Università degli Studi del Molise
Dipartimento di Scienze Economiche Gestionali e Seciali

Appuntamenti con la cultura

La sicurezza informatica: aspetti multidisciplinari

Il futuro dell'e-security: quali garanzie?

Mario PETRONE

Mercoledí 28 Aprile 2004

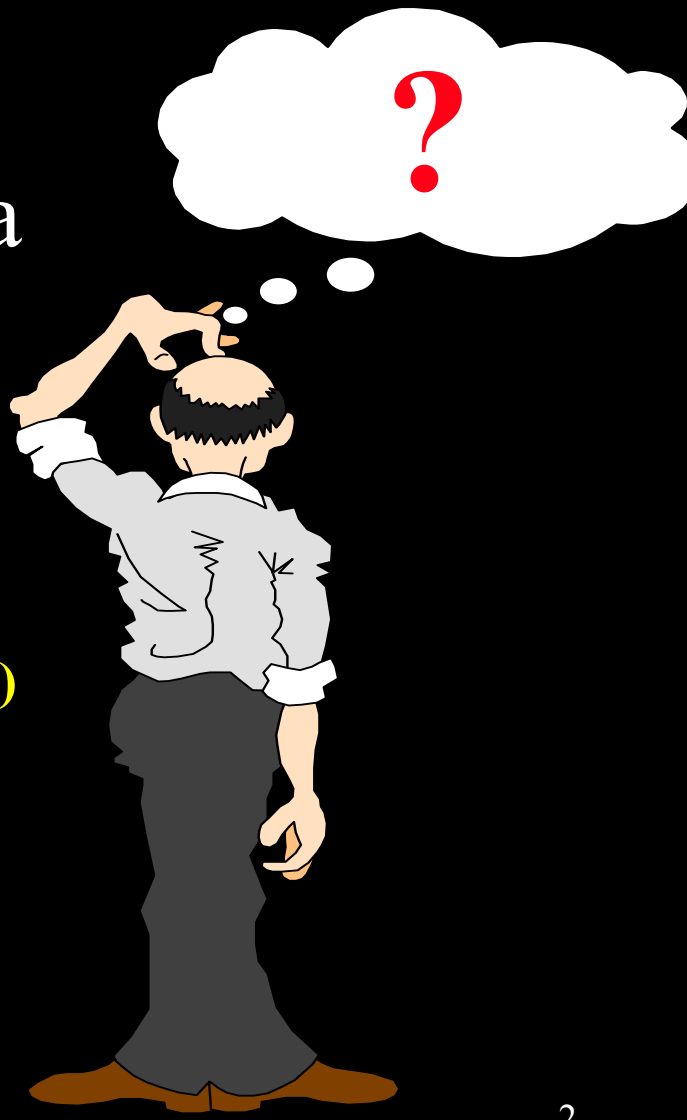
II Edificio Polifunzionale

Via De Sanctis - Campobasso

E-security ➡ quali garanzie?

L'affermazione di Internet ha contribuito a far emergere il problema dell'**insicurezza delle tecnologie ICT**

(Information and Communications Technologies)



Wild Wild Web

- I sistemi sono diventati sempre più complessi e vulnerabili
- Molte aziende non includono la sicurezza nel budget
- Le frodi informatiche sono cresciute velocemente

Questa, come ricorda il Ceo di Rsa, Art Coviello, "è l'età dell'oro per gli hacker, è l'età dell'insicurezza informatica"

La dimensione del problema

- La quasi totalità delle aziende italiane dispone di una rete locale con servizi di e-mail e accesso al web
- L' 84,6% delle aziende dispone di un sito internet
- Il 72,1% delle aziende dispone di una rete intranet
- Il 66,6% delle aziende dichiara di svolgere un'attività in cui viene gestita un'ingente mole di dati personali

Fonte: Il Sole 24 Ore -- ricerca Sirmi per Infosecurity Italia 2003

La dimensione del problema

Se le imprese italiane hanno prestato molta attenzione ai sistemi informativi, non si sono preoccupate altrettanto della sicurezza e riservatezza delle informazioni…

- il 52,8% delle società non è tutelata contro il rischio di essere chiamata a rispondere per reati commessi dal personale continuando a sottovalutare i comportamenti scorretti dei dipendenti
- solo un terzo delle aziende (34,8%) è dotata di una politica e un budget per la sicurezza ICT
- viene trascurata nel 61,7% dei casi la sensibilizzazione del personale sul tema della sicurezza
- solo il 12,9% ha scelto di proteggersi stipulando una polizza assicurativa contro il rischio di attacchi informatici

Fonte: Il Sole 24 Ore -- ricerca Sirmi per Infosecurity Italia 2003

La dimensione del problema

Come viene vissuta dalle aziende la spesa per la sicurezza?

- La sicurezza viene troppo spesso classificata come un costo aggiuntivo, spesso evitabile, non parte integrante dell'investimento in ICT
- L'adeguarsi alle norme di legge è il fattore che guida le scelte nel 51,7% dei casi, segue il timore di subire un attacco (41,3%), la consapevolezza che la sicurezza è un asset aziendale ottiene solo il 37,8% delle risposte

Fonte: Il Sole 24 Ore -- ricerca Sirmi per Infosecurity Italia 2003

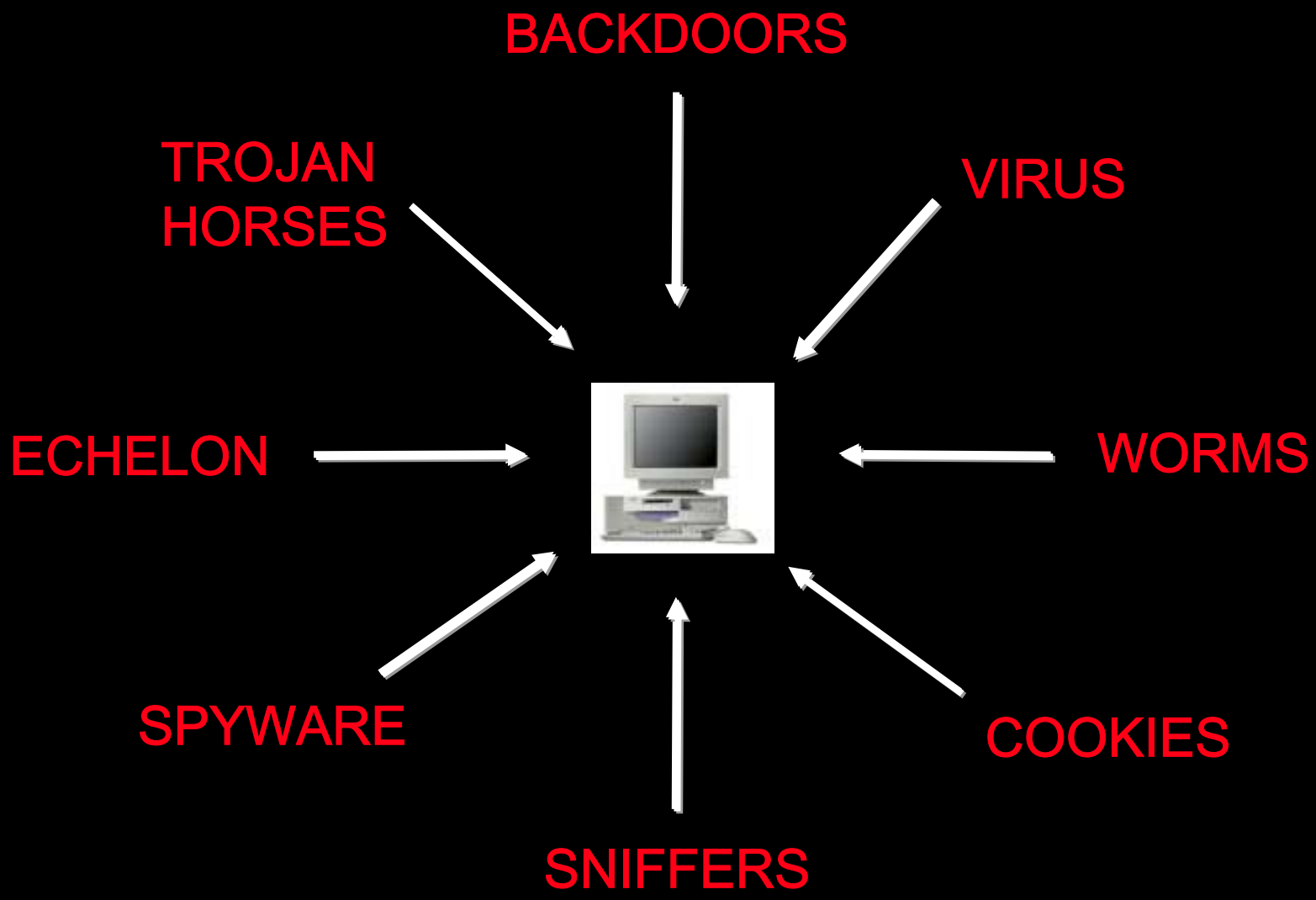
La dimensione del problema

FBI - COMPUTER CRIME AND SECURITY SURVEY: Con quale frequenza avvengono crimini digitali, e quale costo ne consegue per le aziende?

- Su di un campione di 530 soggetti, nel 2003 il 74% afferma di aver avuto uno o più incidenti informatici
- Il 69% dei soggetti dichiara di aver subito attacchi dall'interno, il 67% dichiara di aver subito attacchi dall'esterno
- Solo il 47% è in grado di quantizzare le perdite, ovvero 251 organizzazioni che hanno dichiarato nel 2003 una perdita complessiva $201,797,340, di cui $70,195,900 per furto di informazioni
- Le fonti più citate di attacco o abuso sono i virus (82%) e abuso interno di accesso alle reti (80%)

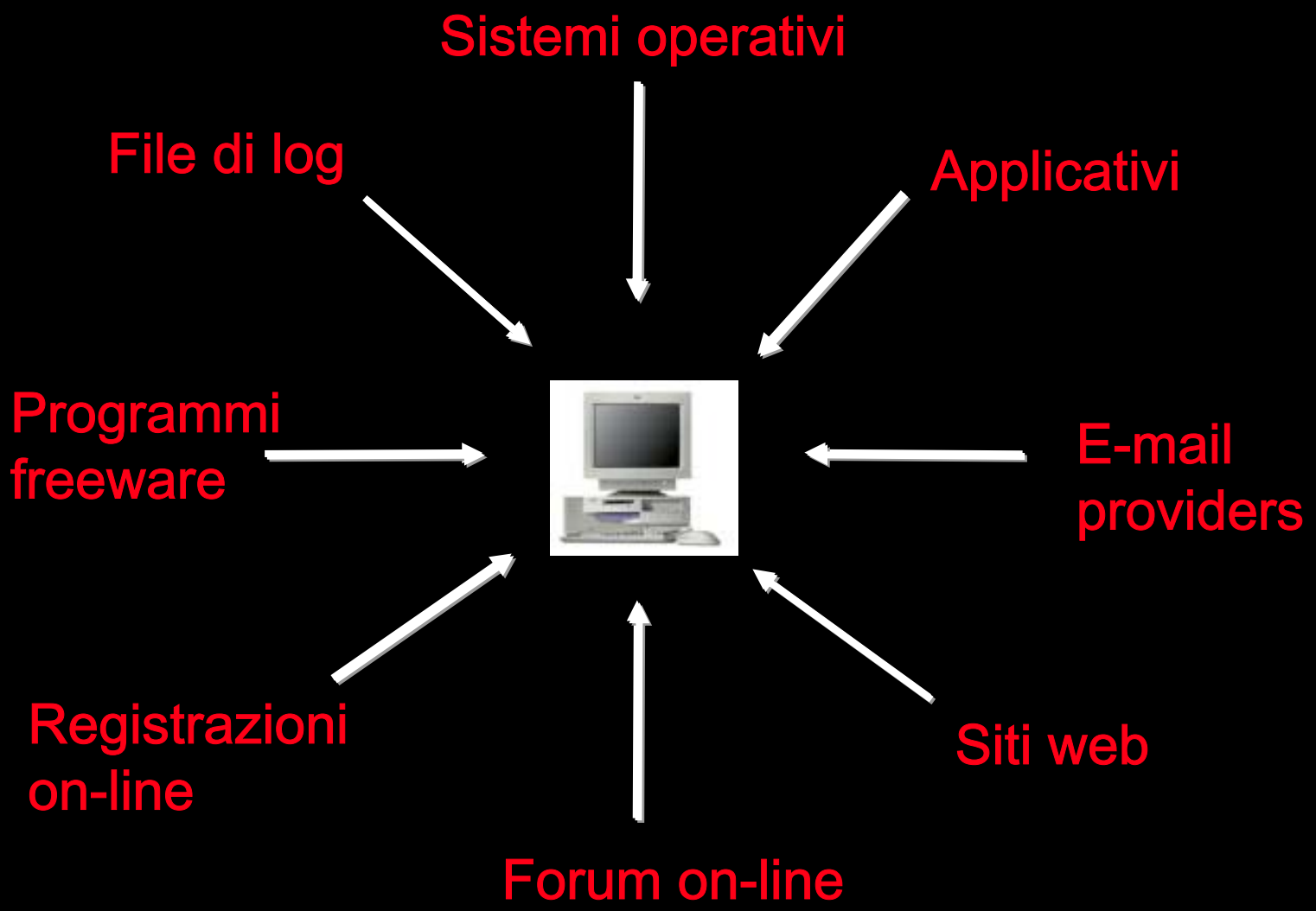
Fonte: 2003 FBI Computer Crime and Security Survey

Lo scenario di riferimento: le minacce più conosciute



Molte sono le minacce alla riservatezza dei dati on-line

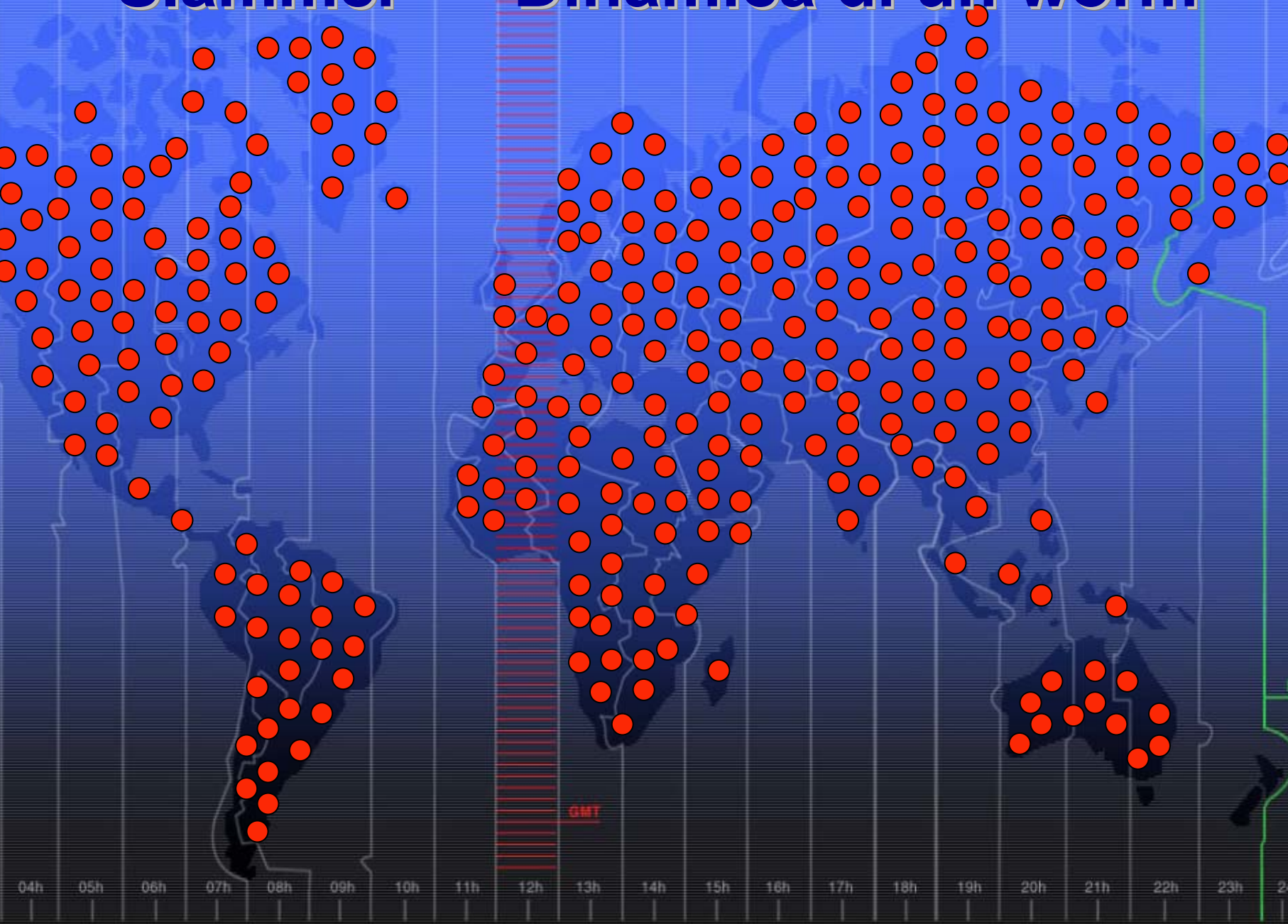
Lo scenario di riferimento: le minacce più insospettabili



... e a molte non è facile pensare

"Slammer" – Dinamica di un worm

"Slammer" – Dinamica di un worm



"Slammer" – Dinamica di un worm

- Raddoppio delle infezioni ogni 8.5 sec
- 75.000 server infettati nei primi 11 min
- Al picco, scanning di 55 milioni di host al sec
- Reti fuori uso, voli cancellati, Bancomat e Postamat fuori uso

L'AFFIDABILITÀ DEL SOFTWARE

Errori presenti nel software o il suo "cattivo" uso determinano gran parte dei problemi di sicurezza

Per capire la natura del fenomeno "sicurezza informatica", e sapersi ad esso rapportare, puo' essere utile capire come un errore presente in un programma possa essere utilizzato per compromettere la sicurezza del sistema su cui opera

L'AFFIDABILITÀ DEL SOFTWARE

Gli errori possono essere stati compiuti in ciascuna delle fasi che costituiscono il ciclo di vita del software: **disegno, progettazione, programmazione, test e installazione**.
Un errore in una di queste fasi si riflette inesorabilmente nella "messa in opera" di un prodotto "vulnerabile", che in particolari circostanze consente a un intrusore di compiere sul sistema attività non autorizzate.

ERRORI DI PROGETTAZIONE (esempio)

Il caso analizzato tratta dell'attacco portato al protocollo ARP (*Address Resolution Protocol*) e noto come ARP Poisoning.

L'attacco è ancora oggi molto diffuso e deriva da una serie di scelte errate commesse in fase di progettazione.

ARP POISONING

Il protocollo ARP è utilizzato in tutte le reti locali che adottano il **protocollo Ethernet** (circa il 98% di tutte le reti locali).
Tale protocollo prevede che tutti gli *host* della LAN siano identificati attraverso un indirizzo numerico di 48 bit noto anche come **MAC *address***. Le informazioni che i vari host di una LAN devono trasmettersi sono racchiuse in uno o più pacchetti, contenenti il MAC address del destinatario e inviati sulla rete.

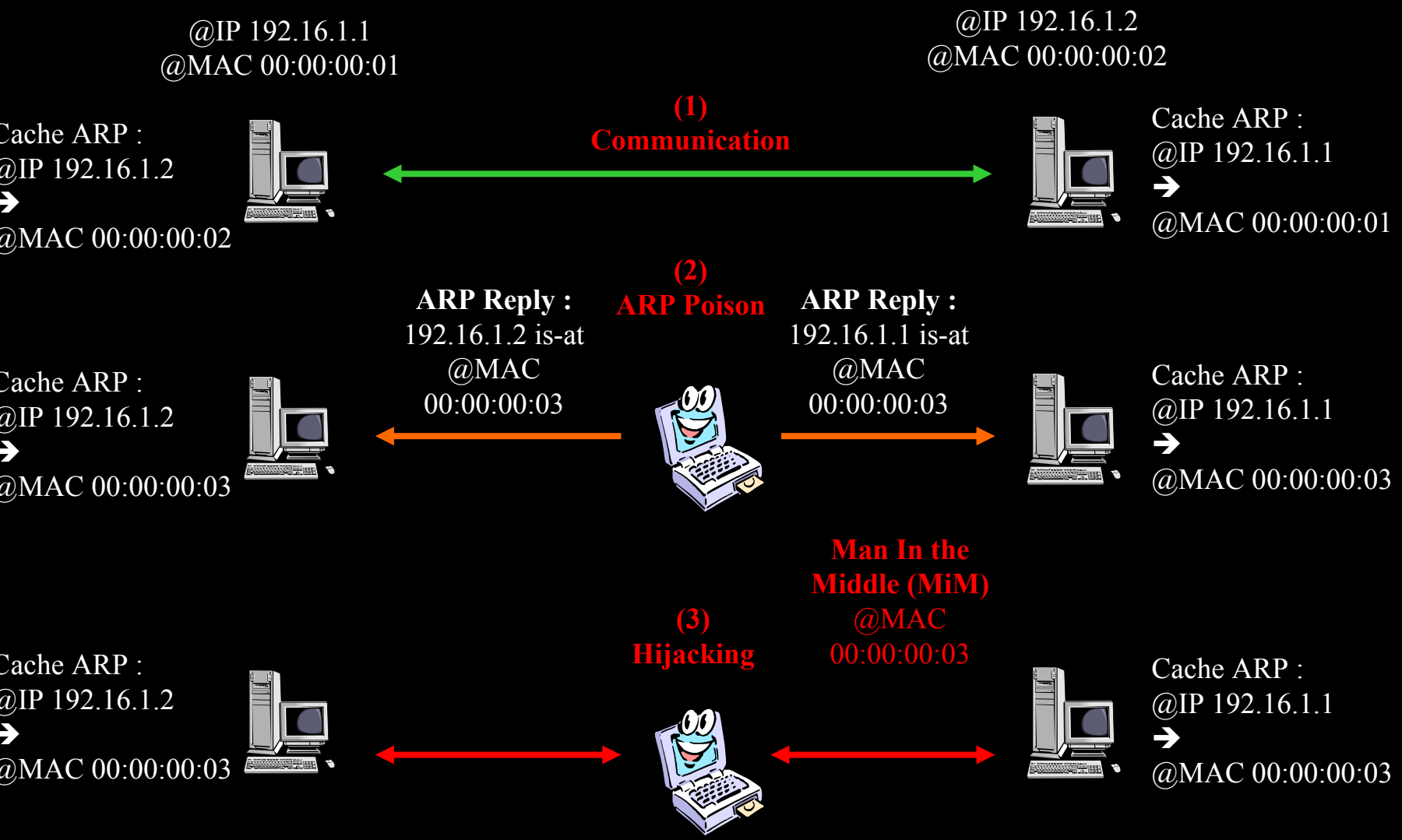
ARP POISONING

Il MAC address non deve essere confuso con **l'indirizzo IP**, che serve, invece, per identificare un host sul una rete Internet. Un indirizzo IP è un numero di 32 bit, che viene espresso come una quadrupla di numeri compresi tra 0 e 255.

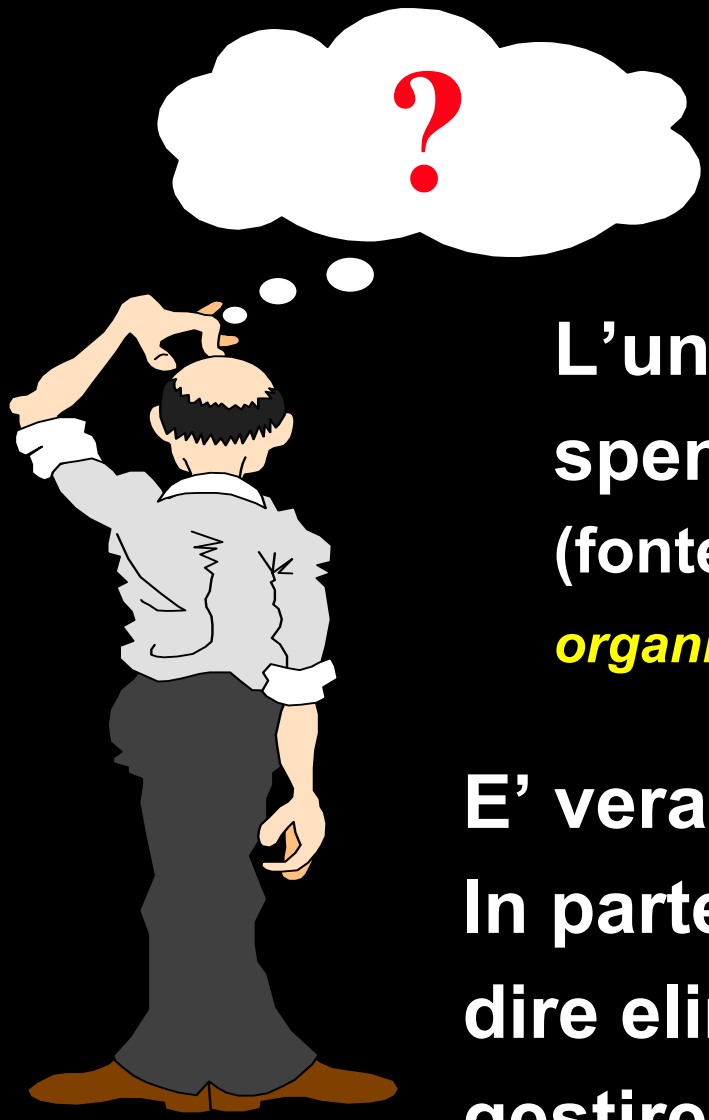
In genere, il MAC address di un host non è noto, ma è noto solo il suo indirizzo IP (Internet Protocol) o indirizzo simbolico.

È il protocollo ARP che nell'ambito di una LAN si preoccupa, dato l'indirizzo simbolico di un host, di individuarne il corrispondente MAC address costruendo una tabella di corrispondenza tra MAC address e indirizzo IP (**ARP cache**).

ARP POISONING



Alcune riflessioni …



La sicurezza: sogno costoso comunque irraggiungibile?

L'unico computer sicuro è quello spento con i cavi staccati.
(fonte: *i pessimisti presenti alla conferenza organizzata a San Francisco da Rsa*)

E' veramente così?
In parte sì, perché sicurezza non vuol dire eliminare il rischio ma saperlo gestire.

Gestione della sicurezza

"***Quello che manca non sono le tecnologie, ma il loro mix equilibrato e le politiche di implementazione, l'analisi dei rischi, la nascita di standard condivisi nel settore***".
(fonte: Michael Rassumussen, responsabile dell'area information security di Forrester Research)

Gestione della sicurezza

CONSAPEVOLEZZA

Le variabili che influiscono sia qualitativamente che quantitativamente sul rischio informatico sono molteplici ed in continuo mutamento, interne ed esterne all'azienda. Diventa impossibile acquistare una soluzione definitiva per la sicurezza

METODO

Non un costo per la sicurezza ma un investimento continuativo per una gestione costante ed integrata della sicurezza informatica al fine di renderla e mantenerla adeguata alle normative civili e penali, alle clausole contrattuali ed alle necessità finanziarie, tecniche e commerciali dell'azienda

Come costruire un sistema di sicurezza?

… seguendo il percorso per la certificazione

BS7799 – ISO/IEC 17799

OBIETTIVI

BS7799-1

Utilizzare un framework condiviso da tutti per…

sviluppare, inplementare e monitorare le modalita' di gestione della sicurezza per…

migliorare la fiducia nelle relazione interaziendali

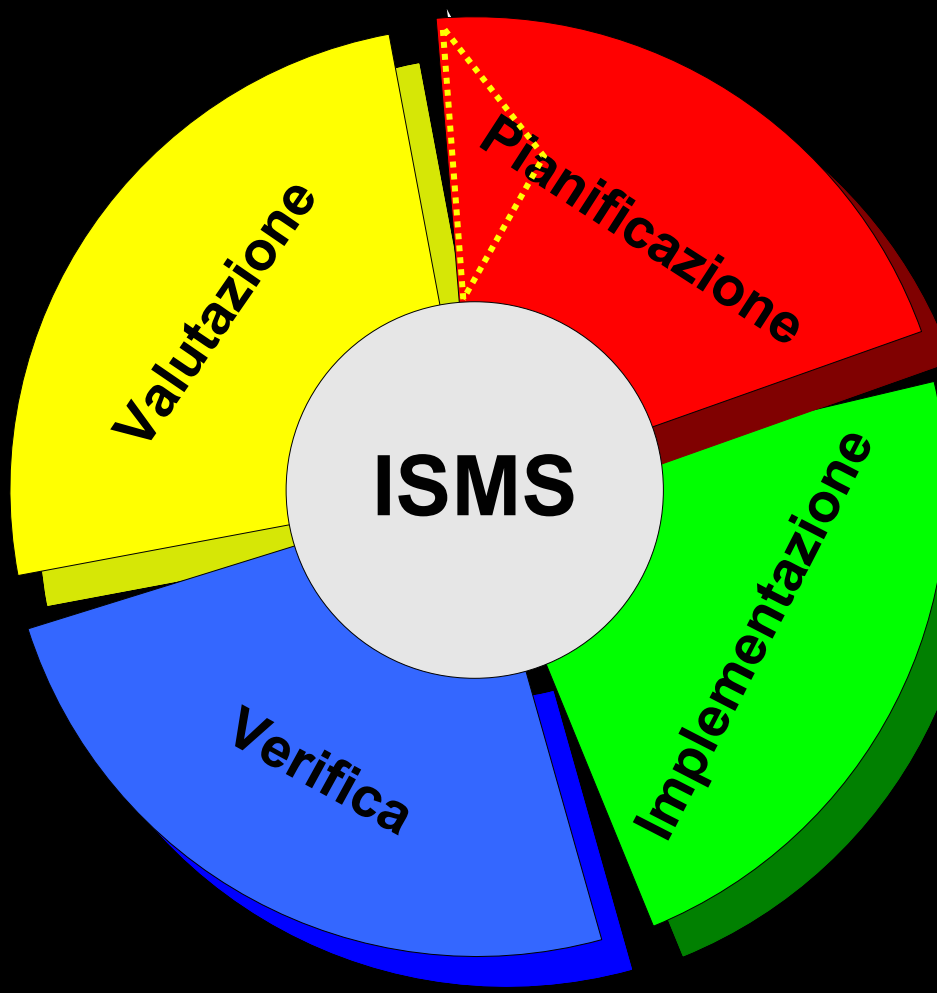
BS7799-2

Indica i requisiti per la certificazione di un…

… sistema di gestione per la sicurezza delle informazione

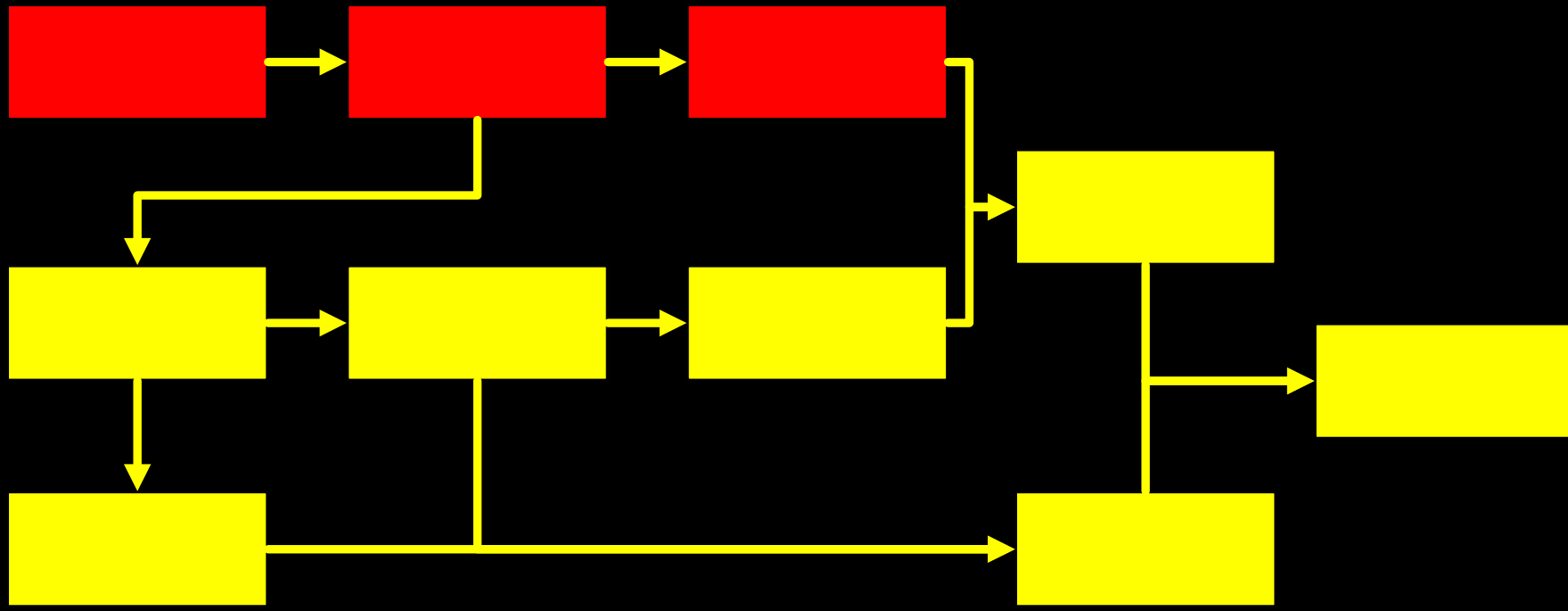
Il percorso di certificazione

Il percorso di certificazione prevede l'esecuzione di 4 fasi sequenziali, con una revisione periodica almeno annuale



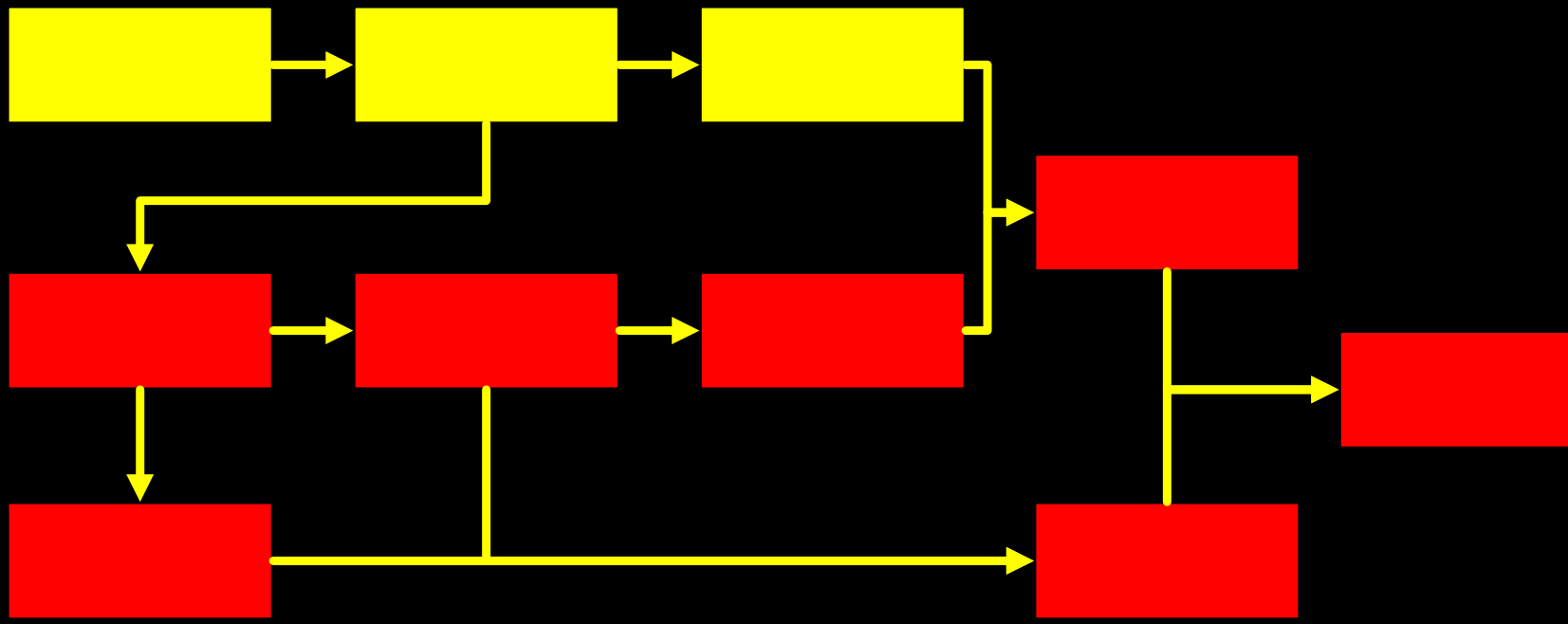
Il percorso di certificazione

L'inventario e la classificazione degli assett permettono all'azienda di comprendere la composizione del proprio effettivo patrimonio "Mission Critical"



Il percorso di certificazione

L'analisi del rischio permette all'azienda di individuare i requisiti operativi, in funzione del valore degli assett, necessari a tutelare e gestire correttamente il proprio patrimonio



$R_t = V_a \times V_m$ Rischio totale = valore asset x valore minacce

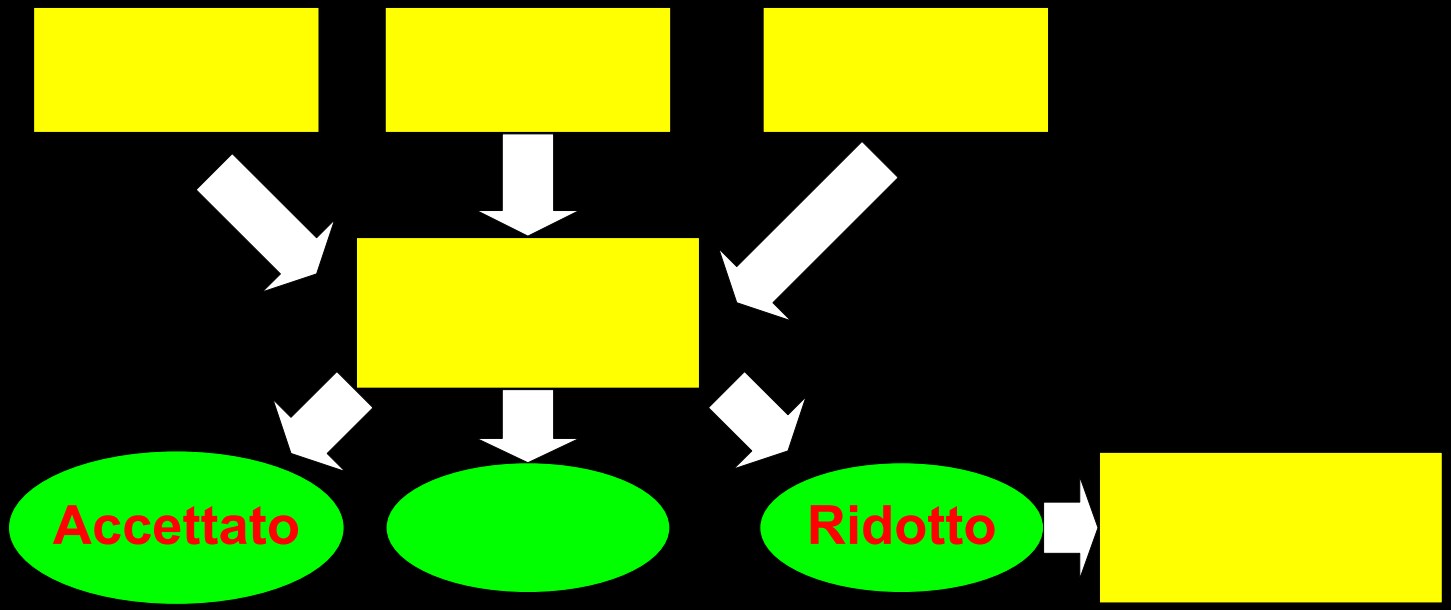
$R_e = R_t - C_e$ Rischio effettivo = rischio totale – controlli esistenti

Il percorso di certificazione

La gestione del rischio permette all'azienda di ottimizzare i propri investimenti in funzione del rapporto costi/benefici

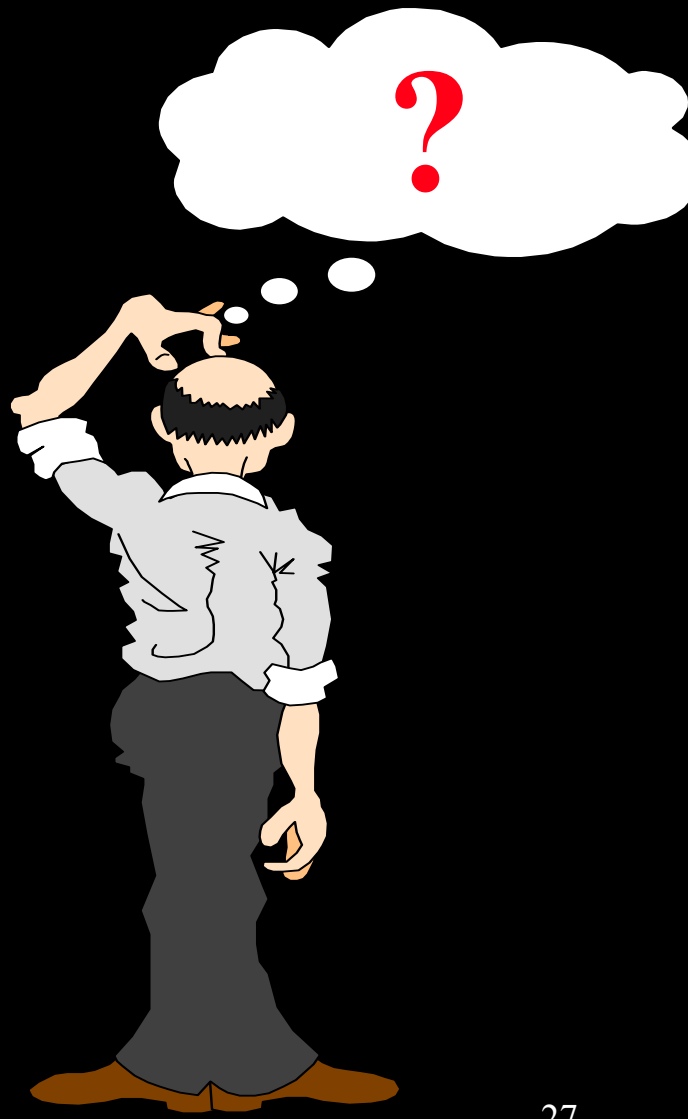
$$R_r = R_a - C_s = R_a$$

Rischio residuo = rischio effettivo – controlli selezionati = Rischio accettato



E-security ➡ quali garanzie?

Conclusione …



Buco nel TCP. Internet a rischio?

Un ricercatore ha scoperto un modo per sfruttare una vecchia debolezza del protocollo TCP che, secondo un rapporto pubblicato dal Governo inglese, rappresenta una concreta minaccia alla stabilità dell'intera Internet.

22/04/04 - News - Londra - Il National Infrastructure Security Co-ordination Centre (NISCC) inglese sta in questi giorni lanciando l'allarme su di una vulnerabilità potenzialmente grave che affligge uno dei protocolli di comunicazione su cui poggia l'infrastruttura di Internet: il **Transmission Control Protocol** (TCP).