Scuola Universitaria Professionale della Svizzera Italiana

SUPSI

Dipartimento Tecnologie Innovative

Sicurezza informatica in ambito aziendale

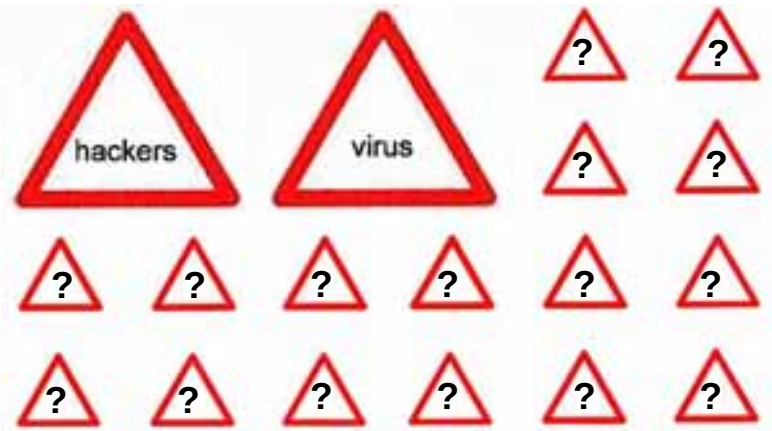
Silvano Marioni, CISSP

Lugano, 23 ottobre 2003

SUPSI

I rischi nel mondo reale

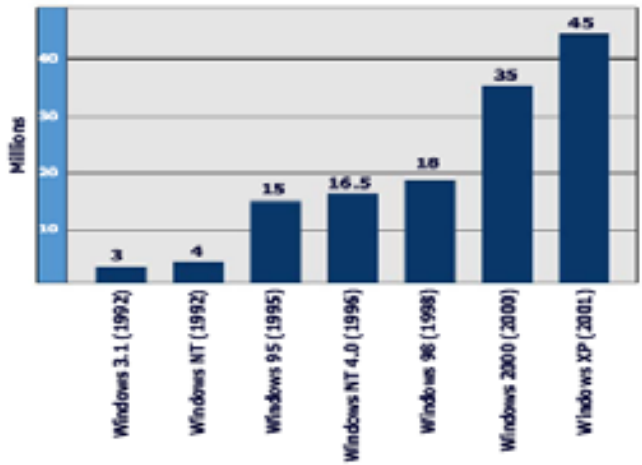
I rischi nel mondo virtuale



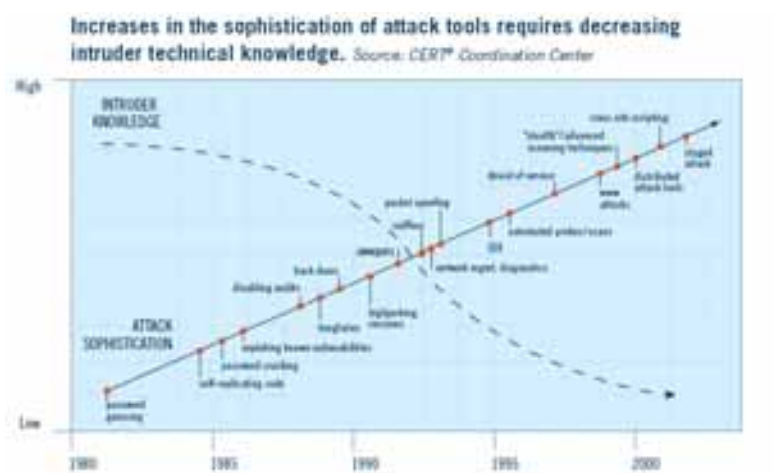
Internet e le nuove sfide alla sicurezza

- I sistemi sono sempre più complessi e difficili da capire
- Assistiamo a una banalizzazione degli aspetti tecnici ed etici
- C’è una mancanza di consapevolezza dei rischi di una società virtuale

Sistemi sempre più complessi



Banalizzazione tecnica e etica

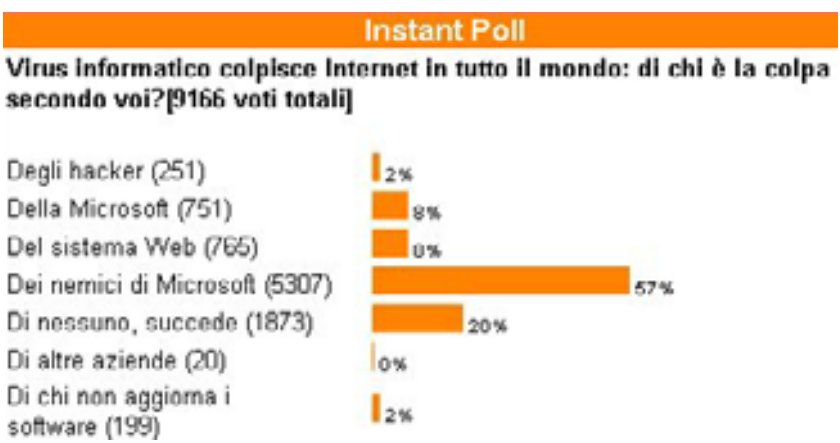


Mancanza di consapevolezza

Attacco Worm Slammer

- Obiettivo: server con software MS SQL Server
- Tempi: diffusione raddoppiata in 8.7 secondi
- Server colpiti: circa 75'000 (in 10 minuti sono stati colpiti il 90% dei server vulnerabili)
- Danni stimati: circa 1 miliardo di dollari
- Correzzione della vulnerabilità: da 6 mesi, erano disponibilità dei patch software per proteggersi dall'attacco

Mancanza di consapevolezza



La Stampa – 28 gennaio 2003

Cosa centra tutto questo con le aziende?

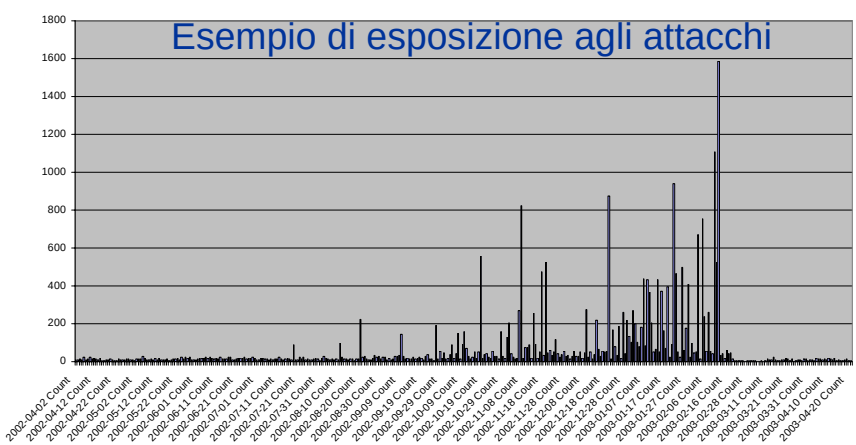
Utilizziamo Internet senza problemi!

- Non c’è nessun motivo per attaccarci
- Usiamo gli ultimi prodotti tecnologici
- Il firewall ci protegge da Internet
- I tecnici gestiscono bene la sicurezza
- L'importante è che riusciamo a lavorare

Non c’è nessun motivo per attaccarci

- Siamo sicuri che non sia mai successo?
- Esiste un monitoraggio degli eventuali attacchi?
- E’ stata fatta una verifica dell’integrità del sistema?
- Siamo sicuri che i nostri computer non siano stati trasformati in « zombie »?

Non c’è nessun motivo per attaccarci



SUPSI-DTI

Usiamo gli ultimi prodotti tecnologici

- Vogliamo essere sempre i primi ad utilizzare le ultime tecnologie?
- I nuovi prodotti soddisfano i nostri requisiti di sicurezza?
- Istalliamo in modo corretto tutto quello che acquistiamo?

Usiamo gli ultimi prodotti tecnologici

Reti wireless a Lugano

Fonte: Stefano Klett 2003

Il firewall ci protegge da Internet

- Abbiamo configurato correttamente le regole del firewall?
- Siamo certi di avere un solo punto di connessione?
- Siamo coscienti che un firewall non blocca tutte le comunicazioni potenzialmente a rischio?
  - Kazaa usa la porta 80
  - Attacchi via mail

Il firewall ci protegge da Internet

```
Microsoft Corporation Security Center [vbercsnhsceuenw-fyfyvf@bulletin.msdn.com]

this is the latest version of security update, the
"October 2003, Cumulative Patch" update which resolves
all known security vulnerabilities affecting
MS Internet Explorer, MS Outlook and MS Outlook Express
as well as three newly discovered vulnerabilities.
Install now to continue keeping your computer secure
from these vulnerabilities, the most serious of which could
allow an attacker to run code on your computer.
This update includes the functionality of all previously released patches.

System requirements: Windows 95/98/Me/2000/NT/XP
This update applies to:
 - MS Internet Explorer, version 4.01 and later
 - MS Outlook, version 8.00 and later
 - MS Outlook Express, version 4.01 and later

Recommendation: Customers should install the patch at the earliest opportunity.
How to install: Run attached file. Choose Yes on displayed dialog box.
How to use: You don't need to do anything after installing this item.
```

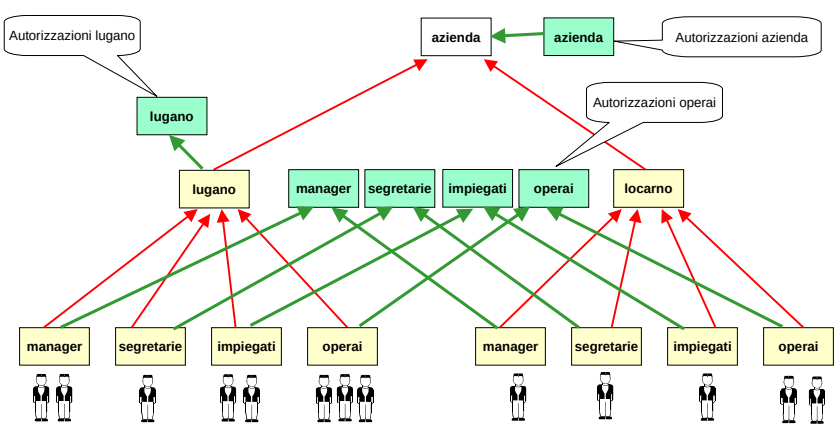
Esempio di social engineering

SUPSI-DTI

I tecnici gestiscono bene la sicurezza

- Gli utenti sono informati e coscienti degli aspetti di sicurezza?
- La direzione si sente responsabile della sicurezza aziendale?
- Abbiamo una visione organizzativa della sicurezza?

I tecnici gestiscono bene la sicurezza



Concetto delle autorizzazioni

L'importante è che riusciamo a lavorare

- Salviamo regolarmente tutti i dati con i backup?
- Proteggiamo i computer portatili e le agende elettroniche?
- Come trattiamo le informazioni elettroniche in entrata e in uscita?
- Siamo conformi alle leggi?

L'importante è che riusciamo a lavorare

- **Art. 2 – Ordinanza sulla tenuta e la conservazione dei libri di commercio**
  - 1. La tenuta dei libri di commercio e il rilevamento dei documenti contabili devono essere conformi ai principi commerciali riconosciuti (contabilità regolare).
  - 2. Se i libri di commercio sono tenuti e conservati su supporto elettronico o in modo analogo e i documenti contabili e la corrispondenza d'affari sono rilevati e conservati su supporto elettronico o in modo analogo, occorre rispettare i principi del trattamento regolare dei dati.

L'importante è che riusciamo a lavorare

- **Art. 100^{quater} - Codice Penale - modifica 21 marzo 2003**
  - Se in un'impresa, nell'esercizio di attività commerciali conformi allo scopo imprenditoriale, è commesso un crimine o un delitto che, per carente organizzazione interna, non può essere ascritto a una persona fisica determinata, il crimine o il delitto è ascritto all'impresa. In questo caso l'impresa è punita con la multa fino a cinque milioni di franchi.

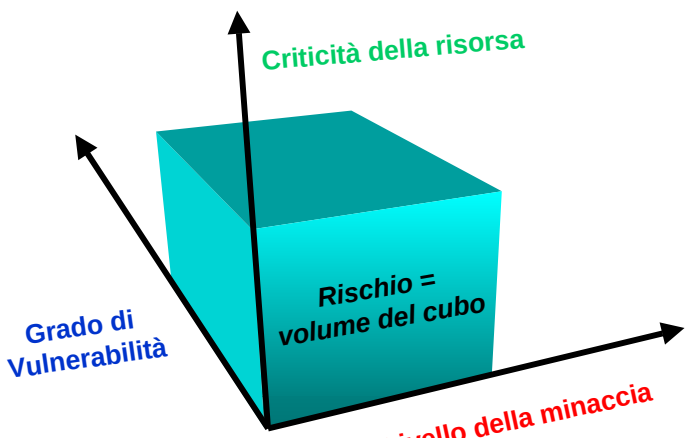
« La sicurezza non concerne la tecnologia ma i rischi e i differenti modi di gestirli.
La sicurezza non è un prodotto ma un processo. »

Bruce Schneier

Definire i requisiti di sicurezza

- Riservatezza
  - Ci sono informazioni riservate in azienda e come sono protette?
- Integrità
  - Quali costi finanziari possono scaturire se le informazioni aziendali sono danneggiate?
- Disponibilità
  - Quale sarebbe la produttività aziendale se i servizi informatici non fossero disponibili?

Valutare i rischi



Adottare una strategia di protezione

- Classificare delle risorse
- Analizzare i rischi
- Definire le politiche di sicurezza
- Progettare le misure di sicurezza
- Sensibilizzare e formare gli utenti

Avviare un progetto di sicurezza

- Analizzare i requisiti
- Progettare le soluzioni
- Implementare
- Gestire e monitorare

Il valore strategico della sicurezza

La sicurezza può diventare un vantaggio competitivo per l'azienda

La SUPSI e la gestione della sicurezza

- La Formazione Continua SUPSI offre i seguenti corsi sul tema della sicurezza:

- 1.12 – La sicurezza informatica in azienda
- 1.15 – La sicurezza dei sistemi e delle reti
- 1.35 – Diritto informatico
- 1.36 – Introduzione alla revisione informatica

« Il sapiente è colui che sa di non sapere »

Socrate