CYBERCRIME

THE CHALLENGE OF FIGHTING CYBERCRIME IN DEVELOPING COUNTRIES

Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection
Cap Verde
28. November 2008

Dr. Marco Gercke
Lecturer for Criminal Law / Cybercrime, Faculty of Law, Cologne University

CYBERCRIME GUIDE

ITU GUIDE

Picture removed in print version

- Aim: Providing a guide that is focussing on the demands of developing
- Including recent developments

Content

- Phenomenon of Cybercrime
- Challenges of Fighting Cybercrime
- Elements of an Anti-Cybercrime Strategy
- Explanation of legal solutions
  - Substantive Criminal Law
  - Procedural Law
  - International Cooperation

CYBERCRIME GUIDE

ITU GUIDE

Picture removed in print version

- Focus of the Guide

DEVELOPING COUNTRIES

CYBER CAFE HANOI

Picture removed in print version

- Most of the infrastructure in western countries (US)
- Difficult to say that there are limits with regard to technical protection measures (great potential of technical development - like WMAX)
- Since 2005 more internet user in developing countries than in industrialised nations
- Getting access remains a crucial problem
- Access to the same sources - potentially the offences

CYBERCRIME GUIDE

ITU GUIDE

Picture removed in print version

- Phenomenon

CLASSIC IT-CRIMES

HACKING

Picture removed in print version

- Illegal access to a computer system was one of the dominating crimes in the early days of computer crimes
- Incredible technical development since that times
- Hacking attacks are still an important phenomenon - especially with regard to the automation of attacks
- But in addition a number of other offences were discovered

EXPLOIT AUCTION

Example (http:wslabi.com)

Picture removed in print version

- Information about system vulnerabilities are published on websites
- In addition these information are offered for sale by some businesses
- Information can be used to increase security as well as to commit computer-related offences

RECENT DEVELOPMENT

ONLINE GAMES (SECONDLIFE.COM)

Picture removed in print version

- New scams related to online-games
- Closer relations between virtual worlds and the real world (exchange of virtual currencies)
- Highly sophisticated phishing-scams

RECENT DEVELOPMENT

Botnets (www.shadowserver.org)

Picture removed in print version

- Current analysis proof that up to a quarter of all computer connected to the internet could be used by criminals as they belong to "botnets"

  Souce: BBC report "Criminals 'may overwhelm the web"
- Some analysis go even beyond that number
- Botnets can for example be used to send out Spam or carry out a DoS attack
- Use of Botnets makes the identification of the offender difficult

RECENT DEVELOPMENT

CYBERTERRORISM

Picture removed in print version

- Increasing activities of terrorist organisations
- Not concentrating on attacks against critical infrastructure - information, recruitment, communication, ...
- Continuing improvement of methods protecting communication from lawful interception
- Integration of the Internet in terrorist financing activities

RECENT DEVELOPMENT

CIPAV

Picture removed in print version

- Intensive discussion about new investigation instruments
- Remote forensic software tools
- In 2001 reports pointed out that the FBI developed a keystroke logger hat can be remotely installed on the computer system of a suspect
- In 2007 the FBI requested an order to use a software (CIPAV (Computer and Internet Protocol Address Verifier) to identify an offender that used measures to hide his identity while posting threatening messages

CYBERCRIME GUIDE

ITU GUIDE

Picture removed in print version

- Challenge

CHALLENGES

- Dependence of the society on information technology
- Availability and power of devices that can be used to commit a crime
- Availability of Information
- Languages
- Missing control instruments
- International dimension
- Speed of information exchange
- Speed of the technological development, power and vulnerability of devices
- Anonymous communication
- Encryption

POSSIBILITIES

- There are no doubts that the ongoing improvement of information technology enables the law enforcement agencies to carry out investigations that were not possible previously
- Automated search for key-words / hash-values
- Great chance for public private partnership (Microsoft's CETS)

EXAMPLE CHILD PORNOGRAPHY

Picture removed in print version

AUTOMATE

- Computer and Networks enable offenders to automate attacks
- Within minutes millions of spam mails can be send out without generating high costs - sending out one million regular letters would be very expensive and take days
- Special software products enable automatic attacks against computer systems

Example (Hackerwatch.org)

Picture removed in print version

AVAILABILITY OF DEVICES

- Internet connected devices as **tool** and **target**
- The number of people who have access to the internet is still growing fast
- New ways of access to networks are implemented (UMTS, WLAN,)
- Capacity of Computers has increased (great potential)
- Number of operations controlled by the use of networks increased

Examples

Misuse of open WLAN-Access Point to hide identity; Terrorists communication via VoIP using encryption technology;

AVAILABILITY OF ACCESS

- Numerous possibilities to get access to the network
- Regular Internet Connection
- Mobile Data Services
- Public Terminals
- Wireless Access Points

Example (Internet Cafe)

Picture removed in print version

ANONYMOUS COMMUNICATION

- "Felt Anonymity"
- Key motivation especially with regard to crimes connected pornography
- Technology available that can hinder law enforcement to trace back the route of an offender (eg. www.anon.de)
- Benefit of Anonymous Communication vs. Effective Law Enforcement
- Possibility to pretend to be some else (Remote Software)

Anonymizer (www.anonymizer.com)

Picture removed in print version

Similar problem with regard to the use of encryption software. Benefits for the Society vs. Effective Law Enforcement

ANONYMOUS COMMUNICATION

Anonymous communication can be reached by:

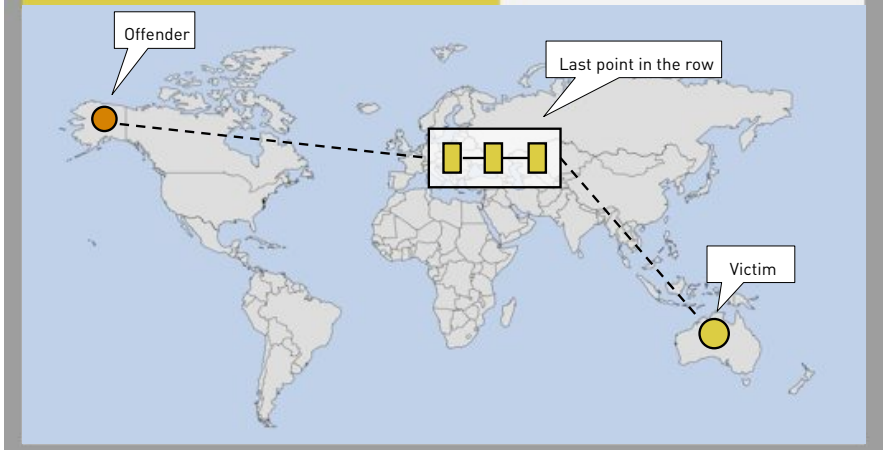
- Use of public terminals
- Use of open wireless networks
- Hacked (closed) networks

Example (Public Internet terminal)

Picture removed in print version

ANONYMOUS COMMUNICATION

ANONYMOUS COMMUNICATION



AVAILABILITY OF INFORMATION

EXAMPLE

Picture removed in print version

- Secret Information are available in the Internet
- Available especially through search engines
- "Google hacking"

AVAILABILITY OF INFORMATION

- Services like Google Earth were reported to be used in several attacks - among them attacks against British troops in Afghanistan and the planed attacks against an airport in the US

Telegraph.co.uk (13.01.2007)

Terrorists attacking British bases in Basra are using aerial footage displayed by the Google Earth internet tool to pinpoint their attacks, say Army intelligence sources.Documents seized during raids on the homes of insurgents last week uncovered print-outs from photographs taken from Google.The satellite photographs show in detail the buildings inside the bases and vulnerable areas such as tented accommodation, lavatory blocks and where lightly armoured Land Rovers are parked.Written on the back of one set of photographs taken of the Shatt al Arab Hotel, headquarters for the 1,000 men of the Staffordshire Regiment battle group, officers found the camp's precise longitude and latitude. "This is evidence as far as we are concerned for planning terrorist attacks," said an intelligence officer with the Royal Green Jackets battle group. "Who would otherwise have Google Earth imagery of one of our bases?

AVAILABILITY OF INFORMATION

TERRORIST HANDBOOK

Picture removed in print version

- Robots used by Search-engines can lead the disclose of secret information
- Handbooks on how to build explosives and construct chemical and even nuclear devices are available
- Internet sources have been used by the offenders in a number of recent attacks

AVAILABILITY OF INFORMATION

RAGNAR'S ENCYCLOPEDIA

Picture removed in print version

- Information regarding the construction of weapons were available long time before the Internet was developed
- Ragnar's Action Encyclopaedia of Practical Knowledge and Proven Techniques
- Approaches to criminalise the publication of information that can be used to

ENCRYPTION

PGP

Picture removed in print version

- 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
- E-Mails, VoIP comminication, files

GLOBAL PHENOMENON

MICROSOFT BITLOCKER

Picture removed in print version

- Availability of encryption technology is a global challenge
- Powerful software tool that enable are available on a large scale in the Internet
- Some of the latest versions of operating systems contain encryption technology

BREAKING A KEY

How long it takes to break a key

Picture removed in print version

- Brute Force Attack: Method of defeating a cryptographic scheme by trying a large number of possibilities; for example, exhaustively working through all possible keys n order to decrypt a message
- Gaps in the encryption software
- Dictionary-based attack
- Social Engineering
- Classic search for hints
- Need for legislative approaches?

STEGANOGRAPHY

- Steganography is a technique used to hide information in some other information
- Example: Hiding a message in picture
- Technique can be used to keep the fact that the exchange of encrypted messages is taking place secret

Steganography

Picture removed in print version

SOLUTION

Technical solutions (with legal component)

- Magic Lantern (US)
- Remote Forensic Software (Germany)

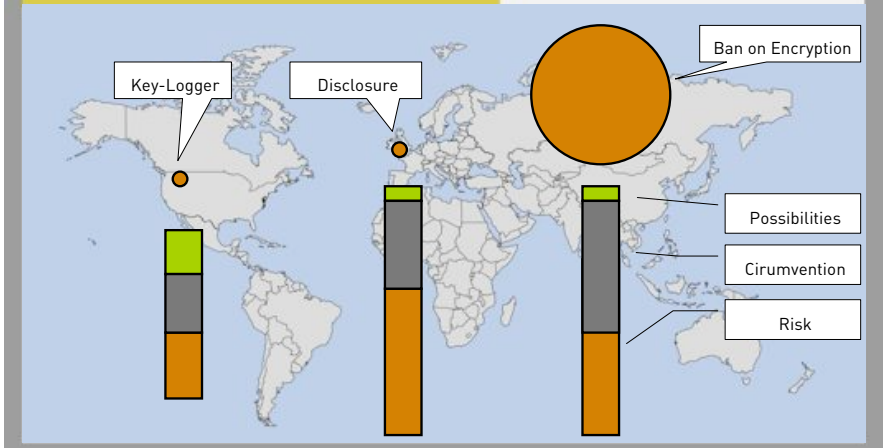
Legal solution

- Use of keyloggers
- Various restrictions on import/export and use of encryption technology
- UK: Obligation to disclose password (Sec. 49 of the UK Investigatory Powers Act 2000)

MAGIC LANTERN

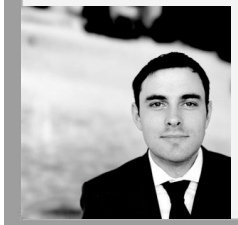
Picture removed in print version

COMPARING APPROACHES



CONTACT

THANK YOU FOR YOUR ATTENTION



Dr. Marco Gercke
Niehler Str. 35
D-50733 Cologne

www.cybercrime.de