SICUREZZA DEI DATI

Vincenzo Calabrò

Perché la sicurezza?

Elevato sviluppo di servizi e tecnologie Internet
Elevate numero di connessioni

Sicurezza Informatica

Garantire
Integrità e
Riservatezza
dei dati

Acquisire un buon livello
di conoscenza informatica

Dotarsi di opportuni strumenti
per tenere alto il livello
di sicurezza

Perché la sicurezza? 2

Dietro agli attacchi a un sistema si celano motivazioni ben più serie di quello che si può pensare; molti tentativi di violazione di una rete vengono effettuati con scopi diversi:

- spionaggio industriale
- sottrazione di informazioni riservate
- vendetta a scopi personali
- diffamazione pubblica di un'azienda
- guadagno di vantaggi economici

Standard sulla sicurezza

Il primo standard sulla sicurezza è stato sviluppato dal Dipartimento di Difesa degli USA ed è contenuto nell'Orange Book.

Diversi livelli:

- D1 – Minimal Protection:
  - non esiste protezione per l'hardware e non ci sono autenticazioni (MS-DOS – Ms-Win – Apple – Mac)
- C1 – Discretionary Security Protection
  - Sicurezza dei sistemi UNIX, protezione HW, autenticazione degli utenti
- C2 – Controlled Access Protection
  - Aggiunge un maggior controllo, rispetto al livello superiore, nell'accesso alle risorse ed ai file
- B1 – Labelled Security Protection
  - Supporta una sicurezza multilivello
- B2 – Structured Protection
  - Ogni risorsa deve essere classificata e le possono essere assegnati diversi livelli di sicurezza
- B3 – Security Domain
  - E' presente un apposito HW per rafforzare la sicurezza del dominio
- A – Verified Design
  - Prevede l'esistenza di tutti i sottolivelli, include la verifica dei processi e controlli stringenti, inoltre l'HW ed il SW devono essere protetti durante la spedizione per evitare intrusioni al sistema

Sicurezza dei dati

"**SICUREZZA**" indica anche:

la capacità di salvaguardare riservatezza, integrità e disponibilità dell'informazione (elaborata su computer, memorizzata su supporti di varia natura o trasmessa lungo canali di comunicazione).

Contrastando ogni minaccia sia di tipo accidentale sia di tipo intenzionale.

salvaguardare la riservatezza dell'informazione

Ridurre a livelli accettabili il rischio che un'entità possa accedere ai dati senza esserne autorizzata

salvaguardare l'integrità dell'informazione

Ridurre il rischio che i dati possano essere cancellati/modificati a seguito di interventi non autorizzate o fenomeni non controllabili e prevedere adeguate procedure di recupero delle informazioni

salvaguardare la disponibilità dell'informazione

Ridurre il rischio che possa essere impedito alle entità autorizzate l'accesso alle informazioni a seguito di interventi non autorizzate o fenomeni non controllabili

Aspetti legali

La legge suddivide la tutela in due parti:

1. Da un lato impone l'obbligo di apporre delle misure di sicurezza, anche se minime, al proprio sistema informatico.

   Il codice penale impone l'adozione di misure di sicurezza necessarie ad impedire l'introduzione nel sistema informatico da parte di chi non è autorizzato, per prevenire:

   - Perdita, o distruzione dei dati
   - Ridurre il rischio di accesso non autorizzato
   - Impedire il trattamento dei dati in modo non consentito

Aspetti legali 2

2. Dall'altro la legge si occupa dei vari crimini informatici:

- **Delitto di accesso abusivo:** fa riferimento all'accesso abusivo ad un sistema informatico protetto da misure di sicurezza anche se minime.
- **Abuso di operatore di sistema:** fa riferimento all'abuso di un soggetto con tale qualifica, al fine di compiere attività "illegali".
- **Delitto di frode informatica:** si intende la "ricerca" di modifica, o sfruttamento, dei sistemi informatici al fine di compiere attività criminose.
- **Impedimento o turbamento di un sistema informatico:** fa riferimento ad abusi che si possono verificare nelle licenze sw, o installazione di particolari programmi, tali da alterare la funzionalità di un sistema a favore dei "produttori" di sw.
- **Detenzione e diffusione abusiva di codici di accesso:** sanziona l'abusiva acquisizione, in qualunque modo, duplicazione e distribuzione, dei mezzi, o dei codici di accesso ad un sistema informatico.

Quando un sistema è sicuro?

Un sistema di trattamento dati può considerarsi sicuro solo rispetto alla sua capacità di soddisfare alcuni parametri preventivamente stabiliti.

Bisogna quindi individuare i criteri di costituzione di un sistema informatico, quali:

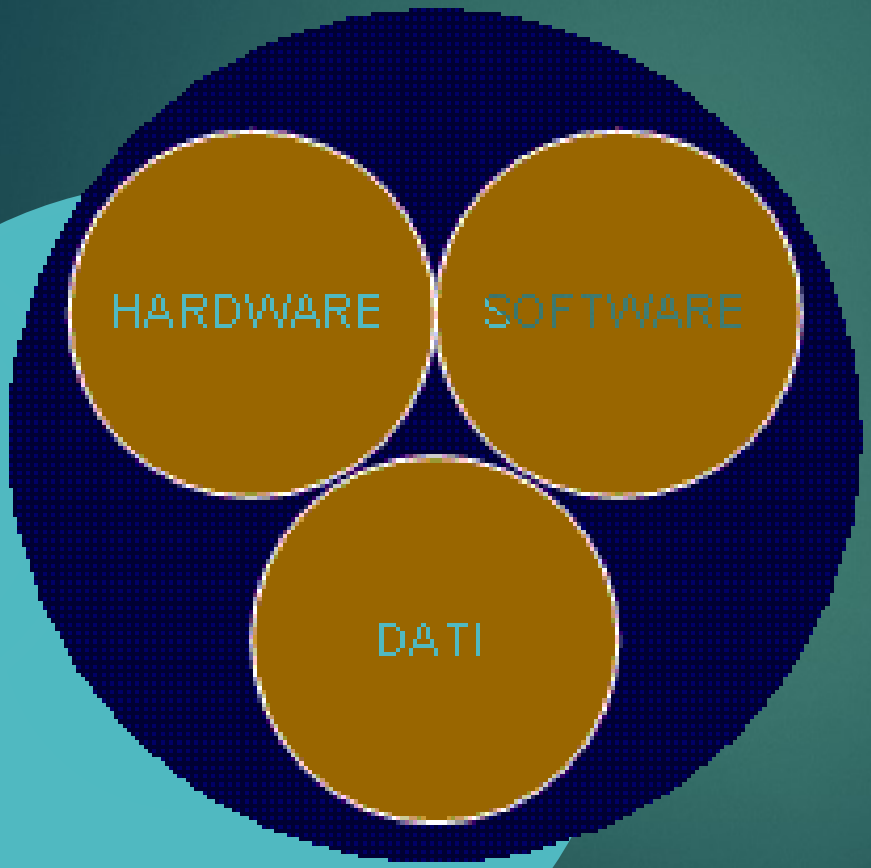
1. Definizione della **politica di sicurezza**
2. **Analisi dei rischi**, possibili minacce ed attacchi
3. Individuazione delle **funzioni di sicurezza** già presenti nel sistema e quelle che dovranno essere adottate

Cosa bisogna proteggere?

Bisogno anzitutto individuare quali sono le componenti del sistema che devono essere protette.

1. **Hardware** – le apparecchiature
2. **Software** – i programmi per il funzionamento del sistema e l'elaborazione
3. **Dati** – le informazioni gestite dai programmi
4. **Supporti di memorizzazione** – possono contenere sw e dati (anche backup)
5. **Reti** – permettono l'interconnessione di vari sistemi e quindi lo scambio di informazioni
6. **Accessi** – la possibilità che viene data ai soggetti di accedere alle risorse
7. **Individui chiave** – fa riferimento agli amministratori di sistema, ed eventuali operatori specializzati

Cosa bisogna proteggere? 2



- SUPPORTI DI MEMORIZZAZIONE
- RETI
- ACCESSI
- INDIVIDUI CHIAVE (Operatori e sistemisti)

Da chi proteggersi?

Per adottare le opportune misure di sicurezza bisogna sapere da chi proteggersi, possiamo fare due distinzioni.

La prima:

1. **Hacker**: colui che entra nei sistemi altrui per divertimento, studio, curiosità o semplicemente per dimostrare di essere in grado di farlo. Nella maggior parte dei casi l'hacker non causa danni al sistema vittima.
2. **Cracker:** è colui che viola i sistemi informatici con l'intento ben preciso di provocare un danno.

La seconda:

1. **Outsiders**: sono coloro che operano dall'esterno del network che intendono attaccare.
2. **Insiders**: sono coloro che sono autorizzati all'uso della rete e che cercano di abusarne.

Obiettivi della sicurezza

L'obiettivo principale della sicurezza informatica è quello di garantire, riducendo i rischi, un adeguato grado di protezione delle risorse, mediante l'attuazione di un progetto di sicurezza globale, che possa essere monitorato nel tempo.

Occorre garantire che il sistema mantenga inalterate nel tempo le seguenti proprietà:

Sicurezza/riservatezza (Confidentiality)

Le informazioni trasmesse, o memorizzate, sono accessibili in lettura sola da chi è autorizzato

Integrità (Integrity)

Solo chi è autorizzato può modificare l'attività di un sistema o le informazioni trasmesse

Disponibilità delle risorse (Availability)

Le risorse devono essere disponibili solo a chi è autorizzato e quando necessario

Obiettivi della sicurezza 2

Autenticazione

Gli utenti possono accedere al sistema solo autenticandosi con login e password

Non ripudio

Impedire che il mittente di un messaggio possa disconoscerlo

Controllo accessi

Limitare gli accessi alle risorse, o ai dati, solo ad alcuni utenti

Anonimia

Protezione dell'identità, o del servizio utilizzato

Politica di sicurezza 1

Definisce un insieme di regole che precisano in quale modo i dati e le risorse devono essere gestite, protette e distribuite all'interno del sistema.

Prevede:

- Un sistema d'identificazione degli utenti
- Una politica degli accessi
- Meccanismi logici e meccanici di protezione dell'integrità dei dati
- Misure normative ed organizzative adeguate

Esistono due filosofie che vengono adottate per lo sviluppo della politica di sicurezza:

1. ***"ciò che non è espressamente permesso è proibito"***
2. ***"ciò che non è espressamente proibito è permesso"***

Politica di sicurezza 2

E' importante che vengano anche definite le azioni che devono essere compiute nell'eventualità che la sicurezza della organizzazione sia compromessa.

Ogni volta che la questa viene violata, deve essere modificata per rimuovere l'elemento inefficiente, dal momento che è ovvio che se vi è stata un'infrazione a questa ne potranno seguire altre.

Bisogna inoltre sviluppare procedure e piani che salvaguardino le proprie risorse da perdite e danneggiamenti; tuttavia il loro costo deve essere proporzionato ai beni da proteggere e alle probabilità di subire attacchi.

Politica di sicurezza 3

Progettazione di una Politica di Rete

Per affrontare la progettazione di una politica di rete bisogna considerare vari fattori tra i quali:

- la politica di sicurezza locale
- l'analisi dei rischi
- l'identificazione delle risorse e delle minacce
- l'uso della rete e responsabilità degli utenti
- le azioni da intraprendere in caso di violazioni alla politica della rete
- le azioni di manutenzione di un sempre adeguato livello di sicurezza

Politica di sicurezza 4

Analisi dei rischi

L'analisi dei rischi consiste nel determinare:

- le risorse che è necessario proteggere
- le tipologie di rischi a cui sono potenzialmente esposte
- come proteggerle

Altri fattori da considerare nella stima del rischio per una risorsa della rete sono:

- La **disponibilità** di una risorsa della rete è una misura di quanto sia importante avere una risorsa adeguata e pronta alle proprie esigenze.
- L'**integrità** di una risorsa è invece una misura dell'importanza che la risorsa o i dati della stessa siano mantenuti consistenti
- Il concetto di **riservatezza** si applica a quelle risorse, quali i file di dati, per i quali si desidera limitare la possibilità di accesso.

Politica di sicurezza 5

Uso della rete e responsabilità

- Bisogna effettuare una classificazione degli utenti, sia interni che esterni alla rete, che necessitano di accedere alle risorse.
- Si devono fornire delle linee di comportamento che definisco l'uso corretto delle risorse.
- Devono essere definiti i diritti degli utenti e le responsabilità cui sono tenuti quando utilizzano le risorse ed i servizi di rete.

Violazione della sicurezza

Ogni volta che viene violata la politica di sicurezza il sistema si trova esposto a minacce.

Si deve classificare se tale violazione si è verificata a causa della negligenza di un utente, di un incidente, di un errore, della non conoscenza, o non curanza della politica corrente.

In ciascuna di queste circostanze, la politica di sicurezza, dovrebbe fornire delle direttive circa le azioni immediate da adottare.

Rischi per un sistema informatico

INTERRUZIONE

Un bene viene tolto dal sistema o non è più disponibile o è inutilizzabile.

INTERCETTAMENTO

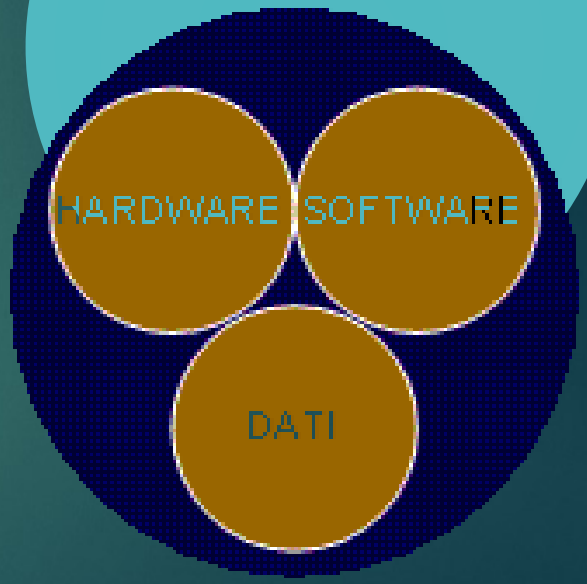
Un'entità (un utente, un programma, un sistema informatico) non autorizzata ottiene l'accesso ad un bene.

MODIFICA

Un'entità (un utente, un programma, un sistema informatico) non autorizzata ottiene l'accesso ad un bene e lo manomette.

CONTRAFFAZIONE

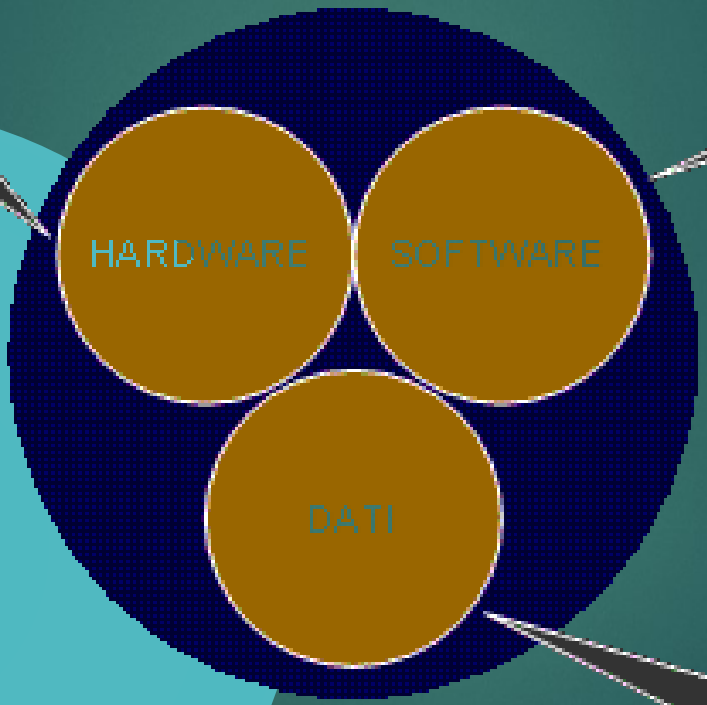
Un'entità (un utente, un programma, un sistema informatico) non autorizzata potrebbe costruire degli oggetti contraffatti all'interno del sistema informatico.



Rischi per un sistema informatico

- Interruzione (denial of service);
- Intercettamento (furto).

- Interruzione (cancellazione);
- Intercettamento;
- Modifica;
- Contraffazione.



- Interruzione (perdita);
- Intercettamento;
- Modifica;
- Contraffazione.

Minacce

Le minacce precedentemente elencate possono avere differenti origini:

- **Accidentali**: calamità naturali, errori del personale addetto all'uso del sistema, guasti hardware, ecc…
- **Occasionali**: scoperta involontaria di informazioni immagazzinate in un sistema per cui non si ha l'autorizzazione di accesso.
- **Intenzionali programmate**: condotte da persone che hanno come preciso obiettivo, quello di attaccare una specifica azienda per causarle danno.
- **Interne involontarie**: comportamenti incauti da parte di persone interne all'azienda che possono causare seri danni (virus).
- **Interne volontarie**: persone interne all'azienda che hanno il preciso scopo di causare un danno all'azienda stessa.

Tipologie e metodi di attacco 1

Dopo aver individuato le minacce, bisogna capire quali siano i possibili attacchi a cui il sistema può essere sottoposto per adottare le relative misure di sicurezza.

Vi sono diverse tipologie di attacco che possono essere così classificate:

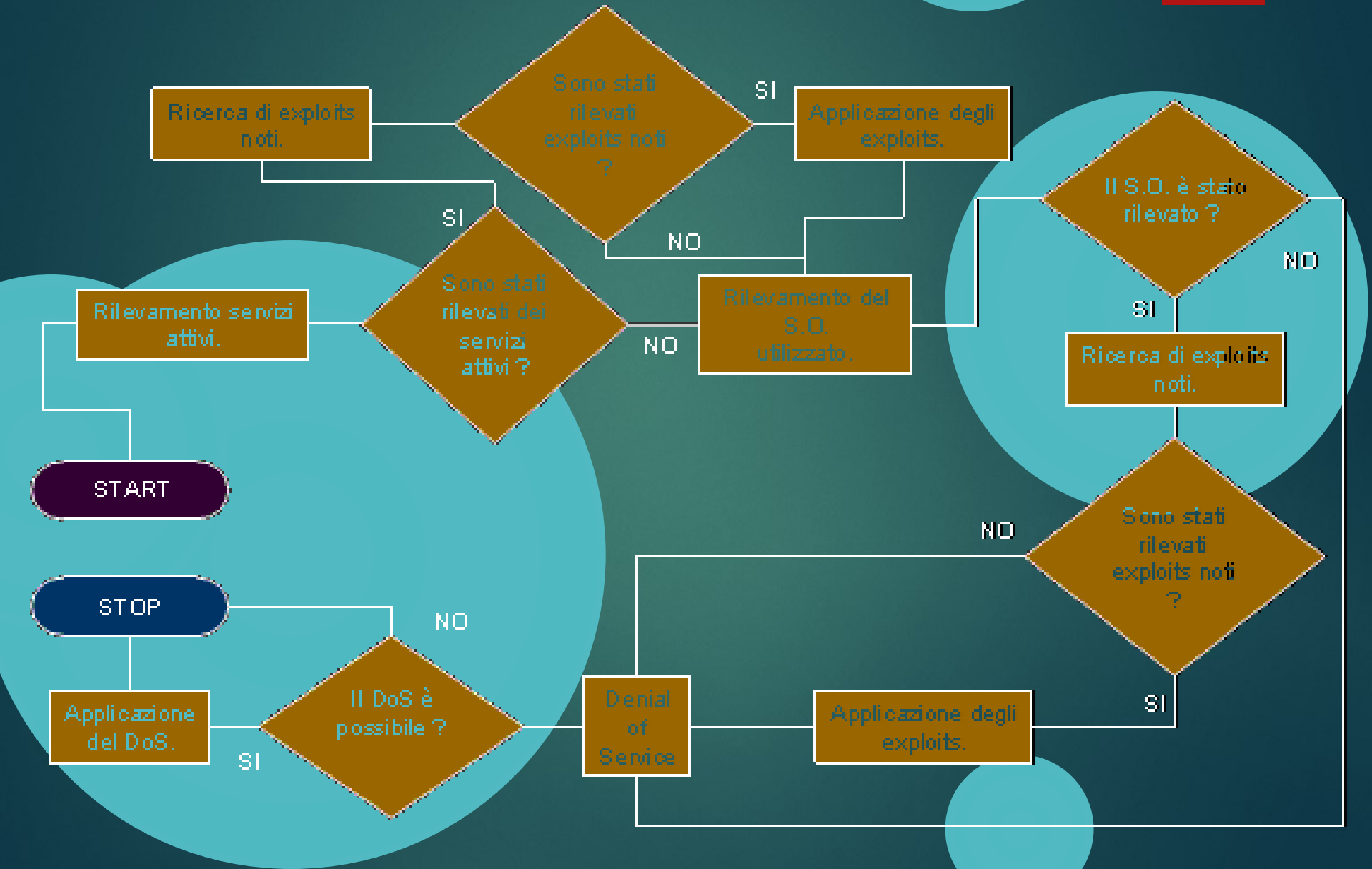
- **Acquisizione di informazioni**: è un insieme di azioni che anticipano un attacco.
- **Accesso non autorizzato**: un intruso ottiene l'accesso ad una rete, o ad un computer, pur non avendone l'autorizzazione, ottenendo informazioni riservate, o provocando danni di vario genere al sistema.
- **Accesso/modifica/cancellazione delle informazioni.**
- **Denial of Service**: l'intruso rende un sistema, un servizio,o una rete non disponibile esaurendone le risorse di rete (banda), connessioni TCP (Syn Floods), o spazio disco (effettuando upload di dati).

Tipologie e metodi di attacco 2

Gli attacchi possono essere realizzati seguendo diverse tecniche, quali ad esempio:

- Sfruttamento di servizi non autenticati
- Sfruttamento di servizi centralizzati
- Sfruttamento di bug nel SW
- Accesso tramite "individuazione" di Login e Password
- Packet Sniffer
- Login Spoofing
- Bombe Logiche
- Denial of Service
- Trojan Horse e Back Door
- Virus e Worm

Tipologie e metodi di attacco 3



Trojan Horses e Backdoors

Ci si riferisce a tutti quei programmi che, sotto le false spoglie di sw "pacifici", si introducono nel sistema vittima e svolgono funzioni dannose, prendendo pieno possesso della macchina.

I rischi sono molteplici, tra cui la perdita di dati, che un intruso possa usare la nostra macchina per ridirezionare il flusso dei dati, navigare con il nostro IP e, se farà danni, i responsabili potremmo risultare noi.

Alcuni esempi:

- **Destructive Trojan:** utilizzati per far danni ad una macchina.
- **Trojan Ladri di Password:** poco utilizzati e permettono di rubare password.
- **Chat Trojan:** sono programmi in grado di svolgere diverse funzioni tramite le chat.
- **Back Door:** sono i tool di amministrazione remota, che permettono di gestire un sistema tramite protocollo TCP/IP. Nati con lo scopo di facilitare il lavoro di chi ha la necessità di lavorare su macchine remote, permettono di avere il pieno controllo del sistema infetto.

Virus e Worm

I **VIRUS** informatici devono penetrare nel programma ospite modificandolo, sia per riprodursi, sia per danneggiare dati e/o programmi presenti su supporti registrabili; sono costituiti da poche centinaia di istruzioni per far notare la loro presenza all'utente del computer.

- **Floppy Boot e MBR Virus**: Infettano un particolare settore dei dischi, quello di avvio; vengono eseguiti nello stesso quando il computer viene avviato, e quindi difficilmente rilevabili da un antivirus.
- **Virus Polimorfico:** Si replica producendo cloni mai uguali a se stesso, quindi tenta di sfuggire celandosi dietro questa imprevista e sempre nuova forma.
- **Dos-Exec File Virus:** sono i più diffusi e attaccano tutti i file eseguibili (.exe, .bat). Sovrascrivono gli ultimi byte di un file, quando viene eseguito esso si installa residente in memoria.

Un **WORM** si può definire come un virus che viaggia e si riproduce lungo le reti, ma differisce da questi per il fatto che non necessita di attaccarsi a file particolari o a settori di disco.

Esso è in grado di auto-installarsi sulla macchina e di auto-inviarsi, come allegato a normalissime e-mail, scritte da lui, a tutti i contatti contenuti nella rubrica, che il virus si preoccupa di cercare sul computer ove si è trasferito...

Come difendersi?

Bisogna fare particolare attenzione al fatto che

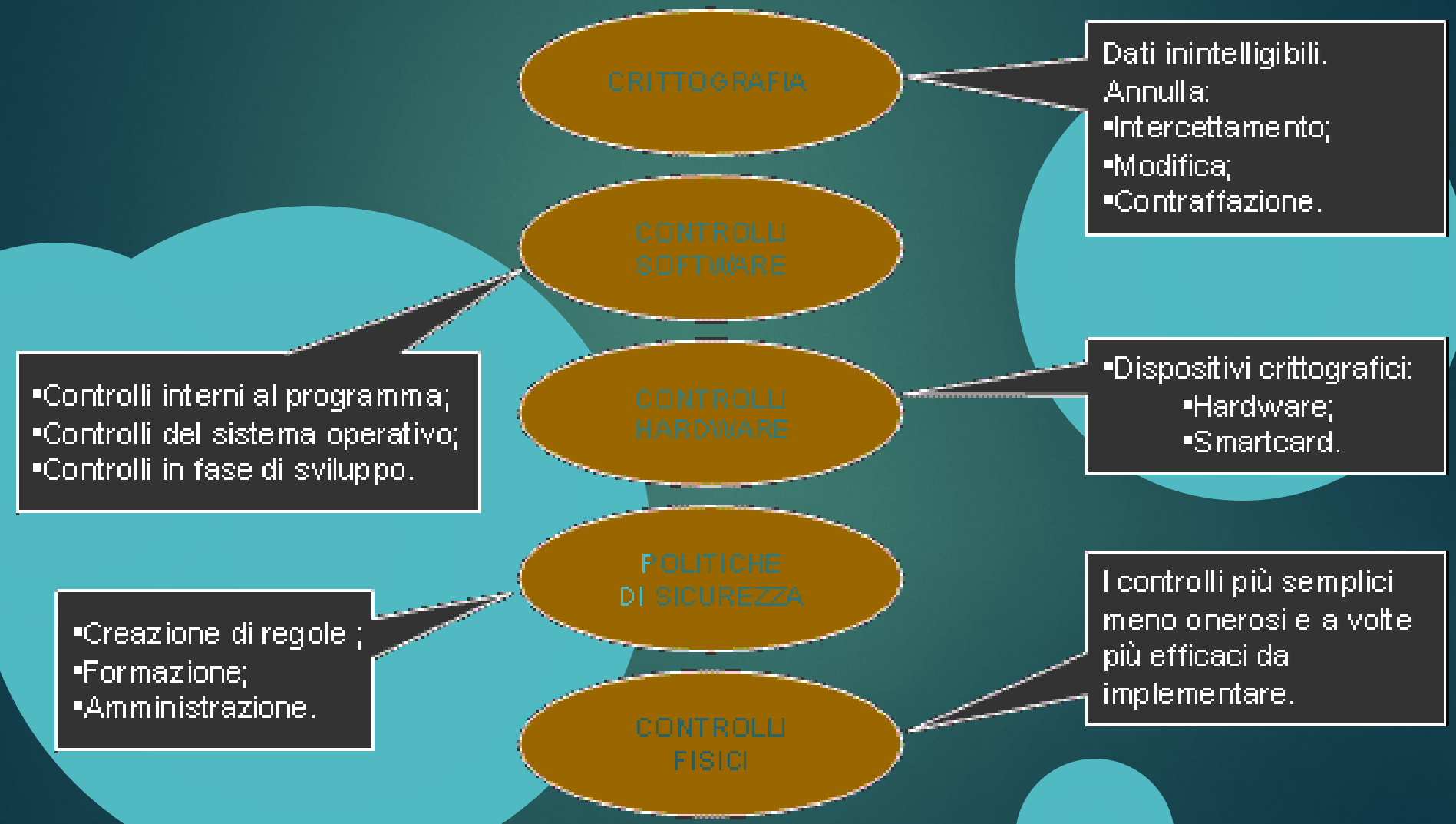
"la sicurezza è un processo, non un prodotto"

Come tale ha molti componenti, che devono essere affidabili e ben studiati e, soprattutto, collaborare fra loro. Infatti, l'efficacia del sistema di sicurezza dipende principale da come i vari componenti collaborano fra loro.

La Progettazione e la realizzazione di un sistema informatico deve tener presente:

A. Gestione degli accessi al sistema
B. Sistema Antivirus Centralizzato
C. Gestione del traffico da e verso Internet
   (Network Analyzer - IDS - Firewall)
D. Backup dati
E. Gruppi di continuità
F. Protezione dell'informazione
   (Crittografia - Steganografia - Firme digitali)

Principali controlli



Efficacia dei controlli

CONSAPEVOLEZZA DEL PROBLEMA

Gli utenti che utilizzano i controlli devono essere convinti della necessità di sicurezza.

PROBABILITA' D'USO

Nessun controllo è utile se non è utilizzato.

SOVRAPPOSIZIONE DEI CONTROLLI

Diversi controlli possono essere applicati contemporaneamente per evitare un possibile danno.

REVISIONE PERIODICA

Pochi controlli hanno un efficacia permanente.

Gestione degli accessi al sistema

Devono essere garantiti i seguenti punti:

- **Autenticaione dell'utente** (login e password)

  E' la prima barriera che un intruso deve superare, in questo modo si riduce il rischio che utenti "sconosciuti" possano accedere al sistema, ed alle sue risorse, senza averne le autorizzazioni.

- **Delimitazione degli spazi logicisi**

  Garantisce un certo livello di privacy, in quanto un utente può accedere a file dati o programmi per cui è stato autorizzato.

- **Tracking dell'attività**

  Permette di controllare le attività svolte da un utente sulla rete e rilevare eventuali comportamenti anomali.

Autenticazione di un utente

Il primo ostacolo che un cracker deve superato per accedere ad un sistema è quello dell'**autenticazione**.

Esistono varie metodologie di autenticazione:

- **Login e Password:** è il metodo più diffuso; se queste non corrispondono a quelle conservate con quelle conservate nel sistema l'accesso viene negato.
- **Carta magnetica**: il riconoscimento viene effettuato inserendo la carta in un apposito lettore e digitando una password.
- **Biometrie**: si tratta di lettori di impronte digitali o vocali, analisi della retina, analisi della firma.

  Il sistema biometrico è composto da:

  - Registrazione – vengono misurate ed immagazzinate le caratteristiche dell'utente.
  - Identificazione – l'utente fornisce la sua "account", il sistema esegue delle misurazioni e confronta i valori con quelli già campionati.

Sistema Antivirus

Per proteggere il proprio sistema da virus (di vario tipo), trojan, spyware, ecc… è necessario dotarsi di opportuni SW che rilevano la presenza di strani file all'interno del sistema, quali:

- **Anti-Virus**: per file infetti da virus, worm, trojan.
- **Anti-Trojan**: per scovare ed eliminare trojan.
- **Spyware Detectors**: per scovare ed eliminare i programmi spia.

Perché questi SW risultino efficaci devono essere seguite determinate regole:

- ✓ *deve essere aggiornato in automatico giornalmente, o settimanalmente*
- ✓ *deve rimanere in esecuzione mentre l'utente lavora*
- ✓ *deve controllare i Files e i contenitori di messaggi di posta*
- ✓ *è opportuno controllare anche tutti i file di dubbia provenienza*

Network Analyzer ed Intrusion Detection System

I **Network Analyzer** sono dei dispositivi che si occupano di monitorare ed analizzare in tempo reale il traffico di rete.

Gli **Intrusion Detection System** sono da considerarsi un'estensione dei *network analyzer*. Il loro incarico, infatti, é quello di registrare e segnalare, nel minor tempo possibile, le violazioni (anche sotto forma di tentativo) dei sistemi informativi.

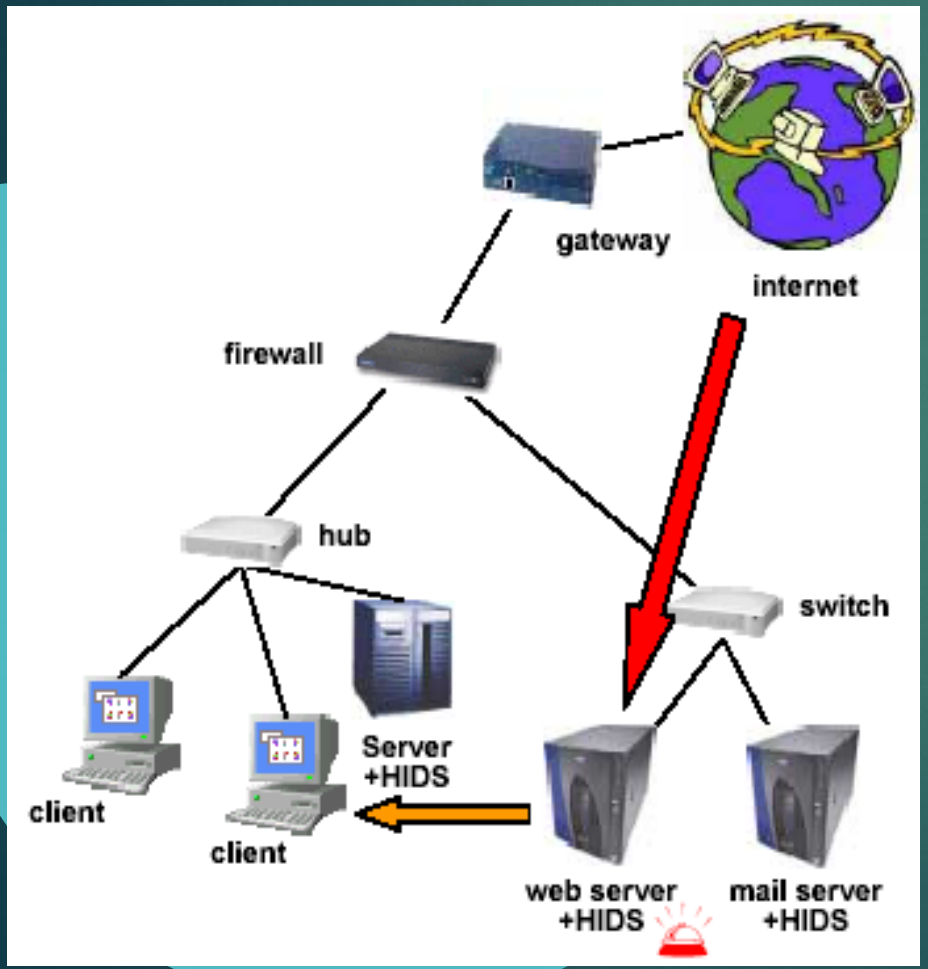
Esistono due tipi di IDS:

- ✓ Host IDS: basati su host ed analizzano in real-time le attività interne al sistema (utenti – applicazioni – log).
- ✓ Network IDS: web server basati su traffico di rete, analizzano in real-time tutto il traffico di rete (sniffing), alla ricerca di attacchi sconosciuti, o particolari tipi di traffico.

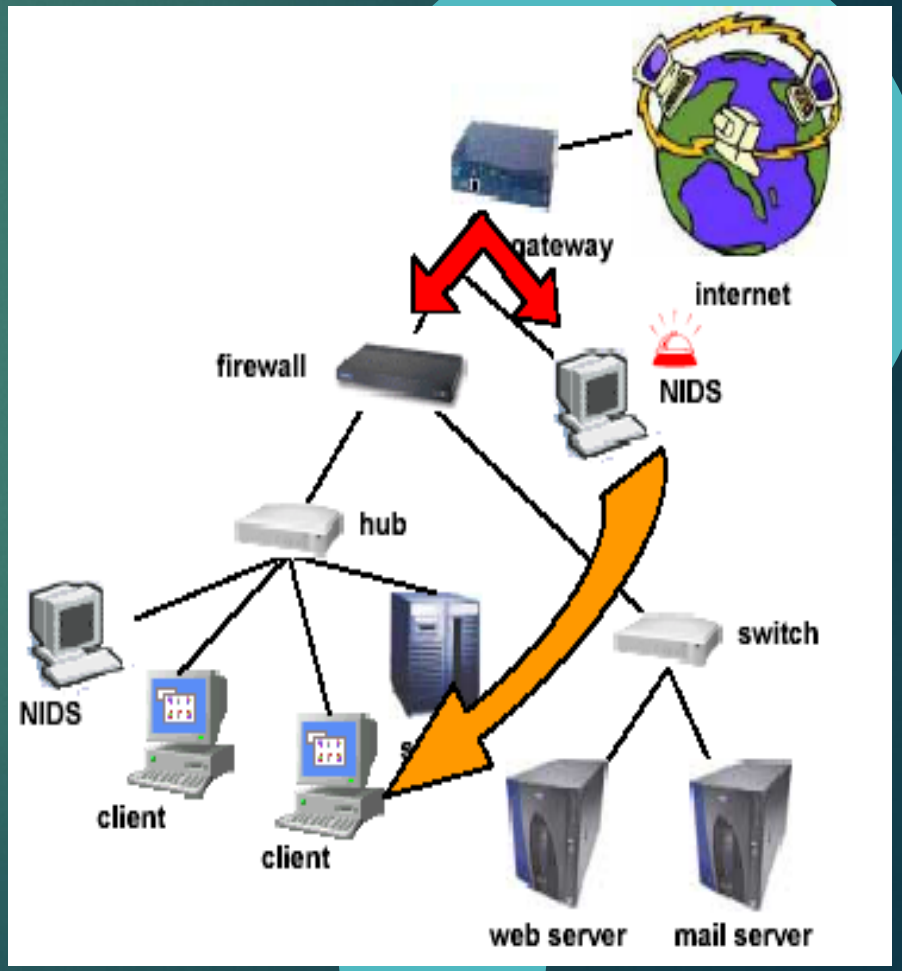
Alcuni tipi di IDS possono interagire con particolari firewall ed attivare contromisure.

Intrusion Detection System

HIDS



NIDS



Firewall

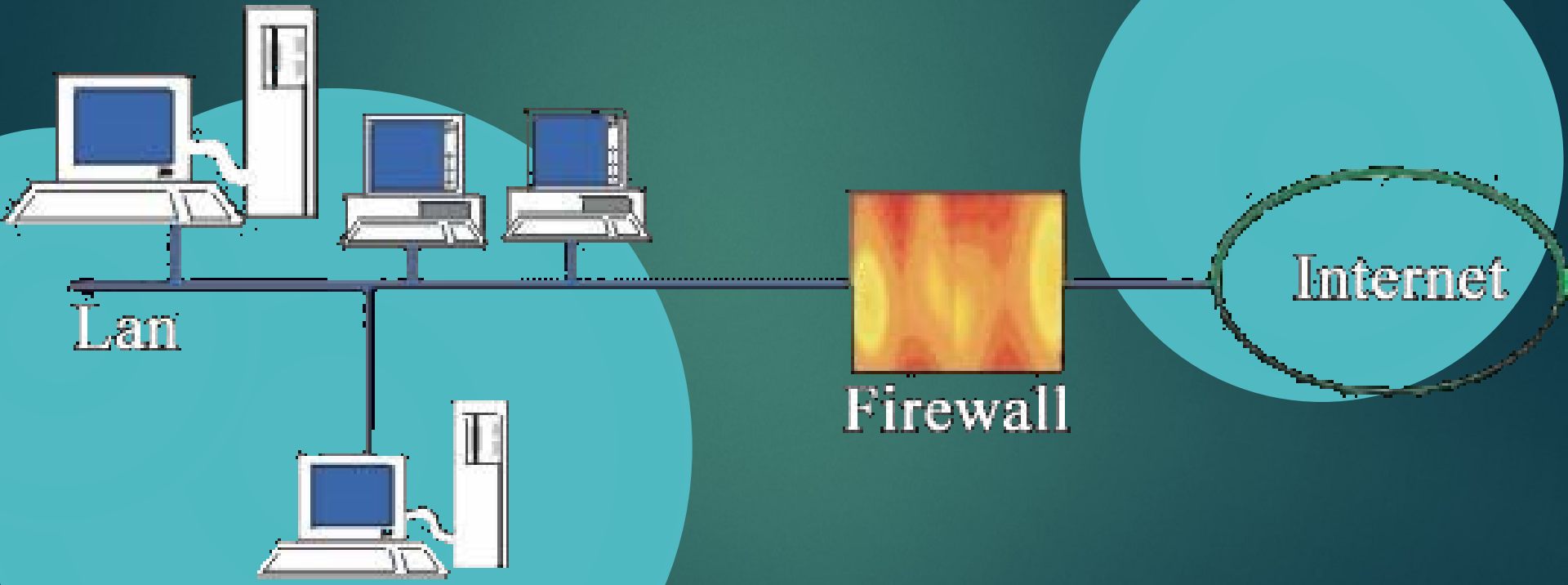
Il F**irewall** può essere pensato come una coppia di meccanismi: uno serve a bloccare il traffico in ingresso e l'altro per veicolare quello in uscita dalla rete.

Possono essere programmati per "controllare", o bloccare diverse attività quali:

- Permettere solo il passaggio di mail
- Proteggere da login non autenticati dall'esterno
- Bloccare il traffico dall'esterno all'interno e permettere il contrario

E' importante ricordare che un firewall non può proteggere da attacchi che non vi passano attraverso, quindi non è sufficiente per realizzare un buon livello di sicurezza.

Firewall 2



Backup dei dati

Un aspetto importante per proteggersi dalla è proteggersi dalla perdita dei dati attraverso l'uso di copie di bakcup.

Possono essere effettuati diversi tipi di backup, su diversi supporti (nastri - dischi -ecc), con diverse tecniche (crtittografati, backup parziali, incrementali, differenziali, ecc...) e tempi di esecuzione differenti.

- Backup remoto
- Backup parziali
- Backup incrementali
- Backup differenziali

Gruppi di continuità - UPS

Una delle cause per cui un sistema può subire dei danni è dovuta alle "oscillazioni" di tensione sulle reti elettriche, che si manifestano con una frequenza variabile in funzione della loro tipologia.

- **Sottotensioni** – cali di tensione elettrica
- **Armoniche** – sbalzi di tensione dovuti a carichi non lineari
- **Sovratensioni** – aumenti di tensione
- **Picchi di corrente** – sovratensioni di brevissima durata
- **Black-out** – assenza di corrente
- **Rumori** – interferenza radio ed elettromagnietiche

Tutti questi disturbi riguardano i Server, i Personal Computer, le periferiche collegate, le Reti locali (LAN) e altri sistemi professionali di tipo elettrico/elettronico.

“Nascondere” le informazioni

Difendere la privacy individuale in un era di crescente computerizzazione sta diventando un problema cardine, in quanto oggi le nostre vite sono controllate in molti modi (transazioni con carte di credito, telefonate, assegni, ecc…).

Proprio per questi motivi, ed altri ancora, è necessario trovare uno, o più metodi che ci permettano di immagazzinare, o trasmettere in modo sicuro tutte quelle informazioni che sono tutelate dal diritto alla privacy, ma anche quelle che, per qualche motivo personale, o aziendale, sono ritenute “riservate”.

Esistono diversi metodi, ecco i principali:

- **Crittografia**
- **Firma digitale**
- **Steganografia**
- **Controlli fisici**

Crittologia

La **Crittologia** è la scienza che studia il discorso e la scrittura segreta ed è suddivisa in due grosse branche:

- **Crittografia**: la scienza di scrivere dei messaggi che nessuno al di là del vero destinatario potrà leggere (dal greco kryptós = nascosto e dal tema, sempre greco, gráphò cioè, scrivere)

- **Crittoanalisi**: la scienza che si occupa della lettura delle informazioni crittografate attraverso la rottura dei sistemi cifranti

Crittografia 1

Crittografia: è quella scienza che fornisce uno strumento adatto a mantenere segrete tutte quelle informazioni che non si vogliono divulgare pubblicamente, in maniera tale che la possibilità di accedervi sia data solo a persone autorizzate.

Possono essere fatte due operazioni:

- **Crittazione:** è l'operazione tramite la quale si nascondono le informazioni ed è effettuata tramite un apposito algoritmo chiamato cifrario; l'informazione da cifrare è noto come testo chiaro.

  La crittazione sfrutta come mezzo fondamentale una chiave per convertire il testo chiaro in testo cifrato o crittogramma.

- **Decrittazione:** è l'operazione inversa rispetto alla crittazione, ossia la conversione da testo cifrato a testo chiaro; anch'essa sfrutta la chiave del cifrario.

Crittografia 2

Quando usarla?

Ci sono due casi generali in cui è necessario avvalersi dell'appoggio della crittografia:

- quando l'informazione deve semplicemente essere conservata sul posto e dunque "confezionata" in modo tale da renderla invulnerabile ad accessi non autorizzati.
- quando l'informazione deve essere trasmessa e dunque la crittazione è necessaria perchè se qualcuno la intercettasse non potrebbe capir nulla di quello che si trova tra le mani.

Crittografia 3

Tecniche

Al giorno d'oggi la parola "crittografia" è usata per indicare una grande varietà di tecniche; entra in gioco la **chiave**, che è una stringa di caratteri che seleziona una tra le molte cifrature potenziali.

Tutti i moderni metodi utilizzano una chiave per eseguire la crittazione e la decrittazione; un messaggio può essere decrittato solo se la chiave di decifratura si "accoppia" con quella di cifratura.

Per alcuni algoritmi le due chiavi sono uguali, mentre per altri esse sono diverse; in base a questa sostanziale differenza gli algoritmi basati sull'utilizzo di chiavi si dividono in:

- **simmetrici** (detti anche a chiave simmetrica o a chiave segreta)
- **asimmetrici** (detti anche a chiave asimmetrica o a chiave pubblica).

Crittografia 4

Sistemi a chiave simmetrica

Tali sistemi possono essere utilizzati per implementare servizi di sicurezza quali:

- **Riservatezza:** proteggere l'informazione da visione non autorizzata. Spesso la protezione riguarda solo il corpo del messaggio e non la testata, trasmessa in chiaro per semplificare l'instradamento del messaggio fino al destinatario.
- **Integrità:** garantire che l'informazione non venga alterata e che il messaggio arrivi esattamente come è stato spedito.
- **Autenticazione:** serve a prevenire la dissimulazione degli utenti, cioè consente al vero mittente di includere nel messaggio informazioni che lo identifichino con certezza.

Crittografia 5

Sistemi a chiave asimmetrica

Le tecniche asimmetriche utilizzano coppie di chiavi complementari invece di una sola chiave segreta.

Un singolo utente possiede una coppia univoca di chiavi complementari:

- una è **pubblica**, nel senso che può essere conosciuta da tutti, ed è usata per cifrare il messaggio.
- una è **privata** ed è tenuta al sicuro dal suo proprietario di modo che solo lui possa utilizzarla.

Le due chiavi sono create in maniera tale che un messaggio cifrato da una delle due può essere decifrato solo e soltanto dall'altra.

In pratica se si vuole spedire un messaggio a una certa persona, si critta quel messaggio con la sua chiave pubblica, e si è sicuri che soltanto quella persona potrà decifrarla con la propria chiave privata: neanche la chiave pubblica utilizzata per cifrare riuscirà a decrittare il messaggio.

Crittoanalisi 1

La **crittoanalisi** è l'arte di rivelare le comunicazioni crittate senza la conoscenza della chiave giusta.

Esistono oggi numerose tecniche di crittoanalisi, ecco quelle più diffuse:

- **Attacco a solo testo cifrato** – L'intruso non conosce nulla circa il contenuto del messaggio, e deve quindi lavorare soltanto sul *ciphertext*, è possibile indovinare qualcosa circa il testo chiaro, questo perché, ad esempio, molti messaggi hanno testate di formato fisso, oppure iniziano in modo facilmente intuibile.

- **Attacco a testo chiaro conosciuto** – Il cracker conosce o può indovinare il testo chiaro corrispondente ad alcune parti di testo cifrato. Il suo compito è quello di decifrare il resto del *ciphertext* avvalendosi di queste informazioni. Ciò può esser fatto, ad esempio, determinando la chiave usata per crittare i dati.

- **Attacco a testo chiaro scelto** – Il crittoanalista è in grado di ottenere qualsiasi testo lui voglia benché crittato con la chiave sconosciuta. Il suo compito è quello di determinare proprio la chiave di crittazione.

Crittoanalisi 2

- **Attacco "uomo in mezzo"** – Questo tipo di attacco è efficace nei confronti delle comunicazioni di crittografia, come ad esempio nel caso dei protocolli per lo scambio di chiavi.

  Supponiamo che due corrispondenti stiano scambiandosi la chiave tramite ed un intruso si pone nel mezzo della linea di comunicazione tra i due. Egli può eseguire uno scambio di chiavi separato con ciascuno dei due, dando ovviamente ad essi la netta impressione di aver scambiato la chiave tra loro e basta. In realtà invece l'attacker potrà decrittare un messaggio proveniente da uno dei due, leggerlo ed eventualmente modificarlo, e successivamente ricrittarlo ed inviarlo all'altro in maniera perfettamente trasparente.
  Un modo per prevenire questo tipo di attacco è quello di fare un hashing della chiave segreta e firmarla, e poi inviarla al corrispondente che può così verificare l'autenticità del mittente e del messaggio.

- **Attacco "timing"** – Questo tipo di attacco è relativamente recente ed è basato su ripetute misurazioni dell'esatto tempo di esecuzione delle operazioni di esponenziazione. Questo attacco è efficace contro RSA, Diffie Helmann, e contro il metodo delle curve ellittiche.

Firma Digitale 1

La Firma Digitale è l'equivalente informatico di una tradizionale firma apposta su carta, più precisamente è un sistema tecnico-informatico basato sulla crittografia a chiave pubblica, al momento è l'unica firma elettronica legalmente riconosciuta e ha maggior valore di quella cartacea, in quanto non può essere disconosciuta .

La Firma Digitale garantisce:

- l'**autenticità** del documento (sicurezza della paternità)
- l'**integrità** del documento (certezza che non sia stato alterato)
- la sua **validità**

La Firma Digitale consente:

- la sottoscrizione di un documento informatico
- la verifica, da parte dei destinatari, dell'identità del soggetto firmatario
- la sicurezza della provenienza e della ricezione del documento
- la certezza che il documento non sia stato alterato
- la segretezza dell'informazione contenuta nel documento

Firma Digitale 2

Come funziona

1. Chi redige il documento elettronico, digita la parte privata della firma digitale, tale operazione è possibile grazie ad un apposito software che la genera.
2. Chi riceve il documento elettronico, accerta che il documento non abbia subito contraffazioni o manipolazioni, mediante la prova che, apponendo la parte pubblica della chiave, quest'ultima si incastri con quella privata ricevuta.
3. Il documento elettronico ricevuto e così controllato, è valido a tutti gli effetti di legge.

Chi genera le firme?

La chiave privata della firma è generata da apposito software prodotto da chi realizza tale tipo di servizio.

La parte pubblica della firma deve invece essere certificata da uno dei certificatori iscritti nell'elenco tenuto dall' Autorità per l'informatica della Pubblica Amministrazione(AIPA).

Steganografia

E' "la scrittura nascosta", o meglio l'insieme delle tecniche che consente di comunicare in modo tale da nascondere non tanto il contenuto (come nel caso della crittografia), ma la stessa esistenza della comunicazione agli occhi di un eventuale osservatore.

L'obiettivo della steganografia è quello di nascondere un messaggio ***dentro*** un altro messaggio, dall'aspetto innocuo, in modo che il nemico non possa neppure rilevare l'esistenza del primo messaggio.

Esistono diverse tecniche di staganografia, la più diffusa è chiamata:

Steganografia sostitutiva

Tale tecnica si basa sulla seguente osservazione:

la maggior parte dei canali di comunicazione trasmettono segnali sempre accompagnati da qualche tipo di rumore; questo rumore può essere sostituito da un segnale, il messaggio segreto, che è stato trasformato in modo tale che, a meno di conoscere una chiave segreta, è indistinguibile dal rumore vero e proprio, quindi può essere trasmesso senza destare sospetti.

Controlli Fisici

Oltre alle misure di sicurezza precedentemente elencate che possono essere utilizzate per proteggere il sistema ed i dati in esso contenuti, possono essere anche utilizzati ulteriori accorgimenti.

Le misure di sicurezza a livello fisico evitano danneggiamenti di strutture o dati.

Tra questi accorgimenti possiamo citare, ad esempio:

- **Accesso controllato ai locali dei sistemi**
- **Registrazione degli accessi**
- **Continuità elettrica**
- **Protezione dei nastri di backup (**da danneggiamenti casuali, o volontari)
- **Controllo degli accessi ai dati**
- **Autenticazione degli utenti**
- **Delimitazione degli spazi logici**
- **Tracking dell'attività**

DOMANDE?

www.vincenzocalabro.it