Openness versus Protection

Protecting assets in an open and connected world

In order to be open and connected, protection of your assets must be well designed.

Partly with standard measures – partly dedicated for the needs in your unique situation.

Living in an open and connected world requires continuous risk-evaluation on a micro-scale, like you do in “real world”.

Foto: Mühlesteg brücke, Zürich, Alf Moens
In “real world”…..

In traffic you continuously evaluate risks:
- Cross a street
- What speed
- Overtaking
- Slippery

Despite that there are rules:
- Traffic rules
- Rules of engagement

And protective measures
- Design of street and street plan
- Brakes, flashing lights, head lights

Still you sometimes decide to:
- Go faster than the speed limit
- Ignore a red light
- Cross in front of a tram

And sometimes someone misses out:
- Speeding tickets
- Ambulance

Foto EMI records, the Beatles, Abbey Road

Protecting you assets - the basics

- Standardising
- Network separation
- Firewall
- Virusscanner
- Keep software up-to-date
- Use different passwords for different purposes
- Classification
- Make regular backups

Open is not the same as public!
If your data is not confidential you still need to protect the integrity.

Techniques are: checksums / hashes

sha256:
4d7124af2b3f232a323217240655e3d093b65fb66df0e4a16d3207d617d031a2e

And above all:

**Be Alert**

In case of emergency call you local CERT team.
Open but Vigilant

Foto Alf Moens
Bulk Cyber Crime - Indiscriminating

Phishing:
- Credentials for sending more spam
- Credentials for financial fraud

Malware
- Control computer
- Gather information
- Used in a botnet for spam or DDOS

Computer Hijacking
- Combination of malware and cryptographic control
- Ransomware
- Financial fraud, small scale

Advanced Persistent Threats - APT

- Personalised attacks – no spam
- Targeted for individuals or officials
- Persistent = continuous
- Attack tries to stay below radar, undetected
- Uses multiple attack vectors
  - Targeted e-mail
  - Relation building
  - Crafted PDF
  - Gifts *with an extra* (USB devices)
  - APT = espionage
  - Industrial, political, science

Diagram: Wikimedia.org
Lightpaths are direct connections, they don’t go through any networks

They are in use for:
- Private connections to a supercomputer

Advanced protection - Cryptography

Encryption:
- Laptop – tablet – smartphone
- Should be turned on by default
- Standard facilities on all major platforms are good
- E-mail encryption with s/Mime or PGP
- Cloud storage
E-mail Signing

E-mail is a primary attack vector

Don’t open or respond to unexpected e-mails
- A colleague sending a personal message you do not expect
- An offer you can’t refuse
- Very urgent e-mails
Without verifying the source

Use digital signatures with PGP or X.509 certificates

Legal Framework Cloud Services

A comprehensive and complete framework for:
• Legal (contracts)
• Privacy
• Information Security aspects of cloud computing

Including a
• adaptor agreement (privacy)
• security checklist
Adopted by all Dutch universities

Compiled for Cloud Services, applicable to all services

Foto: clouds on a fligth to Indianapolis, Alf Moens
Compliance and Control with SURFaudit

- **Control Framework**
  - Policies and governance
  - People
  - Physical Security
  - Continuity
  - Access Control (Confidentiality and Integrity)
  - Logging and Monitoring
- **Based on ISO27002:2013**
- **Scoring on CMM scale**
  - 1: ad hoc
  - 2: reproducible
  - 3: based upon policies
  - 4: continuous improvement
  - 5: based on best practices
- **Standardised process of assessments**
- **Bi-yearly benchmarks**

Results benchmark 2013

- 25 participating universities
- Boxplot presentation: Median, +/- 25% and extremes
- Assessments based on evidence in control framework
- Evidence definition supplied by internal auditors
Do you need to worry?

For bulk cyber crime: Yes, everyone does.
For APT: maybe, depends on what you are working on
Is your work and your data of interest for others?

For more information:
- www.integraalveilig-ho.nl
- Your local security officer
- www.surf.nl

In the end, it is you

- You are handling valuable information every day
- The basic protection is supplied by your IT department, sometimes you'll need to switch it on
- Only you can determine whether it is effective and sufficient
- Like in traffic, look left, look right, think twice before you click.