Gestione della Sicurezza di un sistema informativo

Un approccio fenomenologico

(a cura dell'**Ing. Paolo Spagnoletti – CeRSI - Luiss**)

CeRSI: Centro di ricerca sui Sistemi Informativi

LUISS (Libera Università Internazionale degli Studi Sociali) "Guido Carli" is one of the most prestigious Italian private universities, strongly co-operating with the main Italian research centres, industries, and public administrations.

The Centro di Ricerca sui Sistemi Informativi (CeRSI) is in charge of the research, education and advice on computer science and information systems matters.

INDICE DELLA PRESENTAZIONE :

1. Principi della Sicurezza di un Sistema Informativo
2. I diversi approcci disciplinari
3. La prospettiva delle scienze sociali
4. Teorie criminologiche e computer crime
5. Una metodologia per la progettazione di un ISMS
6. Case study
7. Pensiamoci
8. Riferimenti bibliografici e sitografici
9. Varie – Q&A

Five Security Principles

Confidentiality

Integrity

Availability

Non-repudiation

Authentication

Source:HK ITSD

Principles of information security

- confidentiality –
  - prevention of unauthorised disclosure of information
- integrity –
  - prevention of the unauthorised modification of information
- availability –
  - prevention of the unauthorised withholding of information or resources
- Non-repudiation –
  - provide proof of the origin such that the sender cannot deny sending the message, and the recipient cannot deny the receipt of the message.
- Authentication –
  - Checking the identification offered by a counter-party

INDICE DELLA PRESENTAZIONE :

1. Principi della Sicurezza di un Sistema Informativo
2. I diversi approcci disciplinari
3. La prospettiva delle scienze sociali
4. Teorie criminologiche e computer crime
5. Una metodologia per la progettazione di un ISMS
6. Case study
7. Pensiamoci
8. Riferimenti bibliografici e sitografici
9. Varie – Q&A

Different disciplinary approaches
to information and information security

- Engineering
- Computer Science
- Information Systems

Engineering

Process, record, transmit	physical signals
Focus on	physical machines
Theory	Engineering and Physics

Technical Security Solution

Computer Science

Process, record, transmit	structured data
Focus on	virtual machines
Theory	Mathematics and Logic

Rational Logical Security Solution

Information Systems

Process, record, transmit	data with meaning
Focus on	organizations
Theory	Social Sciences

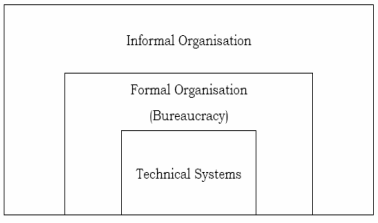
Pragmatic Understanding of security

INDICE DELLA PRESENTAZIONE :

1. Principi della Sicurezza di un Sistema Informativo
2. I diversi approcci disciplinari
3. La prospettiva delle scienze sociali
4. Teorie criminologiche e computer crime
5. Una metodologia per la progettazione di un ISMS
6. Case study
7. Pensiamoci
8. Riferimenti bibliografici e sitografici
9. Varie – Q&A

Information Systems: Basi teoriche

- organisational environment as constituted of the technical, formal and informal (TFI) parts which are in a state of continuous interaction (Liebenau and Backhouse '90)



"Informal norms are fundamental, because formal norms can only operate by virtue of the informal norms needed to interpret them, while technical norms can play no role…unless embedded within a system of formal norm."

Stamper, R. *et al* (2000) 'Understanding the roles of signs and norms in organisations – a semiotic approach to information systems design', Behaviour & Information Technology, 19, 1: 15-27.

Criticità

- Crescita della complessità organizzativa: reti distribuite geograficamente, interoperabilità interorganizzativa, condivisione e gestione delle informazioni, fiducia
- Nuovo concetto di sicurezza: non solo c*omputer*, ma aspetti comportamentali e umani
- Nuove forme di soluzioni: no ad approcci generali e a breve termine, ma coerenza e strategia

Scienze sociali e Sicurezza dei SI

- holistic and social science perspective to IS Security management
- interpretive and phenomenological approach to computer incidents
- focus on human behaviour
- new methods to prevent, detect and investigate computer crimes based on SCP
- ISMS standards as methods to manage the human-system interaction

INDICE DELLA PRESENTAZIONE :

1. Principi della Sicurezza di un Sistema Informativo
2. I diversi approcci disciplinari
3. La prospettiva delle scienze sociali
4. Teorie criminologiche e computer crime
5. Una metodologia per la progettazione di un ISMS
6. Case study
7. Pensiamoci
8. Riferimenti bibliografici e sitografici
9. Varie – Q&A

Cybercrime

sistema informatico:

- obiettivo del crimine (attacchi alla conf, int, e disp, crime against computers)
- repository di informazioni utilizzate o generate nel commettere un crimine (sistema passivo di memorizzazione, computer assisted crime)
- strumento che consente di commettere un crimine (strum. di comunicazione per cybercrime, computer mediated crime)

cybercrime: crimine che lascia tracce digitali (Casey)

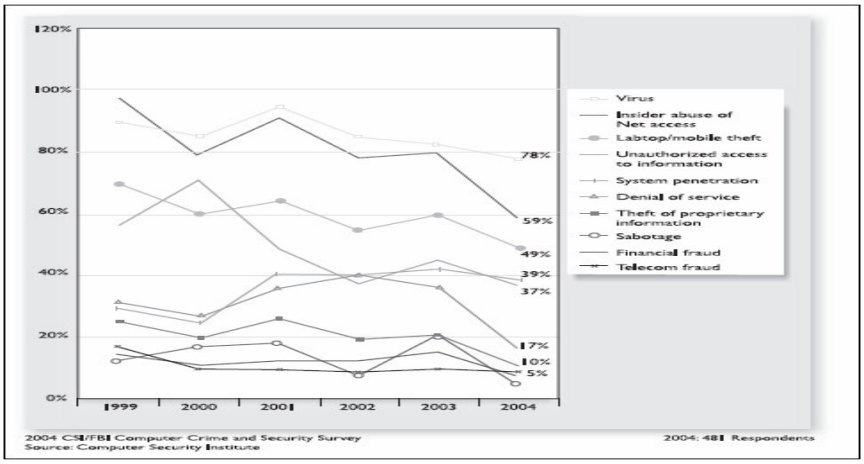
Computer Abuse

"any incident *associated* with computer technology in which a victim suffered or could have suffered loss and a perpetrator by intention made or could have made gain"- Parker, 1976

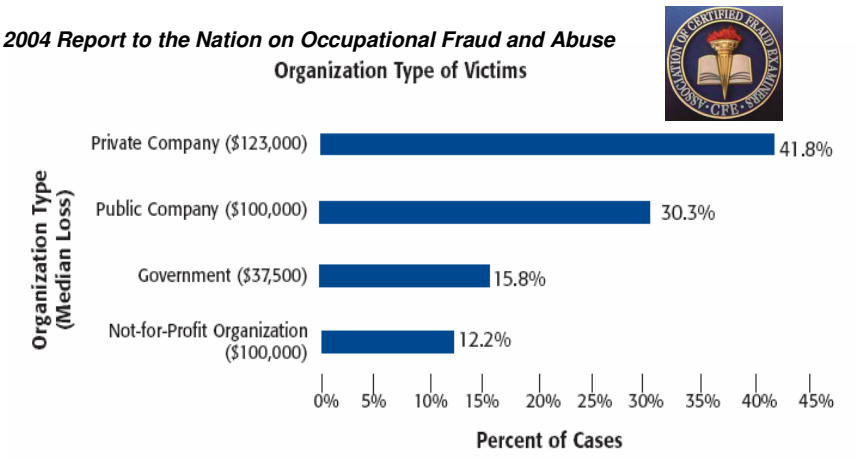
- Hacking
- Virus
- Illegal physical access
- Abuse of privileges

- **Drift**: related on the unpredictable behaviour of actors involved and on the openness of technology. The outcome of tactics, ruses and improvisations (**Ciborra 2000**)
- we consider IS security problems as an emergent property of reflexive interaction between a system and its context, instead of considering them as a consequence of a system's function (**Dhillon 1997**)

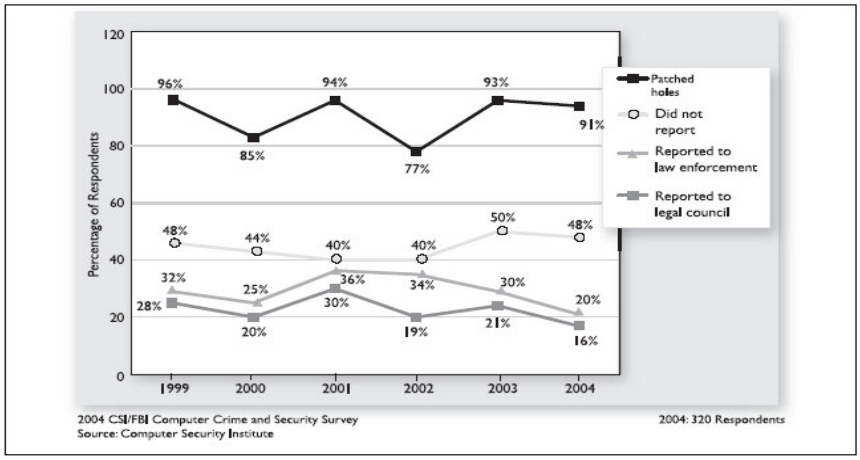
Origine degli attacchi



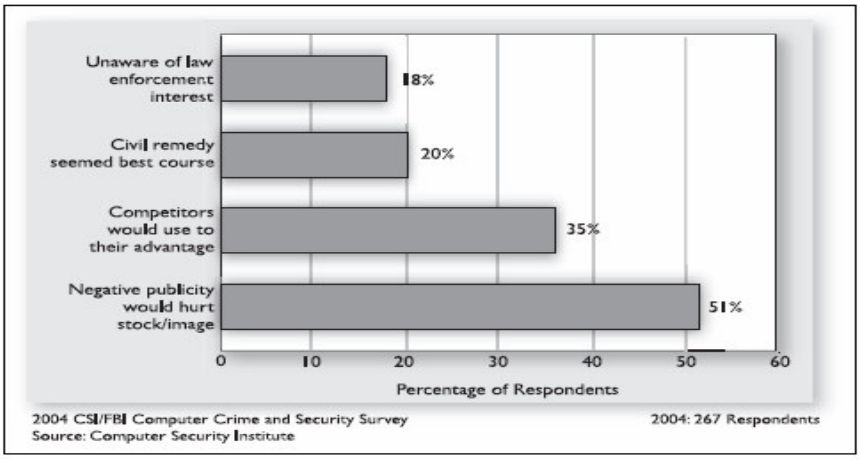
Danni economici: frodi interne



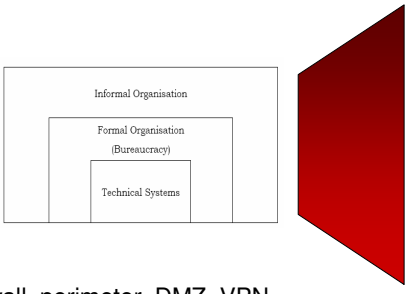
Azioni intraprese



Ragioni organizzative



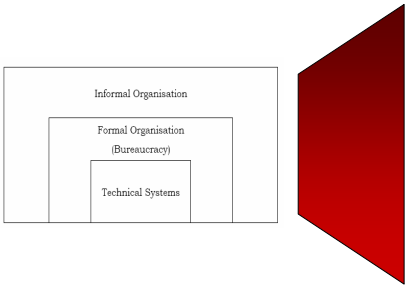
Approccio olistico alla gestione della Sicurezza dei SI



Appropriate Security Technology

- firewall, perimeter, DMZ, VPN, vulnerability test, OSSTM, Disaster Recovery Institute, CoBIT, etc..

Approccio olistico alla gestione della Sicurezza dei SI

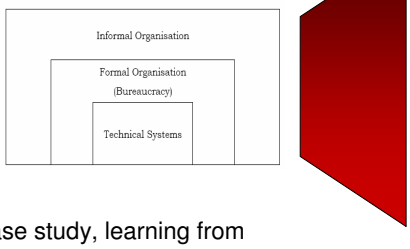


Appropriate Security Policy and rules

- ISMS standards, ISO 27000 ex BS7799, analisi rischio OCTAVE, CoBIT, ITIL, etc..

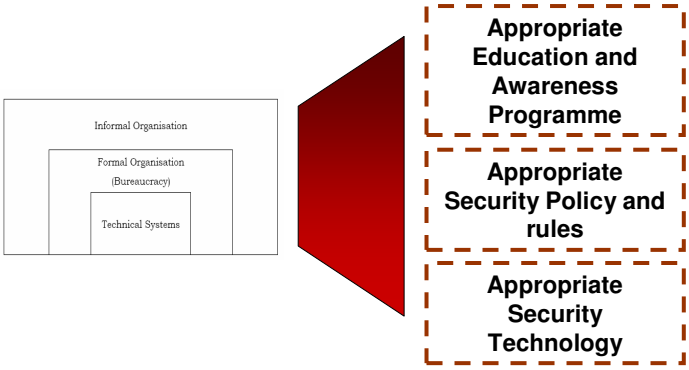
Approccio olistico alla gestione della Sicurezza dei SI

Appropriate Education and Awareness Programme



- case study, learning from incidents, stakeholder analysis, games, education, etc..

Approccio olistico alla gestione della Sicurezza dei SI



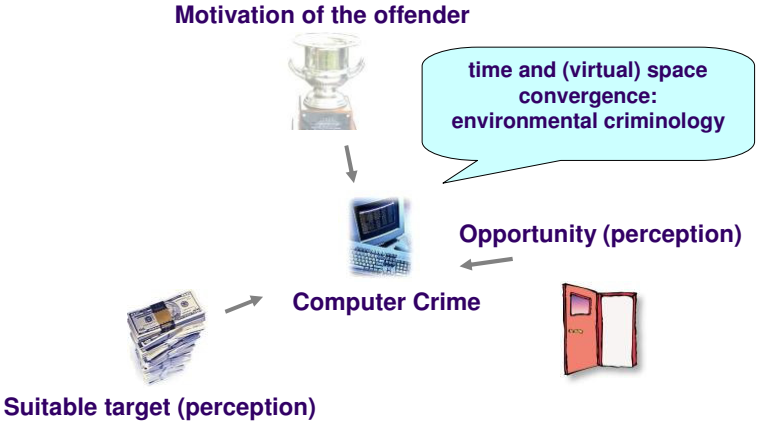
Teorie criminologiche e crimini informatici: SCP

- “crime results partly from the opportunities presented by physical environment”
- Situational Crime Prevention (SCP) refers to a preventive approach that relies upon reducing opportunities for crime
- Routine Activity (Cohen, Lawrence and Felson ‘79), Environmental Criminology (Brantingham and Brantingham ‘91) and Rational Choice Perspective (Cornish, Derek and Clarke ‘86)

Le teorie dell'SCP

- **motivated** offender and a **suitable target** (or victim) converge in space and time in the absence of a **capable guardian**
- the actor may behave "rationally" according to his **perceptions** of the world and situation around him, and these perceptions may or may not be accurate
- "Environmental criminology" studies the locational dimension of crime. This theory is based on the analysis of the offender decision making process and the spatial and temporal variation in crime patterns

SCP e crimini informatici



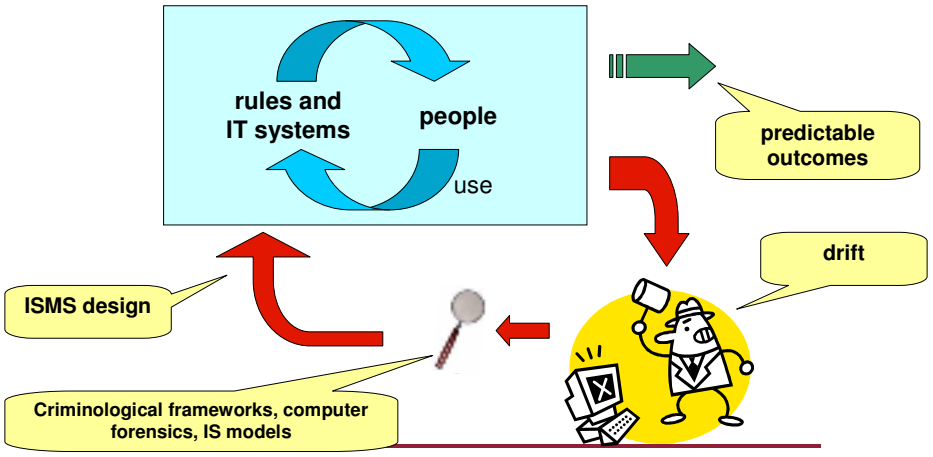
INDICE DELLA PRESENTAZIONE :

1. Principi della Sicurezza di un Sistema Informativo
2. I diversi approcci disciplinari
3. La prospettiva delle scienze sociali
4. Teorie criminologiche e computer crime
5. Una metodologia per la progettazione di un ISMS
6. Case study
7. Pensiamoci
8. Riferimenti bibliografici e sitografici
9. Varie – Q&A

Obiettivi della ricerca

- comprensione dei fenomeni mediante l'adozione di framework teorici validati nel più ampio contesto della criminologia
- feedback dei risultati delle analisi nella fase di progettazione di specifiche misure di prevenzione nell'ambito del sistema di gestione della sicurezza
- riduzione dei computer crimes mediante lo studio di contromisure a tutti i livelli del modello TFI

Il modello proposto



Il framework

INCREASING THE EFFORT	*INCREASING THE RISKS*	*REDUCING THE REWARDS*
Target Hardening	Entry/Exit Screening	Target Removal
Access Control	Formal Surveillance	Identifying Property
Deflecting Offenders	Surveillance by Employees	Removing Inducements
Controlling Facilitators	Natural Surveillance	Rule Setting

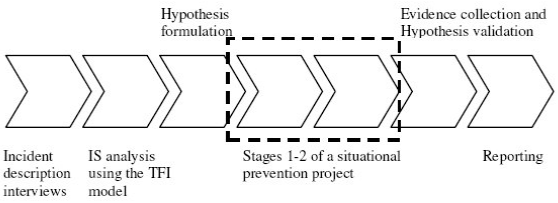
Research agenda:
to develop, for each technique listed in the previous table, a list of technical mechanisms, formal rules and/or informal actions aimed at achieving the specific objective in the IS field. This set of techniques is in-exhaustive and can be upgraded using empiric studies on computer related crimes

La metodologia

- underpinning theories: based on the TFI model and on the SCP framework described above
- Purpose: to understand incidents better and to improve the ability in preventing and detecting them, using an holistic approach in the analysis of computer crimes and abuses
- tools, techniques and procedures belonging to computer and network forensic tradition with analytical frameworks drawn on social and criminological theories

Dettagli della metodologia

1. **description of incident and of organisational environment, performed through an interview to different stakeholders;**
2. **detailed analysis of the Information System, using the TFI model in order to classify the different levels. In this stage technical and procedural documentation will be collected and analysed;**
3. **hypothesis formulation based on acquired information;**
4. **collection of data about the nature and dimensions of the specific crime problem through a literature review and other information sources;**
5. **analysis of situational conditions that permit or facilitate the commission of the crimes in question based on the outcomes of stages 2 and 4;**
6. **evidence collection through computer and network forensic techniques and tools and validation of formulated hypothesis;**
7. **generation of a detailed report that describe the entire investigation process and the specific environment conditions and "facilitators", using the TFI model and the SCP framework**



INDICE DELLA PRESENTAZIONE :

1. Principi della Sicurezza di un Sistema Informativo
2. I diversi approcci disciplinari
3. La prospettiva delle scienze sociali
4. Teorie criminologiche e computer crime
5. Una metodologia per la progettazione di un ISMS
6. Case study
7. Pensiamoci
8. Riferimenti bibliografici e sitografici
9. Varie – Q&A

Contesto

- conferenza IT
- sistema di revisione dei contributi
- la storia
- il paper…

"Strategic Information Security Management: an analysis of an IT Conference review process" P. Spagnoletti, A. D'Atri – (submitted to ECIS 2006 Conference – November 2005)

Pensiamoci

- l'approccio fenomenologico consente una comprensione degli incidenti di natura informatica ancorata al contesto organizzativo, normativo e tecnico in cui si verificano
- l'utilizzo di metodologie e framework teorici basati su diverse discipline consente la definizione di una vera e propria strategia per la gestione della sicurezza
- approccio top-down alla progettazione delle contromisure
- dalla "social engineering" alle teorie sociali applicate ai sistemi informativi…

Bibliografia

- Ciborra C. and associates (2000): From control to drift: the dynamics of corporate information infastructures, Oxford University Press.
- Clarke, Ronald V. (ed.). 1992. Situational Crime Prevention: Successful Case Studies. Albany, NY: Harrow and Heston.
- Dhillon, G. (2000) Challenges in Managing IS Security in the new Millennium, Chapter 1 of Challenges in Managing Information Security, Idea Group Publishing
- Dhillon, G. and Backhouse J. (2001) Current Directions in IS Security Research: Toward Socio-Organisational Perspectives. Information Systems Journal 11(2): 127-153
- Liebenau and Backhouse (1990) Understanding Information: an Introduction, Macmillan
- Mitnick, K. (2002) The Art of deception. Indianapolis: Wiley Publishing, Inc.
- Willison, R. (2004) Understanding the Offender/Environment Dynamic for Computer Crimes: Assessing the Feasibility of Applying Criminological Theory to the IS Security Context. Proceedings of the 37th Hawaii International Conference on System Sciences – IEEE
- Yin, R. (1981), The Case Study Crisis: Some Answers, Administrative Science Quarterly 26: 58-65