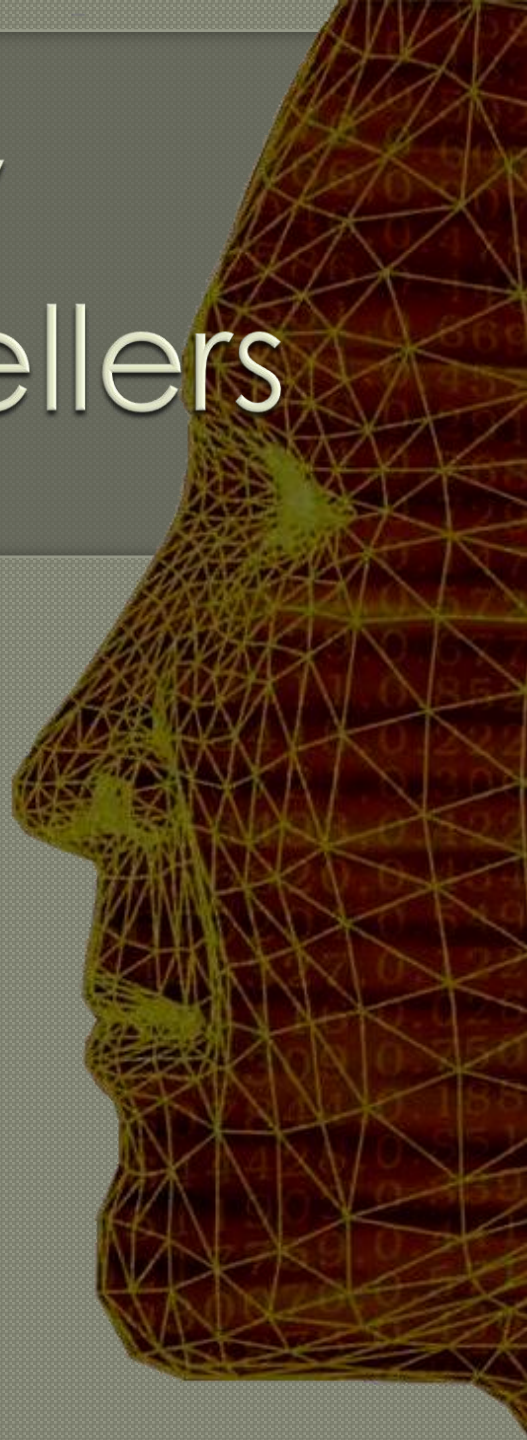
Data security for frequent travellers



Dr. Holger Frommert

InCompass International Consultancy Services Ltd.

The problem

- Frequent business travellers are using usually portable IT equipment – laptops, net books, etc.
- Each year are lost only in Washington any 15.000 laptops with an average damage of US$ 87.000 considering the data loss and the equipment – FBI report year 2005
- No data is reported about USB sticks and the corresponding effects
- Hot spots in this problem are airports and hotels
- The access of not authorized persons to data is especially in hotels and offices a problem

Content of the presentation

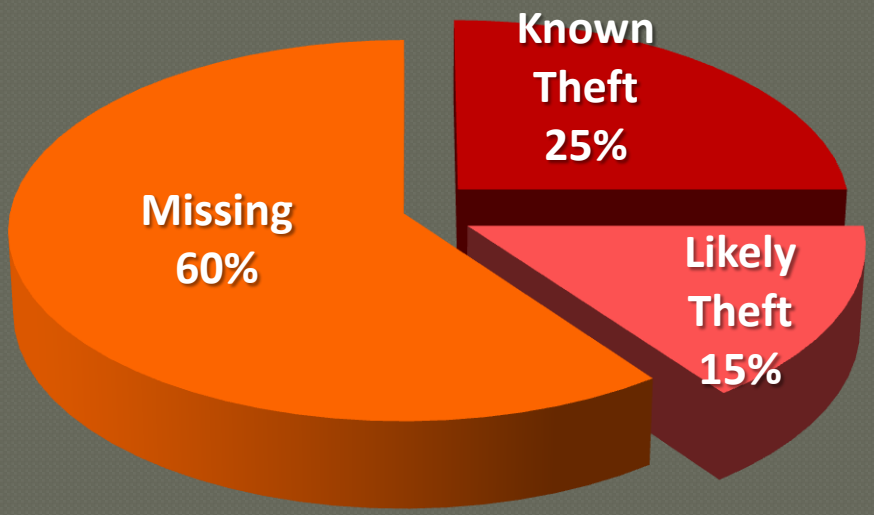
- IT Security Solutions
  - Conventional Data protection
    - Antivirus
    - Firewall
    - Anti-Spyware
  - Stored data
    - Total equipment loss
    - Passwords and access control
    - Encrypted files
    - Encrypted partition
    - Equipment supervision
  - Data transmission
    - SSL
    - VPN
    - Encrypted mail
  - Social Engineering
    - Social Networking
    - Classical Social engineering
    - Office security

Important, widely known, here not more detailed!

Focus in this presentation is the work in unknown security environments.

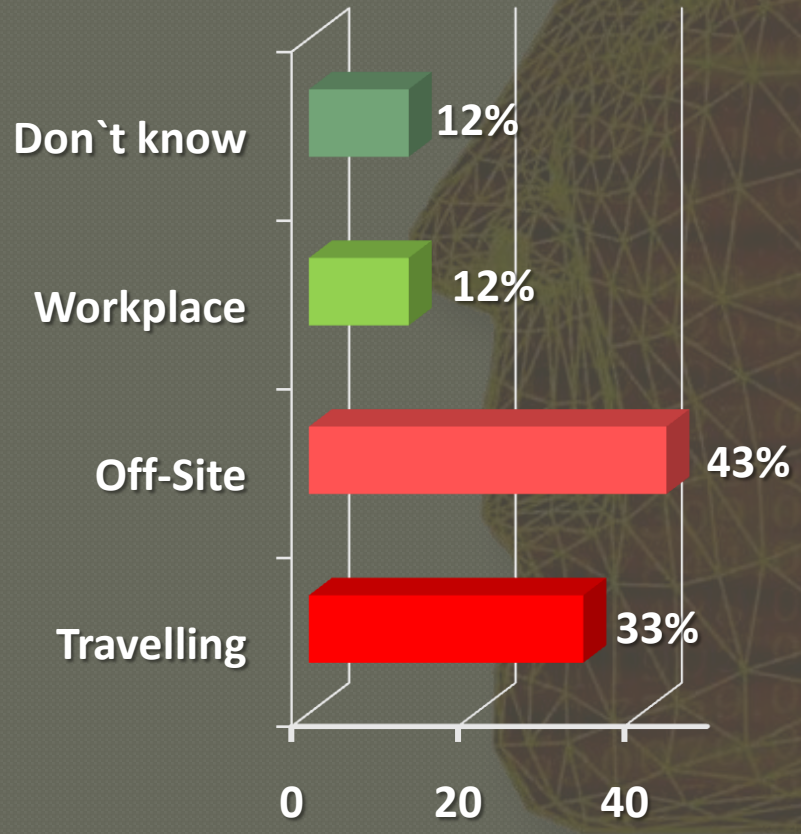
Total loss of laptops

Classification of loss



Data accoring Ponemon Institute
in order of Intel 2010

Condition of loss

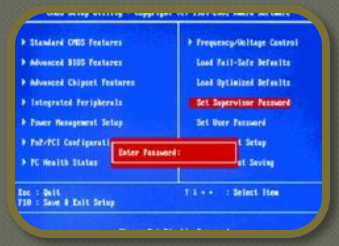


Solutions Anti-Theft

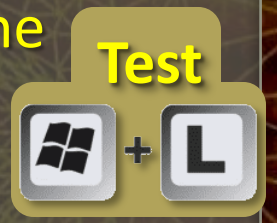
Against theft, especially in travel situations are different solutions on the market:

- Mechanical fixing of the equipment, valid also in office environments
- Electronical solutions based on proximity of the equipment to the owner
- Software solutions which are connecting to an server if the equipment is used in internet
- Localization tools based on IP or GPS data, permitting a photo with the web cam of the thief
- Prices for security solutions are starting with five €

Password and access control



- Apply the board own possibilities to define passwords – starting with the BIOS and including the user management with the corresponding password protection
- It's possible to integrate fingerprint technology for access control into the system for small money – less than 50 € - Many new laptops have now fingerprint reader incorporated
- According to the protection needs of the data is possible to couple fingerprint with smart card technology – especially for governmental use
- Windows 8 will come with an integrated face recognition access control over webcam



Encrypted files

- Confidential information should be stored encrypted to the local disk
- There are many different tools for data encryption on the market, including very effective freeware applications like PGP
- PGP is a very safe tool, the most of the commercial solutions are based in PGP

Encrypted partition or disk

- Similar like the file encryption works the encryption of a folder, partition or disc
- Here is the same situation – PGP or TrueCrypt are safe and widely distributed
- With a key length of 1024 bit or more the economical effort to break the code is so high that this option in very unlikely

The current trial version encrypt all – files until entire disks, after 30 days the encryption of disk space is removed – cost for the full version is € 91

Equipment supervision

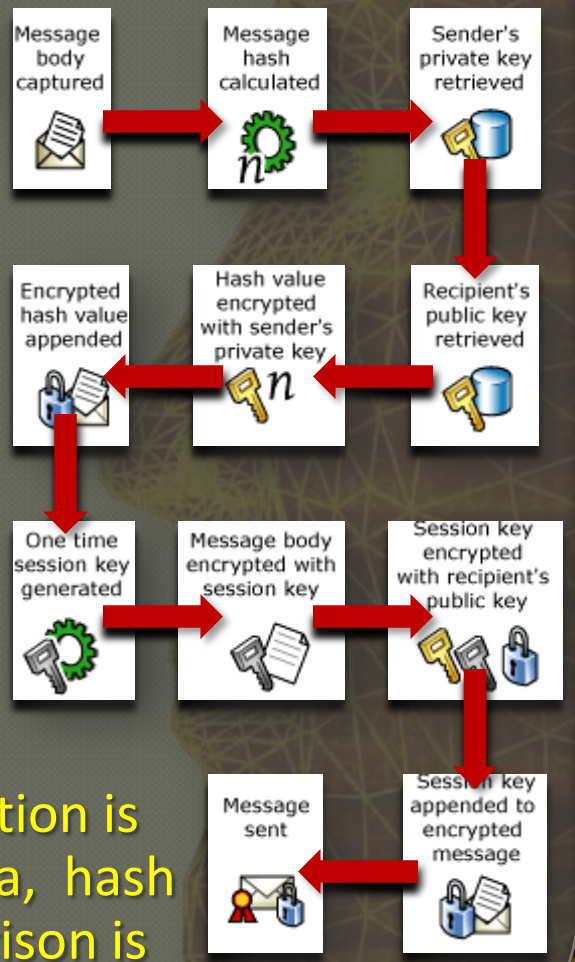
- Especially in unsafe working and storing conditions is mandatory to supervise the equipment history
- There are special software which is logging access data, from storing devices until reporting all actions
- The results should be evaluated continuously and considered in the own security efforts
- There are lots of commercial offers and freeware applications

Data transmission security

- Own WLAN connection must be safe - WEP
- In wireless LAN option's should be disabled the SSID Broadcast option
- If possible use identification of MAC address for authentication in enterprise networks
- Links to the internal enterprise network should go over DMZ and use SSL or VPN
- All internal or external data transmission activities are traceable – therefore possible object of attacks

Encrypted and signed mails

- Similar to encrypted files is possible to encrypt a document or mail content for only one specific receptor using his public key and the own private key
- The receptor must have only the public key to decrypt the content
- Signing the content with the same tool permit to detect changes in the content
- PGP is here a good and cheap solution



Decryption is vice versa, hash comparison is the signature

Social enigeering

- “Social engineering” is the intent to get confidential information by social contacts (call from “administrator”, maintenance or configuration needs by third persons)
- Many user are credulous and are facilitating reserved information, like passwords or other relevant information
- Typical possibility “configuring the WLAN for the hotel router”, etc.

Social Networks

- Facebook and MySpace are ideal places for “social networking”
- Many user are publishing there personal information reused for passwords
- The contact information is used for milieu analysis and personal evaluation, giving so the start point for social networking
- The published photos should be presentable also in any years

Office security – workplace

- Usually the office administrator is in charge of security tasks
- But you should have activated the firewall and control the shared elements, folders, files, etc.
- Log the PC out if you are leaving the place
- Check the installed USB devices
- In extreme cases of suspicions install keylogger application
- Try to encrypt all sensitive data
- Use strong passwords
- Don't share the passwords

Cloud computing and public storing areas like Google

- Cloud computing and file share over internet is currently “in”
- For confidential data must be considered the specific place of the used servers
- The legal access to the data is according to the country where the server is placed – so there are big differences between UN, US and Eastern Europe
- Also must be considered the access security in time and speed as required
- File sharing and cloud computing with sensitive data should be employed only in the enterprise environment or encrypted

Guide for several day trips

- Make a full backup before starting the trip
- According to the working and living conditions install the corresponding security software before mentioned
- 5 € for an electronic device for unauthorised movements of the laptop are well invested
- This is also in the hotel useful – the alarm works here also
- Use an USB stick for security copies of the new files created in the time of the trip – daily backup
- Don't store the USB stick besides the laptop – take it with you
- Supervise the equipment activities permanently

Conclusions

- Periodical backup is the best option to avoid data loss – actual work saved on USB stick
- Standard security options are compellable (Antivirus, Firewall, etc.)
- Permanent access control and data encryption avoid data robbery by third persons
- There are solutions for all budgets, freeware until enterprise solutions
- It´s up to your self to make your working environment safe!

Contact data

Dr. Holger Frommert (PhD)
Ave. Fotógrafo Frederico Cano 113/40
03540 Alicante – Spain

holger_frommert@gmx.net
holger_frommert
++34 667 862 1479
++49 173 386 0703

Interesting Links

- Vulnerability check from Microsoft – For Windows < XP
  - http://www.microsoft.com/downloads/en/details.aspx?FamilyID=1283b765-f57d-4ebb-8f0a-c49c746b44b9
- PGP
  - GNU version
  - ftp://ftp.es.pgpi.org/pub/pgp/gnupg/gnupg-w32cli-1.2.2.zip
  - Commercial version
  - http://www.pgp.com/downloads/desktoptrial/desktoptrial2.html
- USB – control
  - http://www.montpellier-informatique.com/predator/en/index.php?n=Main.Telechargement
  - http://www.hhdsoftware.com/Downloads/usb-monitoring-control
- Keylogger
  - http://www.tucows.com/search.html?search_scope=win&search_terms=keylogger&search_type=all