Sicurezza dei Sistemi Informatici
Introduzione

Contenuti

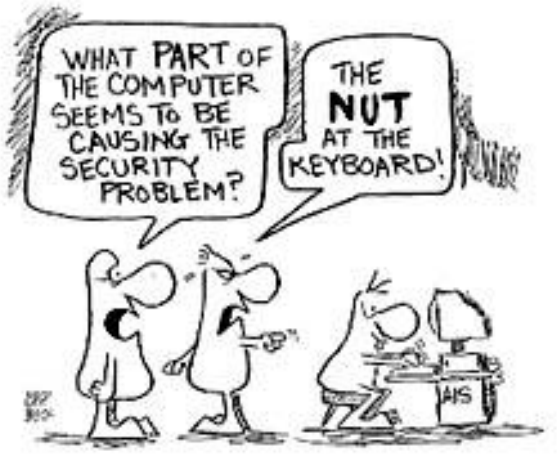
- Minacce: Da cosa deve essere protetto un sistema informatico?
- Danni: Quali sono i danni per l'azienda?
- Risorse: Cosa proteggere?
- Hackers e Crackers: Da chi proteggerlo?
- Obblighi di legge: Cosa impone la legge in materia ?
- Crimini informatici: Che tipo di reati sono previsti per coloro che violano un sistema informatico?

Minacce : esempi

- Accesso ad informazioni riservate: numeri di carte di credito, dati personali, segreti industriali, comunicazioni interne aziendali,…
- Frode: alterazione di un sistema informatico o modifica di dati e programmi al fine di ricavarne profitto con danno altrui.
- Sabotaggio
- Errori del personale
- Problemi «tecnici»: guasti hardware , blackout, bug software
- Calamità naturali

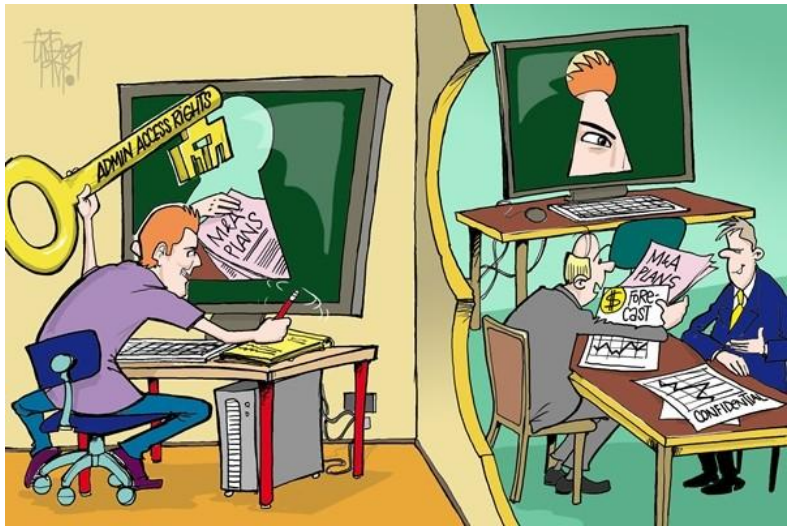
Minacce : Accidentali/Involontarie

- Calamità naturali (incendi, terremoti, alluvioni,…)
- Guasti hardware, bug software, interruzione alimentazione, sbalzi di tensione,…
- Errori e comportamenti incauti del personale



Minacce : Intenzionali

condotte da persone che hanno come preciso obiettivo, quello di attaccare una specifica azienda per causarle danno



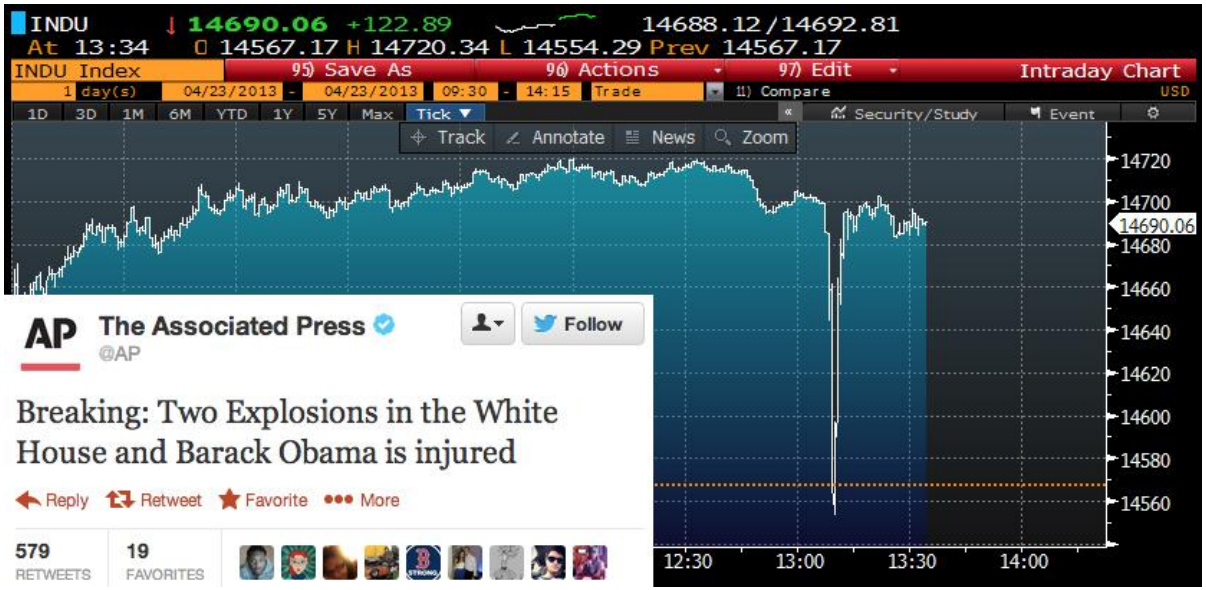
Finalità:

- Accesso ad informazioni riservate
- Spionaggio industriale
- Vendetta a scopi personali
- Diffamazione pubblica di un’azienda
- Furto
- Truffa
- Estorsione di denaro…

Furto di informazioni riservate

Inchiesta repubblica

Frodi...


INDU 14690.06 +122.89 14688.12/14692.81
At 13:34 O 14567.17 H 14720.34 L 14554.29 Prev 14567.17
INDU Index 95) Save As 96) Actions 97) Edit Intraday Chart
1 day(s) 04/23/2013 - 04/23/2013 09:30 - 14:15 Trade 11) Compare USD
1D 3D 1M 6M YTD 1Y 5Y Max Tick
Track Annotate News Zoom
Security/Study Event
14720
14700
14690.06
14680
14660
14640
14620
14600
14580
14560
12:30
13:00
13:30
14:00
AP
The Associated Press
@AP
Follow
Breaking: Two Explosions in the White House and Barack Obama is injured
Reply Retweet Favorite More
579 RETWEETS
19 FAVORITES

Danni

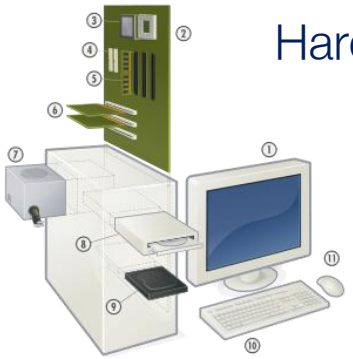
- Perdita di fiducia dei clienti
- Blocco di operazioni critiche
- Accesso ad informazioni riservate
- **Denial of Service** (Interruzione di servizio)
- Impossibilità ad adempiere obblighi contrattuali
- Perdita di informazioni
- Compromissione integrità dei dati

$1.600 Miliardi - Stima a livello mondiale della perdita relativa all'anno 2000 dovuta al fermo macchina risultante da intrusioni e da diffusione di virus.

In sintesi...


Minacce
Accesso ad informazioni riservate
Blackout
Errori di utilizzo
Sabotaggio
malfunzionamenti Hardware/Software
Frodi
Operatività Aziendale
Interruzione servizio
Perdita della fiducia dei clienti
Compromissione integrità dei dati
Accesso ad informazioni riservate
Impossibilità di adempiere ad obblighi contrattuali
Blocco di operazioni critiche
Danni
Perdita di informazioni

Cosa proteggere?



Hardware

Software

Dati e supporti di memorizzazione

Accesso ai Locali

Reti

Hackers e Crackers

Hackers

Crackers

Hackers e Crackers

Hacker - colui che entra nei sistemi altrui per divertimento, studio, curiosità o semplicemente per dimostrare di essere in grado di farlo. Nella maggior parte dei casi l'hacker non causa danni al sistema vittima.

Cracker - è colui che viola i sistemi informatici con l'intento di provocare un danno.

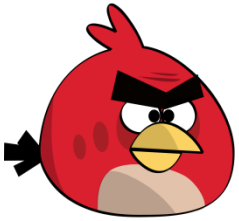
Per approfondire…

storia_hacker , storia_hacker2 , storia_hacker3

Tipi di hacker , tipi di hacker 2

Outsiders e Insiders

Outsiders - persone esterne all'organizzazione il cui sistema informatico è oggetto dell'attacco

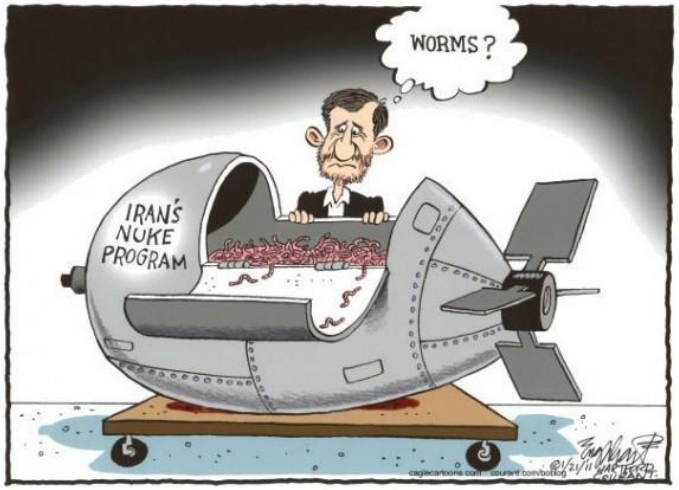


Insiders - persone interne all'organizzazione che hanno accesso al sistema, talvolta si tratta delle stesse persone che hanno partecipato al suo sviluppo o che ne hanno una conoscenza approfondita

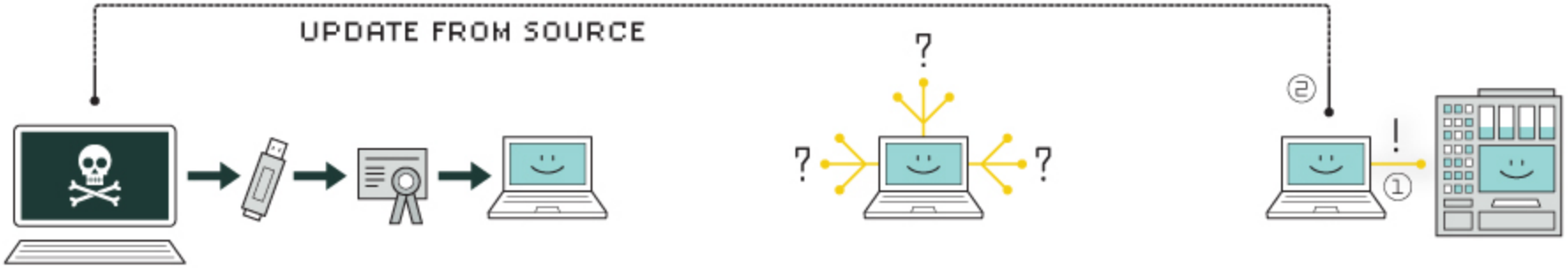
Hackers

Chi sono gli Hackers?

Cyber-War: Stuxnet



HOW STUXNET WORKED



1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Obblighi di legge

Il **codice penale <u>impone</u>** l'adozione di misure di sicurezza atte ad impedire l'introduzione nel sistema informatico da parte di chi non è autorizzato, per…

- Prevenire la **perdita** o la **distruzione** dei dati
- Ridurre il rischio di **accesso non autorizzato**
- Impedire il **trattamento** dei dati **in modi non consentiti**

Crimini informatici

La legge definisce nel **codice penale**:

- Delitto di accesso abusivo: fa riferimento all'accesso abusivo ad un sistema informatico protetto da misure di sicurezza anche se minime.
- Abuso di operatore di sistema: fa riferimento all'abuso di un soggetto con tale qualifica, al fine di compiere attività "illegali".
- Delitto di frode informatica: alterazione di un sistema informatico o modifica di dati e programmi al fine di ricavarne profitto con danno altrui.
- Impedimento o turbamento di un sistema informatico: fa riferimento ad abusi che si possono verificare nelle licenze software o a causa dell'installazione di particolari programmi, tali da alterare la funzionalità di un sistema a favore dei "produttori" di sw.
- Detenzione e diffusione abusiva di codici di accesso: sanziona l'abusiva acquisizione, in qualunque modo, duplicazione e distribuzione, dei mezzi, o dei codici di accesso ad un sistema informatico.