Sicurezza Informatica

Franco Sivilli
fsivilli@unich.it

Sicurezza Informatica - Obiettivi

Conoscere gli aspetti più significativi della sicurezza informatica attraverso l'illustrazione delle features più diffuse:

- Politica di sicurezza
- Sicurezza dei sistemi operativi
- Firewall
- IDS
- A/virus
- VPN
- Wlan
- Auditing
- Misure contro la perdita dei dati:
  - Sistemi di backup su nastri
  - Gruppi di continuità
  - Sistemi fault tolerant
  - Unità e dischi ottici
  - Disaster recovery
  - Sicurezza ambientale

Concetto di Sicurezza

Lo stato o condizione nel quale le misure protettive adottate, garantiscono il mantenimento delle funzioni e prestazioni richieste ed il contenimento del DANNO entro limiti accettabili PRESTABILITI (rischio minimo), anche in presenza di minacce capaci di sfruttare le vulnerabilità del sistema.

"..sicurezza non vuol dire solo tecnologie, prodotti ed architetture ma anche comportamenti, soluzioni organizzative, procedure e soprattutto diffusione della cultura relativa"

Evoluzione del concetto di Sicurezza

- *COMSEC (protezione delle comunicazioni)*
- *COMPUSEC (in più al precedente, protezione dei sistemi stand-alone da furti di informazioni o dall'inserimento di malicious code)*
- *ICTSEC (sicurezza delle info a seguito dell'introduzione delle reti)*
- *INFORMATION ASSURANCE (tempestiva rivelazione e reazione)*

Concetto di Sicurezza - Principi

Confidenzialità (o riservatezza o segretezza): le informazioni devono essere accessibili solo a chi è autorizzato (soggetti o entità sw/hw).

Integrità (o autenticità): le informazioni non devono essere modificabili (la cancellazione è una forma di modifica) da chi non è espressamente autorizzato. L'integrità si riferisce ai dati, mentre l'autenticità si riferisce alle persone fisiche coinvolte nelle comunicazioni.

Disponibilità: le informazioni devono essere utilizzabili quando occorrono, pensando anche alle evoluzioni dell'ICT.

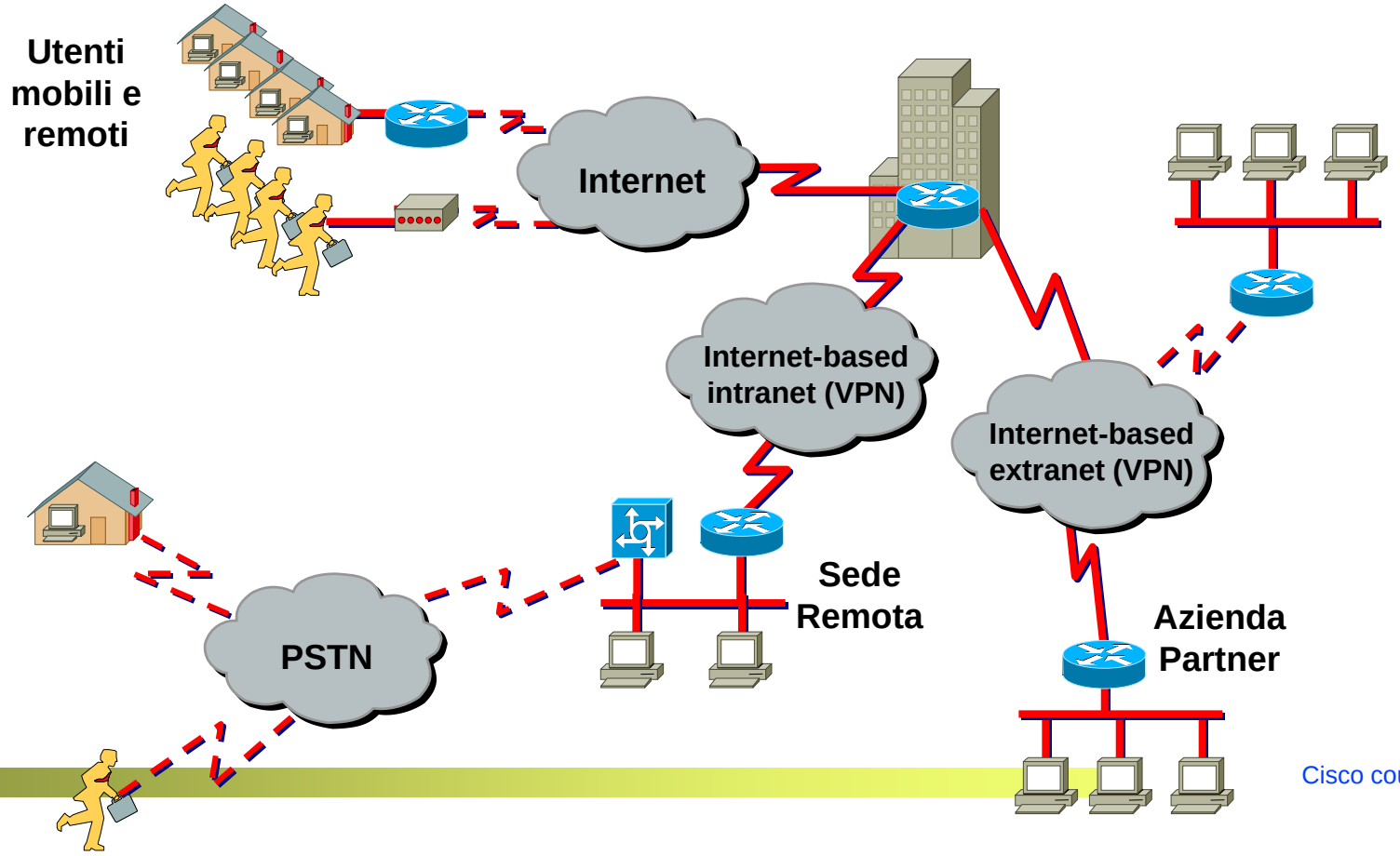
Identificazione e autenticazione: devono essere assicurate anche per i processi;

Non ripudio: impossibilità di negare una transazione effettuata

DIO (Defensive Information Operation): Detecting & Reacting.

Perché la Sicurezza

- *Perché le reti aziendali non sono più chiuse ma sono aperte su Internet*



Definizione di Incidente

Ogni tipo di attacco, intrusione, virus o perdita di dati

..QUALCHE DATO..

IL 75% DEGLI INCIDENTI SONO CAUSATI DALL'INTERNO

Piano per la sicurezza

Il **Piano della sicurezza** è il documento di analisi della sicurezza. Abbattere il rischio vuol dire adottare misure di sicurezza per ridurre il rischio.

Piano per la sicurezza – Linee guida

ANALISI DEL RISCHIO (metodi qualitativi come la matrice del rischio o metodi quantitativi basati su noti algoritmi)
POLITICA DI SICUREZZA
GESTIONE DEL RISCHIO
PIANO OPERATIVO
AUDIT
FORMAZIONE
ORGANIZZAZIONE

Definizione di Politica di Sicurezza

“ Una politica di sicurezza è una raccolta formale di regole alle quali coloro che hanno accesso alle informazioni o alla tecnologie della organizzazione devono uniformarsi.”

–(RFC 2196, Site Security Handbook)

Fattori determinanti generali

- La missione dell'azienda
  - **Militare**
  - **Privata**
  - **Formativa**
- Le politiche o le regole alle quali l'organizzazione è collegata
  - **Integrazione e non sovrapposizione**
- Apertura verso il mondo esterno
  - **Rete locale isolata**
  - **Collegamento ad Internet**

In breve..

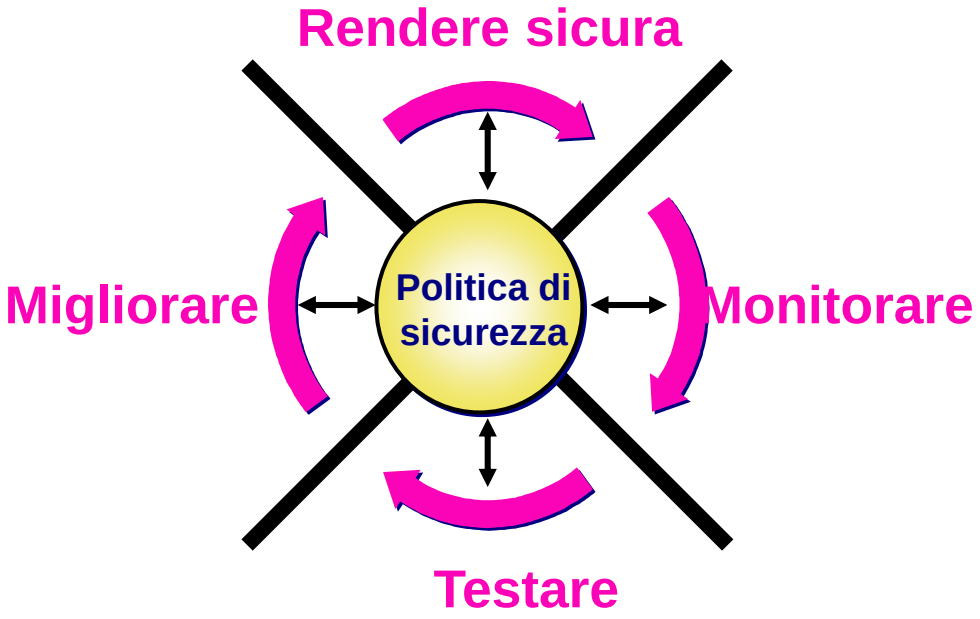
- Determinare cosa proteggere (obiettivi di sicurezza)
- Capire da cosa proteggere (funzioni di sicurezza)
- Calcolare la probabilità degli eventi
- Implementare misure di protezione che bilancino costo ed efficacia (meccanismi di sicurezza)
- Revisionare il processo continuamente (ogni volta che si scopre una debolezza)

Rischi in assenza di una la politica di sicurezza

- Danno di immagine
- Danni legali
- Danni economici
- Perdita di fiducia dei clienti

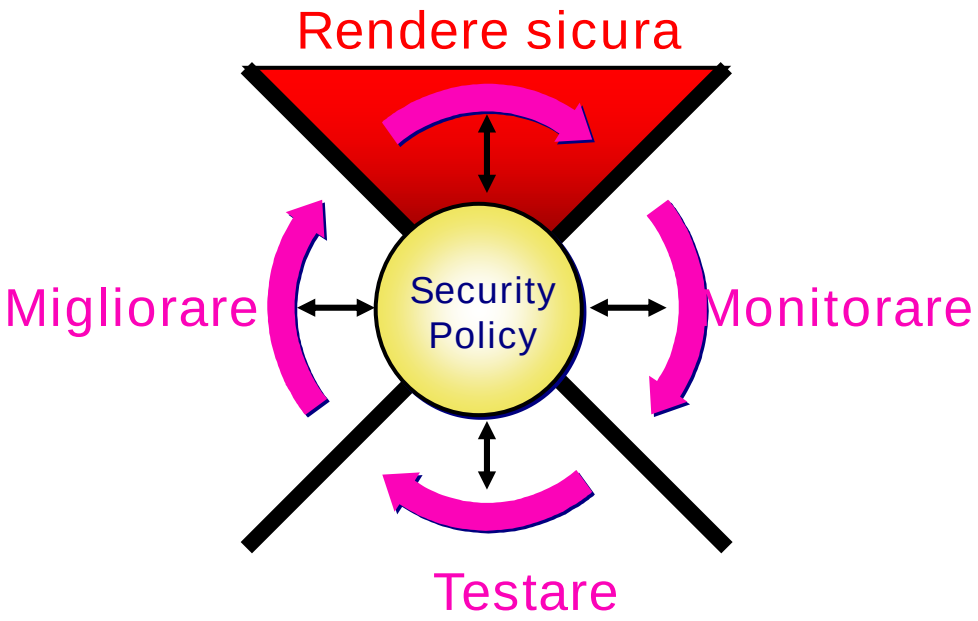
La sicurezza della rete

- **E’ un processo continuo incentrato sulla politica di sicurezza:**
  - Step 1: Rendere sicura
  - Step 2: Monitorare
  - Step 3: Testare
  - Step 4: Migliorare



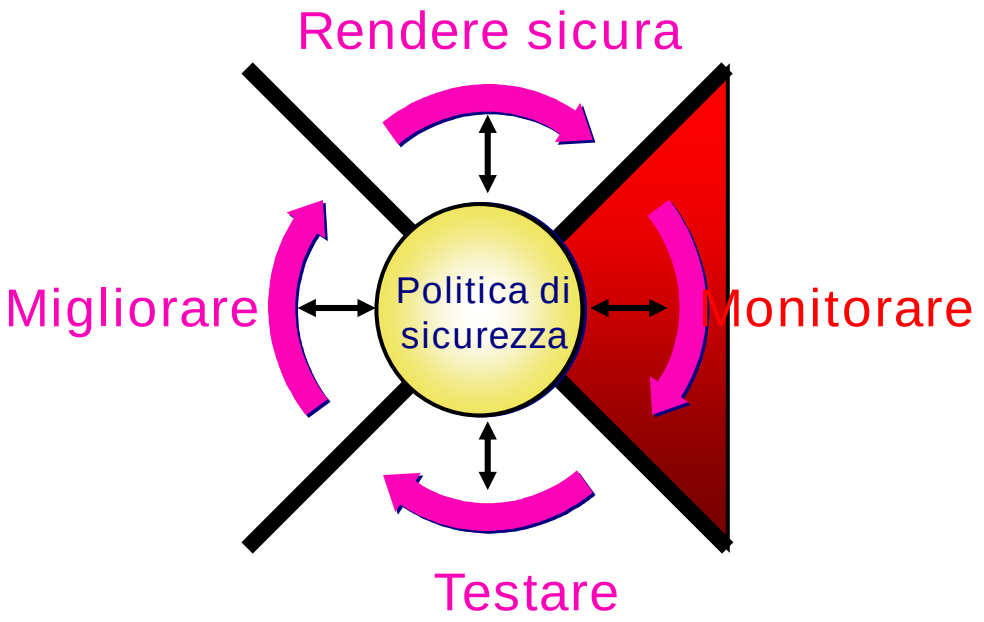
Rendere sicura

- **Implementare soluzioni applicative per fermare o prevenire accessi o attività non autorizzate e per proteggere le informazioni**



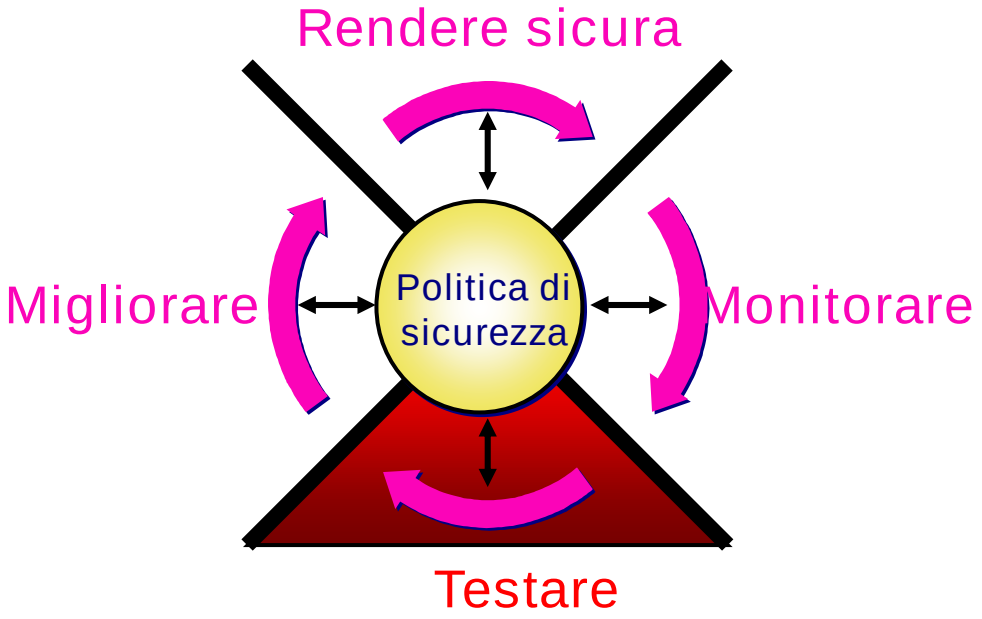
Monitorare

- **Individuare le violazioni alla politica di sicurezza**
- **Implementare system auditing and real-time intrusion detection**



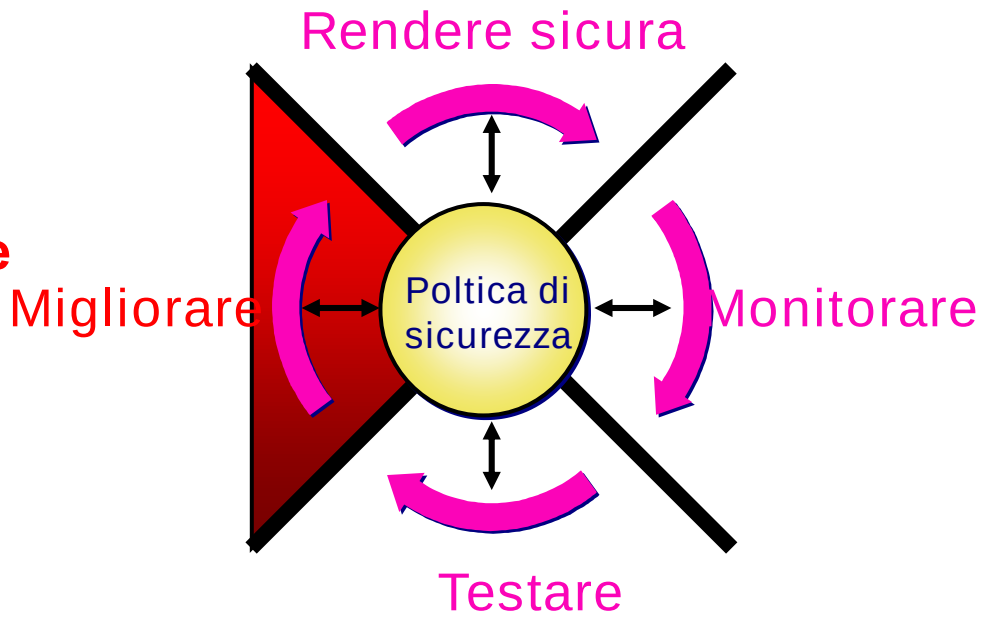
Testare

- **Validare l'efficacia della politica di sicurezza attraverso il system auditing e lo scanning delle vulnerabilità**



MIGLIORARE

- **Usare le informazioni delle fasi di monitor e di test per migliorare l'implementazione della sicurezza.**
- **Modificare la politica di sicurezza appena sono identificate le vulnerabilità ed i rischi.**



Rendere sicuri i dati

- **Autenticare gli utenti (per impedire accessi non autorizzati)**
- **Cifrare i dati (per impedire furti o alterazioni di dati)**
- **Monitorate le minacce (identificate I problem e utilizzate l'autoriparazione)**

Rendere sicuri i documenti

- **Privacy sul lavoro (tutela costante sulla sicurezza in ambiente di stampa)**
- **Conformità (protezione workflow documentali)**
- **Anti contraffazione (per impedire manomissioni di documenti e frodi))**

.....iniziamo dal Sistema operativo ....

Principi per un S.O. sicuro

- Least privilege
  - **Solo i diritti di accesso necessari**
- Economy of mechanism
  - **Il sw che gestisce la sicurezza deve essere piccolo e di semplice progettazione**
- Complete mediation
  - **Ogni accesso è controllato**
- Permission based
  - **La condizione di default è: “non è consentito l’accesso”**
- Separation of privilege
  - **Più di una condizione deve essere necessaria all’accesso : qualcosa che si ha (smart card) più qualcosa che si conosce (password)**
- Least common mechanism
  - **Per ridurre il rischio della condivisione degli oggetti**

PRINCIPI PER UN S.O. SICURO

Modelli di protezione nei S.O.

- Condivisioni protette da password (accede chi conosce la pwd)
  - Una password ad ogni risorsa condivisa
  - In Windows diversi livelli di pwd: read o read-write
- Autorizzazioni di accesso (assegnazione diritti al singolo utente o a gruppi di utenti)
  - Vengono assegnate dall'Amministratore ad ogni utente
  - Sono di 5 tipi:
    - Read (legge e copia i file nella cartella condivisa)
    - Execute (Esegue i file della cartella)
    - Write (Crea nuovi file nella cartella)
    - Delete (Elimina i file dalla cartella)
    - No access (impedisce l'accesso alla cartella, file o risorse)

PRINCIPI PER UN S.O. SICURO

- **Modelli di protezione nei S.O.**

  - .. Continua .. Autorizzazioni di accesso

    Impostazioni parametri per l'utente (policy):

    tempi di accesso,

    area di memoria di massa personale,

    data di scadenza (impostata per accessi temporanei)

PRINCIPI PER UN S.O. SICURO

- **Modelli di protezione nei S.O.**

  - Smart Card log-on

    Si utilizza una smart card personale in luogo di user+password. Questo presuppone l'implementazione di una PKI aziendale

PRINCIPI PER UN S.O. SICURO

- **Modelli di protezione nei S.O.**

  - Hardening del sistema

    Porre in essere tutte quelle procedure atte alla rimozione dei servizi non necessari dalla configurazione della macchina in esame ed all'aggiornamento, tramite l'apposizione delle apposite patch, di quelli che devono essere necessariamente presenti.

    E' un'attività che deve essere attuata più volte nel tempo (Multiple time)

Caratteristiche di sicurezza

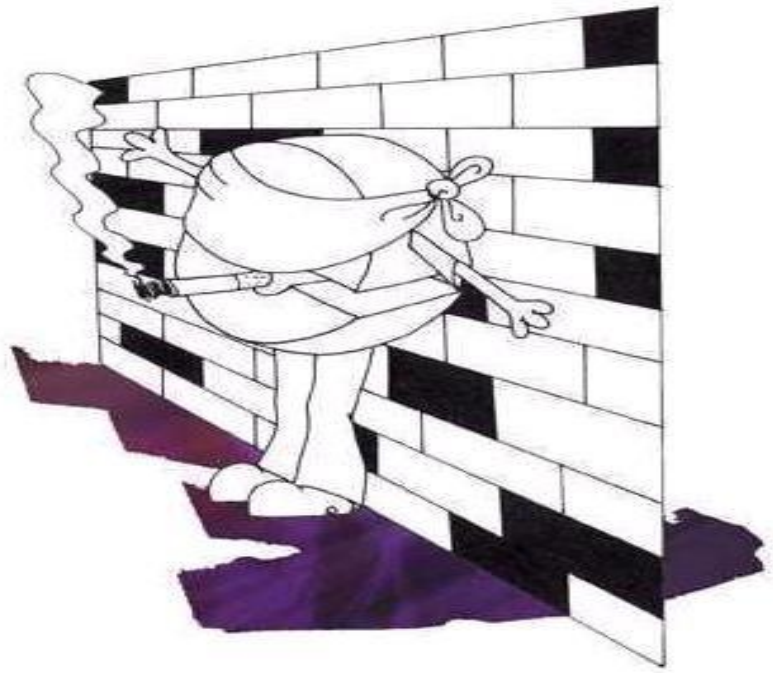
- **Miglioramenti della protezione**

  - Sicurezza perimetrale: il Firewall
  - VPN (Virtual Private Network)
  - Auditing e sistemi di Intrusion detection
  - Crittografia e meccanismi di autenticazione (vedasi lezione specifica)
  - Antimalware e exploit
  - Intelligenza artificiale

Caratteristiche di sicurezza

- **Miglioramenti della protezione: firewall**

Firewall



Caratteristiche di sicurezza

- **Miglioramenti della protezione: firewall**

  E' un sistema misto hw/sw avente lo scopo di proteggere la rete aziendale da eventuali intrusioni da utenti di altre reti.

  Analizza il traffico in entrata ed in uscita, bloccando quello che non risulta conforme alle regole di sicurezza preventivamente impostate.

  Registra il volume di traffico e le informazioni sui tentativi di accesso non autorizzato.

  E' un sistema di difesa "perimetrale" perchè difende dalle intrusioni non autorizzate provenienti dall'esterno. Per perimetro si intende "il punto" in cui una rete fidata (trusted) si connette ad una rete non fidata (untrusted).

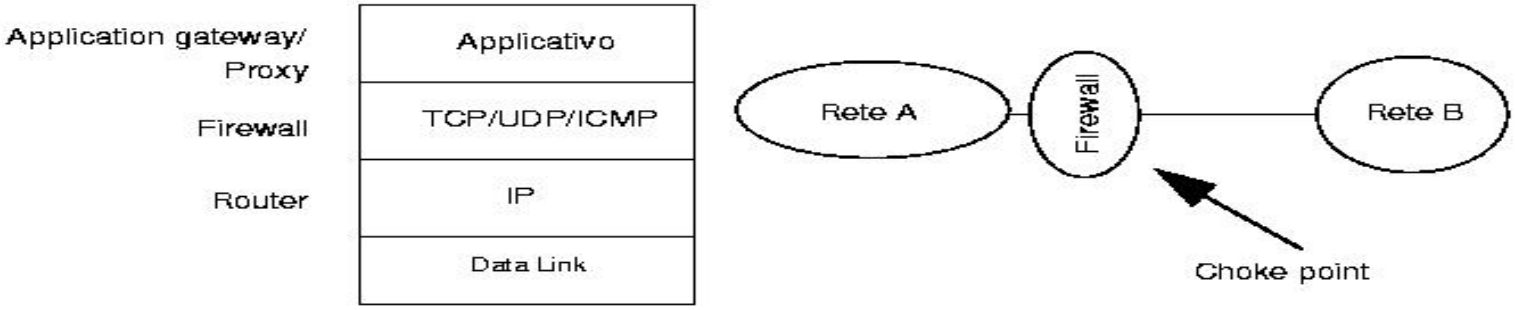
Caratteristiche di sicurezza

- **Miglioramenti della protezione: firewall**

Cosa è un firewall

Un firewall è un componente di sicurezza che:

- opera a livello TCP [UDP, ICMP];
- collega due reti restringendo l'accesso tra l'una e l'altra;



Caratteristiche di sicurezza

- **Miglioramenti della protezione: firewall**

Caratteristiche di sicurezza

- **Miglioramenti della protezione: alcune architetture firewall**
  - **Packet filtering**
  - **Stateful packet inspection**

Caratteristiche di sicurezza

- **Miglioramenti della protezione: architetture firewall**

  Packet filtering firewall

  Abilita/Disabilita il trasferimento di dati tra due reti basandosi su indirizzo IP del mittente e del destinatario, sui protocolli usati (es. http, ftp) e la relativa porta. In questo tipo di firewall il filtering è stateless (non tiene traccia delle sessioni).

  Non analizza il contenuto informativo dei pacchetti (payload)

Caratteristiche di sicurezza

- **Miglioramenti della protezione: architetture firewall**

  Stateful packet inspection firewall

  Aggiunge alle funzionalità del packet filtering firewall anche il controllo delle sessioni controllando anche il contenuto dei pacchetti.

  I packet in ingresso che non inizializzano una nuova sessione devono essere correlati ad una sessione già esistente per poter essere permessi. In pratica fa entrare solo pacchetti che fanno parte di sessioni già iniziate

Caratteristiche di sicurezza

- **Miglioramenti della protezione: VPN**

La VPN (Virtual Private Network) è una connessione cifrata tra reti private utilizzando una rete pubblica come Internet.

Le aziende usano le VPN per stabilire collegamenti sicuri (uso della crittografia) chiamati tunnel utilizzando una infrastruttura di rete pubblica, come Internet. Le VPN sono i furgoni blindati per il trasporto sicuro tra due posti attraverso una rete viaria pubblica.

Caratteristiche di sicurezza

- **Miglioramenti della protezione: tecnologia usata nelle VPN - IPSEC**

La sicurezza delle VPN è garantita da un insieme di protocolli, algoritmi di hash e algoritmi di crittografia chiamato IPSEC

Caratteristiche di sicurezza

- **Miglioramenti della protezione: servizi offerti da IPSEC**

•Confidenzialità (è garantita della crittografia simmetrica con scambio delle chiavi DH o asimmetrica)

•Integrità dei dati (il destinatario può verificare che i dati ricevuti non sono cambiati o alterati)

•Autenticazione dell'origine dei dati (il destinatario ha la certezza che i dati provengano da quella origine)

•Univocità (garantisce la non duplicazione dei pacchetti)

Caratteristiche di sicurezza

- **Miglioramenti della protezione: auditing**

E’ il processo di revisione dei record degli eventi nel log di protezione.

Nei record sono indicati gli utenti che hanno tentato di accedere con successo o meno a risorse specifiche.

Permette agli amministratori di identificare le attività non autorizzate e l’utilizzo della rete.

Caratteristiche di sicurezza

- **Miglioramenti della protezione: auditing**

Il processo di controllo registra le seguenti funzioni:

- Tentativi di accesso
- Connessione e disconnessione alle risorse designate
- Interruzione della connessione
- Disabilitazione account
- Apertura e chiusura di file
- Modifica dei file
- Creazione ed eliminazione cartelle
- Modifica cartelle
- Eventi e modifiche del Server
- Modifica delle password
- Modifica dei parametri di accesso

Caratteristiche di sicurezza

- **Miglioramenti della protezione: IDS (Intrusion Detection System)**

Se il firewall è analogo alla porta blindata in una abitazione, un IDS è analogo ad un sistema di allarme.

Il firewall previene le intrusioni, un IDS le segnala a chi di competenza.

Caratteristiche di sicurezza

- **Miglioramenti della protezione: IDS (Intrusion Detection System)**

  Possiamo distinguere 4 tipologie di IDS:

  Signature-based intrusion detection: basato sul pattern matching con un insieme di campioni conosciuti chiamati signature. Riconosce solo attacchi noti a priori, ma è comunque molto affidabile. E' meno soggetto ai falsi positivi (allarme per un evento che non è un attacco)

  Profile-based intrusion detection basato sul matching statistico con un comportamento creato come standard. E' in grado teoricamente di identificare qualsiasi attacco, ma può generare molti falsi positivi

  Network-based intrusion detection: analizzano il traffico della rete mediante vari sensori collegati ai vari segmenti della rete.

  Host-based intrusion detection: analizzano il traffico dell'host su cui è installato. Proteggono solo quell'host.

Caratteristiche di sicurezza

Miglioramenti della protezione: antimalware

malware:Software avanzati in grado di impartire ordini, talvolta distruttivi, ai sistemi operativi attaccati - l'utilizzo dei Virus è ancora il sistema più diffuso per arrecare danni o attaccare un PC (attualmente si conoscono 50.000 virus attivi).

Sottocategorie più diffuse

- ***Virus associati a programmi:* stesso nome del programma cui si associano ma estensione diversa.** *Es. word.com viene eseguito prima di word.exe – il virus può chiamarsi word.com*
- ***Virus macro:quando si apre un file contenente un virus macro (****es. Word****) il virus si associa all'applicazione ed infetta altri file cui l'applicazione accede.***
- ***Virus polimorfici:variano ogni volta che si autoriproducono, risulta più difficile rilevarli***
- ***Virus furtivi:si nascondono per non essere rilevati. Intercettano l'ispezione eseguita dall'antivirus e restituiscono informazioni errate segnalando che il virus non esiste.***

Esistono anche virus che attaccano Firewall o Router implementando attacchi di tipo Denial of Service

Caratteristiche di sicurezza

- **Miglioramenti della protezione: antimalware**

Diffusione: Attraverso lo scambio di supporti informatici o attraverso la rete

Effetti: Il computer non si avvia, i dati risultano illeggibili o danneggiati, il computer funziona in modo anomalo, una partizione è andata persa, l'hard disk è stato riformattato.

Soluzioni: Installare un valido ANTIVIRUS e aggiornare costantemente le impronte virali - NON EFFICACE per i virus "nuovissimi" (ogni mese vengono scoperti più di 500 nuovi virus o varianti di virus già esistenti).

Attività a rischio: Utilizzare files o programmi memorizzati su supporti informatici di provenienza incerta o contenenti software non originali e prelevare files e programmi dalla rete, aprire gli allegati ad un file di posta elettronica sospetto e, ultimamente, anche solo leggendo una e-mail

Caratteristiche di sicurezza

- **Miglioramenti della protezione: antimalware e posta elettronica, qualche consiglio**

1. **Aggiornare l'Antivirus costantemente**
2. **Tutti i Client di posta sono potenziali bersagli dei virus**
3. **Non fare click con il mouse su link contenuti nel messaggio**
4. **Non lanciare mai dei file eseguibili in una finestra pop-up visualizzata nel messaggio di e-mail**
5. **Installare i più recenti aggiornamenti per la sicurezza del vs client di posta**
6. **Non aprire allegati con le seguenti estensioni: .bat, .vbs, .shs, .pif, .scn.**
7. **Non aprire gli allegati con una doppia estensione del file**
8. **Configurare Windows in modo da vedere le estensioni dei file per intero**
9. **Aprire gli allegati dopo averli salvati e controllati con un a/virus**

Caratteristiche di sicurezza

- **Miglioramenti della protezione: intelligenza artificiale**

L’intelligenza artificiale o machine learning è globalmente riconosciuta quale potente alleato nella rilevazione anticipate delle minacce informatiche avanzate

L’efficacia di questi strumenti matematici applicati alla cyber security dipende dalla capacità degli algoritmi di elimanre il rumore di fondo, di leggere i dati come farebbe un esperto analista e di fornire al SOC (Security Operation Center) strumenti di monitoraggio e informazioni utili ad una rapida identificazione delle reali minacce.

Caratteristiche di sicurezza

- **Miglioramenti della protezione: algoritmi di intelligenza artificiale**

Cosa devono fare:

- **Analisi di big data in tempi utili;**
- **Definizione di modelli matematici efficacy;**
- **Rimozione del rumore di fondo**
- **Processo di continuo miglioramento degli algoritmi**

Caratteristiche di sicurezza

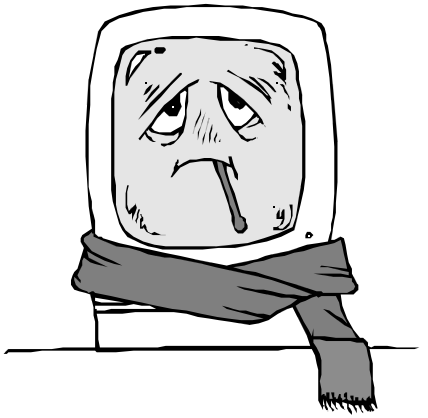
- **Miglioramenti della protezione: algoritmi di intelligenza artificiale**

Approccio non supervisionato:

- **Apprendere in maniera autonoma il comportamento della rete;**
- **Identificare le attività anomale;**
- **Rilevare automaticamente pattern e relazioni;**
- **Lavorare senza informazioni a priori**
- **Non necessità di input umani**

PERDITA DI DATI

Cause dei problemi



- Problemi a livello di componenti hw
- Malware /exploit
- Eliminazioni accidentali o dolose dei dati
- Incendi dolosi o dovuti a problemi elettrici
- Disastri naturali (temporali, inondazioni, terremoti)
- Interruzioni e sbalzi di corrente
- Furti e vandalismi

Misure contro la perdita di dati

- **Sistemi di prevenzione**

  - Sistemi di backup su nastri
  - Gruppi di continuità preferibilmente centralizzati
  - Sistemi fault tolerant
  - Unità e dischi ottici

Misure contro la perdita di dati

- **Backup, qualche consiglio :**
  - Non dare per scontato che sia qualcun altro ad occuparsi del backup
  - Non considerare eseguito con successo un backup senza verificare che sia stato effettivamente portato a termine
  - Non dare per scontato che i dati relativi al backup siano “utilizzabili”
  - Eseguire il backup con gli strumenti giusti

Misure contro la perdita di dati

- **UPS – componenti fondamentali:**
  - Fonte di energia per l'alimentazione dei Server (batteria)
  - Servizio di gestione della procedura di arresto
    - Impedisce ad altri utenti di accedere al Server
    - Invia un msg di avviso all'Amministratore e/o Utenti per salvare i lavori correnti

L'UPS va dimensionato (KVA) in base alla server farm che deve asservire

E' preferibile avere un Gruppo Elettrogeno associato all'UPS

Misure contro la perdita di dati

- **Sistemi Fault tolerant:**
  - Sistemi RAID
  - Clustering
  - Storage Area Network

Misure contro la perdita di dati

- **Sistemi Fault tolerant : RAID (Redundant Array Of Indipendent Disk)**

E’ una matrice ridondante di dischi indipendenti. Ci sono vari livelli che offrono diverse combinazioni di prestazioni, affidabilità e costi.

I livelli più usati sono *0, 1,3, 5*

Misure contro la perdita di dati

- **Sistemi Fault tolerant : RAID (Redundant Array Of Indipendent Disk)**

Livello 0	**Chiamato anche disk striping. I dati sono distribuiti tra i diversi dischi dell'array con nessun dato di verifica degli stessi. Il sistema riconosce come unica unità l'array di dischi. Il vantaggio è quello di avere più spazio.**
Livello 1	**Chiamato di mirroring. Es. due dischi in RAID 1 vuol dire che i dati del primo disco sono replicati sul secondo;**
Livello 2	**Dati protetti su N dischi e i dati di verifica su m dischi;**
Livello 3	**Ogni blocco di disco virtuale (l'array è un disco virtuale) è suddiviso e distribuito attraverso tutti i dischi di dati. I dati di verifica di parità sono archiviati su un disco di parità separato;**
Livello 4	**Blocchi di dati come nel liv. 0. Dati di verifica di parità archiviati su un disco;**
Livello 5	**Blocchi di dati come nel liv. 0. dati di verifica di parità distribuiti su più dischi;**
Livello 6	**Come RAID 5 con l'aggiunta di dati di verifica calcolati in modo indipendenti.**

MISURE CONTRO LA PERDITA DI DATI

- **Sistemi Fault tolerant : Clustering**

Un ambiente a Cluster è una collezione di macchine fisiche, detti nodi, che comunicano le une con le altre attraverso un private network.

Il Cluster ha un unico indirizzo pubblico sulla rete aziendale.

Ogni nodo ha propri processori, memoria Ram e di Massa, ma tutti i nodi hanno accesso ad una memoria di massa condivisa (Es. disk array Raid 5).

Una tipica configurazione è 2 nodi Active/Stand by

Misure contro la perdita di dati

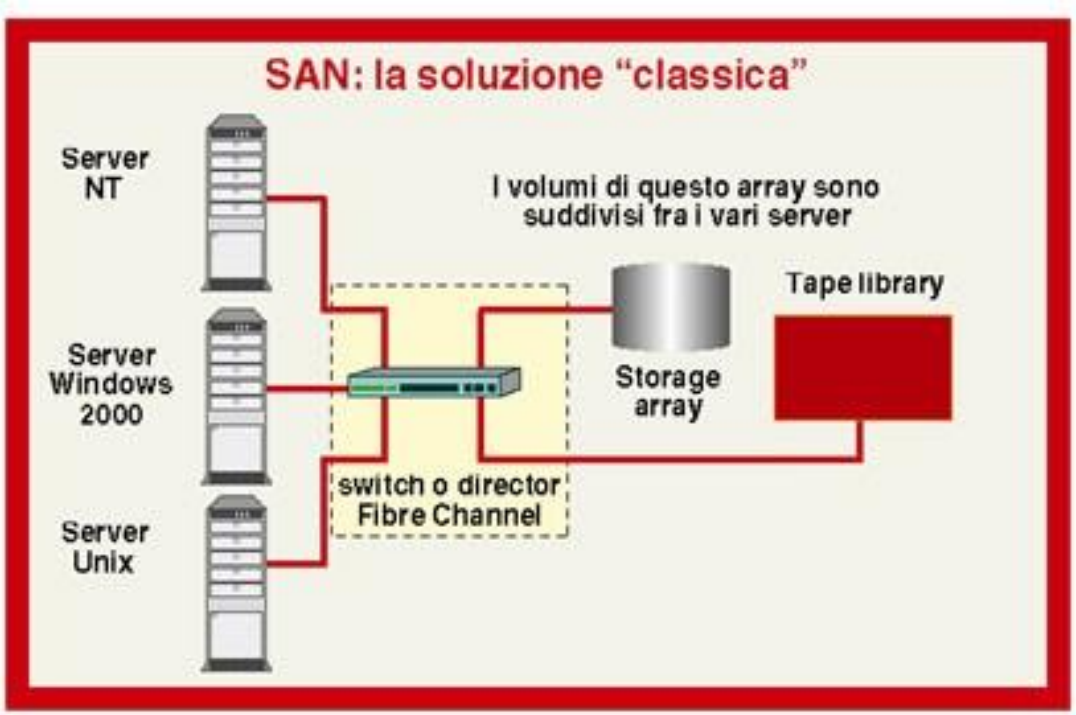
- **Sistemi Fault tolerant : Storage Area Network**

La progettazione di una SAN è strettamente legata alla realtà aziendale che deve asservire.

In questo caso il Server diviene un single point of failure

Misure contro la perdita di dati

- **Sistemi Fault tolerant : Storage Area Network**



Vademecum per tenere in buona salute il proprio PC

- Aggiornare Windows
- Controllate i processi che si caricano all'avvio (msconfig da command line→ scheda avvio)
- Aggiornare tutto il sw (inclusi a/virus e firewall)
- Fare regolarmente il backup
- Navigate sicuri (disabilitare l'accettazione di cookie, attenti ai pop-up)
- Non fidatevi degli allegati (contattare il mittente per gli attach dubbi)
- Non abboccate agli spam
- Controllate di non avere attivo il desktop remoto
- Configurate bene l'instant Messenger (accettate solo utenti facenti parte dei vs contatti)
- Controllate la presenza di vulnerabilità (tool ShieldsUp! su www.grc.com)
- Tenete d'occhio la barra del system tray (devono essere presenti l'a/virus, il firewall e tutti I prg di monitoring)

Disaster recovery

- **Linee guida**

1. **Individuare i fattori controllabili**
2. **Determinare qual è il metodo di prevenzione migliore**
3. **Implementare ed imporre le misure preventive scelte**
4. **Verificare la disponibilità di metodi di prvenzione nuovi e migliori**
5. **Eseguire regolarmente la manutenzione dell'Hw e del Sw**
6. **Fare formazione del personale**
7. **Preparare un piano per l'Hardware (scorta di parti di ricambio)**
8. **Preparare un piano per il Software**
9. **Preparare un piano per i Dati**

Sicurezza Ambientale

- **Non dimentichiamo l'ambiente …**

1. Temperatura costante : 18°-22°
2. Umidità costante : 50%-70%
3. No polvere e fumo
4. No rumore
5. No interfenze elettromagnetiche
6. No vibrazioni
7. Protezione dei cavi con corrugati appositi
8. Sistema di controllo Accessi in Sala Server
9. Sistema di rilevazione e spegnimento incendi
10. Sistema di segnalazione condizioni ambientali
11. Rinforzo infrastrutturale

Fine

fsivilli@unich.it