

# **Percorso basico Modulo I**

## **Essere consapevoli nell'uso quotidiano degli strumenti informatici**

Security Summit 2009

Milano, 24-26 Marzo

# Programma

- Sicurezza come gestione del rischio
- I dati: un valore da proteggere
- I codici maligni
- Manutenzione dei sistemi
- Separazione di attività e ruoli
- Frodi via Internet
- Posta elettronica e navigazione web
- La rete
- Conformità alle norme
- Principi di sicurezza

# Sicurezza: perché?

- Cercheremo di capire qual'è l'utilità della sicurezza IT in azienda o in un'organizzazione...
- ... e di assicurarci che questa utilità esista davvero
- L'importanza della sicurezza deriva direttamente dall'importanza dell'IT
  - ◆ Spesso sottostimata
  - ◆ Qual'è il ruolo dell'IT in azienda?
  - ◆ “Semplifica le cose, ma posso farne a meno...”
- Spesso l'imprenditore non ha chiaro il ruolo degli strumenti informatici nella sua azienda

# Evoluzione della sicurezza ICT

- Gestione puramente tecnologica
- Generica attenzione alla rilevanza di risorse e minacce
- Sicurezza come gestione del rischio
- Contemporaneamente:
  - ◆ IT Governance: allineare la gestione dell'IT (e della sicurezza) agli obiettivi del business e ai rischi dei processi operativi
  - ◆ Attenzione agli aspetti umani (social engineering, motivazioni)
  - ◆ Integrazione con la sicurezza fisica?

# Individuare risorse e minacce

- Spesso l'imprenditore non ha chiaro il ruolo degli strumenti informatici nella sua azienda
- Le risorse sono informazioni, non i computer, su quelle si investe:
  - gli elenchi di clienti e fornitori;
  - la rubrica telefonica e gli appuntamenti;
  - la fatturazione;
  - le comunicazioni con i fornitori, ad esempio via posta elettronica;
  - i rapporti con la banca, con l'Agenzia delle Entrate e con altri Enti pubblici;
  - la documentazione per la gestione del personale e per la conformità alle normative;
- Anche su palmari, cellulari, portatili...
- Quali minacce sono realistiche? Non sempre l'imprenditore lo sa, poche le sa il tecnico
  - nessuno dei due conosce le probabilità

# Individuare risorse e minacce

- Le risorse sono informazioni, non i computer, su quelle si investe:
  - gli elenchi di clienti e fornitori;
  - la rubrica telefonica e gli appuntamenti; le comunicazioni con i fornitori, ad esempio via posta elettronica;
  - i rapporti con la banca, con l'Agenzia delle Entrate e con altri Enti pubblici;
  - la documentazione per la gestione del personale e per la conformità alle normative;
- Anche su palmari, cellulari, portatili...

# Le minacce

- Utenti locali (gestione dei diritti)
- Virus e bestiario
- Hacker (???)
- Concorrenti, governi ecc.
- Criminalità tradizionale (frodi, ricatto)
- Cyberwar/cyberterrorismo/cybervandalismo???
- Social engineering
- Differenze: mezzi, obiettivi, possibilità di contrasto

# L'approccio tecnologico

- La sicurezza consiste nel garantire integrità, disponibilità e riservatezza delle risorse
- Quanto è utile questa definizione da un punto di vista operativo?
  - ◆ Quanto dobbiamo investire in sicurezza?
  - ◆ Per proteggere cosa?
  - ◆ Quanto ci aiuta utilizzare uno strumento invece di un altro?

# La sicurezza è un processo: PDCA

**PLAN: Analisi del rischio/**

**progettazione  
dell'ISMS**

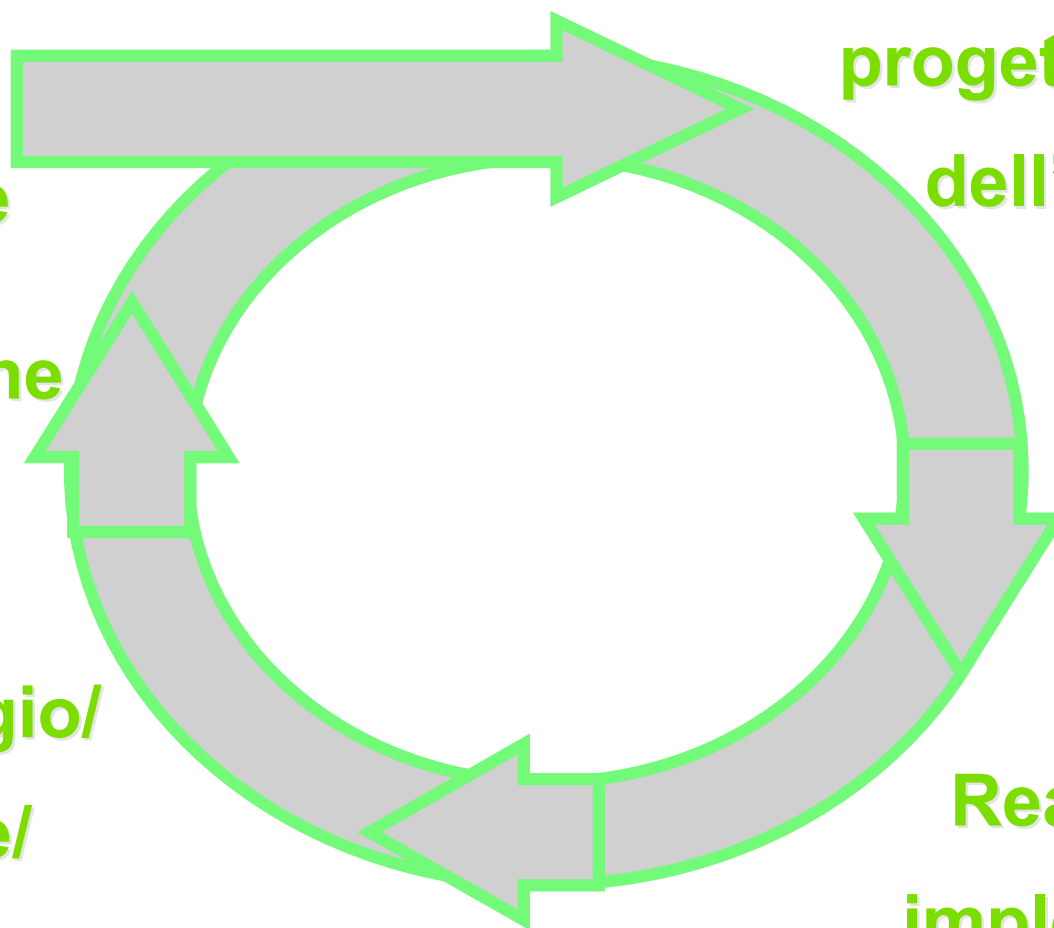
**ACT: Correzione**

**CHECK:**

**Monitoraggio/  
revisione/  
verifiche**

**DO:**

**Realizzazione/  
implementazione**



# ISMS ISO 27001 / 27002

- modello Plan - Do – Check - Act
- Obiettivi derivati da:
  - ◆ obiettivi di business dell'organizzazione e relativi rischi
  - ◆ compliance
  - ◆ principi propri (es. etici) dell'organizzazione
- Definizione di una politica di gestione dell'ISMS
- Definizione di un approccio per il risk assessment
- Identificazione, analisi e valutazione dei rischi

# Obiettivi e processi

- Primo problema: quali aziende sono realmente organizzate in processi?
- Chi fornisce o richiede gli obiettivi?
- La sicurezza deve essere parte integrante dei processi, è uno dei parametri da valutare nella loro definizione, insieme a costo, efficienza ecc.
- Se si “appiccica dopo” è messa a confronto con tutti gli altri parametri, primo fra tutti il costo

# Esempio: il Dlgs 196/03

- Prevede di riconoscere e gestire non solo i dati ma anche i “trattamenti”
- Porta naturalmente ad una visione per processi
- Molte aziende hanno “scoperto” trattamenti o addirittura dati nel corso dell'adeguamento
- Non sempre erano dati di poco valore per l'azienda...
- Stiamo parlando di processi di business, solo dopo vengono i processi IT

# Il rischio

- Rischio = impatto x probabilità
- Valutazione del rischio per i processi aziendali: la formula ci aiuta davvero?
- Valutare l'impatto di:
  - ◆ Costi di ripristino
  - ◆ Downtime
  - ◆ Proprietà intellettuale
  - ◆ Danni di immagine
  - ◆ Ritardi nei processi
  - ◆ Danni nascosti?

# Probabilità

- Siamo in grado di valutare la probabilità degli incidenti?
- Una probabilità dello 0,5 annuo di perdere 100.000 euro è diversa da una probabilità dello 0,05 di perderne 1.000.000
- I rischi si sommano (due valutazioni di questo tipo danno una probabilità quasi dello 0,1)
- Mancano i dati, ma...

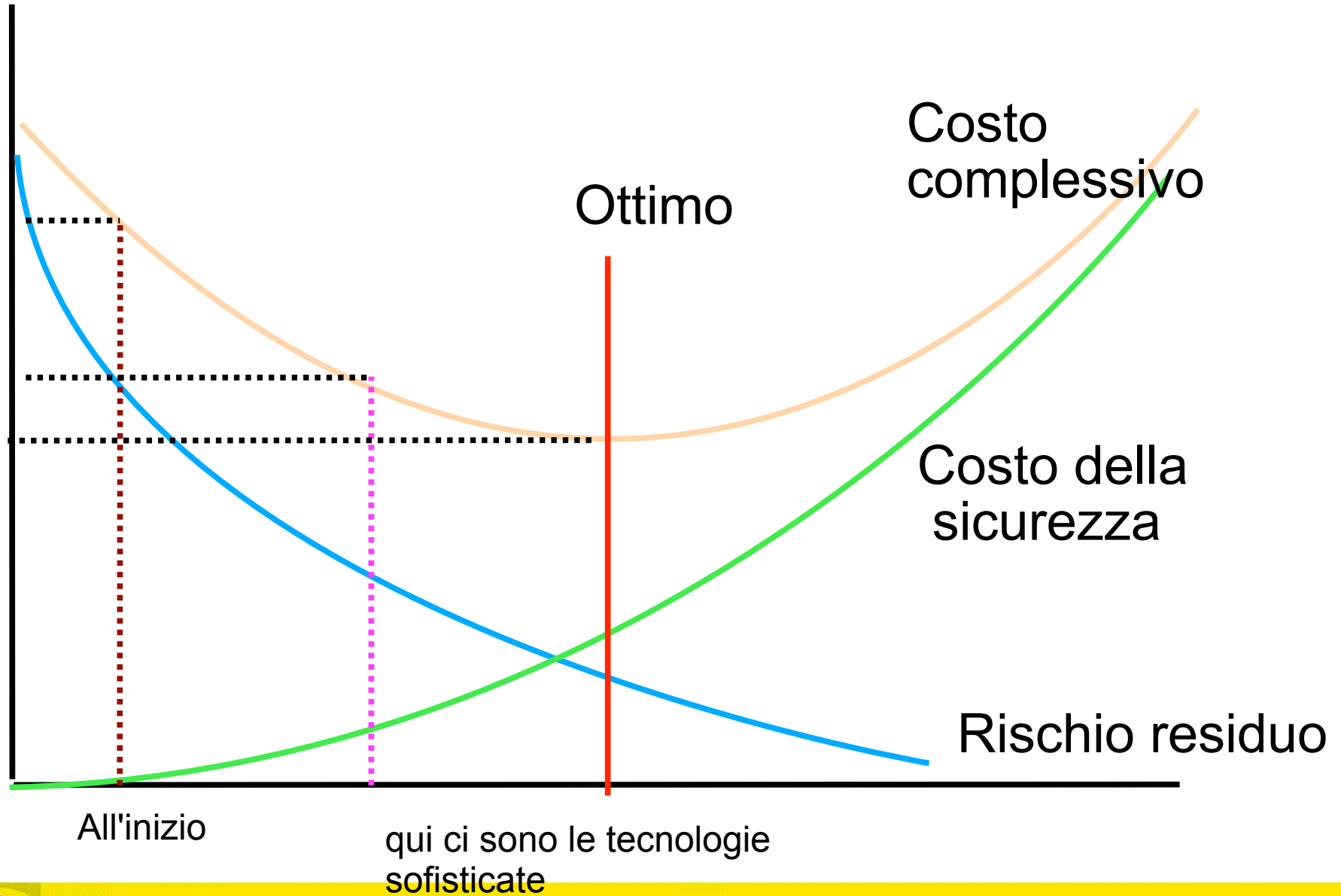
# Metodologie di valutazione del rischio

- Qualitative: alto, medio, basso
- Quantitative: non basta sostituire con 1,2,3 o con 0-20%,21-70%,71-100%: i numeri devono essere motivati
- Controprova: se un evento ha una probabilità del 20% di causare un danno di 20.000 euro in un anno... perché non del 25%, o 18.000?
- Le metodologie quantitative attirano, perché permettono di definire “facilmente” gli investimenti

# sicurezza e gestione del rischio nella PMI

- E' l'imprenditore a conoscere le proprie risorse di valore, ma spesso non lo sa...
- Il rischio è parte dell'impresa, ma:
  - in Europa, la PMI sono spesso fornitori di imprese più grandi; le esigenze (normative) di gestione del rischio delle grandi ricadono anche sulle piccole; in questi casi non sono nell'interesse della piccola impresa
  - La necessità di rapporti globali spinge verso l'IT e ne rende necessaria la protezione
- La sicurezza non è un problema tecnologico: le tecnologie non mancano

# MiniMax



# Problemi del MiniMax

- Il calcolo del rischio nei sistemi informativi è un concetto teorico
  - per di più è diverso da impresa a impresa
- Gli investimenti devono essere “ottimali”: spendere nella tecnologia sbagliata non riduce il rischio
- A forza di investire, la complessità e quindi il rischio possono aumentare

# Da dove vengono le vulnerabilità?

- Le vulnerabilità non sono solo “buchi” software da correggere con “patch” o “fix” dei fornitori
  - ◆ Problemi architetturali
  - ◆ Problemi di gestione dei ruoli
  - ◆ Comportamenti poco accorti
  - ◆ Errori di configurazione
- E in più:
  - ◆ Mancanza di backup
  - ◆ Poca sicurezza fisica e ambientale
  - ◆ ...

# I punti fondamentali

- Individuare risorse e minacce
- Evitare la perdita accidentale di dati
- Aggiornare i sistemi
- Contrastare i codici maligni
- Separare le attività
- Attenzione alle frodi
- Cautela con la posta e la navigazione
- Protezione della rete locale e wireless
- Conformità alle norme (e gli standard?)
- Cura del comportamento del personale

# Evitare la perdita accidentale dei dati

- Pochi fanno backup regolari
- Meno li gestiscono correttamente
- C'è quasi una cultura di “rassegnazione” favorita dalle frequenti reinstallazioni
- Eppure, si sa che i dischi si guastano...
- Ma anche:
  - si perdono i cellulari
  - si rubano i portatili
  - si rubano per sbaglio anche i backup
  - ...

# Contrastare i codici maligni

- Ci interessa catalogare il bestiario?
- L'antivirus non basta più
  - Antispyware, personal firewall...
- E' importante un componente che intercetti le modifiche al sistema (generalmente antispyware)
- Le suite integrate possono andare bene
  - attenzione ai costi per componenti inutili
  - attenzione al carico del sistema
  - non sono ottimali su tutti i componenti
  - semplificano la gestione
  - non diversificano

# Separare le attività

- Forse la singola misura più efficace in assoluto
  - la meno adottata, perché è anche la più scomoda
- Troppe applicazioni fatte male
  - sono cambiati i sistemi ma non gli sviluppatori
  - ma a volte basta correggere dei diritti
  - un compromesso su un'applicazione è meglio che cedere tutti i diritti
- Le applicazioni da ufficio non hanno bisogno di privilegi particolari
- Certo, i giochi e il P2P sono un'altra cosa...

# Attenzione alle frodi

- E' più un problema culturale che tecnico
  - riportare il concetto del “mattoncino” a Internet
  - immaginare di essere turisti in un paese straniero
  - chi si fa imbrogliare nel mondo reale (es. da falsi impiegati) si farà imbrogliare anche su Internet
  - in compenso, su Internet si fanno imbrogliare anche altri
  - ragionare bene su qualsiasi cosa che chieda **informazioni** e soldi
  - comunque le frodi non si eliminano

# Cautela con la posta e la navigazione

- Sono i canali principali attraverso cui adesso sono attaccate le piccole imprese
  - a meno di usi “promiscui” come il p2p
- Evitare le eccessive integrazioni se non sono necessarie
  - possono essere utili i plug-in che aumentano i controlli
- Imparare i “segnali” del browser
- Valutare di appoggiarsi a fornitori
  - es. per la posta
  - evitare i tecnofili entusiasti ;)

# Protezione della rete locale e wireless

- Firewall e personal firewall sono ormai in tutti i router/modem e S.O.; si tratta di usarli
- E' attiva (e a volte usata) anche molta connettività wireless:
  - Wi-Fi
  - bluetooth
- Anche qui, si tratta di configurare quello che c'è e disattivare quello che non si usa

# Conformità alle norme

- Le norme sono scritte spesso con in mente grandi aziende e contesti specifici
  - alle piccole imprese capitano fra capo e collo
  - emblematica l'evoluzione della normativa sul trattamento dei dati personali
- Aziende simili hanno problemi simili
  - sfruttare le associazioni?
- Conformità a norme e standard derivano anche dall'essere fornitori
  - anche gli standard sono pensati nell'ipotesi di una disponibilità illimitata di competenze
  - o disponibilità di personale...

# Cura del comportamento del personale

- In una piccola impresa non c'è posto per politiche complesse
- Servono:
  - chiarezza, condivisione, commitment
  - la politica scritta serve come tutela legale
- Preparazione del personale
- E' necessario ricordarsi che i ruoli sono meno definiti
- Social engineering: è un problema, ma le lene riescono a imbrogliare anche gli imbroglianti...

# Principi fondamentali della sicurezza

- Esistono alcuni concetti fondamentali, ormai accettati che devono guidare la progettazione e la valutazione della sicurezza di sistemi IT
- Non valgono solo per sistemi dedicati alla sicurezza, anzi:
  - ◆ I sistemi specializzati sono quelli che più facilmente seguono già questi principi
  - ◆ È il mancato rispetto nel resto dell'IT che causa problemi di sicurezza

# Aspetti architeturali

- La sicurezza non viene fornita da singoli componenti, ma dalla sinergia di tutto il sistema
- Più la sicurezza è integrata nel sistema
  - ◆ Più è efficace
  - ◆ Meno è onerosa e di disturbo
- Molti meccanismi di sicurezza sono in realtà meccanismi di buona gestione
  - ◆ es. inventario
  - ◆ Sistemi di logging centralizzato
  - ◆ ...

# Sicurezza dall'inizio

- Più tardi viene affrontata la sicurezza in un progetto:
  - ◆ più è difficile inserire delle misure efficaci
  - ◆ più è costoso inserirle
- alcune scelte possono essere poco significative sotto altri aspetti, ma molto per la sicurezza
- La scelta dei meccanismi deve derivare da una valutazione del rischio

# Security through obscurity

- È la sicurezza basata sulla speranza che l'attaccante non conosca le nostre difese
  - ◆ è diverso dal “non conoscere la chiave”
- È generalmente considerata debole
  - ◆ nel momento in cui l'informazione esce, la sicurezza è persa
  - ◆ in realtà il “segreto” è noto a molti
  - ◆ manca la peer review, particolarmente in crittografia
- Questo non vuole dire che dobbiamo raccontare a tutti le nostre difese

# Ridondanza e difesa “in profondità”

- Nessun meccanismo è perfetto
- Neanche i meccanismi di sicurezza sono perfetti
- Cosa succede se:
  - ◆ viene scoperto un “baco”
  - ◆ c'è un errore di configurazione
- Le protezioni devono essere ridondanti
- È (apparentemente?) contrario all'efficienza nell'investimento
  - ◆ Spesso è difficile anche da valutarne gli effetti

# Segregazione

- Attività diverse, con diverse criticità e requisiti devono essere separate:
  - ◆ perché dalla compromissione dell'una non derivi la compromissione dell'altra
  - ◆ per ridurre i vincoli sulla progettazione e gestione
- Può essere fatta a diversi livelli:
  - ◆ reti e sistemi: firewall su intranet, vpn...
  - ◆ codice: funzioni separate per gli aspetti di sicurezza
  - ◆ personale: sistemisti con diversi ruoli e “clearance”, credenziali...
  - ◆ ambienti: test, produzione...

# Semplicità

## KISS: keep it simple, stupid

- Le cose complesse sono difficili da rendere sicure
  - ◆ difficili da progettare
  - ◆ difficili da implementare correttamente
  - ◆ difficili da capire/analizzare/monitorare
  - ◆ difficili da verificare
  - ◆ difficili da aggiornare/ modificare

# Valutare le assunzioni sugli altri livelli

- Progettando meccanismi a un certo livello, bisogna valutare quali assunzioni si fanno:
  - ◆ sui livelli superiori
    - ★ es. se qualcuno inserisce dei dati a caso l'applicazione se ne accorge
  - ◆ sui livelli sottostanti
    - ★ es. nessuno riesce ad accedere ai dati sulla nostra linea dedicata

# Fail safe

- Se un meccanismo fallisce, il risultato deve essere maggiore sicurezza e meno funzionalità, non viceversa
  - ◆ es. filtro finale di default deny
- È più “scomodo” ma:
  - ◆ evita che un guasto renda inutili le difese
  - ◆ permette di rilevare immediatamente i guasti
- È conseguenza di meccanismi che abilitano il necessario
- Es. firewall vs. IDS

# Log, monitoraggio, alert

- I meccanismi devono fornire informazioni su tentativi di violazione ed errori
- In generale serve raccogliere più dati per poter effettuare verifiche
- I controlli devono poter essere incrociati fra diversi meccanismi
- Chi può manomettere i dati raccolti?
- Problema tipico: marche temporali

# Input validation

- Non bisogna fare ipotesi sui dati che vengono forniti ai programmi
  - ◆ si devono controllare i dati per verificare che soddisfino i vincoli e la sintassi previsti
- Questo aspetto è particolarmente critico per le applicazioni in rete
  - ◆ chi si connette al nostro server non è detto che usi il nostro client
  - ◆ può generare **qualsiasi** pacchetto/dato voglia

# Flessibilità

- Per i meccanismi di sicurezza è importante offrire flessibilità perché:
  - ◆ la sicurezza si trova sempre ad adeguarsi ad altre scelte
  - ◆ se meccanismi di sicurezza non sono compatibili con le nuove esigenze...
    - ★ vengono disabilitati
    - ★ devono essere riprogettati (e pagati) daccapo

# Diversità

- Utilizzare strumenti/configurazioni inusuali può essere un vantaggio o uno svantaggio
- Vantaggi:
  - ◆ gli attacchi standard possono essere inefficaci (es. quelli degli script kiddies)
  - ◆ le vulnerabilità comuni possono non esserci
  - ◆ l'attaccante è probabilmente meno preparato sul sistema
- Svantaggi
  - ◆ anche le soluzioni comuni possono essere inefficaci
  - ◆ è più difficile (e costoso) trovare le competenze necessarie

# Diversificare

- Diversificare è una nota strategia nella gestione del rischio
- Richiede che gli “investimenti” siano indipendenti
- Richiede anche che non si tratti di una semplice aggiunta di fattori di rischio
  - ◆ Se si sostituiscono due apparati uguali con due diversi, ognuno dei quali è in grado di causare il danno complessivo, non si è diversificato

# Qual è l'architettura migliore?

- Quella che si conosce meglio
- È utile avere i sorgenti e la garanzia di una peer review
  - ◆ il fatto che il codice sia open source non è in sé una garanzia

# Misurare la sicurezza

- Non possiamo “misurare” la riduzione del rischio, ma possiamo misurare altri parametri che ci aiutano a capire quanto sono efficaci le nostre scelte
- Domande:
  - ◆ Sono più sicuro dell'anno scorso?
  - ◆ Ho speso bene i miei soldi?
  - ◆ Come sono messo rispetto ad aziende simili?

# Misurare quanto costa l'insicurezza

- Tempo perso:
  - ◆ Nel ripristino di sistemi danneggiati
  - ◆ Nella gestione di malfunzionamenti
  - ◆ Nell'esame di sospetti incidenti
  - ◆ Nella gestione di incidenti
  - ◆ In danni diretti (spesso unico aspetto considerato)
  - ◆ In correzioni a posteriori (sostituzione o aggiunta di prodotti, fix di codice...)

# Quando si riducono i costi?

- Non è una misura della riduzione del rischio
  - ◆ Manca la componente probabilistica
  - ◆ Aiuta comunque a capire l'efficacia degli investimenti
  - ◆ Adatto a valutare la protezione da eventi frequenti
- Difficilmente può essere scomposta per singoli controlli
  - ◆ Dato che la sicurezza è una sinergia di controlli...
- Lo scenario non è statico
  - ◆ Per l'anno successivo è necessario considerare cosa può essere cambiato

# Altre misure

- Virus rilevati
- Segnalazioni di strumenti interni
- Segnalazioni relative al codice (es. nei controlli di qualità o in test)
- Tempi di applicazione delle patch
- ...