce sterzate. Il test di urto frontale contro un muro serve invece a verificare la robustezza dell'abitacolo. Analogamente esistono diversi test per verificare la sicurezza informatica di un ambiente. Illustriamo brevemente i più comuni.

- **Port-scanning**

  Il Port scanning è una scansione sistematica della rete alla ricerca dei sistemi attestati sulla rete. Per ogni sistema individuato esso ricerca le porte TCP e UDP aperte, i servizi ICMP

attivi. Questa scansione cerca di ricavare a grandi linee la topologia di rete e di individuare le difese perimetrali (firewall, router etc). Questo test viene solitamente eseguito tramite tool automatici.

- **Operation System Identifications**

  Questo test individua il tipo e la versione di sistema operativo presente sulla macchina. Questa conoscenza permette di provare solamente solamente le vulnerabilità relative alla versione di sistema operativo individuato. Questa informazioni permette quindi di restringere significativamente il cerchio delle vulnerabilità da provare e di abbassare i tempi di esecuzione dei successivi test.

  Questo test viene solitamente eseguito tramite tool automatici.

- **Network Mapping**

  Il Network Mapping mira a tracciare un disegno della rete nel modo più preciso e fedele possibile. Cerca di individuare gli apparati di rete presenti (firewalls, router, switches, access server etc), il loro modello, la loro configurazione e il loro ruolo all'interno della rete. Esso isola i segmenti di rete più critici. Attraverso le scansioni o query particolari sul NIS si possono apprendere le relazioni con altri network e ricercare relazioni di "Trust".

- **Vulnerability scanning**

  Una volta identificati la versione di Sistema Operativo e i servizi attivi, si può passare alla fase di enumerazione e "exploiting" delle vulnerabilità. Essa richiede particolari conoscenze sui sistemi operativi e sulle loro vulnerabilità. Sono richieste competenze avanzate sulle tecniche di programmazione sufficienti per la scrittura del codice necessario per diverse piattaforme. Per scrivere questi script è necessaria la conoscenza di linguaggi a basso livello come C e Assembler e naturalmente essere a conoscenza di particolari tecniche per "l'exploiting" dei programmi. Senza queste conoscenze non è possibile creare questi strumenti e si deve ricorrere ai tool automatici. Esistono tool automatici per ricercare le vulnerabilità. Essi effettuano dei test per capire se esistono queste vulnerabilità, ma poi non provano effettivamente ad entrare sui sistemi sfruttandole. Per questo motivo spesso generano falsi positivi. Inoltre essi provano solo un insieme predefinito di vulnerabilità.

- **Web Vulnerability scanning**

  I siti web rappresentano la strada privilegiata dalle aziende e dai singoli cittadini per farsi conoscere, per trattare affari e per erogare servizi. Il Web Vulnerability scanning deriva dai Vulnerability scanning. Esso analizza i soli siti Web: valuta la corretta gestione degli accessi a pagine inesistenti, il formato delle pagine, la correttezza sintattica di tutti gli script presenti sul sito e i controlli effettuati sui dati inviati al sito.

- **Denial of Services test**

  I Denial of Services (Negazione del servizio) sono attacchi mirati a interrompere l'erogazione di un servizio. Questi attacchi cercano di solito di esaurire la banda di rete oppure una risorsa del servizio erogato. In questi casi il sistema non riesce più a soddisfare le richieste legittime in un ragionevole intervallo di tempo. Un risultato analogo lo posso raggiungere confondendo gli apparati di rete. In questo caso il servizio viene interrotto perché le richieste non raggiungono il server ma si “perdono” nella rete. Il concetto fondamentale è che risulta più facile fermare un sistema che non ottenere un accesso

illegale. Questi attacchi sono i più comuni e rappresentano una minaccia costante per le reti aziendali.

Per effettuare test che simulino questi tipi di attacchi le competenze richieste sono minime, infatti tutti gli strumenti necessari sono già pronti e scaricabili da Internet.

- **War-dialing**

  Il war-dialing è una scansione delle linee telefoniche di una azienda alla ricerca di accessi alla rete informatica. Questo test ricerca le possibilità di intrusione sfruttando modem o altri apparati di interconessione tra la rete telefonica e la rete informatica. I punti di ingresso ad una rete aziendale via rete telefonica sono innumerevoli: per interventi di emergenza fuori orario lavorativo, per i dipendenti in trasferta, per partner e fornitori, per una piccola filiale. Poiché questi punti di accesso sono noti ad un sottoinsieme fidato di persone, gli amministratori tendono a considerarli "sicuri" e quindi non adottano tutti le misure di protezione adottate per gli accessi ad Internet. Questo errore di valutazione risulta spesso fatale. Un pirata informatico può fare una scansione dei numeri telefonici assegnati ad una azienda ed individuare facilmente questi accessi. Affianco agli accessi ufficiali l'attività di war-dialing rileva anche eventuali modem installati dai singoli dipendente per accedere da remoto alla propria postazione. Questi accessi "clandestini" rappresentare una "back door", cioè una porta di ingresso non protetta. I Test di War-dialing individuano questi accessi permettendo all'azienda di rimuoverli.

- **Sniffing**

  Lo Sniffing è l'ascolto di tutto il traffico di rete alla ricerca di informazioni utili. Se l'accesso ai sistemi non avviene su canali crittati allora ascoltando il traffico di rete un hacker può carpire le credenziali degli utenti legittimi ed entrare sui sistemi. L'intruso può inoltre leggere messaggi di posta elettronica confidenziali, file contenenti informazioni finanziarie e così via. I Test di Sniffing mostrano quali informazioni può carpire un eventuale ascoltatore indesiderato.

- **Social Engineering**

  I Test di Social Engineering mostrano se è possibile carpire informazioni riservate ad dipendenti di un'azienda con l'inganno.

Come si rilevano gli intrusi?

Per proteggere l'accesso ai locali di una banca ci sono pareti in cemento armato, metal detector alla porta e vetri infrangibili. Nonostante questo è possibile che un ladro riesca ad entrare all'interno della banca confondendosi tra i clienti della stessa. Per questa ragione la banca è dotata di un sistema interno di allarme azionabile da un cassiere e di una guardia giurata.

Tornando al nostro calcolatore, abbiamo visto gli strumenti per proteggere i sistemi, gli accessi ai sistemi e il traffico tra la rete interna e le varie reti esterne. Pur avendo attivato tutte queste precauzioni, un intruso potrebbe riuscire a trovare un modo di aggirarle. Se l'attacco avviene dall'interno, cioè da una persona che può accedere direttamente alla rete locale, l'intruso può riuscire ad accedere alle macchine senza passare dal firewall. Se un intruso attacca un sistema sfruttando una vulnerabilità appena scoperta di un servizio lecito, allora riesce a superare il firewall e ad accedere al sistema aggiornato aggirando gli strumenti di autenticazione. È quindi essenziale capire chi c'è sulla rete? Cosa sta facendo? È un traffico corretto? Lo strumento informatico per controllare il traffico e distinguere i flussi autorizzati dagli attacchi è l'"Intrusion Detection System (IDS).

Strumenti elettronici di controllo, come gli IDS rilevano eventuali attacchi o incidenti di sicurezza e li segnala in tempo reale. Se individuiamo un intruso all'opera, allora possiamo prendere tempestivamente delle contromisure per limitare i danni del pirata, per individuarlo e perseguirlo penalmente.

Come funzionano gli IDS?

Gli Intrusion Detection System seguono tutti uno stesso schema nel trattamento dei dati:

- **collezionare** gli eventi in atto su una sorgente (calcolatore o rete)
- **analizzare** i dati ricercando attacchi o anomalie
- **rispondere** all'attacco con un allarme e con le opportune contromisure.

Esaminiamo più da vicino ciascuna fase ed individuiamo le principali differenze tra i vari tipi di IDS.

Prima di tutto come raccoglie un IDS le informazioni? Quali sono le sue fonti?

Tornando all'esempio della banca, la guardia giurata raccoglie le sue informazioni controllando dei monitor collegati alle telecamere di sorveglianza e guardando direttamente cosa succede nei locali della banca.

E gli IDS che informazioni collezionano?

Gli IDS possono catturare tutto il traffico in transito su una rete rimanendo in ascolto in maniera silenziosa. In questo primo caso si chiamano IDS Network Based. Gli IDS possono controllare gli eventi generati da un calcolatore risiedendo sullo stesso. In questo secondo caso si chiamano IDS Host Based.

Raccolti i dati, come il analizzano? Un IDS come riconosce il traffico lecito dagli attacchi?

Tornando all'esempio della banca, la guardia giurata distingue i rapinatori dagli ostaggi perché i primi sono armati e puntano la pistola contro le altre persone mentre i secondi sono disarmati e con le mani in alto. Anche gli IDS sono in grado di riconoscere le "armi" dei attaccanti dal traffico normale usando una tecnica chiamata **"misure detection".** Come "arma", molti attaccanti usano delle sequenze precise di comandi finalizzate a verificare la robustezza del sistema e a violarlo sfruttando una vulnerabilità nota. Queste sequenze di azioni sono chiamate "**firme dell'attacco**". Questo tipo di IDS analizza il traffico cercando la presenza di firme note. Come gli antivirus questi sistemi richiedono un aggiornamento frequente delle firme per proteggersi dai nuovi attacchi. Questi sistemi individuano solo attacchi noti quindi lasciando il sistema esposto a nuove forme di violazione. Questo metodo genera pochi falsi allarmi. Questa soluzione è tipicamente utilizzata dagli IDS di tipo commerciale.

Esiste una seconda tecnica chiamata **"anomaly detection"**. Questo secondo metodo riconosce il traffico normale generato dagli eventi legittimi e segnala come possibile attacco tutto il traffico anomalo presente sulla rete. Questa tecnica richiede una fase di rodaggio per apprendere quali sono gli eventi legittimi. Questo metodo è in grado di riconoscere come anomalo anche il traffico generato da un nuovo tipi di attacco, tuttavia genera molti falsi positivi appesantendo il lavoro degli amministratori. Il metodo "anomaly detection" è attualmente usato solo da alcuni IDS sperimentali per scopi di ricerca.

Il terzo elemento nella scelta di un IDS è la tecnica di risposta ad un attacco. Come un intervento rapido della guardia può sventare una rapina, così una risposta rapida di un IDS ad un attacco riesce a limitare i danni e spesso ad individuare i colpevoli. In alcuni casi gli IDS forniscono, oltre agli allarmi, anche strumenti per bloccare l'attacco in corso.

Alcuni IDS Network Based prevedono funzionalità aggiuntive come la rete alla ricerca di vulnerabilità note.

IDS network based

Gli Intrusion Detection Network Based System catturano i pacchetti in transito sulla rete. Essi analizzano tutto il traffico in chiaro in transito sulla rete alla ricerca di firme note di attacco.

Molti di questi sensori analizzano il traffico in modalità "stealth" cioè leggono il traffico in transito sulla rete ma hanno un proprio indirizzo di rete. I pirati hanno grosse difficoltà a localizzarli. L'installazione di questi IDS ha un impatto molto limitato sul funzionamento di una rete preesistente.

Come collegarli alla rete?

Molti apparati di rete forniscono una porta dedicata per gli IDS a cui inviano una copia dei pacchetti in transito. I questo caso l'IDS è in grado di controllare tutto il traffico gestito dall'apparato. Se una rete è piatta allora posso posizionare l'IDS in un qualunque punto della rete e catturare tutto il

traffico. Se una rete invece è segmentata in tante sottoreti, con apparati sprovvisti di porte dedicate al controllo del traffico, allora essa non si presta ad accogliere un IDS.

Dove posizionare un IDS per avere il maggior beneficio per l'azienda?

- **L'IDS può posizionarsi all'esterno del Firewall principale.**

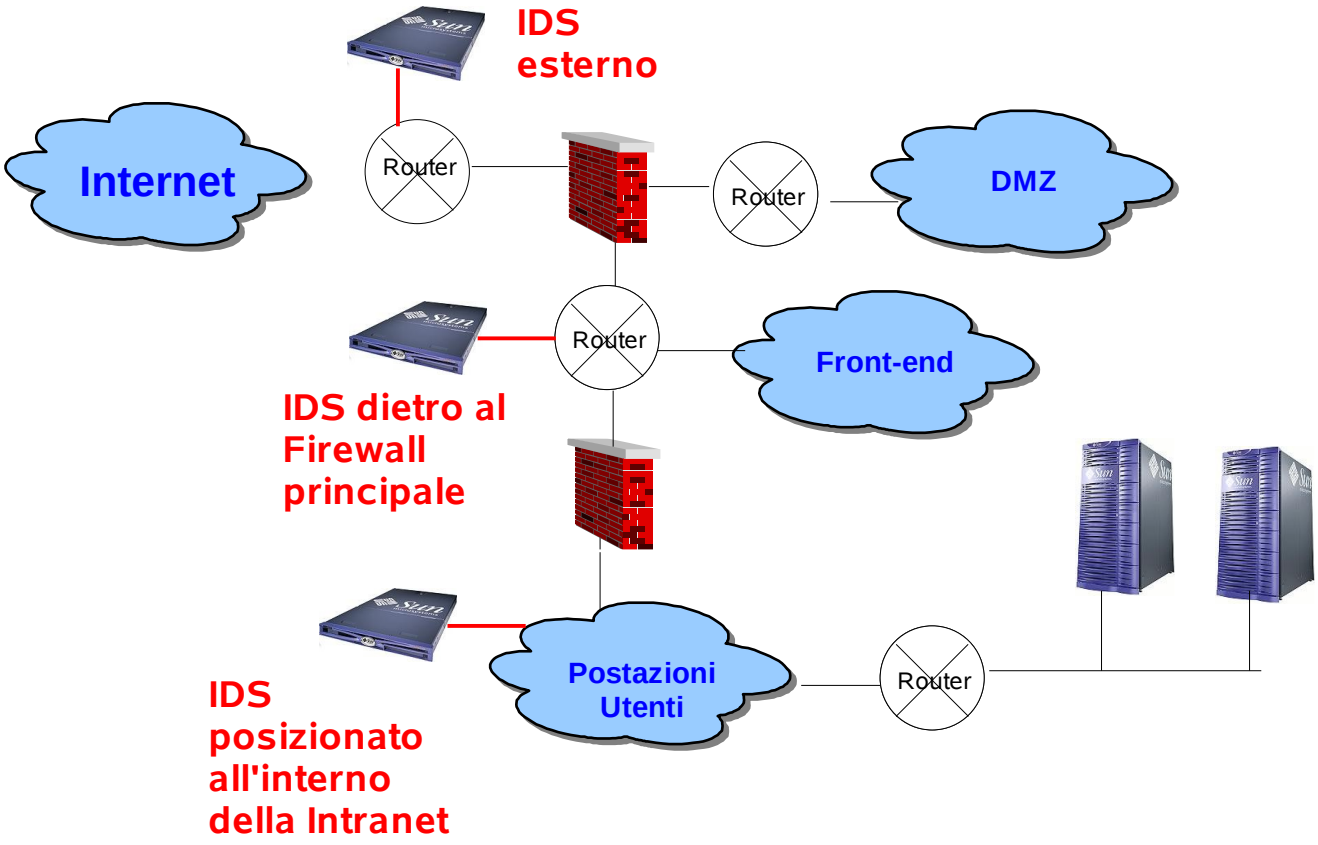
  Questa soluzione permette di rilevare tutti gli attacchi provenienti dall'esterno e diretti contro la rete aziendale, inclusi tutti quelli fermati dal Firewall. Essa fornisce una panoramica completa delle minacce a cui la nostra rete è esposta. Tuttavia essa non è in grado di dire se l'attacco è stato bloccato dal Firewall. Questa soluzione ovviamente non rileva nessun attacco proveniente dalla rete locale.

- **L'IDS può posizionarsi all'interno del Firewall principale.**

  Questa soluzione permette di rilevare tutti gli attacchi provenienti dall'esterno e diretti contro la rete aziendale che sono riusciti a superare il Firewall. Scartando gli attacchi fermati dai Firewall, questo IDS rileva solo gli attacchi potenzialmente pericolosi. Questa soluzione mostra gli eventuali limiti della configurazione dei Firewall.

- **L'IDS può essere posizionato nella rete aziendale.**

  La rete aziendale è la rete in cui sono posizionati i dipendenti. Questo IDS si preoccupa di proteggere la rete aziendale da attacchi interni e da attacchi esterni che hanno superato le difese perimetrali. In questa posizione l'IDS ha un grosso carico di lavoro infatti analizza tutto il traffico aziendale.

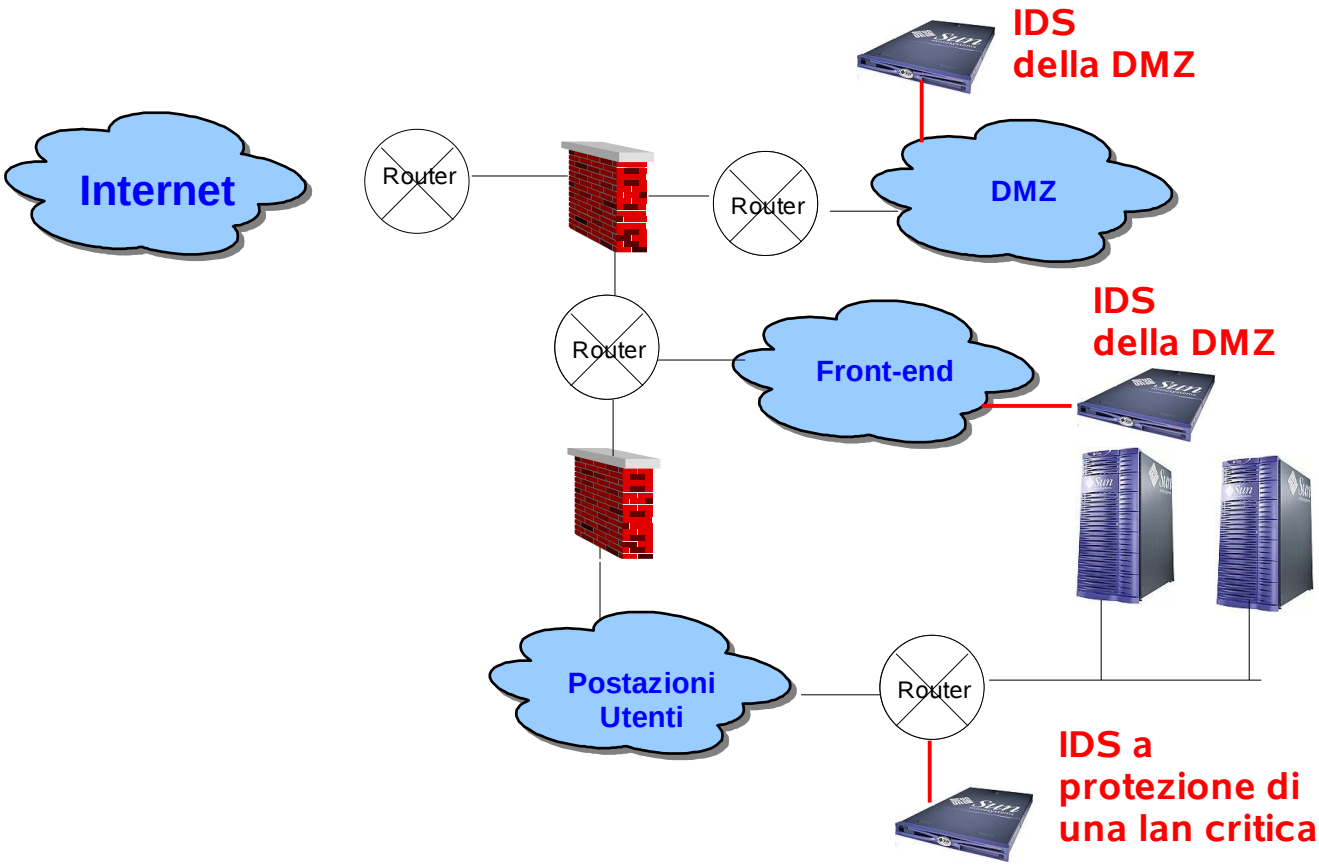


- **L'IDS può essere posizionato nella DMZ.**

  Questo IDS protegge e controlla tutti i calcolatori presenti sulla DMZ, sia da attacchi provenienti dalla rete interna che da attacchi provenienti dall'esterno capaci di superare i Firewall. Questa soluzione mostra gli eventuali limiti della configurazione dei Firewall. L'IDS controlla inoltre tutto il traffico tra le macchine della DMZ.

- **L'IDS può essere posizionato in una sottorete critica.**

  Questo caso è un caso analogo al precedente. Nella sottorete critica sono posizionati di solito i server più importanti per l'azienda.



IDS Host Based

Come i Firewall Host Based, gli Intrusion Detection Host Based System sono dedicati a controllare gli eventi in corso sul solo sistema su cui risiedono. L'analisi sul singolo sistema è molto più completa. Essa infatti integra l'analisi del traffico di rete con l'analisi dei file di sistema e dei processi attivi. Gli IDS Host Based normalmente ricevono le informazioni ed individuano gli incidenti analizzando i log e gli strumenti di audit forniti dal sistema. Essi rilevano se l'intruso è riuscito ad entrare nel sistema e quali danni ha fatto. D'altra parte se un pirata compromette una macchina, allora può disabilitare il suo IDS.

Come nel caso dei Firewall Host Based, questa soluzione è adatta a proteggere sistemi particolarmente critici o postazioni mobili (come i portatili).

Perché usare gli IDS?

Proviamo a capire quali vantaggi possono derivare dall'introduzione di un IDS all'interno di un ambiente informatico.

1. **Scoraggiare impiegati e consulenti maliziosi.**

   Spesso impiegati e consulenti si collegano direttamente alla rete locale e raggiungono i server senza passare dal firewall. Se una persona percepisce un inadeguato livello di controllo del sistema allora è portato a pensare: “voglio provare ad entrare, tanto non se ne accorge nessuno!” Se i dipendenti e i consulenti sono a conoscenza della presenza di strumenti di controllo del traffico, come un IDS, allora sono scoraggiati e a volte desistono.

2. **Individuare gli attacchi a servizi leciti.**

   Molte intrusioni sui sistemi provenienti da Internet sfruttano vulnerabilità note dei servizi forniti dal sistema. Il firewall non è quindi in grado di rilevare questi attacchi all'interno del traffico lecito e li lascia passare. Esiste sempre un intervallo di tempo tra la scoperta di una vulnerabilità e l'installazione della patch associata. Durante questi periodi gli IDS possono individuare comportamenti anomali dovuti ad attacchi ai sistemi e limitare i danni.

3. **Individuare le analisi preliminari.**

   Come una banda prima di effettuare una rapina ad una banca effettua sopralluoghi della scena del crimine, così un pirata prima di attaccare un sistema raccoglie informazioni tramite una combinazione di più azioni lecite e/o illecite finalizzate. Un esempio tipico di analisi preliminare è la ricerca di tutte le porte aperte sul sistema (probing). Se un IDS individuano un probing allora gli amministratori possono controllare il potenziale hacker riuscendo a bloccarlo prima che danneggi i sistemi.

4. **Fornire informazioni utili sull'intruso e sulle azioni da esso compiute.**

   Gli IDS raccolgono molte informazioni sugli attacchi in corso, sui sistemi coinvolti, sugli servizi interessati e sulla fonte degli attacchi. Tutte queste informazioni permettono spesso di poter perseguire penalmente i criminali.

Ho registrato tutto!

Tipicamente, i sistemi informatico registrano le attività svolte dal sistema stesso in file chiamati "file di log". Il file di log rappresenta per un sistema informatico ciò che la scatola nera rappresenta per un sistema di trasporto aereo. A seguito di un indicente posso ricostruire cosa è successo.

Che cosa registro?

Nella scatola nera di un aereo vengono registrate tutte le informazioni utili per capire a posteriori cosa è successo: le comunicazioni con la torre di controllo, le informazioni degli apparati di bordo, l'assetto dell'aereo, i comandi di volo dati dal pilota. Ovviamente non vengono registrati quanti caffè sono stati distribuiti dalle hostess oppure le conversazioni tra i passeggeri.

Analogamente è fondamentale capire quali eventi generati dal sistema o dagli applicativi tracciare.

Ma quali sono le informazioni significati da archiviare?

Alcuni sistemi consentono la abilitare una registrazione degli eventi estremamente dettagliata, capace di tracciare le singole "system call" (chiamate di sistema) effettuate dal comandi e dai programmi. Ma è utile una registrazione così dettagliata?

Non esiste una risposta universale a queste domande. Caso per caso dovremo individuare l'adeguato livello di registrazione tenendo conto di diversi elementi:

- **L'importanza delle informazioni trattate**

  Il livello di sicurezza richiesto dai sistemi di una base militare è differente dal livello di sicurezza richiesto per il sito di un cinema. Nel caso dei sistemi militare può essere fondamentale registrare ogni singola operazione e le persona che l'ha eseguita; nel caso del sito del cinema può essere sufficiente registrare solo gli errori e gli eventi anomali per ricostruire la dinamica di un incidente.

- **Requisiti di legge**

  La legislazione vigente può richiedere la registrazione di alcuni eventi (ad esempio l'accesso ai sistemi) se il sistema tratta alcuni tipi di dati (ad esempio dati sanitari).

- **Capacità di archiviare informazioni**

  Se un sistema produce un log molto dettaglio ma poi sovrascrive il file ogni minuto per mancanza di spazio allora il file prodotto non è di nessuna utilità. L'esempio precedente posta all'eccesso un problema diffuso nella gestione dei file di log: i log prodotti devono poi essere archiviati.

- **Capacità di analizzare i log prodotti**

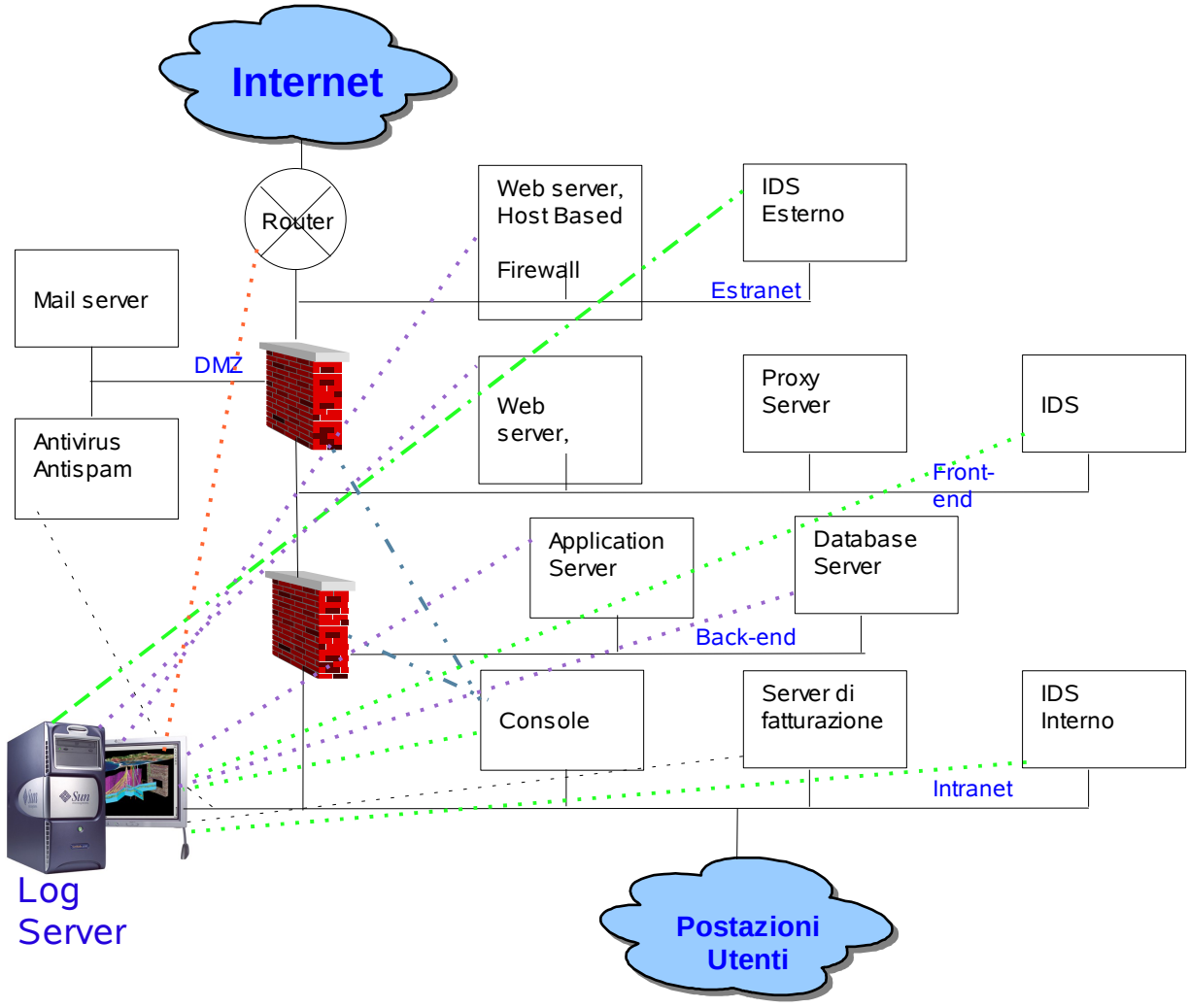
  Perché siano utili i log generati devono poi essere anche analizzati per individuare eventuali problemi. A seguito di un incidente, l'amministratore deve essere in grado di capire dai log prodotti cosa è successo. Con un log troppo ridotto l'amministratore non è in grado di capire chi a fatto cosa. Con un log troppo esteso un amministratore può non essere in grado di individuare gli eventi significati in tempo utile in mezzo a tutti i dati raccolti.

Nei file di log i sistemi operativo registrano una serie di eventi, inclusi gli errori occorsi e la diagnostica degli apparati hardware. Non a caso, molti strumenti di diagnosi e risoluzione delle problematiche hardware e software fanno riferimento ai log di sistema per ottenere le informazioni sugli eventi occorsi.

Concentrazione dei log e la correlazione degli eventi

Gli applicativi e i sistemi possono memorizzare dati in file testuali o i file binari. Il primo tipo di archiviazione è di immediata lettura ma risulta più facilmente alterabile da un intruso. Un file di log binario richiede un tool specifico per la consultazione ma è più difficile modificarlo senza lasciare traccia.

Il file archiviato sul sistema risulta sempre comunque alterabile da parte di un eventuale intruso. Per questa ragione può essere utile archiviare una coppia dei file di log anche su di un altro sistema dedicato a questo scopo e chiamato “log server". I “log server” risolvono i problemi di capacità di storage di apparati come i router e gli switch.



Su questi server, raccogliamo una copia della tracciatura degli eventi generati da sistemi differenti tra loro (firewall, apparati di rete, sistemi...). Un pirata quando attacca un ambiente lascia tracce su sistemi diversi. Ad esempio, sui firewall rimane traccia di un tentativo di accesso a servizi bloccati, sui router rimane traccia di flussi anomali, sui DNS server rimane traccia di un traffico superiore alla norma e sul sistema rimane traccia di operazioni errate finalizzate a sfruttare una vulnerabilità nota. Presi singolarmente i precedenti eventi potrebbero essere stati causati da un errore o da un evento accidentale. Considerati complessivamente essi segnalano che i sistemi sono sotto attacco. Per rilevarlo tempestivamente può essere utile correlare tra loro gli eventi generati sulle diverse componenti di rete. I prodotti di correlazione degli eventi permettono di normalizzare i log generati da diverse fonti, di analizzarli e di rilevare tracce di attacchi lasciati su più sistemi.

Conservare i log

Abbiamo visto come usare i log per l'analisi dei problemi e come concentrare tutti i file su un log server. Il log server è una soluzione utile per proteggere i dati e centralizzare la loro gestione. Ma volendo conservare tutti i log per un lungo periodo di tempo, la memorizzazione sui dischi del log server potrebbe risultare una soluzione costosa ed inefficiente. Una buona gestione dei log richiederebbe di archiviarli periodicamente su supporti off-line come cassette, CDROM, DVD, DLT... Per aumentare la sicurezza della gestione di questi media possiamo prevedere di crittografare i dati prima di archiviarli e di identificare l'insieme di persone autorizzate a consultarli.

Ognuna di queste opzioni ha un certo costo in termini di prodotti e di risorse uomo quindi è essenziale identificare i log da conservare a lungo termine e determinare per quanto tempo conservarli. I log candidati ad essere conservati per lungo tempo sono quelli relativi a sistemi che trattano dati personali sensibili, transazioni economiche, progetti militari... ed infine le informazioni di carattere strategico per l'azienda. Chiaramente le politiche di archiviazione dei log devono essere il frutto di scelte strategiche dei dirigenti aziendali. Esse devono evitare sia di sottodimensionare gli archivi che di sovradimensionarli per evitare di produrre all'azienda stessa più costi che benefici.

Sono stato attaccato, panico... cosa faccio?

Nei capitoli precedenti abbiamo affrontato il problema di proteggere e di controllare il nostro sistema. In questo capitolo forniremo alcuni consigli su come comportarci se un hacker ha superato tutte le misure di sicurezza adottate.

Come reagire?

Consideriamo per esempio i gestori di un sito web per la gestione dei conto correnti. Essi hanno protetto la loro rete con un Firewall e un IDS, l'accesso ai web server con un sistema di autenticazione robusta e hanno aggiornato periodicamente tutto il software. Hanno attivato un log esteso dei server e memorizzate le informazioni su un sistema dedicato. Una mattina, arrivando in ufficio, essi si trovano di fronte a quello che non si sarebbero mai aspettati di vedere: un defacement del sito web (ovvero collegandosi al sito compare una pagina completamente diversa da quella solita). Questo disastro è stato causato da un intruso. Panico!!! Ed ora? Cosa fare?

I gestori del sito si trovano di fronte ad una serie di priorità da gestire:

- la scoperta delle eventuali manomissione dei dati
- la scoperta della vulnerabilità sfruttata e la conseguente chiusura della stessa
- la ricerca dell'autore dell'attacco per tutte le azioni legali che conseguono.
- l'immediata rimessa in linea del sito originale

La prima preoccupazione di un hacker, una volta penetrato in un sistema è quella di nascondere la propria presenza, operando in maniera molto rapida e precisa anche sui file di log e cercando di cancellare tutte le tracce. Se gli amministratori reagiscono velocemente possono individuare l'intruso ancora all'opera. Scoprire le tracce lasciate dall'Hacker ha un duplice scopo:

- capire come è entrato e prendere le adeguate contromisure
- raccogliere prove sul crimine compiuto per poter perseguire penalmente i responsabili

La raccolta e l'analisi dei dati deve seguire regole precise se vogliamo ottenere prove rilevanti per un procedimento penale. Questa analisi è effettuata da esperti di sicurezza interni od esterni all'azienda. I dati considerati sono la configurazione dei sistemi danneggiati, i dati degli IDS e i log archiviati. La metodologia di analisi, chiamata "Analisi Forense", permette inoltre di individuare la vulnerabilità sfruttata dal pirata e le contromisure da adottare. Imparare dagli errori e dagli attacchi è il solo modo per prevenire il ripetersi di tali eventi.

Per poter imparare dai propri errori occorre:

1. individuare la causa dell'evento e le componenti coinvolte
2. cercare i meccanismi capaci di prevenire tali incidenti (ad esempio l'installazione di un aggiornamento) e il motivo per cui non sono stati applicati (ad esempio un intervallo di tempo troppo lungo tra due aggiornamenti del sistema)

3. verificare se gli strumenti di controllo hanno segnalato tempestivamente il problema
4. adottare le contromisure individuate ed aggiornare le procedure

Soltanto dopo aver raccolto i dati necessari si può procedere a ripristinare il sistema. Prima di tutto abbiamo bisogno di una copia integra del sistema (sistema operativo, applicativi, dati...). Ci serve in poche parole una copia di back-up del sistema e dei dati. Se vogliamo ridurre al minimo la perdita dei dati è essenziale effettuare frequenti salvataggi dei dati (almeno delle modifiche effettuate dopo l'ultimo salvataggio).

Installiamo di nuovo la macchina usando questi back-up. A volte il nuovo sistema risulta non funzionare correttamente poiché è sprovvisto di alcuni dati o di alcuni file. Se questi errori emergono durante un ripristino di emergenza allora corriamo il rischio di impiegare molto tempo per risolverlo e di perdere informazioni importanti. La soluzione a questo problema è effettuare test periodici di ripristino dei sistemi per verificare la bontà dei dati salvati.

Reagire in fretta

Il danno agli affare e all'immagine dell'azienda o dell'ente sono strettamente legati al periodo intercorso tra l'attacco e il ripristino della situazione iniziale. Le probabilità di perseguire l'intruso diminuiscono con il passare del tempo. È quindi fondamentale rispondere in fretta.

Se i gestori dei sistemi improvvisano la reazione da adottare allora probabilmente reagiranno per tentativi in modo disordinato. In queste situazioni gli amministratori possono essere presi dal panico e perdere definitivamente informazioni rilevati. Se la società invece si è dotata di una procedura per la gestione delle emergenze allora reagirà tempestivamente attivando i gruppi appropriati. Se una persona sa chi contattare in caso di errore, guasto o incidente allora lo segnalerà tempestivamente.

Reagire in tempo reale: Business Continuity

Ritorniamo all'esempio del sito bancario. Se ho effettuato un back-up giornaliero dei dati allora perdo tutte modifiche sui calcolatori dall'ultimo back-up. L'unica soluzione a questo problema è un piano di “Business Continuity”. Il piano di Business Continuity permette di riprendere il servizio dal punto in cui era stato interrotto su un nuovo sistema.

Proviamo a capire quali sono i passi per costruire un piano di Business Continuity:

1. Individuare i servizi e quindi le componenti da inserire nel piano.

   Per esempio, prevedere un piano di Business Continuity per i terminali dei dipendenti probabilmente più costoso di un giorno di inattività dei dipendenti o della perdita di una parte del lavoro dell'ultimo giorno. Invece perdere le transazioni bancarie di una giornata lavorativa ha un costo molto maggiore di prevedere un piano di Business Continuity dei sistemi che gestiscono i conti correnti dei clienti.
2. Identificare i requisiti d’erogazione per ogni servizio inserito nel piano (le connessioni di rete, il software, i dati...).
3. Valutare se il nuovo ambiente debba avere la stessa potenza di calcolo e di memoria di

quello originale. Spesso i sistemi di emergenza possono essere meno potenti poiché gestiscono solo un sottoinsieme di operazioni critiche.

4. Identificare l'ubicazione di tutti i sistemi critici e stabilire la sede per i sistemi di Business Continuity.

   Se l'erogazione del servizio deve essere garantita anche in presenza di grosse calamità (alluvioni, terremoti, eruzioni vulcaniche, attacchi terroristici...) allora i sistemi di emergenza di devono in una regione distinta.

5. Stabilire il meccanismo di allineamento in tempo reali dei dati sul sistema di emergenza con quelli sul sistema principale.
6. Definire le responsabilità e le azioni da intraprendere per il ripristino del servizio sul sistema di emergenza, se il sistema principale è fuori uso.
7. Definire un piano di test per provare periodicamente i sistemi di emergenza ed addestrare il personale.

Requisiti di legge per il trattamento dei dati personali

Per i sistemi che trattano dati personali e sensibili il del D.Lgs. n. 196/2003 fornisce requisiti di legge sul salvataggio dei dati.

I seguenti articoli dell'appendice B del D.Lgs. n. 196/2003 “Codice in Materia di protezione dei dati personali” forniscono indicazioni precise sul salvataggio delle informazioni trattate e il ripristino dei servizi.

Art. 18 *Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.*

Art. 23 *Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.*

Come avere giustizia?

Supponiamo di essere nello scenario peggiore: un intruso è entrato sui nostri sistemi e ha fatto diversi danni. Vogliamo avere giustizia! Cosa fare? Come reagire?

Prima di tutto **contattiamo le forze dell'ordine**, in particolare la "Polizia Postale e delle Telecomunicazioni" e seguiamo tutte le sue indicazioni. Se la comunicazione è tempestiva allora i poliziotti possono rintracciare l'intruso prima che esca dai nostri sistemi. In poche con una denuncia tempestiva la polizia può arrestare l'intruso in flagranza di reato.

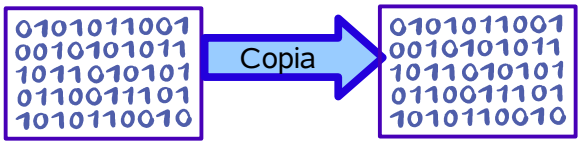
Il secondo passo è **isolare i sistemi compromessi scollegando tutte interfacce di rete.**

Un errore molto comune è quello di spegnere i sistemi. Spegnendo il sistema perdiamo tutti i dati presenti in memoria. Se l'intruso si è limitato a lanciare comandi in memoria e non ha installato nulla allora spegnendo la macchina perdiamo ogni sua traccia. Le procedure di chiusura di molti sistemi operativi aggiornano la configurazione di sistema. In questa operazione possiamo perdere altri dati fondamentali. Le prove devono essere analizzate sia dai periti dell'accusa sia da quelli della difesa. Spegnendo i sistemi, tutti i dati raccolti a caldo non possono essere esaminati dalla difesa e quindi perdono di valore legale. Un secondo errore è pensare che è sufficiente fare il back-up prima di spegnere il sistema. In poche parole dobbiamo isolare i sistemi ma non spegnerli se vogliamo vedere condannato l'intruso.

Isolati i sistemi infetti possiamo contattare un esperto di Analisi Forense per raccogliere le prove.

Analisi Forense

L'Analisi Forense è l'attività svolta da un perito per la raccolta di prove relative al crimine informatico.



Il primo passo è la duplicazione "**bit x bit**" del contenuto della memoria e di tutti i dischi del sistema su un supporto non riscrivibile. Un sistema se riceve l'ordine di cancellare un file dichiara la porzione di disco contenente tale file come riscrivibile. I file rimossi restano presente sul disco fino a quando il sistema non scrive un nuovo file proprio in quella porzione di disco. Soltanto con una duplicazione bit per bit dei dischi possiamo salvare i frammenti di file rimossi ancora presenti sul sistema.

Il secondo passo è raccogliere tutti i log dell'ambiente: i log dei Firewall, i report degli IDS, i log dei router, i log dei sistemi compromessi archiviati sui log server...

A questo punto i periti analizzano una copia dei dati raccolti alla ricerca di tracce dell'intruso. Lavorando su una copia dei dati non riscrivibile, i periti possono eseguire test ripetibili.

Per prima cosa i periti analizzano i file di log per capire da dove è entrato l'intruso, da dove proviene e che operazioni ha svolto sul sistema. Essi ricercano i nuovi file e i programmi installati

dagli intrusi sui sistemi.

Normalmente gli intrusi non installano nuovi programmi ma modificano quelli di sistema per introdurre porte di accesso invisibili. Ad esempio modificano il programma SSH far entrare come amministratore di sistema chiunque si presenti come l'utente “pluto”. Per gli utenti di sistema il comando SSH continua a funzionare come prima. Gli intrusi di solito alterano i comandi di sistema per nascondere il loro operato mentre si trovano all'interno della macchina. I comandi alterati più di frequente sono quelli per la visualizzazione dei processi attivi, delle porte aperte, dell'associazione tra processo e porta... Una parte importante dell'Analisi Forense è la ricerca dei comandi di sistema e dei principali applicativi alterati dall'intruso.

La tecnica più usata è la MD5 Analisys. MD5 è una “hash function” descritta nel capitolo dedicato alla crittografia. In questo caso i periti calcolano l'hash di tutti i file binari e degli script di sistema e li comparano con quelli rilasciati dal produttore. Se l'hash risulta diverso allora il file è stato modificato. I periti analizzano poi in che modo questi comandi sono stati alterati.

Glossario

ACL (Access Control List)
Le ACL contengono l'elenco degli utenti che possono accedere ad una determinata risorsa e il tipo di accesso autorizzato (inserimento, lettura, modifica cancellazione...).

Analisi del rischio
L'analisi del rischio è un'attività che precede la stesura della politica di sicurezza. L'analisi identifica i rischi connessi all'ambiente informatico e le vulnerabilità che li causano.

Analisi Forense
L'analisi Forense è la ricerca delle tracce lasciate da un intruso in un ambiente violato e la raccolta di prove, a valore legale, per perseguire il pirata.

Antivirus
L'antivirus è un programmo atto a proteggere i sistemi dai virus e per ripulire i sistemi infettati.

Attacco
Gli attacchi deliberati sono un insieme di azioni finalizzati ad interrompere l'erogazione di un servizio (compromissione della disponibilità), ad alterare le informazioni contenute (compromissione dell'integrazione), ad accedere a informazioni protette (compromissione della riservatezza) e ad impossessarsi di una risorsa o di un sistema.

Attacco di replica
L'attacco di replica consiste nel catturare le informazioni di autenticazione ed nell'autenticarsi in un secondo momento tramite le informazioni catturate.

Attacco fisico all'ambiente
Gli attacchi fisici sono tutti gli attacchi portate sulle componenti fisiche dei sistemi.

Autenticazione
L'autenticazione è il meccanismo che permette verificare l'identità di un utente o di un server.

Autorizzazione
L'autorizzazione è il meccanismo discrimina le operazioni lecite in base al profilo associato all'utente. Di volta in volta può controlla, permette, impedisce o limitare lo svolgimento delle operazioni richiesto dagli utenti.

Back door
Back door o porta di servizio è un "pezzo di codice" malevole che crea un punto di accesso non lecito al sistematica.

Back-up
Il back-up è la creazione di una copia delle informazioni e dei software presenti sui sistemi, utilizzabile per ripristinare i sistemi dopo un incidente.

Bomba logica
La bomba logica è un particolare virus o codici malevole che si propagano in maniera silenziosa aspettando un particolare evento o una determinata data per eseguire un'operazione illecita sistema, tipicamente un'azione distruttiva.

Boundary Router.
Un Boundary Router è un router con installato il Firewall o un suo agente con la funzione di filtrare i pacchetti.

Business Continuity
Business Continuity è l'insieme dei processi e piani per la gestione delle emergenze e il ripristino dei servizi interrotti nel minor tempo possibile

Card
Le Card sono le tessere che memorizzano le chiavi private dell'utente in un formato protetto e forniscono la chiave solo se ricevono un PIN (Personal Identification Number) segreto.

Certification Authority (Ente Certificatore)
Una Certification Authority (CA) è un ente preposto ad emettere certificati digitale.

Certificato digitale
Un certificato digitale serve ad autenticare una chiave pubblica. Ogni certificato contiene la chiave pubblica dell'entità, le informazioni dell'entità (l'indirizzo di posta elettronica dell'entità o l'indirizzo del sito web oppure il nome e cognome della persona), le indicazioni del tipo di certificato e i dati relativi all'ente certificatore (Certification Authority) che l'ha emesso. Il certificato è firmato con la chiave segreta dell'ente certificatore.

Check- sum
Il Check-sum è il riassunto di un file utilizzato durante una sua trasmissione o una sua archiviazione per il controllo dell'integrità delle trasmissioni.

Conclusione
La fase di conclusione di un progetto è l'insieme di tutte le attività di chiusura di un progetto e di dismissione delle sue risorse.

Confidenzialità
Protezioni delle informazioni spedite, nessun altro oltre al ricevente potrà leggere/decifrarle

Crittografia
La crittografia è la scienza che si occupa di rendere incomprensibili le informazioni a chi non possiede un'opportuno segreto di lettura.

Crittografia a chiave privata
Gli algoritmi a chiave privata sono algoritmi crittografici che utilizzano la stessa chiave sia in fase di codifica del messaggio che in fase di decodifica. Il mittente e il destinatario condividono la stessa chiave di codifica.

Crittografia a chiave pubblica
Gli algoritmi crittografici a chiave pubblica sono basati su una coppia di chiavi: la chiave pubblica e la chiave segreta. La chiave pubblica serve per codificare i messaggi e la chiave segreta serve per decodificarli. Dalla chiave pubblica non è possibile ricavare la chiave segreta e quindi non è possibile decodificare i messaggi.

Dati Giudiziari
..."dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di

procedura penale;

I dati pubblici della società sono l'insieme dei dati disponibili ed accessibili a tutti le persone interne od esterne all'azienda...(Articolo 4 del Decreto Legislativo 196/2003) In trattamento dei dati giudiziari richiede l'adozione di misure di sicurezza specifiche descritte nel Decreto Legislativo 196/2003.

Dati personali
...“dato personale”, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale... (Articolo 4 del Decreto Legislativo 196/2003) Le misure di sicurezza da adottare nel trattamento dei dati personali sono descritte nel Decreto Legislativo 196/2003.

Dati sensibili
...”dati sensibili”, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale...(Articolo 4 del Decreto Legislativo 196/2003) In trattamento dei dati sensibili richiede l'adozione di misure di sicurezza specifiche descritte nel Decreto Legislativo 196/2003.

Deduzione (attacco di)
Gli attacchi di deduzione sono condotti incrociando informazioni provenienti da fonti differenti, alcune lecite ed altre illecite.

Denial of Service
I "Denial of Service" costituiscono una famiglia di attacchi finalizzati ad impedire l'erogazione di un servizio da parte di un sistema.

Dialer
I Dialer sono un tipo particolare di spyware che modificano, in maniera silenziosa, il numero di telefono delle connessione modem o ADSL redirigerlo su un altro numero più costoso e ottenendo un illecito guadagno.

Directory
Il Directory è un repository che fornisce una lista di informazioni sugli oggetti memorizzati.

Disaster Recovery
Il Disaster Recovery è il piano per il ripristino dei sistemi dopo un incidente o un'interruzione

Disponibilità
La disponibilità garantisce che una risorta o una informazione sia accessibili quando un utente legittimo chiede di accedervi.

DMZ (Zona Demilitarizzata)
La rete DMZ è una sottorete aziendale protetta connessa con le reti locali e/o con Internet tramite un Firewall. Essa contiene abitualmente i server con i servizi erogati in rete.

DNS (Domani Name Service)
Il servizio DNS è un servizio Internet che associa al nome logico di una macchina il suo indirizzo IP.

Ente Certificatore
Un Ente Certificatore è un ente preposto ad emettere certificati digitale.

Ente Certificatore Accreditato
Un Ente Certificatore Accreditato è una enti riconosciuto dal CNIPA ed autorizzato ad emettere certificati digitali per la firma elettronica a valore legale.

Erogazione
La fase di erogazione di un progetto è lo svolgimento delle attività necessarie per il raggiungimento degli obiettivi del progetto.

Evento accidentale
Eventi accidentali sono tutti quegli incidenti che occorrono ai sistemi senza una volontaria azione umana, che compromettono la corretta erogazione del servizio.

Firewall
I Firewall proteggono un sito da attacchi che sfruttano vulnerabilità dei protocolli TCP/IP, filtrando i pacchetti TCP/IP secondo le regole definite al loro interno. Essi possono agire sulla rete (Netwock Based Firewall) o sui singoli calcolatori (Host Based Firewall).

Firma digitale
La firma digitale è uno strumento per identificare il mittente del messaggio. Inoltre il mittente non può ripudiare la paternità del messaggio.

Hacker
Un hacker è una persona che attacca un sistema informatico per ottenere privilegi sulle macchine, per accedere ad informazioni e per alterare dati senza averne il diritto o per impedire che un sistema eroghi i propri servizi.

Hardening
L'hardening di un sistema è l'impostazione del miglior livello di sicurezza possibile su di una sistema, in modo da proteggerlo da attività non lecite sia tramite rete che da utenti connessi al sistema stesso.

Hash
L'Hash è il riassunto di un file utilizzato in crittografia nella realizzazione della firma digitale, durante l'analisi forense per individuare modifiche dei codici e nel controllo dell'integrità delle trasmissioni; sinonimo di Checksum.

Hash function
Una “one way hash function” è una funzione matematica che trasforma una stringa di bit di lunghezza variabile in una stringa univoca di caratteri di lunghezza fissa . Queste funzioni sono monodirezionali cioè le operazioni matematiche per ricercare il messaggio dal suo riassunto richiedono risorse di calcolo attualmente non disponibili.

Host Based Firewall
Gli host based Firewall sono Firewall di tipo Packet filtering e controllano il solo calcolatore su cui risiedono invece di una rete.

Host Based IDS
Gli Host Based IDS sono destinato a controllare gli eventi in corso sul solo calcolatore su cui risiedono

Hot fix

Gli hot fix sono dei “pezzi di software” che aggiornano un sistema operativo o di un software, rimuovendo una vulnerabilità riscontrata.

ICMP (Internet Control Message Protocol)
ICMP è un protocollo di livello rete utilizzato per i messaggi di controllo e di errore nelle reti IP.

IDS (Intrusion Detections Systems)
Gli IDS sono sistemi software o hardware che controllano gli eventi occorsi su una rete o su un calcolatore per segnalare problemi di sicurezza.

Integrità
L'integrità assicurare che tutte le informazioni ricevute siano identiche a quelle spedite o archiviate.

Intercettazione
Le intercettazioni sono attacchi finalizzati ad intercettare le informazioni in transito dei sistemi. Essi si pongono l'obiettivo di compromettere la privacy dei dati.

Intranet
La rete Intranet è una rete interna all'azienda che utilizza il protocollo IP, come le reti pubbliche.

Intrusione
L'intrusione su un sistema permette all'attaccante di impossessarsi della macchina e di compromettere l'integrità, la privacy e la disponibilità di un servizio.

Intruso
Un intruso è una persona che accede ad un sistema senza avere i permessi dopo aver compromesso la sicurezza del sistema con un attacco.

IP (Internet Protocol)
IP è il protocollo di livello rete utilizzato in tutte le connessioni Internet.

IPSEC
IPSEC è un protocollo di livello rete (evoluzione del protocollo IP) per la creazione di un canale codificato per gli applicativi di rete.

LDAP (Lightweight Directory Access Protocol)
Il protocollo LDAP è anche uno standard usato per effettuare delle ricerche e delle letture sui directory.

Log (file di)
Tipicamente, ogni sistema informatico di un certo livello fornisce la possibilità di tracciare le attività svolte dal sistema stesso in quello che comunemente viene denominato file di log. Il file di log rappresenta per un sistema informatico ciò che la scatola nera rappresenta per un sistema di trasporto aereo.

Malware
I Malware (Malicious Software) sono programmi il cui scopo è diffondersi sulla rete causando danni ai sistemi colpiti e/o procurando un illecito guadagno al loro inventore.

Meccanismi di Sicurezza
I meccanismi di sicurezza sono l'insieme di funzioni che realizzano la politica di sicurezza.

Media
I media dei calcolatori sono tutti gli strumenti finalizzati a contenere, memorizzare o elaborare le informazioni, come dischi, cassette, nastri, CD o stampanti.

Minaccia
Una minaccia è un'agente ostile che, mediante una specifica tecnica, metodologia o spontanea occorrenza, produce un effetto indesiderato su un elemento del sistema. Una minaccia è considerata non dolosa quando non esiste un'esplicita volontà di provocare danno. Con il termine minacce dolose o intenzionali si intendono quelle minacce portate all'uomo e che hanno un fine doloso, per le quali cioè esiste una esplicita volontà di provocare dando.

Minimizzazione
Rimozione di pacchetti e/o features dal sistema operativo in modo da disegnarlo attorno al servizio che deve offrire.

NAT (Network Adress Translation)
Funzionalità del Firewall e degli apparati di rete che prevede di rimappare gli indirizzi interni in altri indirizzi esterni. Questo traduzione nasconde la struttura degli indirizzi della rete interna e permette di traslare gli indirizzi interni in un insieme più piccolo di indirizzi esterni.

Negoziazione
La fase di negoziazione rappresenta tutta la fase di contatti tra le parti che porta alla firma di un contratto con la terza parte.

One-time password
I sistemi one-time password sono sistemi di password dinamiche da usare una sola volta. In pratica il sistema crea un elenco di password e l'utente utilizza e consuma una password ogni volta che la usa. Il grosso problema di questo strumento è la memorizzazione o la conservazione dell'elenco di password da utilizzare.

PAT (Port Adress Tanslation)
Funzionalità del Firewall e degli apparati di rete che prevede di rimappare le porte dei servi interni in altre porte esterne. Questo traduzione nasconde la struttura delle porte della rete interna.

Patch
Le patch sono “Pezzi di software” che contribuiscono all'aggiornamento di un sistema operativo o di un software. Una patch generalmente aggiunge nuove funzionalità e corregge problemi che sono stati riscontrati durante il ciclo di vita del sistema operativo.

Penetration test
Il Penetration test consiste nel trovare e identificare potenziali vulnerabilità, in modo da correggerle prima che possano essere utilizzate in maniera fraudolenta dagli hackers.

PKI (Public Key Infrastructure)
La PKI è l'infrastruttura per la creazione e la distribuzione dei certificati e per il supporto ad algoritmi e protocolli basati sulla crittografia a chiave pubblica

Politica di Sicurezza
La Politica di Sicurezza è l'insieme organico delle regole formali che stabiliscono come i beni di una società devono essere gestiti, protetti e distribuiti all'interno dell'organizzazione. Essa fornisce le linee guida ad alto livello che devono essere seguite nel progetto, nella implementazione e nella gestione del sottosistema di sicurezza.

Politica di Sicurezza Informatica
La politica di Sicurezza Informatica è la parte della Politica di Sicurezza aziendale legata alla gestione delle informazioni sensibili e degli strumenti per l'elaborazione, la gestione, la memorizzazione e la distribuzione delle informazioni; cioè è la parte legata all'ambiente informatico dell'azienda. Essa fornisce lo strumento per uniformare la realizzazione, la gestione e la manutenzione della sicurezza informatica all'interno dell'azienda stessa.

Probing
Il probing prevede di provare tutte le porte TCP/IP e UDP/IP per individuare i servizi disponibili sui sistemi.

Procedura
Una procedura è l'insieme di azioni/attività che devono essere eseguite per realizzare una certa operazione.

Proxy server
I Proxy server sono dei Firewall dedicato a gestire e filtrate le connessioni di un particolare protocollo. Il Proxy Server riceve una richiesta di connessione da un utente con l'indicazione del destinatario, controlla la conformità di tale richiesta con le proprie regole ed inoltra la richiesta.

Riservatezza
La riservatezza di un sistema garantisce che le informazioni trattate da quel sistema siano accessibili solo ai legittimo utenti.

Root Kit
I Root Kit forniscono una raccolta di script e file di configurazione che aiutano gli hacker a mascherare la loro presenza su un sistema. Spesso essi contengono una versione alterata dei principali comandi di sistema. Questi comandi alterati nascondono le back door installate e i programmi lanciati dall'intruso.

Router
Il router è un apparato di rete che opera sui protocolli di livello rete

Sicurezza degli utenti
La sicurezza degli utenti si basa sui sistemi per la verifica dell'identità dichiarata dall'utente finale. L'autenticazione dell'utente è il processo che realizza questa funzionalità.

Single Sing on
Sistema di autenticazione centralizzato per tutti i sistemi e le applicazioni. In questo caso un utente si identifica una volta sola all'inizio della sessione di lavoro e può accedere a tutti i servizi previsti nel suo profilo. Il sistema di Single Sign on provvede all'autenticazione, all'autorizzazione, alla verifica dei diritti di accesso e alla sincronizzazione delle password.

Smart card
Una Smart Card è una carta che contiene la chiave segreta del possessore e i certificati crittografici associati alla sua chiave pubblica. La smart card, oltre a conservare le chiavi, é dotata di un processore per eseguire al suo interno le operazioni di codifica e decodifica.

Sniffing
Lo sniffing è la cattura e la lettura del traffico in transito sulla rete.

Social Engineering
Il "Social Engineering" è un tipo di attacco molto particolare. Questo attacco cerca di carpire informazioni utili dai dipendenti di un'azienda.

Spam
Lo spam è l'invio di pubblicità non richiesta ad un indirizzo di posta elettronica. Se il numero di messaggi è elevato allora la casella di posta risulterà completamente intasata e l'utente non riuscirà più rintracciare i messaggi lecità all'interno di tutti questi “messaggi pattumiera”.

Spyware
Gli spyware sono software che raccolgono informazioni sull'utente e le sue abitudini. Le informazioni illecitamente ottenute vengono poi utilizzate per attività di spamming oppure per la clonazione di carte di credito...

SSH (Secure Shell)
SSH fornisce il servizio di shell remota, trasmettendo tutti i dati su un canale di comunicazione codificato.

SSL (Secure Socket Level)
Il protocollo SSL è un protocollo di rete di livello transport per la creazione di un canale crittato.

Social Engineering
In un attacco di tipo "Social Engineering" l'hacker cerca di carpire, con l'inganno o con la corruzione, informazioni utili dagli utenti di un ambiente informatico.

Strong Authentication
L'autenticazione robusta prevede un meccanismo dinamico di autenticazione in cui ad ogni sessione è concordata tra l'utente e il sistema l'informazione di autenticazione.

Switch
Lo switch è apparato di rete che opera sui protocolli di livello Data Link.

TCP (Transmission Control Protocol)
Il TCP è un protocollo di trasmissione di rete di livello transport che crea una sessione di comunicazione tra i due processi.

Token card
Le token card sono calcolatrici molto particolari che generano il codice di identificazione tramite la combinazione di un codice personale dell'utente (PIN) e un dato dinamico fornito dal sistema. In questo caso l'utente è identificato tramite la conoscenza di un'informazione e il possesso di un oggetto (token card)

Trojan house (cavallo di Troia)
Il cavallo di Troia è un "pezzo di codice" malevole che crea un punto di accesso non lecito al sistematica. Questo codice viene nascosto all'interno di un programma utile distribuito liberamente dall'hacker.

Trojan Downloader
Il Trojan Downloader è un tipo particolare di “cavallo di Troia”. In questo caso particolare il codice malevolo provvede a trasferire tutti i file del sistema in cui viene installato su una macchina scelta dall'hacker (solitamente un'altra macchina compromessa).

Trustworthiness
La Trustworthiness è la misura in cui l'utente può affidare al sistema informazioni di valore e contare su di esso perché quelle informazioni non siano scoperte prematuramente, a causa di malfunzionamenti o di tentativi dolosi prodotti su di esso.

UDP (User Datagram Protocol)
L'UDP è un protocollo di trasmissione di rete di transport per la comunicazione di due processi senza la creazione di sessioni

Utente
Un utente è una persona autorizzata ad accedere ad un sistema o ad una risorsa.

Virus
I virus sono programmi autoreplicanti che copiano il proprio codice, che attivano ogni istanza creata del proprio codice senza l'autorizzazione e spesso senza la conoscenza degli utenti e che si propagano sulla rete. Essi si riproducono degradando le prestazioni dei sistemi ed eseguono operazioni non lecite manomettendo dati e sabotando i sistemi. I danni causati variano dal solo propagarsi del virus che assorbe le risorse ambientali al danneggiamento e cancellazione di dati e codice alla diffusione delle informazioni contenute sulla macchina.

VPN (Virtual Private Network)
Le VPN sono delle reti virtuali sicure costruite sopra dei canali non sicuri. Le VPN costruiscono un canale virtuale tra due componenti che garantisce la riservatezza delle informazioni scambiate, l'integrità dei messaggi e la mutua autenticazione.

Worm
I worm sono un particolare tipo di virus che si limita a degradare le prestazioni dei sistemi, occupando le risorse dei sistemi.