

FRODI INTERNE

L'IMPORTANZA

DELL'I.S. AUDITING



**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

- manipolazione dati / aggiunta dati
- arrotondamento al limite inferiore
- tecnica del salame
- trap doors
- attacco asincrono
- fuga di dati

MINACCE - tipologie

- piggybacking
- virus
- vermi
- bombe logiche
- cavalli di Troia
- DoS

- social engineering

MINACCE - tipologie

- spionaggio
- intrusione - intercettazione
- superzapping
- alterazione programmi
- misuse risorse computer

MINACCE - tipologie *IL CYBERCRIME*

- manipolazione - web hacking
- falsificazione - email spoofing
- accesso illecito - password snooping
- furto di IP - dumpster diving
- misuse - web surfing
- spyware
- phishing

CONSEGUENZE

Tangibili

- finanziarie
- indisponibilità delle informazioni
- clientela che si rivolge ad altri
- produttività del personale ... blocco
- attività di rilevamento, contenimento, riparazione e ricostruzione

CONSEGUENZE

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

CONSEGUENZE

Intangibili

- svantaggio competitivo
- sfiducia dei clienti
- rallentamento / arretramento della posizione di mercato (cattiva pubblicità)
- accesso dei concorrenti a info riservate

PERPETRATORI

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

PERPETRATORI

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

PERPETRATORI

- esterni in proprio / istruiti da terzi
 - concorrenti, criminali
- personale part-time - tempo determinato
- venditori / consulenti
- inesperti accidentali

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 frustrata
- persona consapevole delle carenze



FISIONOMIA

- 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
- spontaneismo vs organizzazione

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

RADICI DELL'INSICUREZZA

- procedure organizzative di salvaguardia all'altezza
- 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**

RADICI DELL'INSICUREZZA

- controllo accessi logici e fisici
- gestione autenticazioni / ID speciali
- revisioni delle autorizzazioni
- approccio need-to-know
- affidabilità dei dati - documenti

RADICI DELL'INSICUREZZA

- adeguatezza delle applicazioni
- attività correttive lacune riscontrate
- compiti del personale
- separazione delle funzioni
- gestione del personale

RADICI DELL'INSICUREZZA

- limitazione uso pdl
- gestione pdl
- limitazione strumenti tecnici sensibili
- procedure di dial-back
- controlli su modifiche rete
- crittografia

RADICI DELL'INSICUREZZA

- procedure rafforzamento / miglioramento livello protezioni in essere
- verifica periodica affidabilità
- *normali controlli di audit*

RADICI DELL'INSICUREZZA

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

sistema di controllo interno

che permetta di gestire correttamente il sistema informativo nel suo volgere quotidiano

RADICI DELL'INSICUREZZA

Le aziende devono difendersi non
prendere criminali



RADICI DELL'INSICUREZZA

E' opportuno ricordare che la stragrande maggioranza dei problemi nel campo ICT 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

Sistema a prova di errore ? *

Purtroppo NO però

.....al termine si otterrà un sistema informativo più affidabile - più sicuro e ... più conosciuto

- sarà più facile far fronte ad attacchi dolosi allargando campo di ricerca/livello di approfondimento identificando le *misure protettive* necessarie e rilevando tempestivamente i fenomeni anomali

GRAZIE

- www.aiea.it
- aiea@aiea.it
- silvano.ongetta@tiscali.it



