REGIONE DEL VENETO

Sintesi delle Linee Guida sulla Sicurezza Informatica

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 ad un guidatore un po' distratto che sta uscendo da un posteggio... Poi quando arriviamo, ci preoccupiamo di sostare 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 all'interno. Per sicurezza, abbiamo sottoscritto l'assicurazione contro furto, incendio... In poche parole proteggiamo noi stessi e la nostra autovettura da pericoli o rischi indesiderabili.

E il nostro computer? Ci siamo mai preoccupati 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.

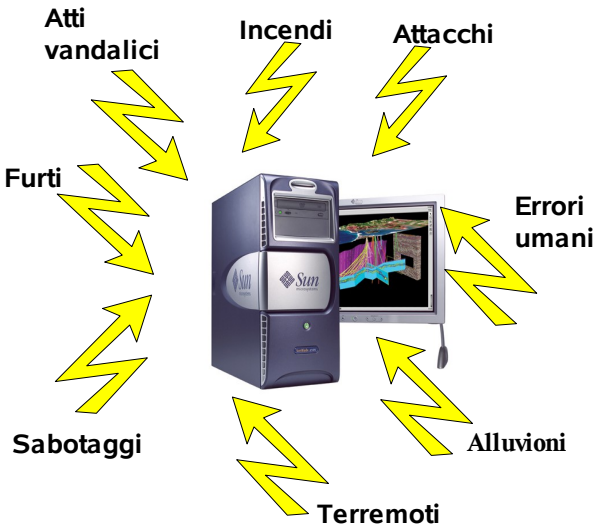
Cosa proteggere?

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 grandi (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 al 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 (sniffing);
- 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 di autenticazione).

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 stesse. 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. Disponendo di 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.

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. Sono infine da ricordare, le 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).

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:

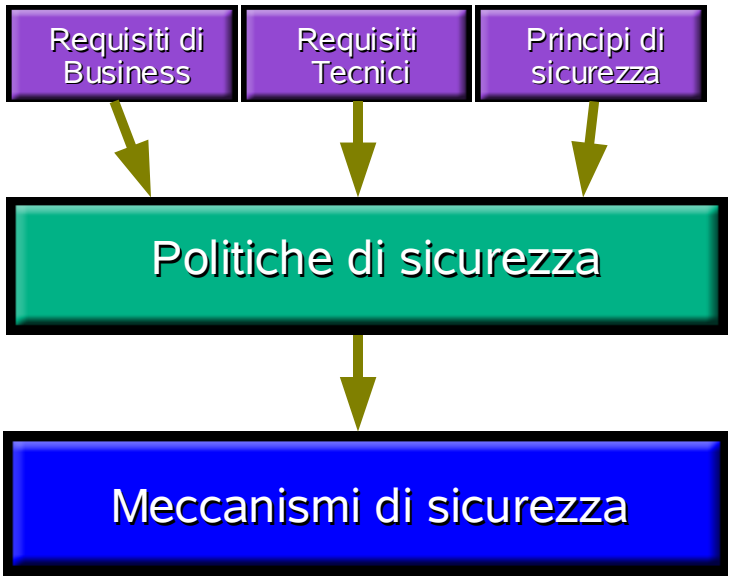
- **Politiche di Sicurezza**

  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.

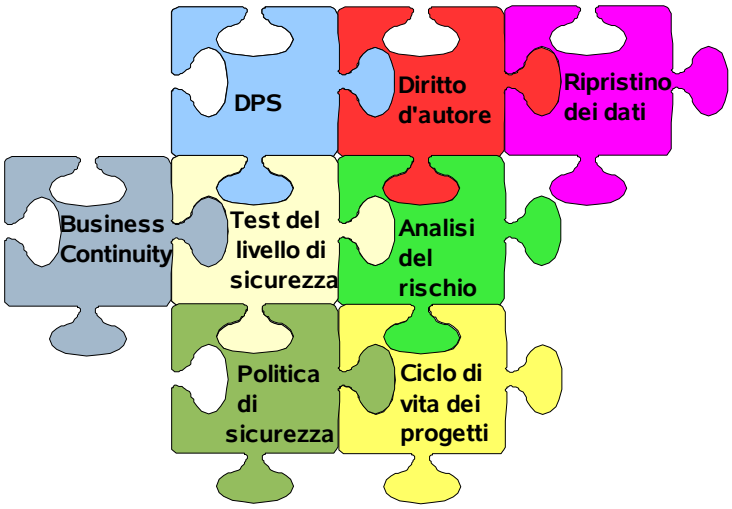
- **Ripristino:**

  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.

Politica di sicurezza

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.



All'interno delle politiche di sicurezza, consigliamo di affrontare le seguenti problematiche.

- **Documento Programmatico sulla Sicurezza (DPS)**

  Chiunque gestisce dati personali e sensibili altrui è tenuto a produrre un “documento programmatico sulla sicurezza” in cui descrive le misure adottate per proteggere l'accesso ai dati sensibili. Questo documento può essere un punto di partenza per la definizione delle Politiche di Sicurezza.

- **L'analisi del rischio**

  Come quantifico il rischio associato a violazione della sicurezza del nostro ambiente?

- **Gestione del ciclo di vita dei progetti**

  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. Analizziamo quindi il ciclo di vita dei progetti, focalizzando l'attenzioni sulle relative problematiche di sicurezza e sulle contromisure da adottare?

- **Rispetto della legge sul diritto d'autore.**

  Verifichiamo la presenza delle licenze richieste per l'uso delle varie componenti software? Registriamo il software sviluppato all'interno per salvaguardare la proprietà intellettuale?

- **Test del livello di sicurezza dell'ambiente informatico**

  Verifichiamo periodicamente le misure di sicurezza adottate effettuando dei “penetration test” o simulazioni di intrusioni? Questi test permettono di verificare il reale livello di sicurezza di un ambiente.

- **Politiche di ripristino**

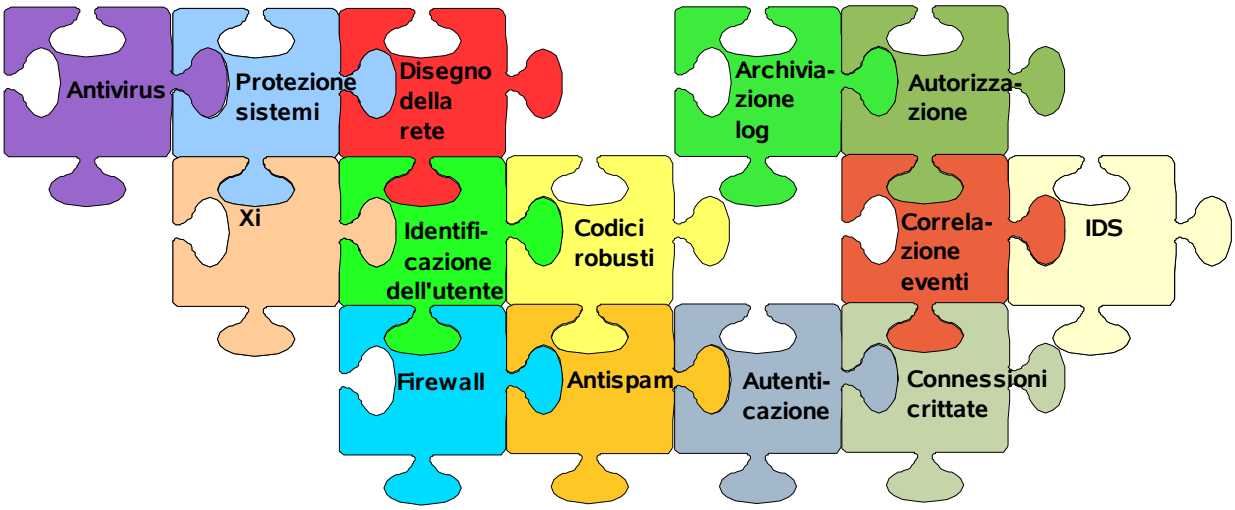
  Definiamo dei piani di salvataggio dei sistemi e delle informazioni tratta? Abbiamo delle politiche di ripristino dei sistemi a seguito di un attacco informatico? Sappiamo come raccogliere le prove per un'eventuale denuncia?

- **Business Continuity**

  Il piano di Business Continuity permette di riprendere il servizio dal punto in cui era stato interrotto su un nuovo sistema.

Meccanismi di Sicurezza

Dobbiamo attivare dei meccanismi automatici per realizzare le regole stabilite dalle politiche di sicurezza. Proviamo a capire in quali settori del nostro ambiente possiamo lavorare per aumentare il livello di sicurezza dell'ambiente.



- **Identificazione dell'utente**

  I meccanismi di identificazione associano ad ogni utente la sua identità.

- **Autenticazione**

  I meccanismi di autenticazione verificano l'identità dichiarata da ogni utente. Ricordiamo i sistemi di autenticazione basati sulle password (con le problematiche di scelta di una password non debole), sistemi di autenticazione robusta, autenticazione biometrica...

- **Autorizzazione**

  I meccanismi di autorizzazione associamo ad ogni utente l'insieme di operazioni lecite per tale utente.

- **Protezione dei sistemi e degli applicativi**

  La protezione dei sistemi si base su un'accurata installazione e configurazione finalizzata a costruire il sistema intorno al servizio erogato e ad innalzare il suo livello di sicurezza. I sistemi devono poi essere aggiornati periodicamente per rimuovere le nuove vulnerabilità.

- **Codici robusti**

  La produzione e la scelta di codice robusto, cioè capace di gestire dati errati in ingresso, riduce le vulnerabilità dell'ambiente.

- **Antivirus**

  Strumenti di antivirus proteggono i nostri sistemi dalle minacce costituite da virus, malware, spyware...

- **Antispam**

  Gli strumenti antispam proteggono le caselle di posta dalla ricezione di mail indesiderate.

- **Riservatezza dei dati**

  La crittografia fornisce strumenti per codificare i dati inviati ed archiviati e garantire la loro riservatezza. È possibile creare canali crittografici sicuri tra due sistemi su cui inviare i dati. La firma digitale fornisce uno strumento di autenticazione e non ripudio delle informazioni scambiate.

- **Disegno della rete**

  Una progettazione oculato della rete può ridurre il campo d'azione di un possibile intruso e quindi limita i danni.

- **Connessioni crittate**

  Le connessioni crittate (connessioni IPSEC, VPN o SSL) creano un canale sicuro sopra una rete insicura su cui scambiare i dati riservati.

- **Firewall**

  Firewall sono la prima barriera di protezione di un ambiente informatico. Essi difendono i punti di accesso al nostro ambiente poiché controllare il traffico in transito ed eliminano tutti i flussi non autorizzati. I Firewall possono proteggere un gruppo di reti o un singolo sistema.

- **Intrusion Detection System (IDS)**

  Gli IDS controllano il traffico di rete e distinguere i flussi autorizzati dagli attacchi. Essi permettono di individuare tempestivamente un intruso all'opera. Una risposta veloce dei gestori dell'ambiente limita i danni del pirata, permette di individuarlo e perseguirlo penalmente. Gli IDS supervisionano il traffico di una rete o gli eventi di un singolo sistema.

- **L'archiviazione dei log**

  I file di log contengono l'elenco delle operazioni particolarmente rilevati e di quelle anomale. La loro archiviazione permette di ricostruire cosa è successo su un sistema: un guasto, un errore o un attacco.

- **Correlazione degli eventi**

  Se i file di log delle varie componenti di rete (server, Firewall, IDS, Router, Switch...) vengono convogliati su un singolo server, allora possono essere usati strumenti di correlazione degli eventi per avere un quadro generale degli avvenimenti e rilevare comportamenti sospetti.