LA SICUREZZA INFORMATICA

Cos’è la Sicurezza Informatica ?

La sicurezza informatica (o information security) è un concetto che esiste da diversi anni, ma solo recentemente sta investendo trasversalmente tutto il mondo della “new economy”. L'esplosione di Internet e delle grandi reti aziendali ha infatti costretto imprese e privati non solo a riflettere sulla necessità di proteggere le informazioni, e i dati che circolano quotidianamente da un computer all'altro, ma a dover fronteggiare attacchi sporadici o organizzati che, in molti casi, creano danni ingenti sia di immagine sia economici. Lo scenario che si presenta oggi a chi opera nel mondo dell'informatica, sia da "addetto ai lavori", sia da "utente", è sempre più complesso: la microinformatica ha favorito la diffusione dell'utilizzo di piccoli elaboratori a livelli che fino a qualche anno fa erano impensabili, gli stessi personal computer ora lavorano sempre più spesso collegati tra loro in reti, che possono essere "locali", in altre parole limitate all'ambiente (ad esempio ufficio) nel quale sono attivi (LAN), oppure definite in un ambito territoriale comprendente, in genere, la città nella quale si opera (MAN), oppure reti "geografiche" (WAN) che consentono di collegare utenti situati in nazioni e/o continenti diversi.

Il continuo aumento di interconnessioni tra queste componenti genera flussi di informazione sempre più complessi, densi ed articolati.

LA SICUREZZA INFORMATICA

IL SISTEMA INFORMATIVO E' L'INSIEME DEI FLUSSI DI INFORMAZIONI OTTENUTE DAI DIVERSI PROCESSI DI RILEVAZIONE, DESTINATI A SUPPORTARE UN SISTEMA DI CONOSCENZE O DI AZIONI O, COMUNQUE, A SODDISFARE LE ESIGENZE DI INFORMAZIONE, DI QUALSIVOGLIA NATURA. AL SISTEMA INFORMATIVO È CORRELATO IL SISTEMA INFORMATICO, COMPRENDENTE GLI STRUMENTI PER SVILUPPARE CONCRETAMENTE I PROCESSI DI RILEVAZIONE, CIOÈ PER OTTENERE E STRUTTURARE LE INFORMAZIONI.

UN SISTEMA INFORMATICO È CONSIDERATO SICURO QUANDO È IN GRADO DI GARANTIRE IL SODDISFACIMENTO DELLE PROPRIETÀ DI **CONFIDENZIALITÀ, INTEGRITÀ E DISPONIBILITÀ** (**C. I. A.** : **CONFIDENTIALITY, INTEGRITY, AVAILABILITY**). PIÙ PRECISAMENTE QUANDO IL SISTEMA È IN GRADO DI GARANTIRE CHE:

- OGNI UTENTE POSSA ACCEDERE ESCLUSIVAMENTE ALLE INFORMAZIONI DI SUA COMPETENZA (**CONFIDENZIALITÀ**).
- OGNI UTENTE POSSA MODIFICARE SOLO INFORMAZIONI DI SUA COMPETENZA (**INTEGRITÀ**).
- OGNI AZIONE, INTRAPRESA DA PERSONE NON AUTORIZZATE, CHE MIRI AD IMPOSSESSARSI, BLOCCARE O DISTRUGGERE UNA QUALUNQUE RISORSA DEL SISTEMA, SIA PREVENTIVAMENTE BLOCCATA (**AVAILABILITY**)

LA SICUREZZA INFORMATICA

Confidenzialità.

Un sistema raggiunge gli obiettivi di sicurezza prefissati quando i dati non sono accessibili o comunque interpretabili dai non aventi diritto. Ciò significa che, anche se i dati dovessero essere intercettati, la loro lettura deve risultare impossibile o, per essere più realisti, eccessivamente complessa.

Si ottiene la confidenzialità nascondendo ai non autorizzati informazioni o risorse. In molti ambiti esistono informazioni e risorse “sensibili” a cui non possono accedere tutti

- Un modo per nascondere le informazioni è la crittografia
- Un altro modo è controllarne gli accessi

Anche le risorse possono essere soggette a restrizioni

LA SICUREZZA INFORMATICA

Integrità.

In un'ottica generale di sicurezza non deve essere possibile alterare i dati oggetto di una qualsivoglia transazione. Dette informazioni devono rimanere appunto integre. Questo fattore riveste particolare importanza, soprattutto se si fa riferimento ad operazioni come la contrattualistica digitale, l'e-procurement e le altre manifestazioni di e-business, in qualsiasi accezione.

- **L'integrità richiede che le informazioni o le risorse "sensibili" non subiscano alterazioni non autorizzate**
  - Integrità dei dati
  - Integrità della sorgente
- **Differenza: si può intercettare un fax in modo completo che contiene informazioni false**
- **I meccanismi per garantire l'integrità si dividono in meccanismi di prevenzione e di scoperta**
- **Integrità: è difficile da esprimere in modo preciso:**
  - è la proprietà che tutto è come dovrebbe essere
- **Spesso si riduce nel proibire la scrittura senza autorizzazione**
- **E' collegata alla segretezza:**
  - modificare il SO è spesso prerequisito per avere accesso a documenti proibiti
  - problema: violazione dell'integrità del SO

LA SICUREZZA INFORMATICA

Disponibilità.

I dati, gli accessi e i servizi fruibili per via infotelematica devono essere disponibili sempre agli aventi diritto. Aggredire questa terza componente, soprattutto nei processi di e-business, significa una sola cosa: no business.

Per disponibilità si intende semplicemente la possibilità di usare una determinata risorsa o un'informazione nel tempo, alcuni attacchi tendono a diminuire e/o ad annullare la disponibilità di alcune risorse

LA SICUREZZA INFORMATICA

"SICUREZZA" indica anche CONTRASTARE ogni minaccia di tipo accidentale :

salvaguardare la riservatezza dell'informazione

Ridurre a livelli accettabili il rischio che un'entitàpossa accedere ai dati
senza esserne autorizzata a seguito di fenomeni non controllabili
(ad es. lo smarrimento di una "penna usb" contenente dai sensibili non crittografati)

salvaguardare l'integrità dell'informazione

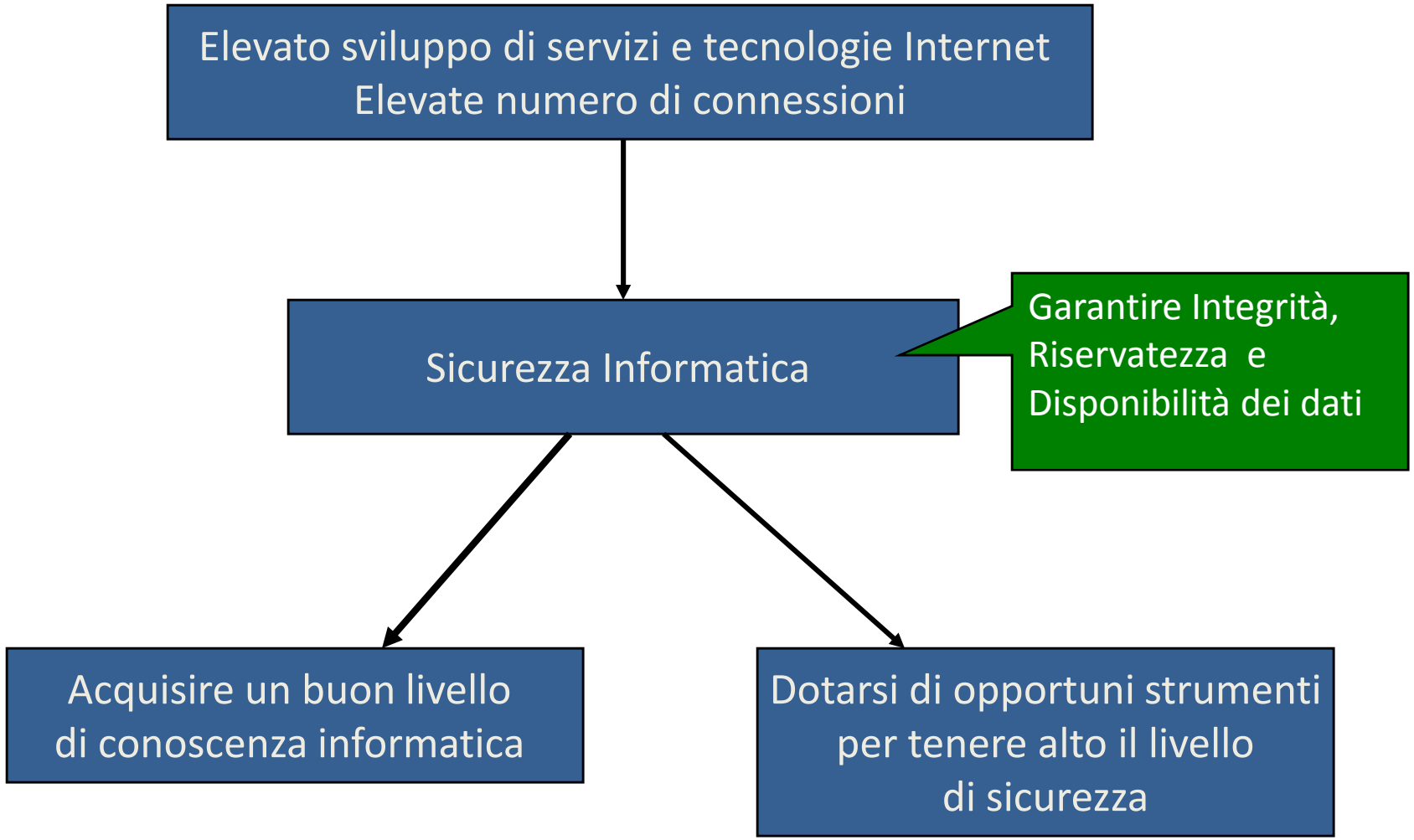
Ridurre il rischio che i dati possano essere cancellati/modificati a seguito di fenomeni non controllabili e prevedere adeguate procedure di recupero delle informazioni
(ad es. rottura di una memoria di massa contenente dati)

salvaguardare la disponibilità dell'informazione

Ridurre il rischio che possa essere impedito alle entità autorizzate l'accesso alle informazioni a seguito di fenomeni non controllabili
(ad es. mancanza di energia elettrica per l'alimentazione dei computer)

LA SICUREZZA INFORMATICA

Ricapitolando, perché la sicurezza?



LA SICUREZZA INFORMATICA

Ricapitolando, perché la sicurezza?

Autenticazione

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

Non ripudio

Impedire che il mittente di un messaggio
possa disconoscerlo

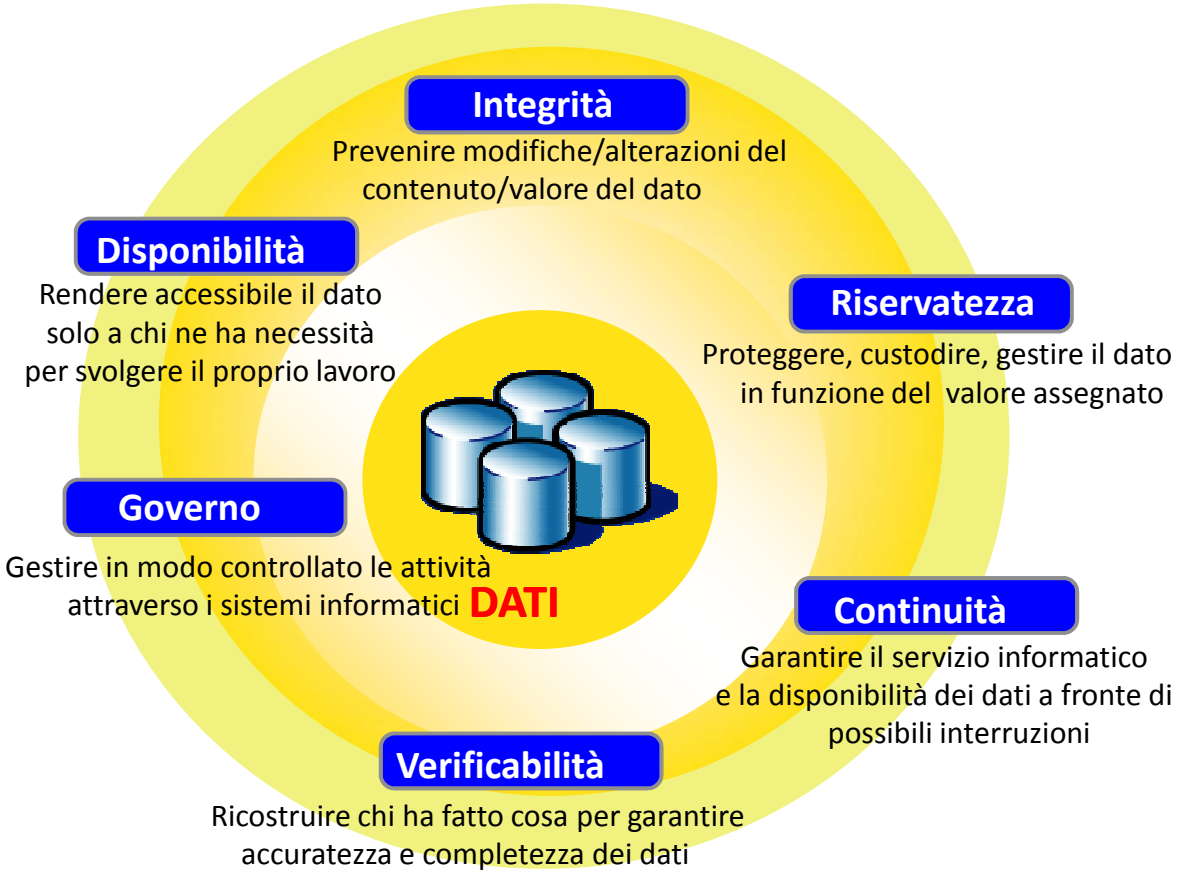
Controllo accessi

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

Anonimia

Protezione dell'identità, o del servizio utilizzato

LA SICUREZZA INFORMATICA



Cosa bisogna proteggere?

IDENTIFICARE LE COMPONENTI DEL SISTEMA INFORMATIVO DA PROTEGGERE (**ASSET -** beni aziendale ,materiali o immateriali, componenti o parte del sistema informativo) :

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

Terminologia

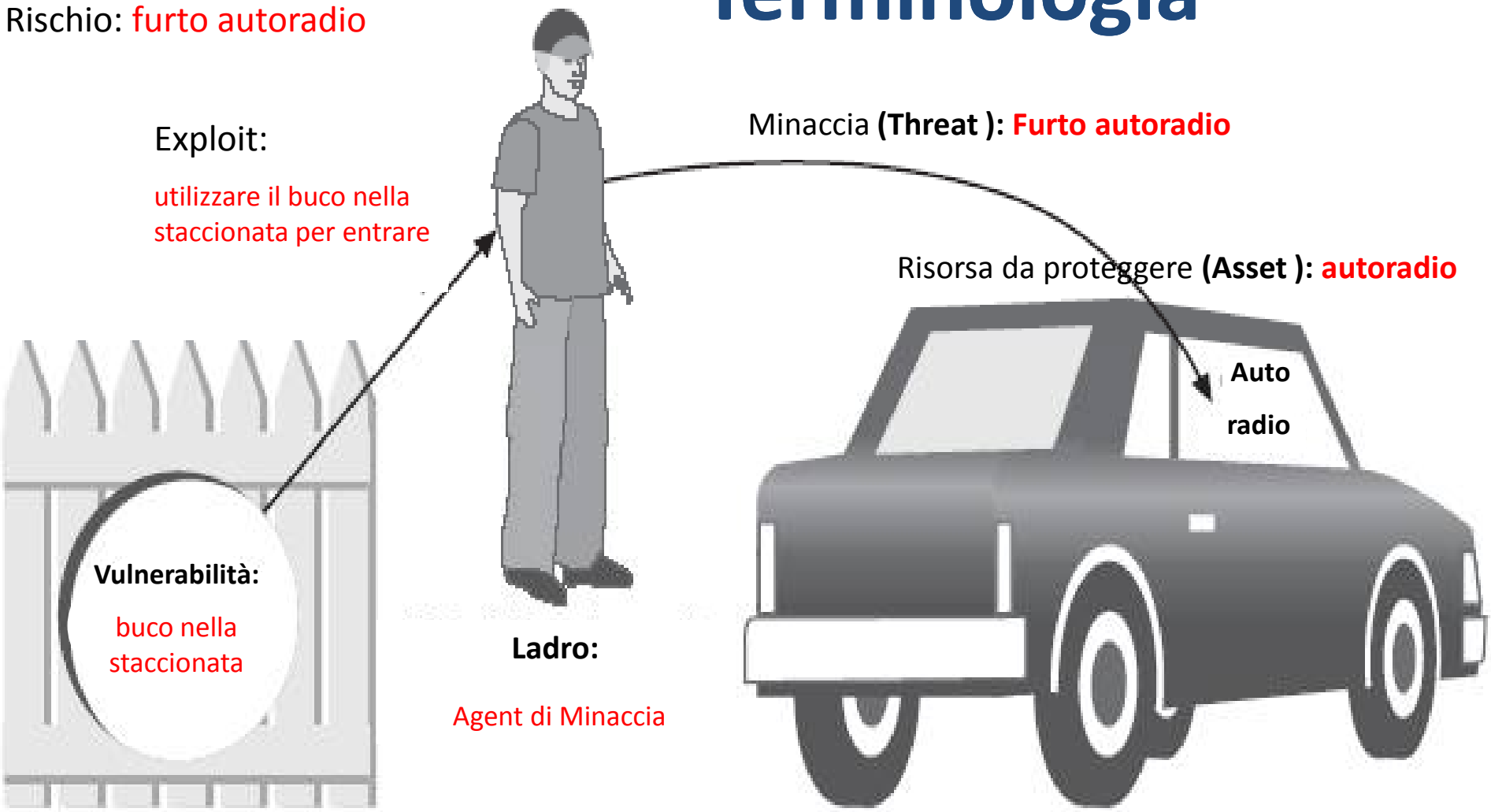
Rischio: furto autoradio

Exploit:

utilizzare il buco nella staccionata per entrare

Minaccia **(Threat): Furto autoradio**

Risorsa da proteggere **(Asset): autoradio**



LA SICUREZZA INFORMATICA

La sicurezza studia le minacce e gli attacchi :

MINACCIA
POTENZIALE CAUSA DI UN INCIDENTE (DELIBERATO O ACCIDENTALE) CHE PUÒ DANNEGGIARE UNO O TUTTI I BENI CHE COSTITUISCONO IL PATRIMONIO INFORMATIVO

VULNERABILITÀ
VIENE DEFINITA COME VULNERABILITÀ UNA DEBOLEZZA PRESENTE NEL SISTEMA OPERATIVO, NELLE PROCEDURE DI SICUREZZA, NEI CONTROLLI INTERNI O NELL'IMPLEMENTAZIONE

in base ai quali stabilisce delle politiche e dei meccanismi.
Tali meccanismi sono poi implementati e verificati .

Quando un sistema è sicuro?

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

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

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

Da chi proteggersi?

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

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

che siano essi Hacker, Criminali informatici, dipendenti infedeli, utenti incompetenti, fenomeni atmosferici o qualsiasi altra cosa vi possa venire in mente……tutti vengono classificati con una sola parola : **MINACCIA**

La "sicurezza" dei dati e delle informazioni è un insieme più ampio della sola "sicurezza" informatica, comprendendo anche la c.d. "sicurezza fisica" dei luoghi, delle persone e della c.d. "logistica". Attuare la c.d. "sicurezza dei dati" non è possibile se non ricorrendo a strumenti di tipo legale, oltre che ad - ovvi - accorgimenti tecnici, e - cosa probabilmente ancora più importante - attraverso accorgimenti organizzativi, intendendo tale termine come l'insieme delle risorse disponibili atte e necessarie alla protezione dei dati e delle informazioni.

Minacce

- Una **minaccia** è una **possibile** violazione della sicurezza
- La violazione non deve necessariamente accadere: è il fatto stesso che può accadere che la rende una minaccia
- E' importante salvaguardarsi dalle minacce ed essere pronti ad eventuali violazioni
- La violazione effettiva è chiamata **attacco** e coloro che la commettono "**attaccanti**"

Classi di minacce

- *Disclosure*: accesso non autorizzato alle informazioni
- *Deception*: accettazione di dati falsi
- *Disruption*: interruzione o prevenzione di operazioni corrette
- *Usurpation*: controllo non autorizzato di alcune parti del sistema

Minacce più ricorrenti

- *Snooping*: intercettazione non autorizzata di informazioni. Disclosure passiva
- *Modificazione o alterazione*: cambiamento non autorizzato di informazioni. Deception attiva. Esempio: attacco “man-in-the-middle”
- *Masquerading o spoofing*: impersonificazione di un’entità da parte di un’altra. Deception/usurpation passiva o anche attiva. Esempio: siti “civetta”. Forme legali: delegazione

Minacce più ricorrenti (2)

- *Ripudiazione dell'origine*: falso diniego che un'entità abbia inviato (o creato) qualcosa. Deception.
- *Diniego di ricezione*: falso diniego che un'entità abbia ricevuto qualcosa. Deception
- *Ritardo*: inibizione temporanea di un servizio. Usurpation.

Minacce più ricorrenti (3)

- *Diniego di servizio*: inibizione a lungo termine di un servizio. Usurpation. Può essere svolta sul server, sul client o in mezzo
- Si verifica quando un server viene sepolto sotto un enorme numero di richieste di servizi che non può trattare e quindi non riesce più a fare il suo lavoro normale
- E’ difficile da evitare in generale

LA SICUREZZA INFORMATICA

Le minacce precedentemente elencate possono avere differenti origini:

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

LA SICUREZZA INFORMATICA

Bisogna capire quali siano i possibili attacchi a cui il sistema può essere sottoposto per adottare le relative misure di sicurezza.

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

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

Politiche e meccanismi

- Una politica di sicurezza è un'indicazione di cosa è e cosa non è permesso
- Un meccanismo di sicurezza è un metodo (strumento/procedura) per garantire una politica di sicurezza
- Esempio:
  - il lab. di inf. di un università stabilisce come politica che non si possono copiare i file dei compiti di un altro studente.
  - Il sistema ha un meccanismo per prevenire la copia di un file da parte di un altro utente
  - Anna non usa tale meccanismo e il sistema è violato

Le politiche

- Una politica di sicurezza stabilisce regole che possono riguardare:
  - le operazioni che si possono usare su certi dati e l'utente che può usarle
  - gli utenti che possono accedere a certi dati.
  - eventuali profili di utente con specifici diritti

Politiche di sicurezza

- La politica di sicurezza si focalizza su:
  - i dati (proteggere)
  - le operazioni (controllare)
  - gli utenti/profili (controllare)
- Tradizionalmente i SO hanno meccanismi che proteggono i dati. Oggi diventa più importante controllare gli utenti

Meccanismi di sicurezza

- Data una politica, che distingue le azioni “sicure” da quelle “non sicure”, i meccanismi di sicurezza devono **prevenire**, **scoprire** o **recuperare** da un attacco
- La **prevenzione** significa che il meccanismo deve rendere impossibile l’attacco
- Spesso sono pesanti ed interferiscono con il sistema al punto da renderlo scomodo da usare
- Esempio unanimanente accolto: richiesta di password come modo di autenticazione

Meccanismi di sicurezza (2)

- La **scoperta** significa che il meccanismo è in grado di scoprire che un attacco è in corso
- E' utile quando non è possibile prevenire l'attacco, ma può servire anche a valutare le misure preventive
- Si usa solitamente un monitoraggio delle risorse del sistema, cercando eventuali tracce di attacchi

Meccanismi di sicurezza (3)

- Il **recupero** da un attacco si può fare in due modi
  - Il primo è fermare l'attacco e recuperare/ricostruire la situazione pre-attacco, ad esempio attraverso copie di backup
  - Il secondo è continuare a far funzionare il sistema correttamente durante l'attacco (fault-tolerant)

Assunzioni e fiducia

- Come possiamo essere certi che la politica descrive correttamente il livello e il tipo richiesto di sicurezza ?
- Esempio: per aprire una porta occorre una chiave, l'assunzione ritenuta da molti valida è che il lucchetto sia a prova di ladri
- In un ambiente in cui ci sono abili scassinatori tale assunzione non è più valida e il sistema non si può più ritenere sicuro

Assunzioni e fiducia (2)

- Un meccanismo M è **sicuro** (rispetto ad una politica P) se non può condurre a stati non ammessi da P
- M è **liberale** se può condurre anche a stati non ammessi da P
- M è **preciso** gli stati a cui può condurre coincidono con quelli ammessi da P

Come ottenere un sistema sicuro

- Fasi
  - Specificazione: descrizione del funzionamento desiderato del sistema
  - Progetto: traduzione delle specifiche in componenti che le implementeranno
  - Implementazione: creazione del sistema che soddisfa le specifiche
- E’ indispensabile verificare la correttezza dei programmi

Considerazioni implementative

- Analisi costi-benefici della sicurezza
- Analisi dei rischi (valutare le probabilità di subire attacchi e i danni che possono causare)
- Aspetti legali (ad esempio uso della crittografia negli USA) e morali
- Problemi organizzativi (ad esempio la sicurezza non “produce” nuova ricchezza, riduce solo le perdite)
- Aspetti comportamentali delle persone coinvolte

Aspetti psicologici

- La sicurezza viene difficilmente apprezzata
- La maggior parte degli utenti di internet non sanno nulla di sicurezza, ma hanno bisogno di sicurezza
- Esiste un conflitto tra sicurezza e facilità d'uso del computer
- Sono necessarie maggiori risorse di calcolo, interagisce con le abitudini, la gestione della sicurezza costa

Aspetti psicologici (2)

- D’altra parte la sicurezza è **necessaria** perché c’è una continua crescita delle violazioni della sicurezza informatica
  - Esistono software d’attacco disponibili su rete
  - Si riscontrano anche attacchi molto sofisticati che arrivano a cancellare le tracce
- Quindi in percentuale cresce il numero degli attacchi che hanno successo ed arrivano a compromettere il sistema attaccato

Rintracciabilità

- Certe “garanzie” possono non bastare:
  - anche azioni autorizzate possono causare violazioni di sicurezza
  - ci può essere un “buco” nei controlli che abbiamo stabilito
- Impossibile la sicurezza al 100%
- E’ importante riuscire a tenere traccia di chi ha fatto le azioni che violano la sicurezza : Rintracciabilità (Auditing)

Rintracciabilità

- L'auditing richiede:
  - selezione delle azioni *pericolose*
  - protezione dei file di log
- Inoltre richiede l'autenticazione degli utenti in modo da poter collegare le azioni pericolose a chi le ha compiute

GRAZIE