

introduzione alla sicurezza informatica

principio fondamentale

- la sicurezza di un sistema informatico è legata molto al processo con cui un sistema viene gestito...
 - pianificazione, analisi dei rischi, gestione dei sistemi, formazione del personale, ecc.
- ... e limitatamente ai prodotti e alle tecnologie che vengono utilizzate
 - firewall, antivirus, ecc.

l'importanza degli aspetti tecnologici

- la conoscenza della tecnologia è comunque importante per...
 - comprendere le vulnerabilità e quindi i rischi
 - adottare contromisure che siano...
 - efficaci
 - economiche
 - scalabili
 - gestibili
 - usabili
 - ...

perché curare la sicurezza?

- evitare di incorrere in **danni economici**
- **conformità** alle leggi (*compliance*)
 - es. D.Lgs. 196/2003
- il motore principale che muove il mercato della sicurezza è la **paura...**
 - di perdite economiche
 - di non conformità alle leggi vigenti

chi dovrebbe badare alla sicurezza (informatica)?

- imprese
- pubblica amministrazione ed enti pubblici
- chiunque utilizzi sistemi informatici per scopi economicamente rilevanti
 - anche se non a scopo di lucro!
 - l'università (quanto vale il sistema di paghe e stipendi dell'ateneo?)
 - lo studente che scrive la tesi (quanto vale il documento "tesi.doc" il giorno prima della consegna?)

terminologia

obiettivi della sicurezza

- confidenzialità o riservatezza o segretezza
 - dati letti solo da chi è “autorizzato”
- integrità
 - dei dati (integrità in senso stretto)
 - i dati non sono stati modificati in maniera incontrollata
 - dell’origine (autenticazione)
 - l’origine dei dati è certa
 - dei sistemi (non compromissione)
- disponibilità
 - dati o servizi sono disponibili per accesso/uso

obiettivi della sicurezza

- non ripudio
 - della ricezione
 - della trasmissione
 - alcuni la considerano una forma di integrità
- privacy (trattamento dei dati personali) imposta per legge
 - comprende confidenzialità, integrità, disponibilità, ecc. dei **dati personali**
 - da non confondere con la confidenzialità

hacker

- hacker
 - esperto di vulnerabilità e attacchi
 - non necessariamente malevolo
 - in italiano l'accezione è spesso negativa
 - termini correlati: cracker, hacktivist, white hat, black hat, gray hat, blue hat, script kiddies, lamer, ecc.
 - vedi wikipedia “Hacker (computer security)”

minacce e affini

- vulnerabilità o vulnerability exposure
 - un problema hw, sw, di configurazione o di procedura che rende possibile un uso improprio di dati o risorse hw e sw
- minaccia (threat)
 - un insieme di circostanze potenzialmente pericolose

es. un bug di explorer assieme alla possibilità di navigare liberamente su Internet costituiscono una minaccia per la sicurezza del sistema degli utenti

minacce e affini

- exploit, exploitation
 - la procedura per sfruttare una vulnerabilità
- attacco
 - tentativo di violazione di riservatezza, integrità o disponibilità tramite lo sfruttamento (exploitation) di una vulnerabilità
- intrusione
 - un attacco riuscito

minacce e affini

- **privilege excalation**
 - l'azione di guadagnare accesso a risorse che normalmente sono precluse.
 - è un attacco andato a buon fine
- **root compromise**
 - situazione in cui l'hacker ha ottenuto il pieno controllo della macchina

contromisure o misure preventive

- contromisura
 - procedura, installazione hw o sw, configurazione o altro atto a diminuire la probabilità che una minaccia possa dar luogo ad un attacco o a limitarne le conseguenze

es. installare un firewall è una contromisura che protegge una intranet da semplici tipi di attacchi

scollegare la intranet da Internet è una contromisura più efficace ma potrebbe essere non “gradita” dall’utenza

soggetti e oggetti

- **soggetto**
 - chi (o cosa) accede ad una risorsa... in modo lecito o illecito, anche inconsapevolmente
- **oggetto**
 - una risorsa da “proteggere”
- **diritti (di un soggetto su un oggetto)**
 - operazioni che il soggetto può compiere sull'oggetto in maniera lecita
 - dal punto di vista dell'oggetto sono detti “permessi”

soggetti e oggetti

- esempio
in unix è vero che i processi di root
possono cancellare qualsiasi file
 - soggetto: un qualsiasi processo dell'utente
root
 - oggetto: un qualsiasi file
 - diritto: cancellazione

policy

- policy
 - un insieme di regole che stabiliscono quali soggetti hanno quali diritti su quali oggetti
 - definisce il concetto di sicurezza in un certo contesto (un sistema, una organizzazione, ecc.)
 - una policy può essere espressa in linguaggio naturale, tramite modello matematico, tramite linguaggio ad hoc
 - in certi contesti (pianificazione) si assume un significato più ampio

meccanismi

- meccanismo

- ciò che per progetto ha lo scopo di far rispettare la policy

es. autenticazione + controllo di accesso sui file permettono di realizzare politiche di “visibilità” dei file tra i vari utenti in windows o unix

azioni di sicurezza

- prevenzione
 - ciò che si fa prima che un certo attacco si manifesti in modo da impedirlo
 - es. installazione di un antivirus
- rilevazione (detection)
 - l'azione di accertare se una violazione della policy è in atto in un certo momento

azioni di sicurezza

- **contrasto**
 - l'azione di fronteggiare un attacco mentre avviene
 - es. cambio la configurazione del firewall per bloccare un certo traffico malevolo
- **recovery**
 - il ripristino della normale operatività del sistema
 - aspetti importanti: tempo, costo
 - certe azioni preventive riducono (o annullano) il tempo e il costo di recovery

azioni di sicurezza

- spesso la prevenzione è meglio degli altri approcci ma...
 - ...può non essere percorribile
 - ...può essere troppo costosa
 - ...può essere non sostenibile dal punto di vista della utilizzabilità del sistema
- **pianificazione**
 - prevede una valutazione dei rischi (e dei costi di recovery) per la scelta delle eventuali misure preventive o di contrasto

fiducia (trust)

- qualsiasi azione di sicurezza è basata su **assunzioni**, o meglio, ripone **fiducia** nel fatto che
 - certi sistemi si comportino correttamente
 - o che certe pratiche siano adeguate o eseguite correttamente

fiducia (trust)

- es. nell'applicare una policy assumiamo che essa...
 - dica chiaramente quando il sistema è in uno “stato sicuro” o meno
 - modelli correttamente i requisiti di sicurezza
- es. nell'adottare un meccanismo assumiamo che esso
 - applichi correttamente la policy
 - che funzioni correttamente

fiducia (trust)

- es. se l'amministratore di sistema applica una patch di sicurezza, come contromisura per una certa vulnerabilità, sta assumendo che...
 - la patch risolva la vulnerabilità
 - nessuno abbia modificato la patch nella comunicazione tra produttore e amministratore
 - la patch sia stata testata approfonditamente dal produttore
 - l'ambiente di test del produttore corrisponda a quello di utilizzo
 - l'installazione vada a buon fine
 - il compilatore usato dal produttore per produrre la patch non abbia bugs
 - ecc. ecc. ecc. ecc.....

assurance: quanto fidarsi?

- quantificare la fiducia che possiamo riporre in un sistema è difficile
- un sistema/processo può essere creato/gestito perché sia facile capire quanto ci si possa fidare di esso
- tali pratiche vanno sotto il nome di **assurance** e prevedono adeguate procedure di...
 - specifica dei requisiti
 - progetto
 - implementazione
 - valutazione (certificazione)
- un sistema che adotta criteri di assurance tipicamente deve passare una fase di **certificazione** che colleziona evidenze del fatto che ci si possa fidare di esso

assurance: Trusted Computing Base

- concetto introdotto con lo standard TCSEC – Dept. of Defense – 1985 (a.k.a. orange book)
- la parte del sistema che è critica per l'attuazione della policy
- ciò che non è nella TCB non deve poter “creare danni” se non funzionante
- una certificazione focalizza l'attenzione sulla TCB
- la TCB deve essere piccola per limitare i costi di certificazione

trusted computing

- attenzione a non confondere il concetto di TCB con il “trusted computing”
- trusted computing
 - concetto introdotto da Trusted Computing Group (TCG)
 - AMD, Hewlett-Packard, IBM, Infineon, Intel, Lenovo, Microsoft, and Sun Microsystems, 2003
 - Trusted Platform Module (TPM): hw che permette al produttore di controllare quale software può girare
 - sicurezza contro software non fidato e manomissioni
 - es. voto elettronico
 - Digital Right Management
 - anti pirateria in ambito multimediale
 - Offre anche altro supporto alla sicurezza
 - es. chiave privata, generazione di numeri “veramente” casuali, ecc.