



Le radici della insicurezza

Security Summit 2010



**I dati sono esposti a rischi dovuti
generalmente allo sfruttamento
accidentale o intenzionale delle
carenze di controllo presenti
nei sistemi informatici**



MINACCE - famiglie

- **Errore**
- **Frode**
- **Perdita di riservatezza**
- **Disastro**
- **Sabotaggio**



MINACCE - tipologie

- intrusione / intercettazione
- manipolazione - web hacking
- falsificazione - email spoofing
- accesso illecito - password snooping
- piggybacking / impersonificazione
- furto di IP - dumpster diving
- misuse - web surfing
- bolnet



MINACCE - tipologie

- DoS / inondazione
- phishing
- social engineering
- pharming



MINACCE - tipologie

- **analisi del traffico**
- **attacco di forza bruta**
- **attacco con msg registrato (packet replay)**
- **modifica / cancellazione messaggio**
- **spamming / bombardamento**



MINACCE - tipologie

- war driving
- war walking

- manutenzione remota
- cloud computing



MINACCE - tipologie

- spyware - malware
- virus
- worm
- bombe logiche
- cavalli di Troia



MINACCE - tipologie

- manipolazione dati / aggiunta dati
- fuga di dati - ricatto
- spionaggio
- arrotondamento al limite inferiore
- tecnica del salame
- alterazione programmi
- back doors
- sfruttamento banchi sistemi



CONSEGUENZE

Tangibili

- finanziarie
- indisponibilità delle informazioni
- attività di rilevamento, contenimento, riparazione e ricostruzione
- produttività del personale ... blocco



CONSEGUENZE

- lavoro per raccolta dati e mantenimento prove valide
- preparazione comunicazioni stampa
- difesa legale (se responsabilità azienda)
- aumenti premi assicurativi



CONSEGUENZE

Intangibili

- calo credibilità - sfiducia dei clienti
- clientela che si rivolge ad altri
- rallentamento / arretramento della posizione di mercato (cattiva pubblicità)
- accesso dei concorrenti a info riservate
- svantaggio competitivo



PERPETRATORI

- **Hacker** (violano misure sicurezza)
 - kid (ragazzi) script
 - hacker solitari - gruppi
 - hacker attivisti
 - hacker criminali
- **Cracker** (disattivano protezioni sw)
- **Phreaker** (sfruttano reti)



PERPETRATORI

- esterni in proprio / istruiti da terzi
- concorrenti, terroristi, organizzazioni criminali
- paesi nemici

- personale part-time - tempo determinato
- venditori / consulenti

- e ...



PERPETRATORI

- dipendenti autorizzati e non
- personale IT
- utenti finali
- ex-dipendenti



FISIONOMIA

- rubare un PC o altre apparecchiature
- rubare senza che venga preso fisicamente qualcosa
- gioco - percezione distorta del crimine
- no coinvolgimento emotivo



FISIONOMIA

- dipendente con alcuni anni anzianità
- dipendente con posizione di supervisore
- persona consapevole delle carenze
- persona frustrata
- persona con problemi finanziari
- dedita al gioco / stupefacenti



FISIONOMIA

- desiderio di rispetto
- ha molto da perdere se scoperto
- attento al giudizio sociale e morale
- non si sente un criminale



FATTORE UMANO

- gusto della trasgressione
- indifferenza - superficialità - incoscienza
- abbassamento costume di vita
- benevolenza verso attori negativi



FATTORE UMANO

- grande disponibilità di informazioni e tecnologia rende molto facile fare oggi ciò che veniva fatto anni fa con più fatica
- società immorale che non insegna l'etica nella famiglia e nella scuola
- commettere crimini è sempre più facile



FATTORE UMANO

- giovani che non si pongono problemi di frodare e trarre in inganno il prossimo
- nelle aziende il codice etico spesso viene redatto/pubblicato per far vedere ... non perché è o deve diventare cultura aziendale
- in tal modo non si realizza un grande sforzo per realizzare il cambiamento



FATTORE UMANO

- non è più necessario associarsi, trovare complicità per commettere crimini
- non ci sono testimoni
- anche se si individua una truffa in atto non è facile prendere il responsabile
- basso rischio di essere individuati



FATTORE UMANO

- per quanto un sistema sia definito sicuro ... c'è sempre un uomo che lo può violare
- spesso le professionalità vengono prese in affitto da società esterne di cui non si valuta a fondo l'affidabilità



FATTORE UMANO

- la maggior parte delle persone è onesta ma ingenua e ... sottovaluta il rischio di



SCOPERTO DA

**Molto spesso più da informazioni provenienti
dall'esterno che da iniziative interne**

FATTORI INEVITABILI



- costo
- rincorsa
- sensibilizzazione
- gli altri



RADICI DELL'INSICUREZZA

Le frodi/gli attacchi sono quasi sempre la manifestazione eclatante e dolorosa di un problema che ha quasi sempre radici profonde nella inadeguatezza di:



RADICI DELL'INSICUREZZA

- supporto/impegno della Direzione
- policy/piano strategico della sicurezza
- identificazione proprietario dei dati
- classificazione delle risorse
- definizione norme specifiche
- procedure organizzative di salvaguardia
- assegnazione responsabilità sicurezza
- sensibilizzazione del personale



RADICI DELL'INSICUREZZA

- **consapevolezza / cultura della sicurezza**
- **misure di sicurezza pubblicizzate** (alcune non necessariamente palesi)
- **supervisione**
- **esame / controllo log**
- **controllo accessi logici e fisici**
- **gestione autenticazioni / ID speciali**
- **revisioni delle autorizzazioni**



RADICI DELL'INSICUREZZA

- approccio need-to-know
- separazione delle funzioni
- affidabilità dei dati / documenti
- adeguatezza delle applicazioni
- attività correttive lacune riscontrate
- compiti del personale
- gestione del personale



RADICI DELL'INSICUREZZA

- limitazione uso pdl
- gestione pdl
- limitazione strumenti tecnici sensibili
- procedure di dial-back
- controlli su modifiche rete
- crittografia
- procedure rafforzamento / miglioramento livello protezioni in essere
- ...



RADICI DELL'INSICUREZZA

... normali aree di controllo audit



SISTEMA DI CONTROLLO INTERNO

Normalmente la misura di sicurezza prioritaria non dovrebbe consistere nel predisporre specifiche barriere anti-“frode”, ma nel pervenire a un adeguato

sistema di controllo interno

che permetta di gestire correttamente il sistema informativo nel suo volgere quotidiano per evitare gli errori



PREVENIRE GLI ERRORI

E' opportuno ricordare che la stragrande maggioranza dei problemi nel campo IT deriva da errori e, se si è in capaci di

prevenire gli errori

quasi sicuramente si è in grado di affrontare le situazioni dove gli "errori" sono voluti e premeditati



COSA FARE E NON FARE

Le aziende devono difendersi da ...

non prendere criminali

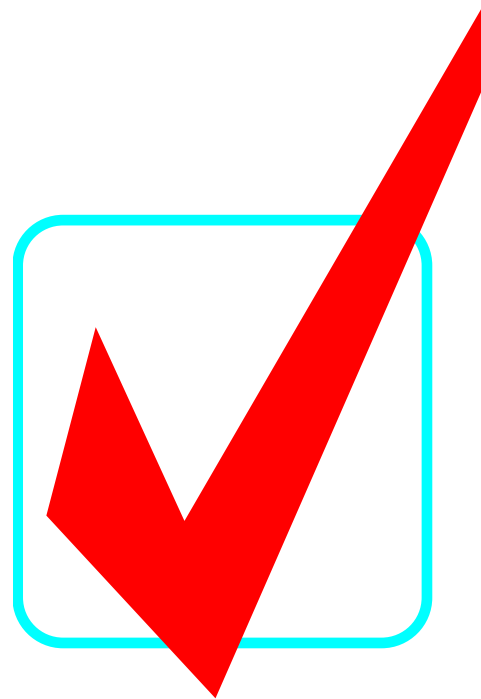


GRAZIE

aiea@aiea.it

www.aiea.it

Security Summit 2010



Security Summit 2010