SE.R.I. - Confindustria Foggia

Corso di aggiornamento sulla sicurezza informatica
anno 2008

Modulo 1

CONCETTI GENERALI SULLA SICUREZZA INFORMATICA

Prof. Crescenzio Gallo
c.gallo@unifg.it

Competenze

Acquisire familiarità con il concetto di *sicurezza informatica*, *sicurezza delle informazioni* e *protezione dei sistemi informativi*

Il corso ha lo scopo di fornire familiarità con i vari modi di proteggere i dati sia su un sistema "stand alone" che in una rete connessa a Internet; in particolare, mettere gli utenti in condizioni di proteggere i dati aziendali contro perdite, attacchi virali e intrusioni.

Contenuti

1. Concetti di base
2. Autenticazione e controllo degli accessi
3. Aspetti pratici
4. Gestione del rischio
5. Organizzazione della sicurezza
6. Le norme sul sistema di gestione della sicurezza


Concetti di base

Obiettivi

Sapere quali sono i principali aspetti della sicurezza delle informazioni: *disponibilità*, *riservatezza* e *integrità*.

Concetti di base

La **sicurezza delle informazioni** è un'esigenza che ha accompagnato la storia dell'uomo fin dalle antiche civiltà.

Oggi ci preoccupiamo di mantenere riservate le informazioni personali, militari e d'affari. Nel V secolo a.C. gli spartani inviavano gli ordini ai capi militari tramite messaggi scritti su una striscia di cuoio che, avvolta su un bastone (lo scitale) di un diametro ben preciso, permetteva di leggere il testo in chiaro lungo il bastone. Giulio Cesare cifrava i messaggi sostituendo ogni lettera con quella che nell'alfabeto segue di qualche posizione.

La **crittografia**, cioè la scienza della scrittura segreta, ha avuto una progressiva evoluzione nel corso dei secoli, fino ai rapidi sviluppi teorici e tecnologici impressi dalla seconda guerra mondiale, che permisero la decifrazione dei codici giapponesi e tedeschi da parte degli alleati.

Concetti di base

Oggi buona parte del pianeta vive nella *società dell'informazione*, basata cioè sull'uso delle informazioni come parte integrante delle attività umane.

Pertanto, la sicurezza delle informazioni è diventata una componente della sicurezza dei beni in generale, o *security*, e non si limita alle tecniche per nascondere il contenuto dei messaggi.

Qualunque programma che si occupi di preservare la sicurezza delle informazioni, persegue, in qualche misura, tre obiettivi fondamentali: la **disponibilità**, l'**integrità** e la **riservatezza** delle informazioni.

La **disponibilità** è il *grado in cui le informazioni e le risorse informatiche sono accessibili agli utenti che ne hanno diritto, nel momento in cui servono.*

Disponibilità

Questo significa che sistemi, reti e applicazioni hanno le capacità necessarie a fornire il livello di servizio e le prestazioni richieste e che, in caso di guasto o di eventi distruttivi, sono pronti gli strumenti e le procedure per ripristinare l'attività in tempi accettabili.

Disponibilità

Per impedire l'*inaccessibilità* delle informazioni, si deve preservare la disponibilità delle condizioni ambientali (energia, temperatura, umidità, atmosfera, etc.) e delle risorse hardware e software a fronte sia di problemi interni (guasti, errori, blackout, disastri e altro), sia di attacchi esterni, per esempio provenienti da Internet, volti a impedire o a ridurre l'accessibilità ai sistemi e alle informazioni.

Disponibilità

Sistemi di backup locale e remoto, ridondanza dell'hardware e degli archivi, firewall e router configurati per neutralizzare attacchi DoS (Denial of Service), sistemi di climatizzazione, gruppi di continuità, controllo dell'accesso fisico, monitoraggio delle prestazioni sono alcuni degli strumenti che servono per mantenere la disponibilità.

Integrità

L'**integrità** è il *grado di correttezza, coerenza* e *affidabilità delle informazioni* e anche il grado di completezza, coerenza e condizioni di funzionamento delle risorse informatiche.

Integrità

Per l'hardware e i sistemi di comunicazione, l'integrità consiste di fattori come elaborazione corretta dei dati, livello adeguato di prestazioni e corretto instradamento dei dati.

L'integrità del software riguarda fattori come la completezza e coerenza dei moduli del sistema operativo e delle applicazioni e la correttezza dei file critici di sistema e di configurazione.

Integrità

Per le informazioni, l'integrità viene meno quando i dati sono alterati, cancellati o anche inventati, per errore o per dolo, e quando si perde, per esempio in un database, la coerenza tra dati in relazione tra loro (per esempio i record coinvolti in una transazione).

Integrità

Procedure di manutenzione e diagnosi preventiva, hardware e software per la rilevazione e prevenzione di accessi illeciti, attacchi virali e intrusioni, applicazioni che minimizzano errori logici e formali di data entry, accesso ristretto alle risorse critiche e controllo degli accessi sono alcuni degli strumenti utili a preservare l'*integrità delle informazioni e delle risorse*.

Integrità

Anche le tecniche di **hashing** (calcolo di un numero di lunghezza fissa a partire da un qualsiasi messaggio o documento) sono usate per verificare che le informazioni non vengano alterate per dolo o per errore (anche di trasmissione).

La **riservatezza** *consiste nel limitare l'accesso alle informazioni e alle risorse informatiche alle sole persone autorizzate,* e si applica sia all'archiviazione sia alla comunicazione delle informazioni.

Riservatezza

*Un'**informazione** è composta generalmente di più dati in relazione tra di loro, ciascuno dei quali non necessariamente costituisce un'informazione.*

Il nome e il numero di conto corrente di una persona, separati, non sono informazioni; è la combinazione dei due dati che costituisce l'informazione.

Riservatezza

La riservatezza dell'informazione può essere quindi garantita sia nascondendo l'intera informazione (per esempio con tecniche di crittografia) sia nascondendo la relazione tra i dati che la compongono.

Riservatezza

La riservatezza non dipende solo da strumenti hardware e software; il fattore umano gioca un ruolo chiave quando vengono ignorate le elementari regole di comportamento:

- tenere le password segrete,
- controllare gli accessi a reti e sistemi,
- rifiutare informazioni a sconosciuti (anche quando affermano di essere tecnici della manutenzione),
- cifrare i documenti e i messaggi riservati e così via.

Altri obiettivi

Altri due obiettivi di sicurezza possono essere considerati un'*estensione dell'integrità* delle informazioni, applicata a eventi più complessi come l'invio di un messaggio o una transazione:

- l'**autenticità** garantisce che eventi, documenti e messaggi vengano attribuiti con certezza al legittimo autore e a nessun altro;
- il **non ripudio** impedisce che un evento o documento possa essere disconosciuto dal suo autore.

Altri obiettivi

Queste due caratteristiche trovano applicazione nella **firma digitale**, che utilizza tecniche di hashing e crittografia per garantire che un documento resti integro e provenga da un autore univocamente identificato.


Autenticazione e controllo degli accessi

Autenticazione (authentication) = *processo mediante il quale si verifica l'identità di un'entità (utente, processo, computer, messaggio).*

Nessun computer, software o utente può **confermare con certezza** l'identità di un utente: si possono solo eseguire test che, se superati, forniscono una garanzia sufficiente sull'identità dell'interlocutore.

L'entità che deve essere autenticata presenta alcune **credenziali** (password, certificato digitale) come prova della propria identità: se sono ritenute valide e sufficienti, l'entità è ritenuta autentica.

L'autenticazione verifica solo che un'entità sia quella che dichiara di essere, senza entrare nel merito dell'accesso al sistema.

Una volta che un'entità è stata autenticata, il passo successivo è assicurare che possa accedere solo alle risorse per cui è **autorizzata** (ad es. mediante controlli di accesso, permessi, privilegi).

L'autorizzazione viene talvolta confusa con l'autenticazione, ma è un concetto ben distinto...

Autorizzazione è il *diritto accordato ad un'entità (hardware, software, individuo) di accedere ad un sistema e alle sue risorse secondo un profilo di permessi ben definito*.

Il controllo del passaporto di un viaggiatore è un esempio di **autenticazione**, nella quale la foto viene confrontata con l'aspetto della persona ed il documento viene validato rispetto all'Ente che lo ha rilasciato...

Il successo dell'autenticazione non implica che il viaggiatore possa varcare la frontiera: la persona potrebbe risultare priva di qualche requisito od essere indesiderata (*accesso negato per mancata autorizzazione*).

Su una rete (e quindi Internet) l'autenticazione è più complessa sia perché eseguita da macchine sia perché le entità della rete di solito non hanno accesso fisico alle entità da autenticare.

Se un individuo riesce ad impersonare un utente valido, non ci sono limiti al danno potenziale per la riservatezza e integrità delle informazioni, oltre agli eventuali danni economici.

In qualche caso può persino essere compromessa la futura capacità di autenticazione degli utenti.

Metodi di autenticazione più diffusi:

- **password**
- **certificati digitali**
- **dispositivi biometrici**
- **token fisici**
- **smart card**

ma nessuno è perfettamente sicuro!

Per impieghi di autenticazione medio-elevati può essere idonea una combinazione di requisiti: ad es. un PDA con capacità crittografiche e biometriche (riconoscimento dell'impronta digitale, della firma e della voce).

I modelli a cui si fa riferimento per progettare un **sistema di autenticazione** dipendono da:

- *tipo di utenti;*
- *distribuzione fisica delle risorse;*
- *valore delle informazioni da proteggere;*
- *altri fattori...*

1) Autenticazione locale: *è quella utilizzata su un computer desktop o portatile.*

L'intero sistema, inclusi i meccanismi di autenticazione e controllo degli accessi, risiede all'interno di un singolo perimetro di sicurezza, all'interno del quale l'utente definisce e tiene aggiornate le informazioni di autenticazione.

Modelli di autenticazione

2) Autenticazione diretta: *usata in passato dai server LAN e dai sistemi time-sharing.*

Il sistema è usato da molti utenti, anche remoti; autenticazione e controllo degli accessi risiedono in un singolo perimetro fisico. E' "diretto" perché centralizzato: un singolo sistema prende le decisioni e contiene il database dei profili utente. Le password sono crittografate.

3) Autenticazione indiretta: *usata nei moderni sistemi distribuiti per consentire agli utenti di accedere a più sistemi in rete.*

Quando un sistema riceve una richiesta di autenticazione, la inoltra ad un **server di autenticazione centralizzato** che verifica e conferma l'identità dell'utente (vengono usati i protocolli RADIUS e Kerberos o Active Directory Windows).

4) Autenticazione off-line: *usata nei sistemi che sfruttano l'infrastruttura a chiave pubblica (PKI).*

Diversi componenti autonomi prendono decisioni sull'autenticazione degli utenti. E' una combinazione dei tre precedenti: autenticazione e controllo accessi risiedono sullo stesso dispositivo, mentre il titolare della sicurezza (la CA, non necessariamente online) mantiene un db centralizzato degli utenti autorizzati.

Esempio: il funzionamento del **protocollo SSL**.

1. un browser si procura il certificato con la chiave pubblica dal server da autenticare (ad es. il sito di una banca);
2. lo autentica con un'altra chiave pubblica prestabilita (nota al browser - "CA attendibili");
3. quindi utilizza la chiave pubblica del server nella fase di scambio dati per la costruzione di una chiave di sessione con cui cifrare le comunicazioni.

Elementi comuni dei sistemi di autenticazione:

- l'**entità** da autenticare;
- le **caratteristche distintive** su cui si basa l'autenticazione;
- un **proprietario** o **amministratore** del sistema di sicurezza;
- un **meccanismo di autenticazione** che verifica le caratteristiche distintive.

Il **meccanismo di controllo dell'accesso** è una funzione successiva all'autenticazione, invocato se quest'ultima ha avuto successo.

Esempio: **Bancomat**.

Entità da autenticare: l'utente.

Caratteristiche distintive: la tessera ed il PIN.

Amministratore sistema di sicu-rezza: la Banca.

Meccanismo di autenticazione: software di vali-dazione delle informazioni fornite dalla scheda e dall'utente.

Se l'autenticazione ha successo e l'utente ha il credito necessario, il meccanismo di controllo dell'accesso autorizza il prelievo.

Esempio: **Sito di e-Commerce**.

Entità da autenticare: il proprietario del sito.

Caratteristiche distintive: chiave pubblica in un certificato digitale.

Amministratore sistema di sicurezza: la CA emittente il certificato digitale.

Meccanismo di autenticazione: il software, nel browser dell'utente, di convalida del certificato del sito (protocollo SSL).

Fattori di autenticazione di un utente(*):

- qualcosa che **sai** (password, PIN, ...);
- qualcosa che **hai** (token, smartcard, ...);
- qualcosa che **sei** (impronta digitale, retina, iride, volto, voce, ... *Attenzione: corpo vs. individuo!*).

(*) Carlton et al., "Alternate Authentication Mechanisms", 1988.

Qualcosa che **sai**

E' uno dei metodi di autenticazione più antichi. Comprende: parole d'ordine (password), frasi (passphfrase), PIN (combinazione numerica) ed in genere informazioni note solo al possessore, da usare in risposta a specifiche domande personali.

L'autenticazione tramite un dato segreto noto solo al possessore è vulnerabile sia per motivi tecnici che per comportamenti insicuri degli utenti: tende ad essere sostituita da combinazioni di più fattori (ad es. scheda + PIN).

Il grado di sicurezza peggiora rapidamente quando l'utente scrive le password su carta o le conserva in file non cifrati!

Qualcosa che **hai**

Il termine **chiave** in informatica deriva in effetti dalle chiavi di casa, ma può essere semplicemente un file, di solito incorporato in un dispositivo fisico (*token*).

L'autenticazione tramite token è la più difficile da violare, poiché l'oggetto fisico deve essere posseduto al momento dell'autenticazione e dell'accesso al sistema.

L'utente sa se il token gli è stato rubato o è stato smarrito; il token non può essere "condiviso" con altri, costa di più, si può guastare, ma soddisfa le esigenze di sicurezza di un ampio spettro di applicazioni.

Si basa su **caratteristiche del corpo umano** e, secondariamente, anche su **comportamenti unici della persona**.

Queste caratteristiche prima includevano un ritratto, la firma, una descrizione scritta, le impronte digitali; oggi i computer permettono di confrontare rapidamente un attributo fisico (caratteristiche biometriche, firma autografa, ...) con una registrazione in un database.

Punti deboli:

- maggiore **costo**;
- possibilità di **intercettazione**;
- identificazione **non certa** (falsi positivi e falsi negativi);
- **variabilità** nel tempo;
- **trafugamento** da parte di terzi con definitiva compromissione dell'autenticazione!

Non esiste - almeno per ora - un **metodo di autenticazione perfetto**: la scelta dipende dai rischi, dai costi e da altri fattori.

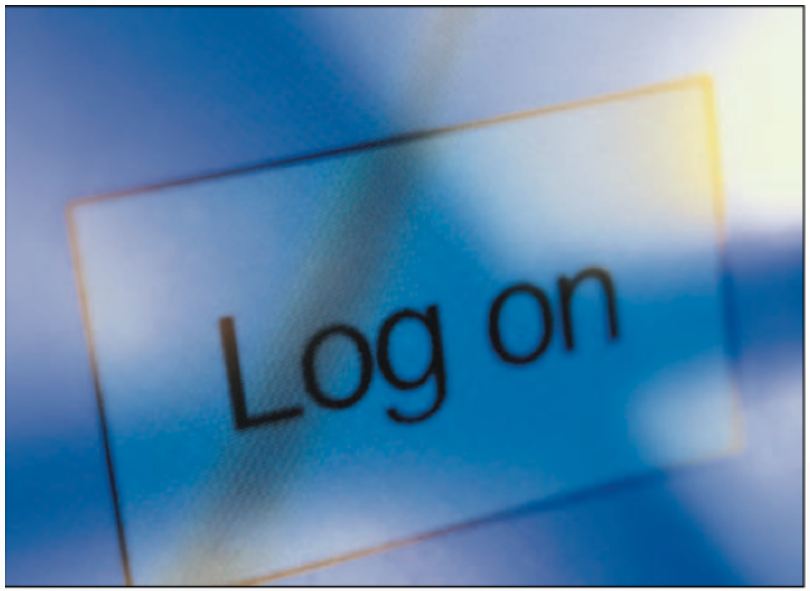
Poiché tutti i metodi presentano inconvenienti e spesso non offrono il livello di protezione richiesto, è sempre più comune utilizzare **meccanismi di protezione multipli**: essi offrono la cosiddetta autenticazione forte perché, usando più fattori, ciascuno di essi contribuisce a neutralizzare i punti deboli degli altri.

Tuttavia, quando si passa dall'autenticazione locale a quella in rete le cose si complicano.

Le tre categorie (qualcosa che sai, hai, sei) si basano su caratteristiche distintive della persona o entità, ma quando tali caratteristiche si traducono in bit che attraversano la rete nessun meccanismo può fornire la certezza assoluta che una password o una lettura biometrica siano fornite dal titolare anziché da altri.

Perciò, insieme ai fattori di autenticazione forniti dagli utenti, sono necessarie tecniche che identifichino univocamente i messaggi scambiati e impediscano agli estranei di inserirsi nel dialogo (*spoofing*).

Le password



Le password sono uno dei più antichi sistemi di autenticazione; i primi computer le conservavano in chiaro in un file.

Nel 1967 fu introdotto l'**hashing** delle password, tuttora utilizzato. Il sistema conserva in un file i nomi utente e l'hash delle relative password; durante l'autenticazione, l'hash calcolato in base alla password digitata viene confrontato con quello registrato: se coincidono, l'utente è autenticato.

Le password

Poiché dall'hash è impossibile ricostruire la password, il sistema è relativamente sicuro (a meno di attacchi *brute force* o *dictionary based*).

L'hash delle password può essere aggirato dai programmi di **keystroke sniffing**.

L'evoluzione degli attacchi ha portato al **network sniffing** (analisi del traffico di rete per carpire password, chiavi di cifratura e altre informazioni).

Un metodo usato per conquistare l'accesso ad un sistema è il **social engineering**: l'attaccante si fa aiutare da un dipendente, inconsapevole, convincendolo a rivelare le informazioni (come username e password) necessarie ad entrare nel sistema.

Social engineering

Uno dei modi più usati consiste nel presentarsi come un tecnico di assistenza, che ad es. ha urgente bisogno del nome utente e password dell'interlocutore allo scopo dichiarato di evitargli la perdita dei dati.

L'attaccante può anche ordinare, con una falsa email apparentemente inviata dal system administrator (vedi **phishing**), di cambiare provvisoriamente la password - come specificato - per lavori di manutenzione.

I) Lunghezza. Più la password è lunga, più è difficile da scoprire: la lunghezza minima è di sei caratteri o più, secondo le dimensioni del set di caratteri.

2) Caratteri. Idealmente una password dovrebbe contenere minuscole, maiuscole, cifre ed altri segni, in modo da aumentare il numero di combinazioni (a parità di lunghezza) e di eludere gli attacchi tramite dizionario.

3) Contenuto. Dovrebbero essere esclusi nomi di persone, luoghi, aziende, animali, prodotti, targhe automobilistiche, date, parole del dizionario ed altri nomi o simboli riconducibili all'utente.

4) Assegnazione. Per diversi prodotti hw/sw non è obbligatorio, ma consigliabile, specificare username e password (il 70% delle reti WiFi è ancora installata senza alcuna protezione!).

5) Periodo di validità. Più frequente è la modifica della password, minore è la probabilità di scoperta.

6) Cambiamento. Ogni password assegnata o scelta da un utente dovrebbe essere nuova e differente.

7) Valore di default. Molti dispositivi sono posti in commercio con nome utente e password preimpostati, da modificare all'atto dell'installazione.

8) Conservazione. Se una password dev'essere annotata o registrata, va conservata al sicuro (in cassaforte, cifrata adeguatamente).

9) Memorizzazione. In teoria una password dovrebbe essere lunga, complicata e memorizzata dall'utente senza lasciarne traccia: ma una password troppo lunga e complicata è meno sicura perché induce l'utente a registrarla (con pericolo di visibilità; meglio una "passphrase").

L'uso consigliato delle password varia a seconda che gli utenti siano **interni** (personale dell'azienda) o **esterni** (come i clienti che si collegano via Internet).

Password interne

Le **password interne** servono all'autenticazione dei dipendenti e di solito non forniscono un alto livello di protezione, visto che gli utenti hanno accesso fisico al sistema.

E' superfluo imporre agli utenti interni password complicate; al contrario, sono consigliabili i seguenti criteri:

1) Usare password mnemoniche (affinché non vengano scritte), ma difficili da indovinare anche per amici e colleghi.

2) Disabilitare la scadenza della password, che induce gli utenti ad annotare le password.

3) Incoraggiare gli utenti a cambiare password in occasione dei cambiamenti di configurazione del computer.

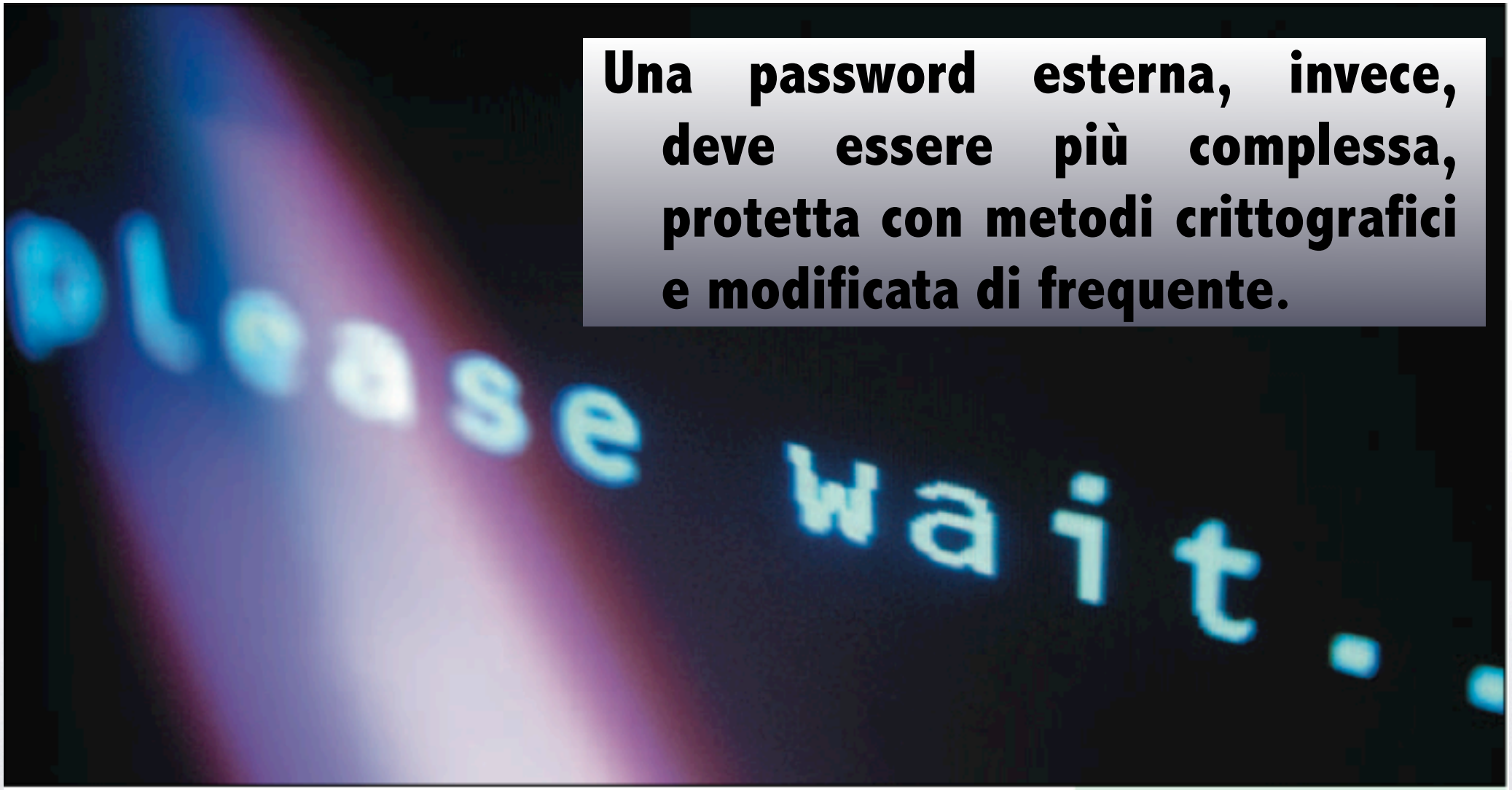
4) Tenere i server e i dispositivi di rete sotto chiave.

5) I posti di lavoro dedicati ad applicazioni critiche (come paghe e stipendi) dovrebbero essere situati in stanze separate chiuse a chiave e non restare mai incustoditi.

6) I sistemi cui si accede tramite **single sign-on** non usano password "interne", ma solo "esterne".

7) Le password degli amministratori devono essere più forti di quelle degli utenti interni.

In pratica, all'interno dell'azienda si cerca di **mediare tra usabilità e sicurezza**: *una password troppo complicata per essere usabile diventa una minaccia alla sicurezza quando è scritta su un post-it!*



Una password esterna, invece, deve essere più complessa, protetta con metodi crittografici e modificata di frequente.

In un'azienda, le **connessioni remote** dovrebbero ricevere un trattamento diverso rispetto alle connessioni interne ed essere filtrate da un dispositivo di sicurezza (*firewall, VPN*).

Ecco alcune raccomandazioni:

1) **Se il sistema gestisce informazioni di particolare valore**, anziché normali password si dovrebbero usare token con password single-use, smartcard, token USB e simili.

2) Le connessioni esterne dovrebbero usare protocolli che impediscano il rerouting (instradamento verso destinazione diversa) della connessione.

3) **Le password esterne dovrebbero resistere** agli attacchi di tipo dizionario.

4) **Le password esterne dovrebbero essere cambiate** periodicamente.

5) **Le password esterne dovrebbero essere fisicamente protette** dagli attacchi interni.

6) **Le password esterne usate su computer portatili** non devono essere conservate sul computer.

Un buon modo per scegliere una **password memorizzabile** che resista ai dizionari è il seguente:

1) **Scegliere una password a caso**, secondo i criteri visti per le password interne.

2) Scegliere una seconda password a caso, non avente alcuna relazione con la prima.

3) Scegliere a caso una cifra o segno di punteggiatura come carattere intermedio.

4) Costruire la password forte concatenando la prima password debole, il carattere intermedio e la seconda password debole.

5) Esaminare il risultato e trovare qualche modello strutturale, ritmo, ripetizioni o qualsiasi significato che permetta di memorizzarlo senza doverlo scrivere.

Ad es. "casale9ferrato" *è una password resistente, ma abbastanza facile da ricordare.*

Token (gettone): ***oggetto (della categoria "qualcosa che hai") utilizzato da un utente (o gruppo di utenti) per pagare qualcosa o per un impiego specifico.***

Ad es. i gettoni che viaggiano su una LAN Token Ring e quelli impiegati dai dispositivi di autenticazione.

Proprietà fondamentali:

1. il titolare dev'essere in **possesso fisico** del token per poterlo usare;
2. un buon token è molto **difficile da duplicare**;
3. una persona può smarrire un token e con esso **perdere l'accesso** a risorse critiche;
4. l'utente si accorge della perdita di un token facendo l'**inventario dei token** in suo possesso.

Autenticazione tramite token

Rispetto ad una password, un token offre notevoli benefici:

1. elimina l'**onere** di dover ricordare password complicate;
2. può contenere un dato segreto molto più **complesso** di quanto sia memorizzabile da una persona;
3. è spesso associato ad un **secondo fattore** di autenticazione, come ad es. un PIN;
4. un token attivo può generare un **output diverso** in diverse circostanze oppure ad ogni utilizzo.

Autenticazione tramite token

Un token può assumere i formati e le dimensioni più svariate: una carta di credito, una chiave, una calcolatrice, un anello ed altro ancora.

Da un punto di vista funzionale, la principale distinzione è tra **token passivi** (che si limitano a memorizzare i dati, come ad es. una tessera Bancomat o un dispositivo RFID) e **token attivi** (dotati di capacità di elaborazione, come ad es. una smartcard con coprocessore crittografico).

Challenge/Response

Una variante di token di autenticazione utilizza il cosiddetto **Challenge/Response**.

Al momento del login, il token riceve dal server un dato (*challenge* = sfida) e lo elabora appropriatamente, utilizzando il proprio dato segreto, per fornire la risposta (*response*) che attesta la corretta identità dell'utente.

Biometria

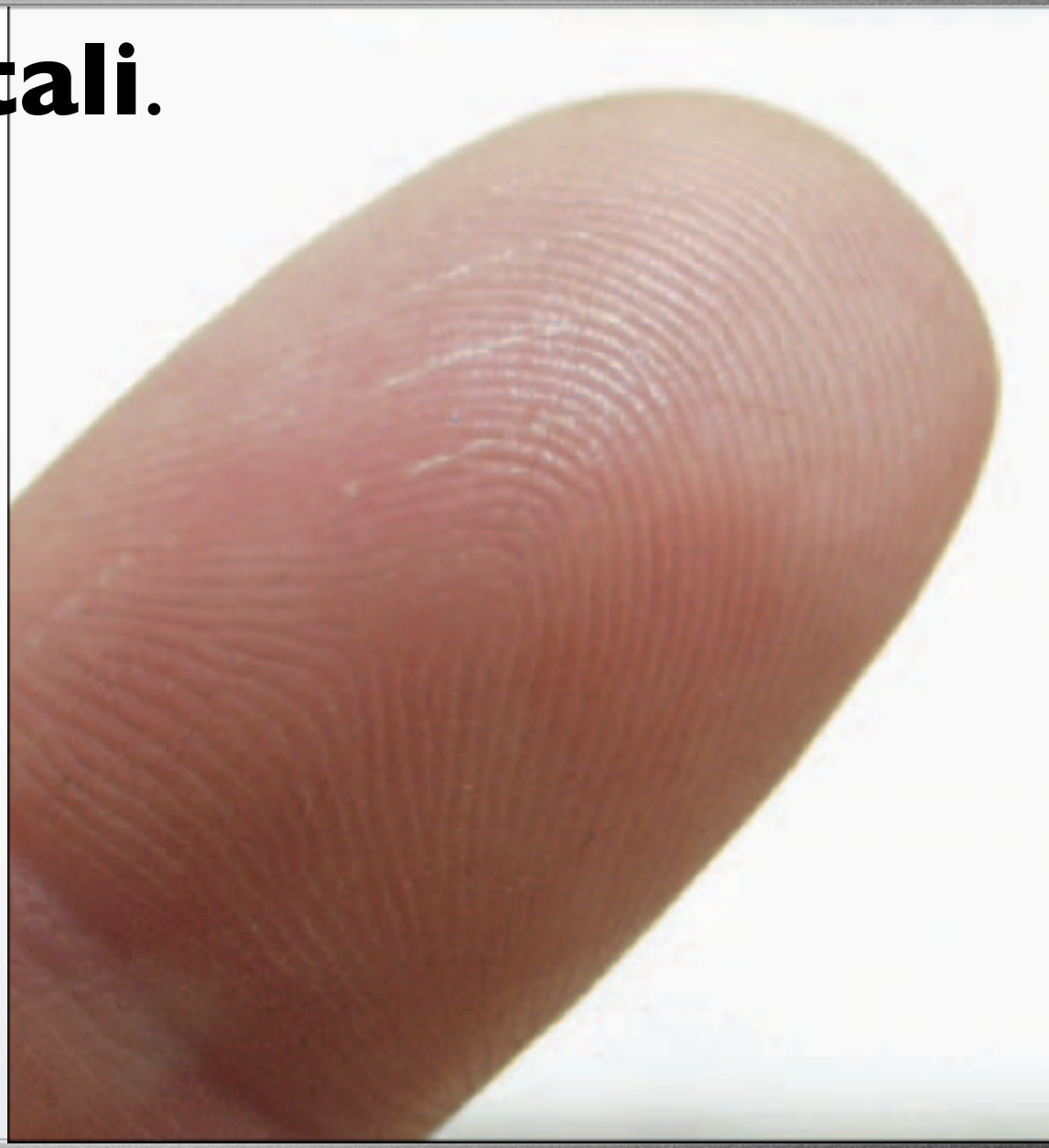
La **biometria** (*bios*=vita e *metron*=misura) è la *scienza* e *tecnologia dell'autenticazione misurando le caratteristiche fisiologiche o comportamentali di una persona.*

Le caratteristiche fisiche utilizzate per l'autenticazione biometrica sono diverse:

I) Impronte digitali.

Usate da un secolo e mezzo, mantengono la loro reputazione di unicità per ogni individuo, gemelli inclusi.

Gli scanner di impronte digitali sono molto diffusi ed hanno un basso costo, molto inferiore a quello degli altri dispositivi biometrici.



2) Geometria delle mani.

Rispetto alle impronte digitali, che richiedono mani pulite, ha il vantaggio di poter essere usata anche in condizioni ambientali difficili, come fabbriche e cantieri.

3) Retina.

La sua scansione è utilizzata in installazioni militari e governative.

Il modello dei vasi sanguigni della retina è unico e stabile, sebbene siano possibili variazioni (come durante la gravidanza).

La fotografia della retina richiede un'esposizione prolungata a bassa intensità luminosa ed è vista come una procedura intrusiva, sebbene non rechi danno agli occhi.

4) Iride.

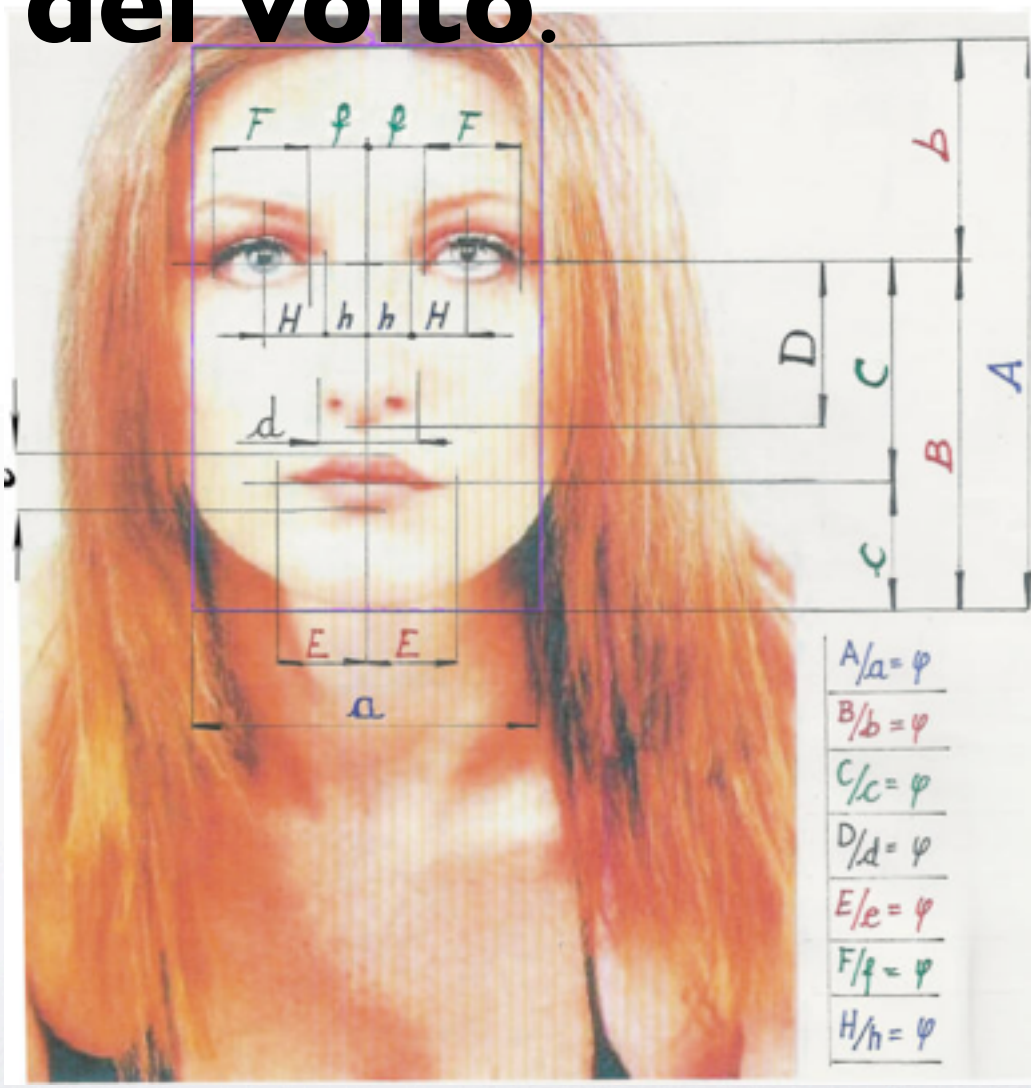
Come per la retina, la sua scansione fornisce un modello unico e stabile ed è oggi una delle tecnologie in rapida ascesa per l'adozione in aeroporti e controlli dell'immigrazione.

La foto è ripresa da una certa distanza e presenta difficoltà simili a quelle della retina.

5) Riconoscimento del volto.

E’ un metodo particolarmente flessibile e può essere utilizzato all’insaputa della persona oggetto della scansione (con i relativi pro e contro).

Può essere usato per cercare un individuo nella folla, a patto che si raggiunga la necessaria precisione di riconoscimento.



6) Impronta vocale.

Come il riconoscimento del volto, l'analisi della voce può essere usata all'insaputa dell'interessato.

E' possibile falsificarla manipolando una registrazione, ma una voce imitata non trae in inganno un analista esperto.

Questa caratteristica a volte è elencata nella categoria dei tratti comportamentali, dato che non si basa sull'osservazione di una parte del corpo.

Schemi di autenticazione biometrica

Altre caratteristiche comportamentali sono:

Firma autografa. I sistemi di riconoscimento affidabili la confrontano con una registrazione che comprende la dinamica del movimento della penna da parte dell'utente.

Dinamica della digitazione su tastiera. Esistono alcuni sistemi che riconoscono i comportamenti dell'utente durante la battitura, come il ritardo tra la pressione di varie coppie di tasti. Un vantaggio è che non occorre hardware aggiuntivo.

Schemi di autenticazione biometrica

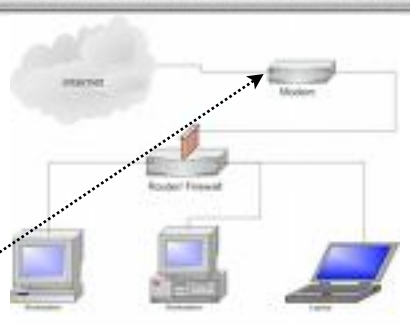
La diffusione dei dispositivi biometrici ha subito un forte impulso (ad es. dati biometrici nei passaporti) dal settembre 2001, quando è iniziato un processo di progressivo spostamento del punto di equilibrio tra **esigenze di sicurezza** e **garanzie personali** (privacy).

Oggi sono già installati in varie nazioni dispositivi biometrici per il controllo delle frontiere che sono basati sulla scansione delle impronte digitali o della retina.

Autenticazione in rete

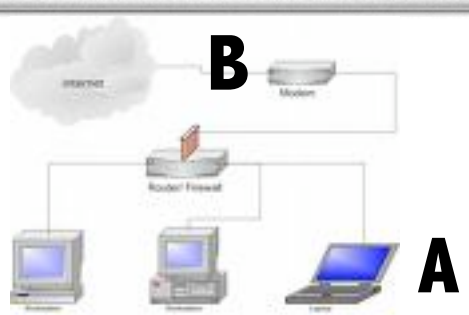
Per autenticare un soggetto (utente o processo) in un **contesto di rete** occorre trovare un compromesso fra *modalità operative* ragionevolmente semplici, un *onere amministrativo* non eccessivo (per i sistemisti) ed un *livello di sicurezza* accettabile.

Autenticazione in rete



Si consideri innanzitutto che, se l'accesso ad un sistema **B** avviene remotamente agendo da un sistema **A**, è necessario che l'utente abbia accesso (disponga cioé di username/password) su B, ma occorre anche - in generale - che disponga di un login sul sistema A da cui effettua l'accesso.

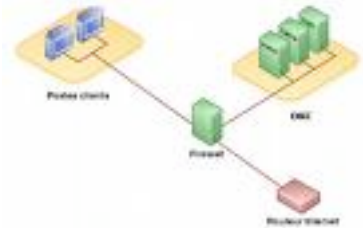
Autenticazione in rete



Per evitare che l'utente debba ricordare troppe username/password per sistemi diversi, si potrebbe decidere di adottare account uguali su A e su B.

Comunque, l'utente sarebbe costretto a ripetere la manovra di login ad ogni accesso remoto, senza contare che dovrebbe comunque cambiare più volte le stesse credenziali sui diversi sistemi.

Autenticazione in rete



In ambiente **Windows** è possibile semplificare le cose organizzando i server in un unico "dominio": con tale termine si intende un *raggruppamento logico di server di rete (domain controller) e altri host (member server) che condividono (e sincronizzano) le informazioni sui profili utente e altre impostazioni di security.*

Autenticazione in rete

Sotto **Linux** esistono diverse strategie per semplificare la gestione degli account multipli (ad es. il file **`.rhosts`** per il "trust" transitivo), tra le quali anche un'architettura basata su Kerberos, equivalente - per concezione e per tecnologia crittografica sottostante - all'approccio per dominii di Windows.

Autenticazione in rete

In ogni caso, l'autenticazione in rete avviene attraverso lo scambio di messaggi tra client e server.

Tali messaggi possono essere intercettati, esaminati, memorizzati e poi ritrasmessi (intatti o alterati) da un attaccante: è quindi assolutamente necessario prevedere un'adeguata protezione crittografica che contrasti tali tecniche.

Autenticazione in rete

Con la **protezione crittografica** è possibile fare in modo che:

(1) per qualunque terzo non autorizzato i messaggi intercettati risultino incomprensibili (riservatezza);

(2) risulti impossibile modificarli in modo da non lasciare tracce (integrità);

(3) risulti anche del tutto inutile archiviare un messaggio intercettato (pur se incomprensibile) e riproporlo invariato in seguito per ottenere una "replica" di un qualche effetto desiderato.

Protocolli per l'autenticazione utente

1. **PAP** (Password Authentication Protocol): prevede il banale invio al server di uno username (in chiaro) e di una password (eventualmente cifrata).
2. **CHAP** (Challenge Handshake Authentication Protocol*): il server invia inizialmente al client un "challenge" casuale di 8 byte (2^64 stringhe possibili). Il client lo utilizza insieme al "segreto" da trasmettere e genera un hash, che invia al server il quale lo verificherà a fronte degli stessi dati in suo possesso.

*Evoluzioni: MS-CHAP, EAP (Extensible Authentication Protocol), PEAP (Protected EAP).

Numerosi servizi di rete di larga diffusione e di grande importanza, a partire dall'NFS (Network File System) per la condivisione dei dischi in rete in ambiente Unix/Linux, si basano su un'architettura **client/server** nella quale lo scambio di messaggi tra le due parti in causa è modellato come una serie di Remote Procedure Calls (RPC).

Il protocollo RPC consente ad un programma residente su un particolare computer di mandare in esecuzione un programma residente su un server.

RPC può appoggiarsi sia su connessioni TCP (Transmission Control Protocol) che UDP (User Datagram Protocol).

Data la delicatezza e la criticità di molti dei servizi basati su RPC, l'autenticazione del richiedente riveste particolare importanza.

Per questo esistono schemi di autenticazione per RPC che fanno uso di tecniche crittografiche ("authentication flavors"), che differiscono principalmente per l'algoritmo crittografico usato, per la modalità con cui avviene lo scambio delle chiavi e per altri dettagli.

Architetture single sign-on

Quando si ha a che fare con sistemi articolati e complessi, composti da una molteplicità di host (connessi tra loro in rete) e di servizi erogati da essi, con un gran numero di utenti e la necessità di autenticarsi con ogni servizio per potervi accedere, ci si può facilmente trovare davanti a una situazione pressoché ingestibile, sia per l'utente finale (costretto a ripetere frequentemente l'operazione di login) sia per gli amministratori di sistema, alle prese con il problema di governare un elevato numero di profili per dversi host o servizi.

Architetture single sign-on

Possibili (quanto inefficaci) soluzioni vanno dalla scelta, da parte degli utenti, di login e password ovunque uguali all' utilizzo di stratagemmi come il meccanismo **.rhosts** per il riconoscimento reciproco dell'autenticazione tra host.

Architetture single sign-on

Una soluzione strutturalmente migliore prende le mosse da una strategia di gestione unificata *degli utenti, attraverso la creazione di un database unico, centralizzato, per tutti i profili (username, password e altri dati) al quale le applicazioni possano magari accedere attraverso un'interfaccia standard, specializzata nel trattamento di questo tipo di dati, come* LDAP *(Lightweight Directory Access Protocol).*

Architetture single sign-on

Il passo successivo però consiste nel congegnare le applicazioni del sistema complessivo in modo che non soltanto l'autenticazione avvenga appoggiandosi alle informazioni contenute in tale database unificato, ma che l'utente debba **autenticarsi una sola volta**, al primo accesso, e in seguito risulti automaticamente autenticato su tutte le altre risorse di rete.

Architetture single sign-on

Tale approccio complessivo all'autenticazione va sotto il nome di **Single Sign-On** (SSO) e, se da un lato offre indubbi benefici in termini di praticità d'uso per gli utenti finali (e, di conseguenza, un aumento di produttività), ha anche effetti positivi sulla sicurezza del sistema, in quanto è evidente che non dovendo più ricordare numerose password l'utente è meno portato a tenerne traccia scritta in luoghi magari poco protetti.

Architetture single sign-on

Inoltre la gestione dei profili risulta **centralizzata** e quindi non solo più **semplice**, ma anche più **sicura** (diminuisce il rischio di dimenticare gli account attivi o le password obsolete, magari già compromesse).

Naturalmente la difficoltà di realizzare un'architettura SSO per l'autenticazione è proporzionale all'eterogeneità del sistema.

Architetture single sign-on

Quando l'ambiente complessivo è omogeneo, la soluzione può essere addirittura già disponibile "gratis", come avviene con il modello Microsoft.

Esso prevede anzitutto un server LDAP(*) come deposito centrale delle informazioni di profilo. Si distinguono poi quattro tipi di logon, pensati per altrettanti modelli di comportamento e di accesso a risorse di rete...

(*) RFC 2251 (LDAP): http://www.faqs.org/rfcs/rfc2251.html

Architetture single sign-on

login interattivo (accesso fisico diretto, anche via Terminal Services);

login di rete (tramite il protocollo Kerberos per l'utilizzo da remoto, in modalità Client/Server, di qualche risorsa o servizio);

login per servizi (che i servizi Win32 effettuano sul nodo locale per poter entrare in attività);

login batch (usato per l'esecuzione di job batch, magari in background).


Aspetti pratici

Politica della sicurezza

Utilizzo della password

La password deve essere:

DI MEDIA LUNGHEZZA

NON PREVEDIBILE

CAMBIATA DI FREQUENTE

PROTETTA

La crittografia

Sistema di cifratura

Algoritmo

Codice segreto

Archiviazione

Trasmissione

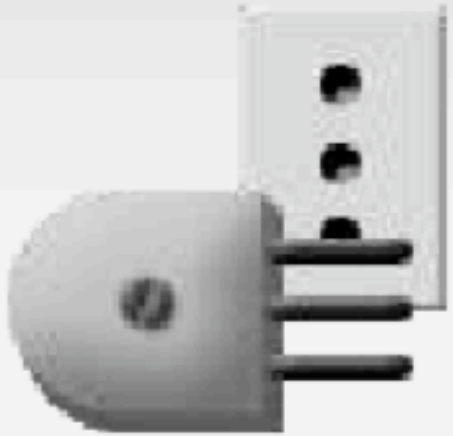
Rischio di perdita dei dati

Icona SALVA

Copie di BACKUP

FLOPPY | CD | ZIP | DATA CARTRIDGE

Garanzia di funzionamento



Gruppo di continuità

Continuità di alimentazione elettrica

Stabilizzatore di tensione

Eliminazione di eventuali sbalzi di tensione che possono compromettere il corretto funzionamento del computer

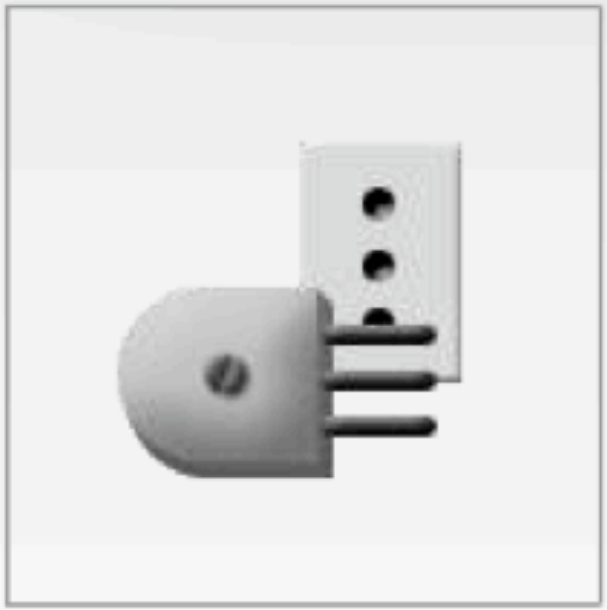
Portatile

Personal Digital Assistant

Telefono cellulare

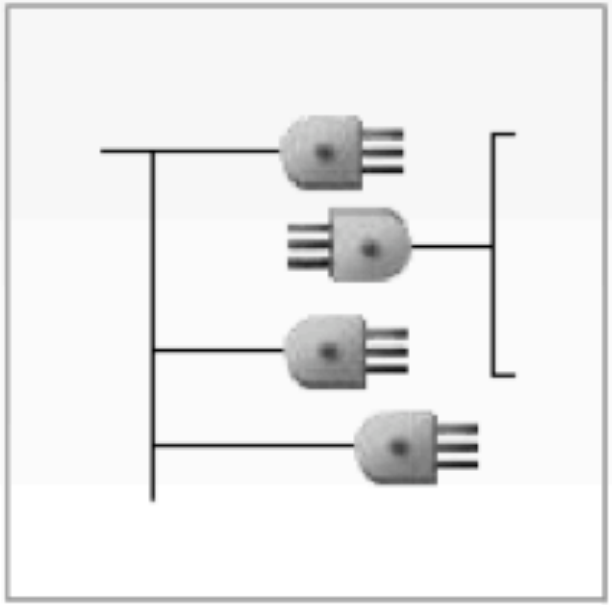
Protezione contro

Smarrimento Furto	Password - Crittografia Conservazione dei dati sensibili su supporti separati



Buono stato delle prese e delle spine elettriche

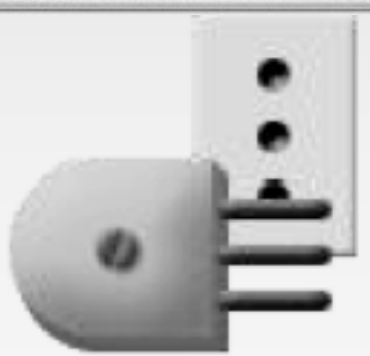
Corretta distribuzione dei collegamenti



Sicurezza del posto di lavoro

Apparecchiature lontane da fonti di calore

Apparecchiature lontane da acqua e umidità



Consumi energetici

circuiti a basso consumo

autospegnimento dello schermo

stato di attesa per la stampante

Impatto ambientale

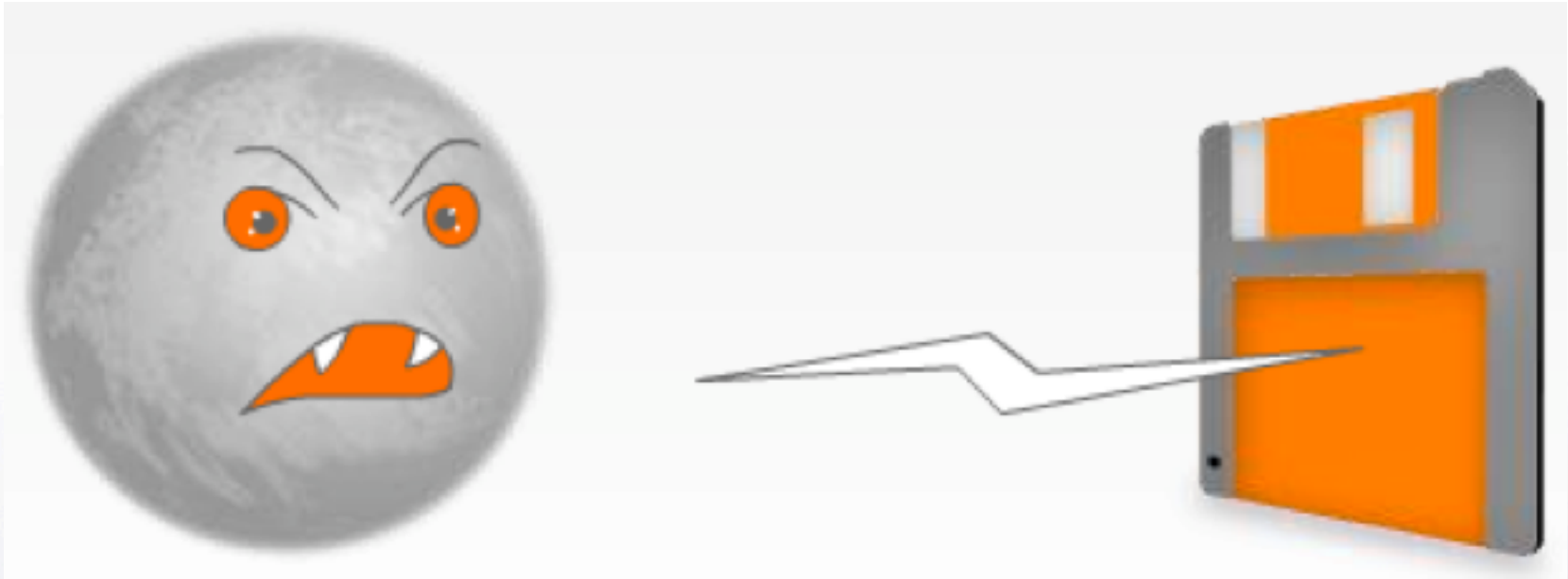
Materiali di scarto

materiali riciclabili

cartucce d'inchiostro e toner ricaricabili

documentazione elettronica

I virus

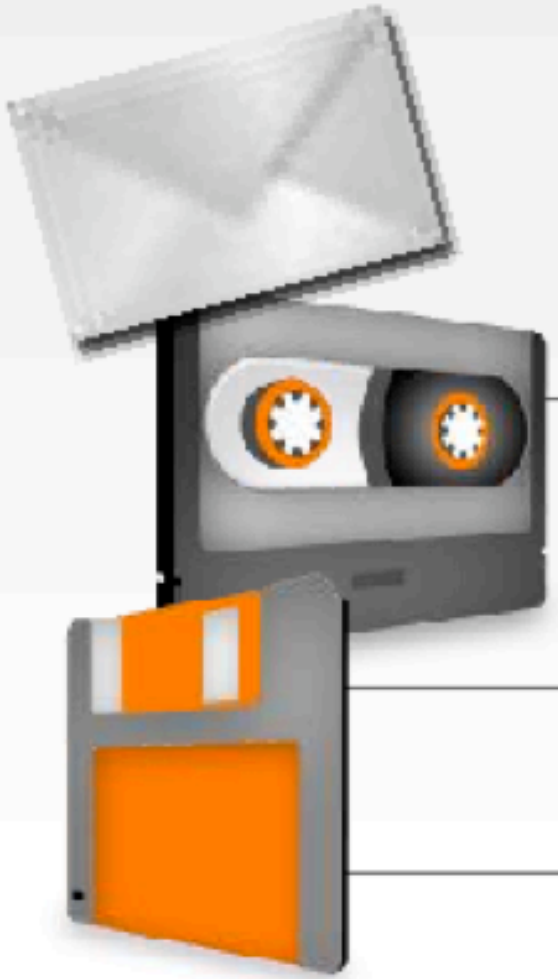


I virus

PROGRAMMI INSERITI IN UN COMPUTER CHE PROVOCANO SERI DANNI, TEMPORANEI O PERMANENTI:

- danneggiamento o cancellazione di archivi
- danneggiamento o cancellazione di programmi, incluso il sistema operativo
- effetti grafici indesiderati sullo schermo
- rallentamento del funzionamento del computer
- segnalazione di errori e guasti inesistenti

Trasmissione dei virus



Input di dati da memorie di massa mobili (floppy, CD, zip, data cartridge…)

Importazione di archivi o programmi via rete

Messaggi di posta elettronica

ATTIVAZIONE DEL VIRUS

- Immediata
- A data fissata
- All'esecuzione di un comando

RIPRODUZIONE DEL VIRUS

- Automatica

Tipi di virus

- File virus
- Boot virus
- Macrovirus
- Network virus

Tipi di virus

- Cavalli di Troia
- Worms

Gli antivirus

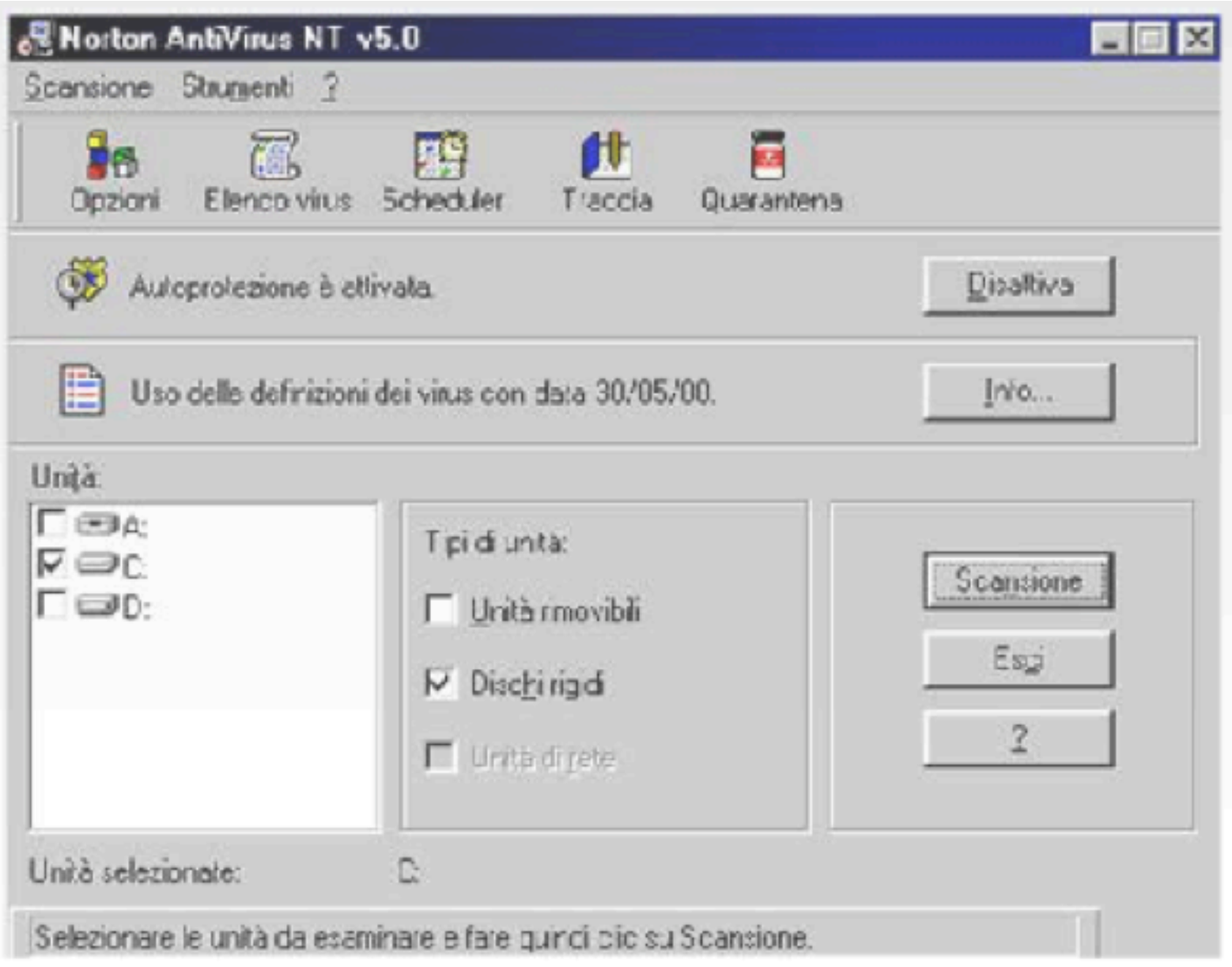
PROGRAMMA IN GRADO DI RICONOSCERE UN VIRUS E DI ELIMINARLO

Prevenzione

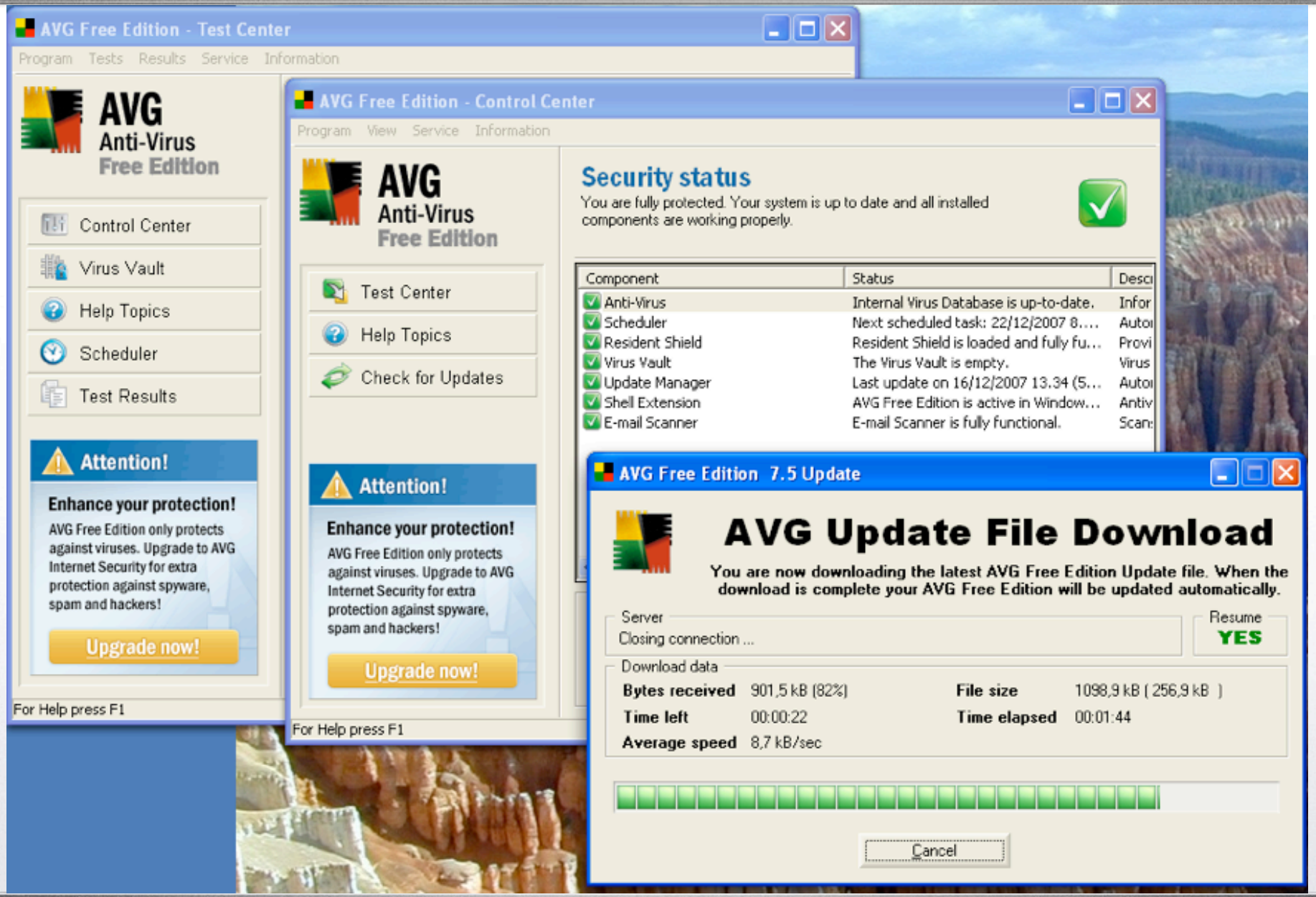
Cura

Aggiornamento

Gli antivirus



Gli antivirus



Protezione dai virus

Controllo periodico del sistema mediante antivirus

Controllo con l'antivirus di:

- dischi mobili
- allegati alla posta elettronica
- file scaricati da Internet

Aggiornamento frequente dell'antivirus

Non eseguire programmi di provenienza non nota

Disattivare l'esecuzione delle macro non note


Gestione del rischio

Obiettivo

Conoscere i principali elementi coinvolti nella valutazione del rischio:

- **beni** da difendere;
- **obiettivi** di sicurezza;
- **minacce** alla sicurezza;
- **vulnerabilità** dei sistemi informatici;
- **impatto** causato dall'attuazione delle minacce.

Beni

Un bene è qualsiasi cosa, materiale o immateriale, che abbia un valore e debba quindi essere protetta.

Gestione del rischio

Nel campo della sicurezza delle informazioni, tra i beni di un'azienda ci sono le risorse informatiche, il personale (utenti, amministratori, addetti alla manutenzione), le informazioni, la documentazione e l'immagine aziendale.

Per un individuo, i beni comprendono non solo risorse informatiche, informazioni e mezzi di comunicazione, ma anche le informazioni personali e la privacy.

Beni

Per esempio, se un attacco via Internet causa a un'azienda il furto di informazioni riservate, magari relative alle carte di credito dei clienti, i beni colpiti sono molteplici: le informazioni, l'immagine, la reputazione, la stessa continuità operativa.

Beni

Un altro esempio è il **defacing**, ovvero l'alterazione di un sito web per rovinare l'immagine del proprietario; è una forma di vandalismo che colpisce sia le informazioni sia l'immagine dell'azienda o persona titolare.

Beni

A livello personale, la privacy degli individui è minacciata da più parti: aziende che non proteggono adeguatamente le informazioni in loro possesso, applicazioni che trasmettono via Internet dati personali, software maligno che spia le abitudini degli utenti (acquisti, navigazione Internet etc.) o che altera la navigazione Internet a scopo di truffa o furto di informazioni.

Beni

I beni possono essere distinti in:

- **beni primari**, quelli che hanno valore effettivo;
- **beni secondari**, che servono per proteggere i beni primari.

Un esempio di bene secondario è la password che permette di accedere a un computer, a una rete, ai dati archiviati e a Internet.

Beni

La password in sé non ha alcun valore, ma è un'informazione che permette a un altro utente o a un estraneo di accedere ai beni primari (sistemi, periferiche, reti, archivi) e di eseguire operazioni a nome dell'utente titolare della password, che ne sarà ritenuto responsabile.

La password, bene secondario, assume un'importanza paragonabile a quella degli archivi e delle attrezzature hardware/software, bene primario a cui la password dà accesso.

Beni

Lo stesso vale per i dispositivi di identificazione e autenticazione, come le Smart Card.

Se la scheda viene utilizzata da qualcuno che si è procurato il corrispondente PIN (Personal Identification Number), il titolare della scheda sarà ritenuto responsabile dell'utilizzo fino alla denuncia di furto o smarrimento.

Beni

Altri esempi di beni secondari sono le attrezzature che permettono all'hardware di funzionare con continuità e sicurezza: gruppi di continuità, condizionatori, alimentatori e altri componenti ridondanti e così via.

I beni secondari, in quanto investimento preventivo per mantenere alta la disponibilità dei servizi informatici, rappresentano un costo ampiamente inferiore rispetto al rimedio a situazioni non previste.

Obiettivi

Gli obiettivi di sicurezza sono il grado di protezione che si intende predisporre per i beni, in termini di ***disponibilità***, ***integrità*** *e* ***riservatezza***.

Per definire gli obiettivi, si classificano i beni in categorie e si assegnano i criteri di sicurezza da applicare.

Obiettivi

Ci sono beni, come le password e i numeri di identificazione, che hanno più requisiti di riservatezza che non problemi di integrità e disponibilità.

Al contrario, le informazioni contabili di una banca che esegue transazioni on line hanno requisiti di disponibilità, integrità e riservatezza.

Le informazioni pubblicate sul sito web di un'azienda richiedono disponibilità e integrità (per esempio per impedire il defacing), ma non certo riservatezza.

Obiettivi

La selezione degli obiettivi in base al tipo di protezione richiesto dai beni, permette un approccio concreto e scalabile in base alle priorità e alle risorse disponibili.

In assenza di una mappa di ciò che è urgente e importante da proteggere, si tende a improvvisare o a voler proteggere tutto, salvo poi mancare anche gli obiettivi minimi quando il costo preventivato supera di gran lunga le disponibilità.

Minacce

Una minaccia è un'azione potenziale, accidentale o deliberata, che può portare alla violazione di uno o più obiettivi di sicurezza.

Minacce

Le minacce possono essere classificate secondo la loro origine: naturale, ambientale o umana.

Per esempio, un allagamento dovuto a forti piogge è una minaccia accidentale di origine naturale che ha un impatto sulla sicurezza, visto che può interrompere la disponibilità dei servizi informatici.

Minacce

Un cavallo di Troia installato all'apertura di un allegato di posta elettronica infetto, è una minaccia deliberata di origine umana e coinvolge tutti gli obiettivi di sicurezza: il computer può cadere sotto il controllo esterno e non essere più completamente disponibile per il suo proprietario (**disponibilità**), le sue informazioni possono essere alterate e cancellate (**integrità**) e dati da non divulgare (password, informazioni personali, informazioni sensibili aziendali) possono essere letti da estranei (**riservatezza**).

Minacce

Una rete wireless che opera senza protezione (a partire dalla cifratura delle comunicazioni) può essere intercettata o, perlomeno, usata per l'accesso a Internet, magari per operazioni illegali riconducibili all'indirizzo IP (e quindi alla responsabilità) del titolare della rete.

In questo caso gli obiettivi violati coinvolgono la riservatezza, la disponibilità e potenzialmente anche l'integrità.

Minacce

L'entità che mette in atto la minaccia viene chiamata **agente**.

Esempi di agenti di minaccia sono un intruso che entra in rete attraverso una porta del firewall, un processo che accede ai dati violando le regole di sicurezza, un tornado che spazza via il centro di calcolo o un utente che inavvertitamente permette ad altri di vedere le password.

Esempi di minacce

(**D** = deliberata, **A** = accidentale, **E** = ambientale)

Minaccia	D	A
Terremoto		
Inondazione		x
Uragano		
Fulmine		
Bombardamento	x	x
Incendio	x	x
Uso di armi	x	x
Vandalismo	x	
Furto	x	
Blackout		x
Linea elettrica instabile		x
Guasto climatizzatore		x
Temperatura alta o bassa	x	x
Umidità eccessiva	x	x
Polvere		
Radiazioni elettromagnetiche		
Guasto hardware		x
Uso improprio delle risorse		x	x
Errori software	x	x
Uso non autorizzato supporti di memoria		x
Deterioramento supporti di memoria			x
Errori degli utenti	x	x
Errori del personale operativo		x	x
Errori di manutenzione	x	x
Accesso illegale alla rete	x	
Uso illegale di password	x	
Uso illegale del software	x	
Indirizzamento illecito messaggi	x	
Software dannoso	x	x
Installazione/copia illegale di software	x	
Interruzione servizio provider Internet		x
Interruzione servizio hosting web		x
Errori di trasmissione			x
Traffico eccessivo	x	x
Intercettazione in rete		x
Infiltrazione in rete	x	
Analisi illecita del traffico	x	
Carenze di personale			x

Vulnerabilità

Mentre una minaccia è sempre portata da un agente esterno (fenomeno naturale o intervento umano), una vulnerabilità è un punto debole del sistema informatico (hardware, software e procedure) che, se colpito o sfruttato da una minaccia, porta alla violazione di qualche obiettivo di sicurezza.

Una vulnerabilità presenta due caratteristiche: è un aspetto intrinseco del sistema informatico ed esiste indipendentemente da fattori esterni.

Vulnerabilità

Una vulnerabilità, di per sé, non causa automaticamente una perdita di sicurezza; è la combinazione tra vulnerabilità e minaccia che determina la probabilità che vengano violati gli obiettivi di sicurezza.

Vulnerabilità

Un centro di calcolo situato nel seminterrato di un centro urbano ha le stesse vulnerabilità in una zona poco soggetta a terremoti come in una zona sismica: quello che cambia è la probabilità che si attui la minaccia terremoto, a scapito della disponibilità dell'impianto.

Vulnerabilità

Un computer dedicato alla contabilità di un negozio, non protetto da firewall e antivirus e privo delle patch di sicurezza del sistema operativo, è assai vulnerabile, ma se è tenuto al sicuro, viene usato solo dal titolare e non è collegato a Internet, può funzionare a lungo senza essere colpito dalle minacce più comuni.

Esempi di vulnerabilità

Infrastruttura
Mancanza di protezione fisica
Mancanza di controllo degli accessi
Linea elettrica instabile
Locali soggetti ad allagamento

Hardware e impianti
Mancanza di sistemi di backup
Suscettibilità a variazioni di tensione
Suscettibilità a variazioni di temperatura
Suscettibilità a radiazioni elettromagnetiche
Programma di manutenzione insufficiente

Comunicazioni
Linee di comunicazione non protette
Uso di password in chiaro
Traffico wireless non cifrato
Presenza di linee dial-up
Libero accesso ai dispositivi di rete

Documentazione
Locali non protetti
Carenza di precauzioni nell'eliminazione
Assenza di controllo nella duplicazione

Software
Complessità interfaccia applicazioni
Mancanza autenticazione utente
Mancanza logging accessi
Errori software noti
Password non protette
Cattiva gestione password
Diritti di accesso scorretti
Uso del software incontrollato
Sessioni aperte senza presenza utente
Assenza di backup
Carenza nella dismissione dei supporti

Personale
Personale insufficiente
Procedure reclutamento inadeguate
Personale esterno incontrollato
Addestramento di sicurezza inadeguato
Uso improprio o scorretto hardware/software
Carenza di monitoraggio

Impatto

L'impatto è la conseguenza dell'attuazione di una minaccia. Esso dipende dal valore del bene colpito e dagli obiettivi di sicurezza violati.

Impatto

Per una piccola azienda, se la minaccia "guasto dell'hard disk" colpisce la vulnerabilità "backup poco frequenti", l'impatto è serio, perché può includere il blocco temporaneo dell'attività e inconvenienti nei rapporti con i clienti.

Gli obiettivi di sicurezza violati sono la disponibilità ed eventualmente l'integrità delle informazioni.

Impatto

Se un dirigente in viaggio connette il portatile a Internet senza protezione (programmi firewall e antivirus), apre un'e-mail infetta e di ritorno propaga l'infezione alla rete aziendale, l'impatto può essere grave e coinvolgere tutti gli obiettivi di sicurezza (disponibilità, integrità e riservatezza).

Impatto

In questo esempio l'agente della minaccia è l'utente, le vulnerabilità sono la cattiva configurazione del portatile e le falle di sicurezza di Windows e la minaccia sta nelle cattive abitudini e incompetenza dell'utente.

L'impatto può includere il blocco temporaneo della rete e dei computer e un'attività generalizzata di disinfestazione con possibile perdita di dati e reinstallazione di software; anche parte dei backup potrebbe essere compromessa.

Rischio

Concettualmente, il rischio è la possibilità che si verifichi un evento dannoso ed è tanto maggiore quanto è forte l'impatto causato dall'evento e quanto è alta la probabilità che esso si verifichi.

Rischio

In una zona statisticamente non soggetta ad alluvioni, il rischio informatico connesso a questo tipo di eventi è trascurabile, anche se l'impatto potenziale è ingente.

In una rete aziendale soggetta a tentativi di intrusione, a parità di protezione, la sottorete delle finanze corre un rischio maggiore rispetto alla sottorete amminstrativa, perché a parità di probabilità di attacco, l'impatto dell'attacco è più grave.

Rischio

In termini numerici, il rischio **R** può essere definito come il prodotto scalare tra la gravità **G** dell'impatto (conseguenze di un evento dannoso) e la probabilità **P** che si verifichi l'evento dannoso (la minaccia):

$$R = G \times P$$

Nella gestione del rischio si possono individuare due fasi distinte.

1) Analisi del rischio. *In questa fase si classificano le informazioni e le risorse soggette a minacce e vulnerabilità e si identifica il livello di rischio associato a ogni minaccia.*

Analisi del rischio

L'analisi del rischio è un processo composto di una sequenza di fasi, che inizia con la **classificazione dei beni** (informazioni e risorse informatiche), prosegue con l'**identificazione delle minacce e delle vulnerabilità** e si conclude con l'**identificazione del livello di rischio**.

Analisi del rischio

Ci sono vari metodi per quantificare il rischio, basati su un approccio quantitativo, qualitativo o combinazione dei due.

L'**approccio quantitativo** è basato su dati empirici e statistiche, mentre quello **qualitativo** si affida a valutazioni intuitive. Entrambi hanno vantaggi e svantaggi.

Il primo richiede calcoli più complessi ma può basarsi su sistemi di misura indipendenti e oggettivi, fornisce risultati numerici (il valore delle perdite potenziali) e un'analisi dei costi e benefici.

Il secondo utilizza l'opinione del personale che ha esperienza diretta in ciascuna delle aree interessate.

2) Controllo del rischio. *In questa fase vengono individuate le modalità che l'azienda intende adottare per ridurre i rischi associati alla perdita della disponibilità di informazioni e risorse informatiche e della integrità e riservatezza di dati e informazioni.*

Controllo del rischio

*Ogni **tipo di minaccia** deve essere trattata separatamente e la **pianificazione delle contromisure** richiede un'analisi di costi e benefici che ottimizzi il valore della protezione.*

Se, per esempio, il rischio per l'intrusione in un server web è stimato di 12.000 euro in un anno e con una spesa annua di 1.000 euro esso scende a 3.000 euro, possiamo calcolare il valore della protezione in 12.000 (rischio iniziale) – 3.000 (rischio dopo l'allestimento delle contromisure) – 1.000 (costo annuale delle contromisure) = 8.000 euro.

Contromisure

*Le **contromisure** di sicurezza sono le realizzazioni e le azioni volte ad annullare o limitare le vulnerabilità e a contrastare le minacce.*

Una parte delle contromisure viene solitamente realizzata nel corso della progettazione di un sistema o di un prodotto. Le altre contromisure vengono adottate in fase di utilizzo del sistema o prodotto.

Contromisure

La **scelta delle contromisure** da mettere in campo è dettata dall'analisi del rischio e dall'analisi costo/benefici delle contromisure.

Considerato un bene, il suo valore e il danno potenziale in base alle vulnerabilità e alle probabilità di attuazione di una minaccia, l'**effetto** di una contromisura si misura con la **riduzione del rischio**.

Contromisure

Se la riduzione del rischio è ampiamente superiore al costo della contromisura, questa è **efficace**.

Se un certo rischio è di scarsa entità e la contromisura risulterebbe più costosa rispetto ai benefici, si può decidere di **accettare il rischio** senza alcuna contromisura.

Contromisure

Lo stesso dicasi nei casi in cui il **rischio residuo** (il rischio che rimane dopo l'adozione delle contromisure) non fosse significativamente inferiore al rischio iniziale.

In pratica, la scelta e adozione delle contromisure è dettata sia dagli **obiettivi di sicurezza** (e relative priorità di urgenza e importanza) sia dal **buon senso economico**.

Contromisure

Si possono classificare le contromisure in tre categorie:

- **di carattere fisico** (generalmente legate alla prevenzione e al controllo dell'accesso a installazioni, locali, attrezzature, mezzi di comunicazione);
- **di tipo procedurale** (definiscono passo per passo le operazioni per eseguire un certo compito oppure regolano il comportamento degli utenti per gli aspetti che riguardano la sicurezza delle informazioni e delle risorse);
- **di tipo tecnico informatico** (realizzate attraverso mezzi hardware, firmware e software e prendono anche il nome di **funzioni di sicurezza**).

Contromisure di tipo tecnico informatico

Le contromisure di tipo tecnico informatico si possono classificare nelle categorie seguenti:

- **identificazione e autenticazione**;
- **controllo degli accessi**;
- **rendicontabilità** (**accountability**);
- **verifica** (**audit**);
- **riutilizzo degli oggetti**;
- **accuratezza**;
- **affidabilità del servizio**;
- **scambio dati sicuro**.

Contromisure di tipo tecnico informatico

Identificazione e autenticazione. *Le funzioni di questa categoria servono a identificare un individuo o un processo e ad autenticarne l'identità.*

L'esempio più comune è la funzione di accesso (login) a un sistema tramite nome utente (per l'identificazione) e password (per l'autenticazione dell'identità). L'autenticazione viene usata anche nelle comunicazioni tra processi e nei protocolli di comunicazione per accertare l'identità del processo o dell'utente associato al processo.

Contromisure di tipo tecnico informatico

Controllo degli accessi. *In questa categoria troviamo le funzioni di sicurezza che verificano se il processo o l'utente, di cui è stata autenticata l'identità, ha il diritto di accedere alla risorsa richiesta (per esempio file, directory, stampanti) e di eseguire l'operazione specificata (per esempio lettura, esecuzione, modifica, creazione, cancellazione).*

Per i processi, anche l'accesso alla memoria è regolamentato, in modo che un processo non possa leggere i dati di un altro processo o, in certi casi, non possa eseguire istruzioni contenute in aree destinate esclusivamente a dati. Analoghe funzioni sono svolte a livello hardware dalla CPU nella sua gestione delle pagine di memoria.

Contromisure di tipo tecnico informatico

Rendicontabilità (accountability). *A questa categoria appartengono le funzioni che permettono di attribuire la responsabilità degli eventi agli individui che li hanno causati.*

L'accountability richiede l'attuazione delle misure d'identificazione e autenticazione degli utenti e l'associazione a ogni processo dell'identità del suo proprietario, come avviene nei moderni sistemi operativi.

Contromisure di tipo tecnico informatico

Verifica (audit). *A questa categoria appartengono le funzioni che registrano gli eventi in un file di logging, con informazioni riguardo a errori e a violazioni di sicurezza.* Grazie a queste registrazioni, è possibile risalire a ciò che è accaduto e prendere provvedimenti.

Contromisure di tipo tecnico informatico

Verifica (audit).

Nel caso di **segnalazione di malfunzionamenti** hardware o di errori software, si possono intraprendere azioni di diagnosi e manutenzione (per esempio la verifica e correzione del file system).

Nel caso di **eventi che riguardano la sicurezza**, il log permette di scoprire irregolarità, come tentativi di accesso illeciti e tentativi di intrusione.

Esempi di **funzioni di logging** sono quelle di Windows, che registra log degli eventi di sistema, applicativi e di sicurezza oppure il demone syslogd dei sistemi Unix/Linux.

Contromisure di tipo tecnico informatico

Verifica (audit).

Nel caso dei **firewall**, il log comprende la registrazione selettiva degli eventi che si desidera tenere sotto controllo: tutti, se non non attiva nessun filtro, oppure solo quelli che superano un certo livello di gravità.

Solitamente i firewall offrono l'opzione di logging remoto che consiste nell'inviare la segnalazione degli eventi a un computer, in modo da poter tenere registrazioni anche voluminose (su lunghi periodi di tempo) e poterle analizzare più facilmente.

Contromisure di tipo tecnico informatico

Riutilizzo degli oggetti. *Questa categoria comprende le funzioni che permettono di riutilizzare oggetti contenenti informazioni riservate: supporti magnetici, supporti ottici riscrivibili, aree di memoria RAM, zone di memoria dei processori (registri, cache, etc.), buffer di periferiche e simili.*

Lo scopo è quello di evitare che informazioni riservate siano lasciate a disposizione di programmi e utenti dopo il loro regolare utilizzo. Le contromisure in questa area hanno il compito di cancellare le aree di memoria e di disco subito dopo il loro utilizzo per il transito di informazioni riservate.

Contromisure di tipo tecnico informatico

Riutilizzo degli oggetti.

Un esempio riguarda le aree di memoria dove transitano le password o altre informazioni in chiaro prima della loro cifratura: buffer, registri e aree di lavoro dovrebbero essere cancellate per evitare che siano lette da altri processi autorizzati ad accedere a quelle aree ma associati a utenti non autorizzati alla conoscenza di quelle informazioni.

Un altro esempio è offerto dalle aree di scambio su disco, come i file di swapping o paging del sistema operativo.

È utile attivare l'opzione di **cancellazione automatica** di questi file alla chiusura del sistema, in modo che utenti non autorizzati non possano esaminarlo a caccia di informazioni riservate.

Contromisure di tipo tecnico informatico

Accuratezza. *Fanno parte di questa categoria tutte le funzioni intese a garantire l'accuratezza delle informazioni.*

Per esempio, perché i file di logging forniscano informazioni attendibili, la registrazione temporale (time stamp) dell'evento deve essere precisa. Questo accade se l'orologio interno è sincronizzato periodicamente con un time server di riferimento.

Contromisure di tipo tecnico informatico

Accuratezza.

Sistemi operativi, switch, firewall e altri dispositivi offrono questa funzionalità, che se necessario va attivata specificando il nome del time server (per esempio **time.nist.gov**).

In campo software, esempi di funzioni a difesa dell'accuratezza delle informazioni sono le funzioni che controllano i limiti di occupazione di buffer e array e quelle che validano la correttezza dei dati immessi dagli utenti.

Contromisure di tipo tecnico informatico

Affidabilità del servizio.

Questa è una vasta categoria di contromisure, perché sono diverse le aree che potrebbero compromettere l'affidabilità dei servizi informatici.

Contromisure di tipo tecnico informatico

Affidabilità del servizio.

Si inizia dalle contromisure per mantenere condizioni di alimentazione elettrica stabile, filtrata e senza interruzione (gruppi di continuità), per passare alle difese dai malfunzionamenti hardware (monitoraggio e manutenzione preventiva) e software (monitoraggio degli errori nei file di logging, aggiornamenti, monitoraggio delle prestazioni, rollback delle transazioni non andate a buon fine, ripristino di uno stato precedente del sistema operativo, ripristino delle partizioni di disco a uno stato integro precedente).

Altre contromisure possono essere sviluppate per difendere sistemi e applicazioni dagli errori degli utenti.

Contromisure di tipo tecnico informatico

Scambio dati sicuro. *In questa categoria ci sono le funzioni destinate a garantire la sicurezza delle trasmissioni.*

Il modello OSI Security Architecture (ISO 7498-2) le classifica nelle seguenti sottoclassi:

- autenticazione;
- controllo dell'accesso;
- riservatezza;
- integrità (dell'hardware, dei dati e dei flussi di pacchetti trasmessi sia in modo connectionless, come UDP, sia connection-oriented, come TCP, anche ai fini della corretta sequenza dei pacchetti);
- non ripudio.

Contromisure di tipo tecnico informatico

Scambio dati sicuro.

Esempi di contromisure in questa area sono l'uso di crittografia a chiave simmetrica e asimmetrica (chiave pubblica più chiave privata) e l'autenticazione tramite Message Authentication Code (il risultato dell'hashing applicato al messaggio più una chiave segreta simmetrica; vengono trasmessi messaggio e MAC; a destinazione il MAC viene ricalcolato sul messaggio più chiave simmetrica e confrontato col MAC ricevuto, così da verificare l'integrità del messaggio e l'autenticazione del mittente).

Funzionalità e garanzia

La sicurezza delle informazioni è caratterizzata da due fattori di base indipendenti: la funzionalità e la garanzia (assurance).

Il termine **funzionalità**, applicato alla sicurezza, conserva il significato generale che ha in altri settori; *è l'insieme di ciò che un prodotto o un sistema informatico fornisce in relazione alla protezione delle informazioni e, di riflesso, delle risorse e dei servizi informatici.*

Il panorama di contromisure descritto in precedenza comprende gran parte delle funzionalità di sicurezza che potrebbero essere necessarie.

Funzionalità e garanzia

Il concetto di **garanzia** è stato introdotto da chi si occupa di sicurezza per esprimere il *grado in cui l'implementazione di una funzionalità riduce una vulnerabilità o la possibilità di attuazione di una minaccia.*

Se la funzionalità rappresenta un elemento di protezione, la garanzia ne indica la validità.

Garanzia

Garanzia. *La garanzia è costituita a sua volta da due aspetti distinti: la correttezza e l'efficacia.*

La **correttezza** è un attributo intrinseco di un prodotto (o componente o procedura), che *riflette il grado di corrispondenza tra le effettive funzioni svolte dal prodotto e le sue specifiche.*

Per esempio, un prodotto capace di riconoscere il 99% delle voci umane adulte con almeno 30 dB di rapporto segnale/rumore, riceverebbe un'alta valutazione di correttezza rispetto alla funzione "riconoscere la voce degli utenti".

L'**efficacia** è invece una proprietà che *mette in relazione la contromisura* (prodotto, procedura o altro) *con il contesto in cui è utilizzata*, in particolare le vulnerabilità, la gravità e la probabilità di attuazione delle minacce, le caratteristiche degli agenti che attuano le minacce, l'importanza del bene da proteggere e così via.

Efficacia.

Per esempio, un sistema di riconoscimento vocale potrebbe risultare adatto per ambienti con livello medio di rischio, ma essere inadeguato a fronte di un rischio elevato e di una minaccia agguerrita.

Potrebbe risultare più efficace un sistema basato su domande a cui solo il legittimo utente possa rispondere o su un dispositivo fisico (tipo smart card) interattivo, da aggiornare ogni giorno per rimanere valido (in modo da perdere validità in caso di furto o manipolazione).

Efficacia.

Un altro esempio ci viene offerto dalle contromisure di natura fisica per impedire l'accesso alle persone non autorizzate.

Le contromisure per il controllo dell'accesso possono limitarsi a una porta blindata o includere sistemi di rilevamento del movimento, telecamere e registratore video, sistemi di allarme con chiamata di numeri telefonici e altri deterrenti per impedire e/o scoraggiare il tentativo di effrazione.

Efficacia.

In fase di analisi del rischio, supponiamo che sia emersa l'esigenza di installare una porta blindata capace di resistere a una determinata forza di sfondamento, priva di cardini a vista e resistente al fuoco. Queste sono quindi le specifiche rispetto alle quali verrà valutata la correttezza dei prodotti.

Ora, anche se abbiamo individuato la migliore delle porte blindate sul mercato, dobbiamo valutare l'aspetto efficacia.

Efficacia.

Per quanto tempo la porta resisterà alle tecniche di scasso più evolute?

Qual è la probabilità che le forze dell'ordine arrivino in tempo per impedire l'accesso alle risorse informatiche, agli archivi e alle informazioni?

Se il rischio è rilevante, probabilmente si dovrà identificare un pacchetto di contromisure che, nell'insieme, costituiscano un percorso ad ostacoli capace di resistere al gruppo d'attacco più determinato.

Efficacia.

Poiché i beni da proteggere possono essere assai diversi da un caso all'altro, il programma di sicurezza dovrà essere personalizzato per la situazione specifica, in modo che la scelta delle contromisure e relative funzionalità e garanzie siano commisurate all'entità del rischio e ai tipi di vulnerabilità e di minacce.


Organizzazione della sicurezza

Obiettivo

Conoscere i principali processi da attivare in un'organizzazione che mira a conseguire la sicurezza delle informazioni.

I processi

La sicurezza delle informazioni è il risultato di un insieme di processi ai vari livelli dell'organigramma aziendale.

Non bastano strumenti e tecnologie per ottenere la sicurezza.

Occorre, in primo luogo, creare un'organizzazione per la sicurezza che assuma la responsabilità di quanto attiene alla sicurezza e coinvolga l'intera struttura aziendale, in modo che tutto il personale contribuisca nel proprio ambito al disegno generale della sicurezza.

Organizzazione della sicurezza

L'organizzazione della sicurezza dovrebbe partire dall'alto, dove gli obiettivi e le politiche di sicurezza sono definiti in termini generali dal top management, per essere poi specificati nei dettagli man mano che si scende attraverso gli strati del modello organizzativo della sicurezza.

Organizzazione della sicurezza

In cima a questo modello ci sono gli obiettivi di business strategici, che ispirano i processi fondamentali di cui si deve fare carico l'organizzazione di sicurezza:

- classificazione dei beni e del loro valore
- censimento di vulnerabilità e minacce
- analisi del rischio
- analisi costi/benefici delle contromisure
- valutazione del grado di protezione
- definizione delle politiche di sicurezza
- pianificazione, implementazione e gestione dei progetti di sicurezza
- monitoraggio della conformità tra le soluzioni adottate e le politiche di sicurezza

e altro ancora.

L'approccio dall'alto al basso permette di *coinvolgere tutti i livelli aziendali interessati*, di *assegnare precise responsabilità*, di *definire politiche coerenti per l'intera struttura aziendale*, di *sensibilizzare ed educare il personale*, di *finanziare adeguatamente il progetto sicurezza* e di *rimuovere gli ostacoli* che si presenteranno quando verranno adottate procedure e strumenti che avranno un impatto sull'operatività quotidiana e sulle abitudini del personale (a tutti i livelli).

Organizzazione della sicurezza

A volte nelle aziende vengono prese iniziative di sicurezza dal basso, con le buone intenzioni di proteggere alcuni obiettivi di sicurezza immediati.

Senza la forza di spinta, l'autorità, la responsabilità, il coinvolgimento generale e i mezzi assicurati dal management superiore, i tentativi dal basso si scontrano facilmente con ostacoli insormontabili e sono spesso destinati a fallire.

Un esempio di politica di sicurezza per le comunicazioni wireless

1.0 Scopo

Questa policy proibisce l'accesso alla rete della ACME SpA attraverso connessioni wireless insicure, cioè non protette tramite autenticazione dell'utente e cifratura dei dati. Solo i sistemi wireless conformi ai criteri di questa policy o che hanno ricevuto una speciale esenzione dal responsabile della sicurezza sono approvati per la connessione alle reti della ACME SpA.

Un esempio di politica di sicurezza per le comunicazioni wireless

2.0 Portata

Questa policy copre tutti i dispositivi di comunicazione dati senza fili (per es. personal computer, telefoni cellulari, PDA eccetera) connessi con una delle reti della ACME SpA. Questo comprende qualunque tipo di dispositivo wireless capace di trasmettere dati a pacchetti. I dispositivi e le reti wireless senza alcuna connessione alle reti della ACME SpA non rientrano nell'ambito di questa policy.

Un esempio di politica di sicurezza per le comunicazioni wireless

3.0 Policy

3.1 Registrazione degli access point e delle schede

Tutti gli access point o stazioni di base connessi alla rete aziendale devono essere registrati e approvati dal responsabile della sicurezza. Questi access point sono soggetti a test di intrusione e a periodici audit. Tutte le schede d'interfaccia wireless di rete usate sui desktop e notebook aziendali devono essere registrate presso il responsabile della sicurezza.

Un esempio di politica di sicurezza per le comunicazioni wireless

3.0 Policy

3.2 Tecnologie approvate

Ogni accesso wireless alla LAN deve utilizzare prodotti e configurazioni di sicurezza approvati dall'azienda.

Un esempio di politica di sicurezza per le comunicazioni wireless

3.0 Policy

3.3 Cifratura e autenticazione via VPN

Tutti i computer con dispositivi LAN wireless devono utilizzare una Rete Privata Virtuale (VPN) approvata dall'azienda e configurata per ignorare tutto il traffico non autenticato e non cifrato. Per conformità con questa policy, le implementazioni wireless devono mantenere una cifratura hardware di ogni connessione con chiavi di almeno 128 bit. Tutte le implementazioni devono supportare un indirizzo hardware (MAC address) registrato e rintracciabile. Tutte le implementazioni devono supportare e impiegare una forte autenticazione degli utenti tramite accesso a un server e database esterno come TACACS+, RADIUS o simile.

Un esempio di politica di sicurezza per le comunicazioni wireless

3.0 Policy

3.4 Impostazione dell'SSID

L'SSID (*Service Set Identifier* – un'intestazione aggiuntiva ai pacchetti mandati su una WLAN che funge da password per chi vuole accedere alla rete - sarà impostato in modo che non contenga alcuna informazione relativa all'organizzazione, come nome dell'azienda, nome della divisione o identificatore del prodotto.

Un esempio di politica di sicurezza per le comunicazioni wireless

4.0 Applicazione

Qualunque dipendente sia riconosciuto responsabile di aver violato questa policy può essere soggetto ad azione disciplinare, fino alla cessazione del rapporto di lavoro.

Un esempio di politica di sicurezza per le comunicazioni wireless

5.0 Definizioni

Termine: *Autenticazione*

Definizione: Un metodo per verificare se l'utente di un sistema wireless è un utente legittimo, indipendentemente dal computer o dal sistema operativo che viene usato.

6.0 Revisioni

- 10 luglio 2007: aggiunta la sezione 3.4
- 20 marzo 2074: sezione 3.3 modificata per includere gli indirizzi MAC

Il ruolo delle politiche di sicurezza

Generalmente sono necessarie ***diverse politiche di sicurezza a più livelli****, da quello superiore riguardante l'intera azienda, scendendo ad argomenti più specifici, come il sistema informatico e i singoli aspetti tecnici.*

Il ruolo delle politiche di sicurezza

La **politica di sicurezza aziendale** *indica tutto ciò che deve essere protetto (beni materiali e immateriali) in funzione del tipo di attività dell'azienda, del modello di business, dei vincoli esterni (mercato, competizione, leggi vigenti) e dei fattori di rischio.*

Questo documento definisce gli obiettivi del programma di sicurezza, assegna le responsabilità per la protezione dei beni e l'implementazione delle misure e attività di sicurezza e delinea come il programma deve essere eseguito.

Il ruolo delle politiche di sicurezza

La **politica di sicurezza del sistema informatico** *definisce, coerentemente con la politica di sicurezza aziendale, in che modo l'azienda intende proteggere le informazioni e le risorse informatiche, senza entrare nel merito delle tecnologie che verranno adottate.*

In questa fase vengono presi in considerazione requisiti di sicurezza di tipo fisico e procedurale, mentre gli aspetti tecnici sono demandati al livello inferiore.

Il ruolo delle politiche di sicurezza

La **politica di sicurezza tecnica** *traduce in requisiti tecnici funzionali gli obiettivi che si desidera raggiungere attraverso le contromisure di tipo tecnico informatico, nel contesto dell'architettura di sistema adottata o pianificata dall'azienda.*

Il ruolo delle politiche di sicurezza

In un'azienda di piccole dimensioni potranno essere sufficienti singole politiche di sicurezza per ciascuno dei due livelli inferiori, ma in presenza di più sistemi, dipartimenti e divisioni, è probabile che le politiche di sicurezza si suddividano per area e per argomento.

Esempi di politiche di sicurezza sono forniti dal SANS Institute alla pagina:

http://www.sans.org/resources/policies/

Disaster recovery e Business continuity

La **Disaster Recovery**, *nel contesto informatico, è la capacità di un'infrastruttura di riprendere le operazioni dopo un disastro.*

La maggior parte dei grandi sistemi di calcolo include programmi di disaster recovery, inoltre esistono applicazioni di disaster recovery autonome che, periodicamente, registrano lo stato corrente del sistema e delle applicazioni, in modo da poter ripristinare le operazioni in un tempo minimo.

Il termine disaster recovery può essere usato sia dal punto di vista della prevenzione contro la perdita di dati sia delle azioni per rimediare a un disastro.

Disaster recovery e Business continuity

Due caratteristiche per valutare l'efficacia di un sistema disaster recovery sono il:

- **Recovery Point Objective** (RPO, il momento nel tempo a cui il sistema è riportato), *e il*
- **Recovery Time Objective** (RTO, il lasso di tempo che intercorre prima di ripristinare l'infrastruttura).

Disaster recovery e Business continuity

Per ridurre la distanza dell'RPO rispetto al presente occorre incrementare il sincronismo della data replication, ovvero la replica di archivi e database su un altro sistema, generalmente remoto per motivi di sicurezza.

Per ridurre l'RTO, ossia il tempo di ripristino, occorre che i dati siano tenuti on line su un sistema di riserva pronto a subentrare in caso di avaria al sistema principale.

Disaster recovery e Business continuity

La **business continuity** *descrive i processi e le procedure che un'organizzazione mette in atto per assicurare che le funzioni essenziali rimangano operative durante e dopo un disastro.*

Il Business Continuity Planning cerca di prevenire l'interruzione dei servizi critici e di ripristinare la piena operatività nel modo più rapido e indolore possibile.

Disaster recovery e Business continuity

Il primo passo nel pianificare la business continuity è decidere quali delle funzioni aziendali sono essenziali e destinare di conseguenza il budget disponibile.

Una volta che siano identificati i componenti principali, si possono installare i meccanismi di failover (sistemi di riserva che subentrano in caso di avaria).

Tecnologie appropriate, come la replica dei database o il mirroring dei dischi su Internet, permettono a un'organizzazione di mantenere copie aggiornate dei dati in ubicazioni remote, in modo che l'accesso ai dati sia garantito anche quando un'installazione cessa di funzionare.

Disaster recovery e Business continuity

La differenza tra disaster recovery e business continuity è che un piano di disaster recovery è *reattivo* e si focalizza di solito sul ripristino dell'infrastruttura informatica.

Sebbene sia logico irrobustire l'infrastruttura informatica per prevenire un disastro, lo scopo principale del piano di disaster recovery è rimediare ai danni all'infrastruttura.

Al contrario, un piano di business continuity non soltanto è *proattivo*, ma ha anche l'obiettivo di mantenere in funzione le attività dell'azienda durante qualsiasi evento, non limitandosi a ripristinare i computer dopo il fatto.

Disaster recovery e Business continuity

Un piccolo esempio della differenza tra ripristino dopo un disastro e continuità operativa viene offerto dall'uso personale del computer.

L'utente che si organizza per un rudimentale disaster recovery, tiene backup periodici dei dati e dei file importanti e tiene sotto mano il software originale; se il sistema si blocca o l'hard disk si guasta, reinstalla il sistema operativo e le applicazioni, applica di nuovo tutte le personalizzazioni (Windows, e-mail, Internet, applicazioni eccetera) e ripristina i dati dal backup, perdendo solo le aggiunte e le modifiche successive all'ultimo backup.

Disaster recovery e Business continuity

L'utente orientato alla business continuity si attrezza con almeno due hard disk e un software di backup automatico delle immagini delle partizioni di disco; quindi pianifica copie complete settimanali e copie incrementali giornaliere.

Se si è dotato di un hard disk di backup ben dimensionato, può anche conservare più immagini delle partizioni per scegliere quale ripristinare secondo le circostanze (per esempio una più affidabile o una più aggiornata).

Anche se si guasta il disco principale, basta sostituirlo e ripristinare le partizioni dai file immagine per riprendere la normale operatività in poco tempo (può bastare un'ora), senza reinstallare nulla.

Disaster recovery e Business continuity

In sintesi, l'obiettivo generale delle attività di sicurezza è mantenere la continuità del business aziendale e, in particolare, del lavoro del personale e del servizio ai clienti.

Hardware, software, sistemi, reti, informazioni, attrezzature e personale sono elementi da proteggere, ma vanno inquadrati nel piano di sicurezza generale con l'obiettivo di assicurare la continuità operativa.


Le norme sul sistema di gestione della sicurezza

*L'***ISO/IEC 17799** *presenta una serie di linee guida e di raccomandazioni compilata a seguito di consultazioni con le grandi aziende.*

Il documento sottolinea l'importanza della gestione del rischio e chiarisce che non è indispensabile implementare ogni singola linea guida, ma solo quelle che sono rilevanti.

Lo standard copre tutte le forme d'informazione, incluse la voce, la grafica e i media come fax e cellulari.

Esso riconosce anche i nuovi metodi di business, come l'e-commerce, Internet, l'outsourcing, il telelevoro e il mobile computing.

Le dieci aree delle linee guida dello standard ISO/IEC 17799

1. Security Policy. Fornire le linee guida e i consigli per la gestione, allo scopo di migliorare la sicurezza delle informazioni.

2. Organizational Security. Facilitare la gestione della sicurezza delle informazioni all'interno dell'organizzazione.

3. Asset Classification and Control. Eseguire un inventario dei beni e proteggerli efficacemente.

4. Personnel Security. Minimizzare i rischi di errore umano, furto, frode o uso illecito delle attrezzature.

5. Physical and Environment Security. Prevenire la violazione, il deterioramento o la distruzione delle attrezzature industriali e dei dati.

6. Communications and Operations Management. Assicurare il funzionamento adeguato e affidabile dei dispositivi di elaborazione delle informazioni.

7. Access Control. Controllare l'accesso alle informazioni.

8. Systems Development and Maintenance. Assicurare che la sicurezza sia incorporata nei sistemi informativi.

9. Business Continuity Management. Minimizzare l'impatto delle interruzioni dell'attività aziendale e proteggere da avarie e gravi disastri i processi aziendali essenziali.

10. Compliance. Evitare ogni violazione delle leggi civili e penali, dei requisiti statutari e contrattuali e dei requisiti di sicurezza.

Le norme sulla sicurezza

Mentre l'ISO/IEC 17799 fornisce le linee guida, gli aspetti di sicurezza e le buone norme da applicare, in sé sufficienti per un'azienda medio-piccola, *lo standard* **BS 7799-2** *fornisce le direttive per istituire un sistema di gestione della sicurezza delle informazioni (ISMS, Information Security Management System) da sottoporre alla certificazione di un ente accreditato*.

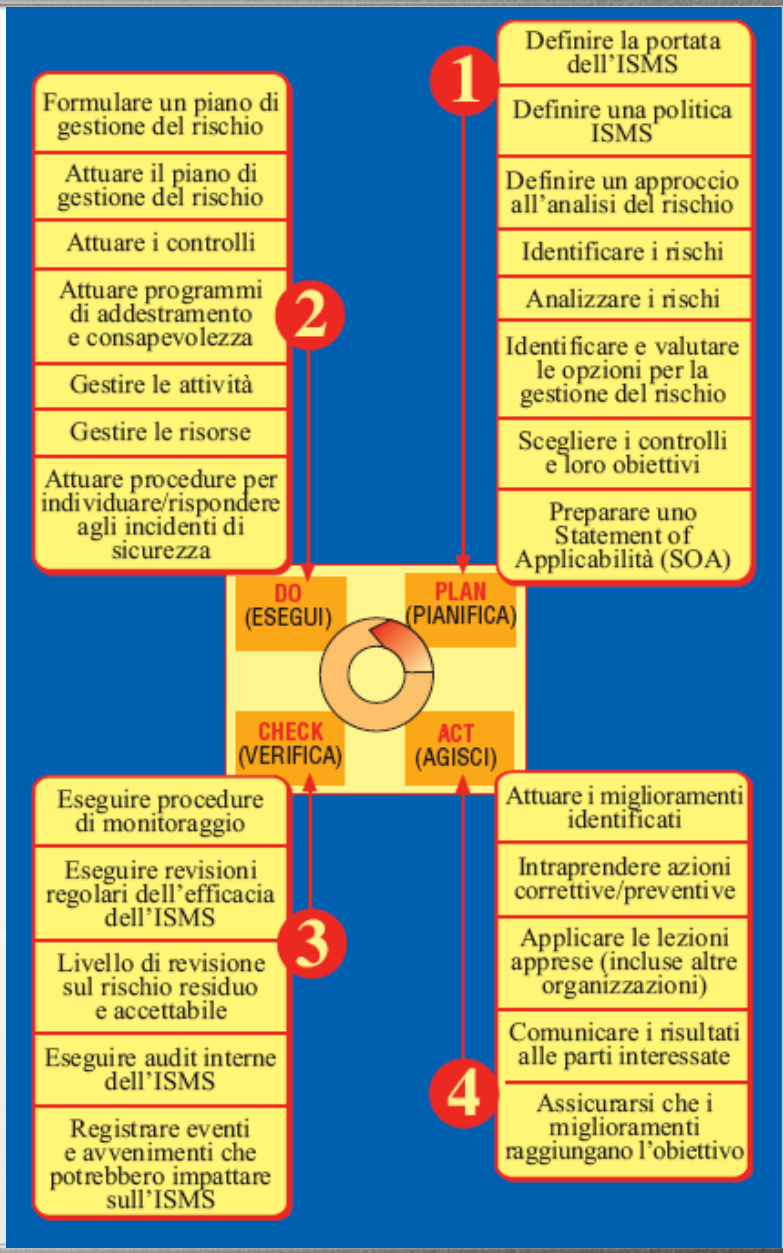
L'applicazione del BS 7799-2 permette all'azienda di dimostrare ai suoi partner che il proprio sistema di sicurezza è conforme allo standard e risponde alle esigenze di sicurezza determinate dai propri requisiti.

Il modello di ISMS definito dallo standard BS7799-2 comprende quattro fasi in un loop ciclico, analogo a quello dell'ISO 9001. Il modello è detto PDCA dalle iniziali delle quattro fasi:

- **Plan** (pianifica: la definizione dell'ISMS),
- **Do** (esegui: l'implementazione e utilizzo dell'ISMS),
- **Check** (verifica: i controlli e le revisioni dell'ISMS),
- **Act** (agisci: la manutenzione e miglioramento dell'ISMS).

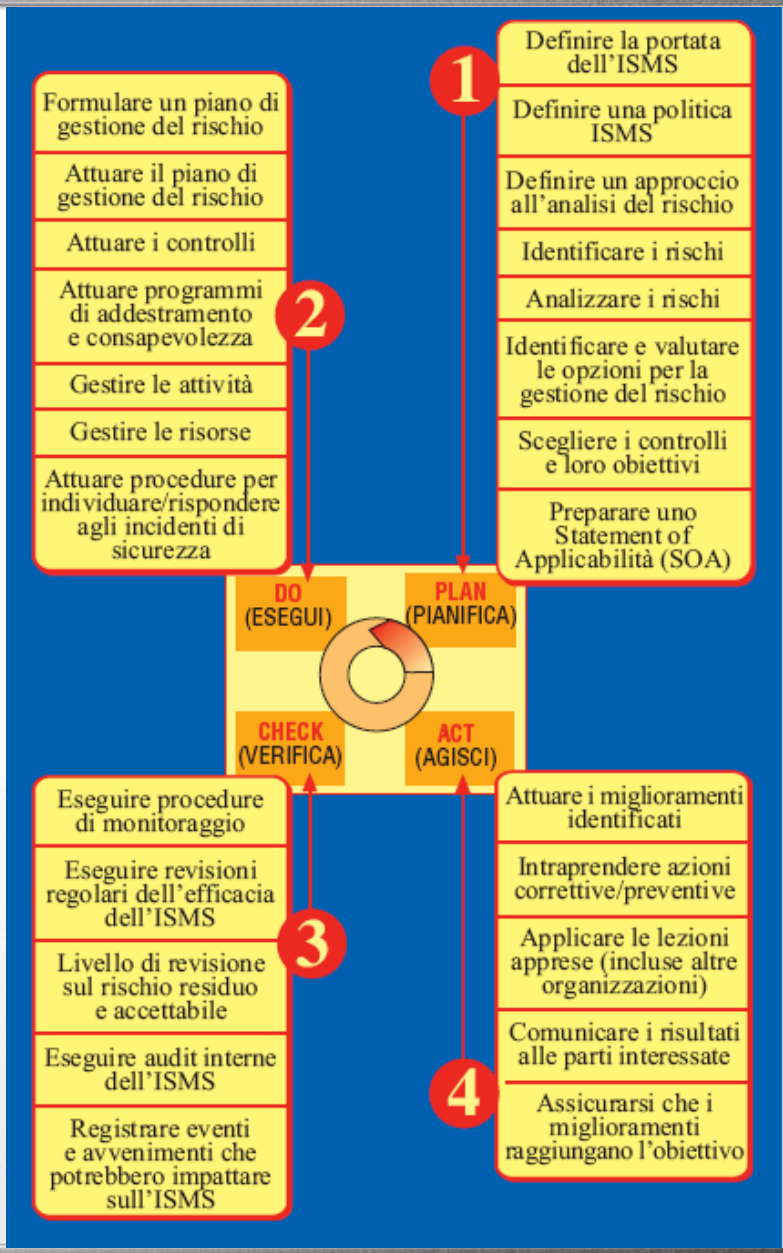
Le quattro fasi dell'ISMS: I) Plan

- definizione dell'ambito di applicazione dell'ISMS
- definizione di una politica di sicurezza di alto livello
- definizione di un approccio sistematico per l'analisi del rischio
- identificazione dei rischi
- valutazione dei rischi
- identificazione delle opzioni per il trattamento dei rischi (eliminazione, cessione e riduzione)
- selezione delle contromisure per il controllo dei rischi
- redazione della dichiarazione di applicabilità, comprendente l'esplicitazione delle ragioni che hanno portato alla selezione delle contromisure e alla non applicazione di misure indicate nell'appendice A della norma.



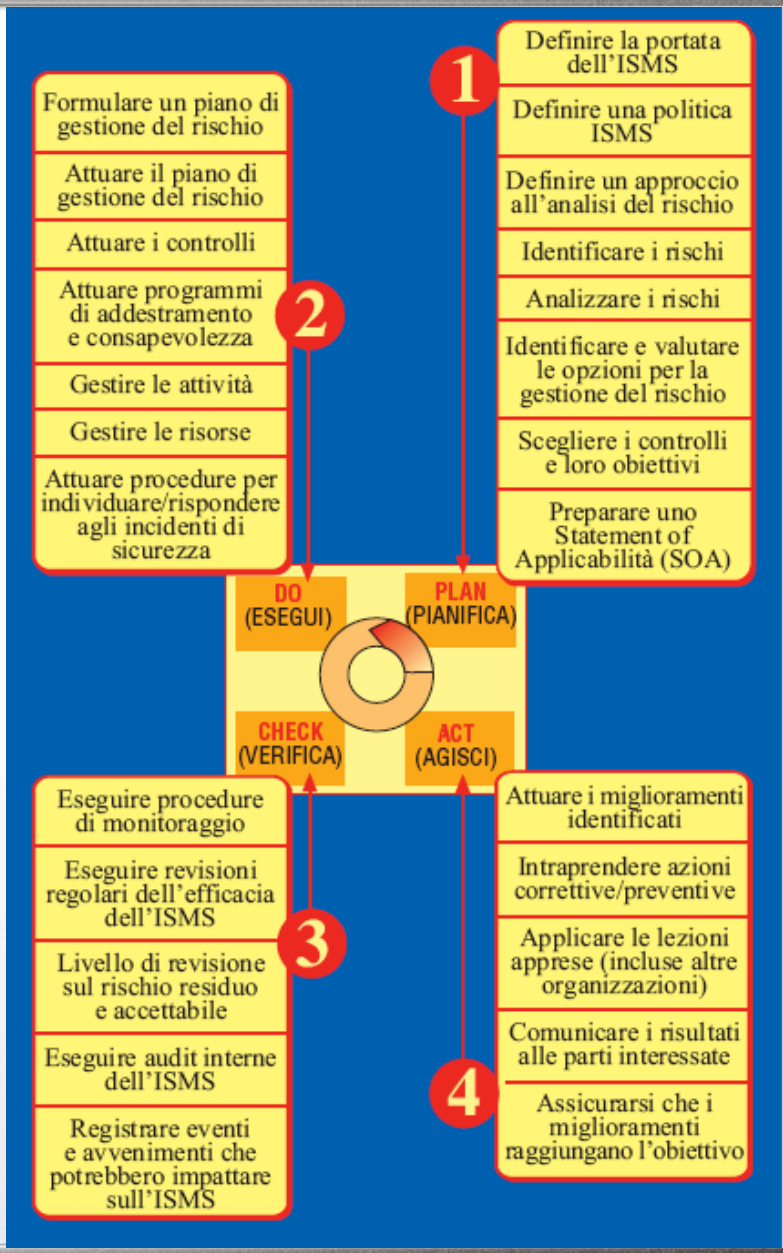
Le quattro fasi dell'ISMS: 2) Do

- formulazione di un piano di trattamento dei rischi
- implementazione del piano
- implementazione delle contromisure selezionate
- svolgimento di programmi d'informazione e di formazione
- gestione delle operazioni connesse alla fase Do
- gestione delle risorse connesse alla fase Do
- implementazione di procedure e altre misure che assicurino rilevazione e le opportune azioni in caso di incidenti relativi alla sicurezza



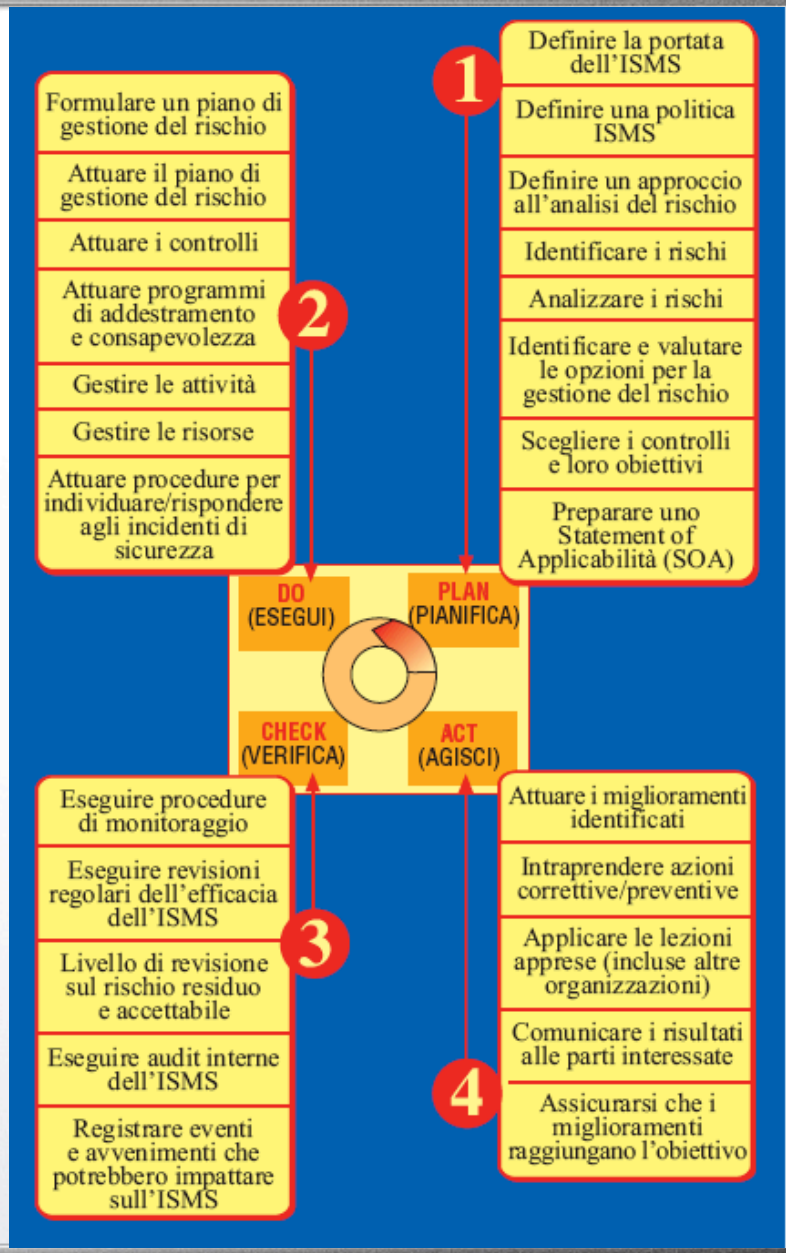
Le quattro fasi dell'ISMS: 3) Check

- esecuzione delle procedure di monitoraggio dell'ISMS
- esecuzione di revisioni del rischio residuo
- conduzione di audit interni all'ISMS
- conduzione di review al massimo livello dirigenziale dell'ISMS
- registrazione delle azioni e degli eventi che potrebbero avere impatti sulla sicurezza o sulle prestazioni dell'ISMS



Le quattro fasi dell'ISMS: 4) Act

- implementazione delle azioni migliorative dell'ISMS
- identificate
- implementazione delle azioni correttive e preventive
- comunicazione dei risultati
- verifica che i miglioramenti raggiungano gli obiettivi identificati alla loro base




Grazie per l'attenzione!