THE ROLE OF THE PRIVATE SECTOR IN FIGHTING CYBERCRIME

Stakeholder Consultation

13 Dec 2011, Port of Spain

Prof. Dr. Marco Gercke

RELEVANCE FOR PRIVATE SECTOR

- Private sector is intensively affected by Cybercrime
- Various attacks: illegal access, illegal data acquisition, data interference, system interference
- Relevance of insider attacks

„DATA INTERFERENCE“

DATA INTERFERENCE

- The term data interference is used to describe a negative interaction with regard to computer data
- Example: Computer virus that deletes information on a hard drive
- A computer virus is a malicious software that is able to replicate itself and infect a computer without the permission of the user in order to carry out operations
- Primary target: Computer data

EXAMPLES

- Relatively harmless virus
- Walker virus: Displays occasionally an animation

Picture removed in print version
Bild zur Druckoptimierung entfernt

Walker Virus

DIGITAL DATA

- One explanation for the emerging importance of digital evidence is the fact that the number of digital documents are intensively increasing
- Costs for storing one MB of data was constantly decreasing during the last decades
- Today it is cheaper to store information digitally than to keep physical copies

ECONOMIC IMPORTANCE

- Extent of economic damages caused by malicious software is controversially discussed
- Statistics do not cover on economic aspects like the time private users do have to spend to protect or reinstall their systems after infection
- Many companies (esp. small and medium size businesses) do not report attacks and costs

Sources: Computer Economics (2007)

DATA BREACHES

ILLEGAL DATA ACQUISITION

- Valuable and secret information are often stored without adequate protection
- Lack of self-protection especially with regard to small businesses and private computer users
- Increasing number of cases
- Very often not criminalized because older regional and international legal frameworks do not contain such provision

Picture removed in print version
Bild zur Druckoptimierung entfernt

KEY-LOGGER

IDENTITY THEFT

- Risks related to the illegal acquisition of data increases with regard to large data bases
- Information that can be obtained by copying such databases can not only be used for criminal purposes but also be sold

Picture removed in print version
Bild zur Druckoptimierung entfernt

SONY

WIKILEAKS

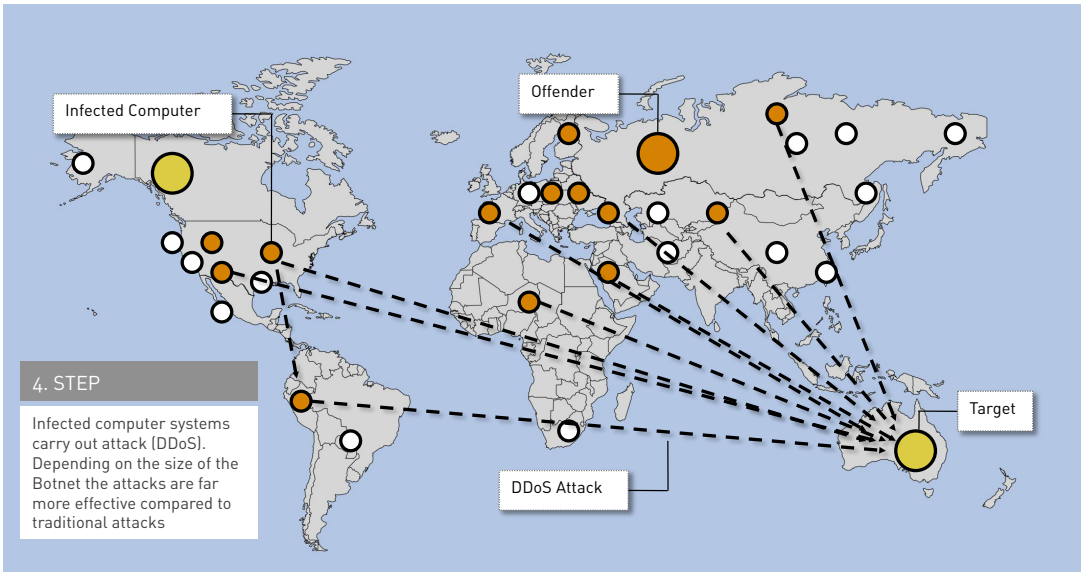
- Information are not only illegally obtained but nowadays often published
- Controversial discussion about the advantages and disadvantages of whistle-blower platforms
- Approaches of major governments to remove the website from the web in 2010 failed
- Often the criminalization of publishing information is limited to state secrets

Picture removed in print version
Bild zur Druckoptimierung entfernt

WIKILEAKS

SYSTEM INTERFERENCE

BOTNET



RESOURCES

- Critical mass is already reached
- Attacks in the context of the Wikileaks discussion highlight that a relatively small number of people can affect large businesses
- This underlines the threat level

CONSIDERATION

- With regard to Internet-related attacks the most powerful resources are not necessary under control of state, military and law enforcement
- Debate about continuing attacks against government computer systems and the inability of states to control secret information published online underlines this

ATTACKS AGAINST CRITICAL INFRASTRUCTURE

STUXNET

- Malicious software targeting Windows operating system
- Using four zero-day exploits

- Discovered in June 2010 by a Belarus-based security company
- Specifically focussing on Supervisory Control And Data Acquisition (SCADA)
- SCADA is for example used in Siemens S7 systems that are used to control critical infrastructure such as power plants

Picture removed in print version
Bild zur Druckoptimierung entfernt

Siemens S7-300

STUXNET

- The malicious software initially spreads through infected USB flash drives
- After the infection the worm also uses other exploits to infect systems within the network

Picture removed in print version
Bild zur Druckoptimierung entfernt

USB DRIVE

PAYLOAD

- Various speculations about the possible payload of the malicious software
- One possible scenario is that it targets the uranium enrichment process in P1 centrifuges as they are used in Irans Nuclear Power Plants

WHAT HAS CHANGED

DEPENDENCE

- Major parts of todays critical infrastructure depend on complex computer-based control systems
- The potential of Stuxnet underlines the risk of attacks against such facilities

Picture removed in print version
Bild zur Druckoptimierung entfernt

CRITICAL INFRASTRUCTURE

INABILITY OF PREVENTION

- In the past one strategy to avoid an infection with malicious software was to disconnect critical infrastructure for the Internet
- However, Stuxnet underlines that such strategy can not prevent an infection
- The malicious software infected computer systems through USB devices

Picture removed in print version
Bild zur Druckoptimierung entfernt

USB DRIVE

„CLOUD COMPUTING“

DECENTRALISED SERVICES

- Availability of high-speed Internet connections and server infrastructure today enables the development of storage concepts that are not anymore based on local but decentralised storage
- „cloud computing“ and „cloud storage“

Picture removed in print version
Bild zur Druckoptimierung entfernt

EXAMPLE: AMAZON CLOUD COMPUTING

DECENTRALIZED SERVICES

- Cloud computing enables the use of complex applications on rather simple devices
- Example: speech recognition services

Picture removed in print version
Bild zur Druckoptimierung entfernt

IPHONE CLOUD

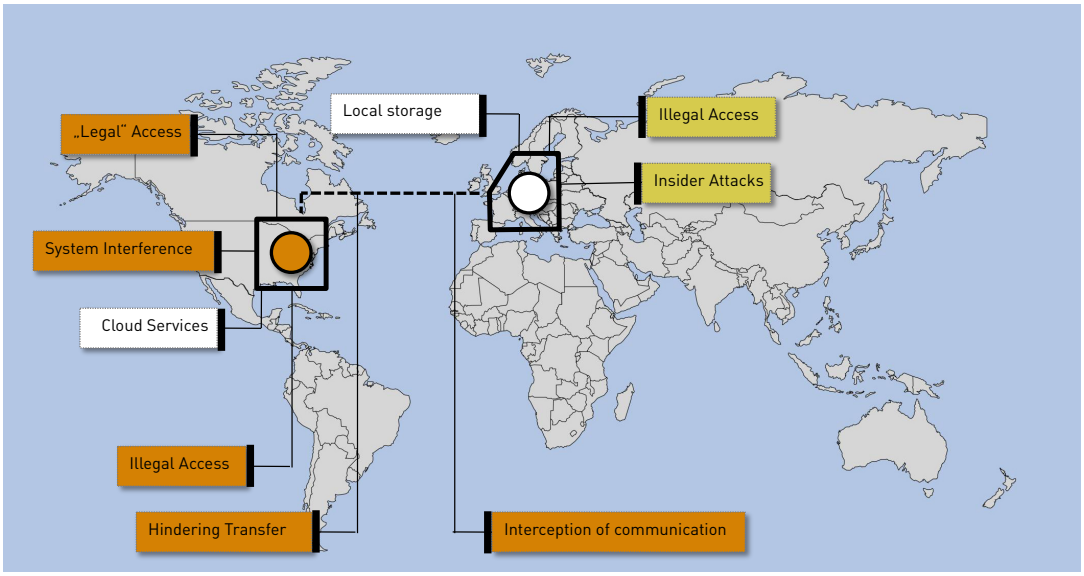
DECENTRALIZED SERVICES

- Examples: Google Maps, Navigation solutions

Picture removed in print version
Bild zur Druckoptimierung entfernt

GOOGLE MAPS

RISKS



OPPORTUNITIES

OPPORTUNITIES

- Availability of computer technology improved the ability of law enforcement to carry out investigations
- DNA sequence analysis and finger print databases are examples for an emerging use of information technology in traditional criminal investigation

Picture removed in print version
Bild zur Druckoptimierung entfernt

FINGERPRINT DATABASE

AUTOMATE

- Software tools are available to automate investigations
- Significant reduction of time for an investigation
- One example is the Software PERKEO that detects child pornography pictures on the basis of hash values

Picture removed in print version
Bild zur Druckoptimierung entfernt

PERKEO

AUTOMATE

- Automation techniques can also be used to identify copyright violations
- One example is file-sharing monitoring where software tools can automatically detect copies of copyright-protected art-work made available
- Another example is the automatic scanning of scientific work (like PhD)

OPPORTUNITIES

- Case example 1: Within an investigation of a murder case law enforcement was unable to identify a murder based on search engine history. They were able to use search engine logs on the suspects computer to identify places he was interested in.

OPPORTUNITIES

- Case example 2: Investigator were able to discover that the suspect was searching for specific terms such as ““undetectable poisons,” “fatal digoxin levels,” “instant poisons,” “toxic insulin levels,” “how to purchase guns illegally,” how to find chloroform,” “fatal insulin doses,” “poisoning deaths,” “where to purchase guns illegally,” “gun laws in PA,” “how to purchase guns in PA,”

Picture removed in print version
Bild zur Druckoptimierung entfernt

PCWORLD

DEVICES PROCESSING DATA

- Devices do often store information that are valuable for traditional investigation
- The user do not necessary have knowledge about such operation
- One example is the iPhone that stored the geo-location of the user and thereby enabled the reconstruction of movements/travel

Picture removed in print version
Bild zur Druckoptimierung entfernt

EXAMPLE: AMAZON CLOUD COMPUTING

TRACES

- “Nobody knows you are a dog” ?
- Internet users leave traces
- Access-Provider for example often for a certain period of time keep records to whom a dynamic IP-address was assigned
- Data retention obligations even increase the volume of data stored (but go along with questions related to the legality of this investigation instrument)

Picture removed in print version
Bild zur Druckoptimierung entfernt

INFORMATION STORED

ENCRYPTION

- Encryption is the process of obscuring information to make it unreadable without special knowledge
- Encryption can be used to ensure secrecy
- Encryption can be used to hide the fact that encrypted messages are exchanged
- Encryption used by criminals can lead to difficulties collecting the necessary evidence

Picture removed in print version
Bild zur Druckoptimierung entfernt

EXAMPLE PGP

ROLE OF THE INDUSTRY

CETS

- Based on a request from a Canadian police man Microsoft developed an investigation / case management software to be used in child exploitation cases
- Provided free of charge to law enforcement around the world

Picture removed in print version
Bild zur Druckoptimierung entfernt

MICROSOFT CETS

PHOTO DNA

- Photo-DNA is another tool that can improve the ability of law enforcement as well as industry to fight against the exchange of illegal content
- Implementation of such technology by industry could reduce the ability of offenders to abuse such service for the exchange of illegal material
- Several well known Internet businesses mentioned at the 2011 IGF that they use such technology to analyse uploaded pictures

LESSON LEARNED

- A lot of the innovations that have been introduced in the area of Cyber-Security were developed within the public sector
- Use of investigation tools by law enforcement can improve the ability to collect evidence
- Industry can play a key role in preventing/detecting crimes

ROLE OF GOVERNMENTS

- Law-makers need to provide the basic legal framework
- Without adequate definitions industry can hardly provide data-bases of known illegal images that can widely be used
- Illegal content is not limited images and videos (this aspects is not reflected in some of the major legal frameworks)

Convention on Cybercrime

2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:
a. a minor engaged in sexually explicit conduct;
b. a person appearing to be a minor engaged in sexually explicit conduct;
c. realistic images representing a minor engaged in sexually explicit conduct.

DEPENDANCE

- Threats of internet based attacks against critical infrastructure
- Energy, Communication, Transportation, Health, Food supply, Finance, Government services, Essential manufacturing, ...
- Even military infrastructure is depending critical technology
- A significant part of critical infrastructure is operated by private businesses

Picture removed in print version
Bild zur Druckoptimierung entfernt

CRITICAL INFRASTRUCTURE

DEPENDANCE

- Alternative Communication Systems that could be used in cases of emergency are not able to cover the necessary resources
- Monoculture with regard to major technical components of computer systems, software and network technology

SASSER COMPUTER WORM

LESSON LEARNED

- Serious threats with regard to attacks against critical infrastructure
- Major parts of the infrastructure is operated and controlled by the private sector
- Protection of critical infrastructure requires public private partnership

ROLE OF GOVERNMENTS

- Critical infrastructure protection can't solely be left to industry
- Where necessary law-makers need to define the role of the different players – especially the role of LEA
- Many legal frameworks do not differentiate between an attack against a regular computer system and attacks against critical infrastructure
- This can hinder the ability of LEA to carry out investigations if sophisticated procedural instruments can not be used

HIPCAR Cybercrime – Sec. 9 (2)

(2) A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification hinders or interferes with a computer system that is exclusively for the use of **critical infrastructure** operations, or in the case in which such is not exclusively for the use of critical infrastructure operations, but it is used in critical infrastructure operations and such conduct affects that use or impacts the operations of critical infrastructure the punishment shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

AVAILABILITY OF INFORMATION

- Information that previously were available only to secret service (e.g. satellite pictures) or from very selected sources (e.g. instructions how to build bombs) are today available via the Internet

Picture removed in print version
Bild zur Druckoptimierung entfernt

SAT. PICTURE (WWW.MAP24.DE)

AVAILABILITY OF INFORMATION

- Industry can play a role in limiting the negative impact of the availability of information about high level targets
- Example is the restriction of resolution in satellite pictures
- Such measures can only have an impact if they are coordinated

GOOGLE EARTH

AVAILABILITY OF HARDWARE

- Some technical solutions that are vital for maintaining Cybersecurity can also seriously hinder investigations if they are used by offenders
- Example: Storage media with hardware encryption
- Use of such technology can make it difficult to get access to information stored and collect the necessary digital evidence

FUJITSU

AVAILABILITY OF HARDWARE

- There are various good examples of strategies developed by industry to ensure a responsible distribution of "dual-use" tools
- One example is the implementation of "know your customers" strategy

EXAMPLE: FUJITSU

LESSON LEARNED

- Industry has the ability to ensure that their products are distributed in a responsibly way
- Circumvention of such protection measure is possible

Cybercrime Research Institute
Prof. Dr. Marco Gercke

Niehler Str. 35
D-50733 Cologne, Germany
www.cybercrime-institute.com