Université de Neuchâtel

Introduction

Hervé Sanglard
University of Neuchâtel
Switzerland

Overview

- Introduction & context
- Legal framework
- Threats & fight (protection)

Introduction & context

Warning & alerts

Events relayed by Internet, TV & newspapers:

- Coordinated hacking
- Efficient new viruses (cryptoviruses)
- Blackmail, extortion, theft of profiles
- Cyber-surveillance of employees
- Credit card frauds

Top 5 Data Breaches in 2020 So Far …

1. **Twitter Hack**
   The social media platform suffered a breach where the hackers verified Twitter accounts of high profile US personalities like Barack Obama, Elon Musk, Joseph R. Biden Jr., Bill Gates, and many more.
2. **Marriott Data Breach**
   On March 31st, 2020, the hotel chain Marriott disclosed a security breach that impacted the data of more than 5.2 million hotel guests who used their company's loyalty application.

Source : https://securityboulevard.com/

Top 5 Data Breaches in 2020 So Far …

3. **MGM Data Dump**

   Last year in 2019, MGM Resorts suffered a massive data breach. The news of the breach incident started to circulate in February 2020 when hackers leaked the personal details of 10.6 million hotel guests for free download. But in the later findings, the number increased by 14 times (nearly 142 million) than the number recorded in February 2020.

4. **Zoom Credentials Up for Sale!**

   Within a short span of time, the application became vulnerable to various security threats and eventually became a victim of the data breach. In the first week of April 2020, the news of “500,000 stolen Zoom passwords available for sale in dark web crime forums” shook the application users.

Source : https://securityboulevard.com/

Top 5 Data Breaches in 2020 So Far …

5. **Magellan Health (Ransomware Attack and Data Breach)**

   One of Fortune 500 companies, Magellan Health was struck by a ransomware attack and data breach in April 2020. The healthcare giant confirmed by stating that about 365,000 patients were affected in the sophisticated cyberattack.

Source : https://securityboulevard.com/

Computer & Network security

- What encompasses this notion ?
- Is this relevant for my job / activity ?
- What can I do ?
- How ?
- Who can help me ?
- How much does it cost ?
- How to guarantee that means are efficient ?
- What mistakes not to make ?

You said security ?

- 3 main objectives (CIA, easy 😉)
  - Confidentiality: to guarantee that access to information is limited only to autorized users
  - Integrity: to guarantee that data are updated only within a voluntary and legitimate action
  - Availability: to be able to satisfy requests in a given schedule, timeframe and performance

You said security ?

- 1 additional objective
  - Audit and proof : procedures must be auditable, to guarantee that proof evidence is not questionable, to verify the right execution of operations
    - audit of components
    - event logs and tracing
    - non repudiation of an operation
    - imputation of an action to a identified user

Context

- Information management becomes strategic
  - Move from industrial era to information era
  - Information becomes a real asset
  - Online sales of products & services
  - Strong development of services
  - Computer is everywhere : it is complex, can fail, is not perfect but brings saves and a better productivity

Context

- Business environment changes
  - Worldwide exchanges
  - Global organisations and networks
  - « Time to Market » speedup
  - Technology plays a more and more important role

Context

- Business relations change
  - Relationships between partners build quicker and shorter
  - Part of subcontracting is increasing
  - Need for faster and more complex communication between partners
  - Pure hierarchic governance tends to disappear
  - Employees are under stress, temporary contracts are concluded, users are mobile
  - Employees make mistakes, are less loyal and less tied to companies, need remote access

Risks

- Psychological risk
- Human nature (negligence, spitfull, …)
- Blindly targed without any discernment for victims
- Consequence : fear situation
- Immaterial and remote risk

"Gartner clients are also reporting that after years of quarterly reporting on cybersecurity to their boards, that boards are now pushing back and asking for improved data and understanding of what they have achieved after years of such heavy investment."- Gartner The Urgency to Treat Cybersecurity as a Business Decision, 2020

Internal risks

- Manipulation errors
- Bad resources handling (abuse, underused)
- Time loss due to information retrieval
- Production loss in case of failure
- Internal attacks from inside (employees, consultants, …)

Exists since the setup of PC networking inside companies !

External risks

- Are the consequence of
  - interconnection of companies networks
  - connection to Internet
- Hackers with varied goals
  - game, money, competition
  - economic warfare between countries, companies and against illegal organisations

Exists since EDI projects and the birth of WWW !

Myths & reality

- Computer and network never fail ?!??
- Hardware is very reliable
  - Automated tests are rather easy to achieve
- Software is NOT reliable
  - New technology
  - Infinite possibilities
  - 1 bug per 10 lines of code
  - More than 10’000’000 lines of code in modern operating systems and applications
  - Still no formal proof

Myths & reality

- Managers
  - Often do not understand strategic stake
  - Sometimes do not consider their systems as production systems
  - Domain is complex and plenty of complex terms
  - Do not allocate realistic budgets
- Setup & maintenance
  - Sometimes achieved by non professionals
  - Underestimated altough very complex
  - Hardware & Software is evolving very quickly
  - Must be low cost …

Myths & reality

- Users
  - Are often not correctly trained (learn on the heap)
    - Network and sharing concept ?
    - File management and access rights ?
  - Do the strict minimum (no time)
  - Make mistakes (under stress or inadvertently)

- Information handling
  - Complex problem by nature, even for specialists
  - Information filing not unique (filename, folders, ..)
  - User is not given a sense of responsibility in terms of data confidentiality

Potential damages

- Immaterial asset or knowledge
- To guarantee the secrecy of an information
- Content is more precious than container
  - Container has a fixed, evaluable cost (hardware, software)
  - Content value is not quantifiable (customers file)
  - Modification, destruction, theft
- System availability
- Data accessibility and integrity

Company responsibilities

- Shareholders (governance):
  - Which impacts have potential or effective incidents?
  - Are company interests preserved, is the financing of risks correct, suitable, coherent ?

- Managers (management):
  - Which policy to define and which responsibilities to give in order to apply it ?

Company responsibility

- Executive people (operations):
  - How to apply managers choices ?
  - How to pilot action plans, control them, audit efficiency ?
- Employees (operations):
  - How to apply daily rules and instructions ?
  - Which reporting to do?

Legal framework

Swiss Penal Code - Excerpts

Art. 143 - Unauthorised obtaining of data

1. Any person who for his own or for another's unlawful gain obtains for himself or another data that is stored or transmitted electronically or in some similar manner and which is not intended for him and has been specially secured to prevent his access is liable to a custodial sentence not exceeding five years or to a monetary penalty.

2. The unauthorised obtaining of data to the detriment of a relative or family member is prosecuted only on complaint.

Swiss Penal Code - Excerpts

Art. 143bis - Unauthorised access to a data processing system

1. Any person who obtains unauthorised access by means of data transmission equipment to a data processing system that has been specially secured to prevent his access is liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty.

2. Any person who markets or makes accessible passwords, programs or other data that he knows or must assume are intended to be used to commit an offence under paragraph 1 is liable to a custodial sentence not exceeding three years or to a monetary penalty.

Swiss Penal Code - Excerpts

Art. 144 Criminal damage
Art. 144bis Damage to data
Art. 147 Computer fraud
Art. 148 Misuse of a cheque card or credit card
Art. 197 Pornography
…

See also:
https://www.admin.ch/opc/fr/classified-compilation/19370083/index.html

Swiss Data Protection Law (LPD)

LPD is obsolete, dating from 1992
In revision
Voted theses days in the Parlement (9/2020)
Risk of being excluded from EU tenders

See also:
https://www.edoeb.admin.ch/edoeb/fr/home.html
https://smetille.ch/en/welcome/
https://libguides.graduateinstitute.ch/c.php?g=652466&p=4675641

General Data Protection Regulation (GDPR, RGPD in French)

The General Data Protection Regulation (GDPR) applies since 25 May 2018:

1. to any organization, public and private, whatever its size (company, ministry, administration, local authority, association, etc.);
2. which processes personal data on its behalf or not;
3. established on the territory of the European Union;
4. or which, not established on the territory of the European Union, directly targets European residents (for example, a Swiss website offering a delivery service in France with payment in euros).

General Data Protection Regulation (GDPR, RGPD in French)

Data controller. the one to dictate how and why data is going to be used by the organization.

- To collect the personal information of your customers, site visitors, and other targets. You must have legal authority to do so.
- What to collect.
- To change or modify the data that you get.
- Where and how to use the data and towards what purpose.
- Whether to keep the data in-house or to share it with third parties. You also figure out whom to share the data with.
- How long the data is kept, and when to dispose of it.

General Data Protection Regulation (GDPR, RGPD in French)

Data processor. the one who carries out the actual processing of the data under the specific instructions of the data controller to perform some of the following :

- Design, create, and implement IT processes and systems that would enable the data controller to gather personal data.
- Use tools and strategies to gather personal data.
- Implement security measures that would safeguard personal data.
- Store personal data gathered by the data controller.
- Transfer data from the data controller to another organization and vice versa.

General Data Protection Regulation (GDPR, RGPD in French)

Main principles

- No personal data may be processed unless this processing is done under one of the six lawful bases specified by the regulation (consent, contract, public task, vital interest, legitimate interest or legal requirement). Data subject has the right to revoke it at any time.

- Controllers and processors of personal data must put in place appropriate technical and organizational measures to implement the data protection principles.

- Business processes that handle personal data must be designed and built with consideration of the principles and provide safeguards to protect data (pseudonymization, full anonymization, …) with privacy in mind.

General Data Protection Regulation (GDPR, RGPD in French)

Rights of the data subject

- **Information and Access right**

  Gives people the right to access their personal data and information about how this personal data is being processed.

- **Rectification and erasure right (right to be forgotten)**

  Data subject has the right to request erasure of personal data related to them on any one of a number of grounds within 30 days

- **Right to object and automated decisions**

  Allows an individual to object to processing personal information for marketing, sales, or non-service related purposes. This means the data controller must allow an individual the right to stop or prevent controller from processing their personal data.

General Data Protection Regulation (GDPR, RGPD in French)

Remedies, liability and penalties

- **a warning in writing in cases of first and non-intentional noncompliance**
- **regular periodic data protection audits**
- **a fine up to €10 million or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater, if there has been an infringement of the following provisions:**
  - the obligations of the controller and the processor
  - the obligations of the certification body
  - the obligations of the monitoring body

… and what a damage of reputation!

General Data Protection Regulation (GDPR, RGPD in French)

Remedies, liability and penalties (next)

- **a fine up to €20 million or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater, if there has been an infringement of the following provisions:**
  - the basic principles for processing, including conditions for consent
  - the data subjects' rights
  - the transfers of personal data to a recipient in a third country or an international organisation
  - any obligations pursuant to member state law
  - noncompliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority or failure to provide access

General Data Protection Regulation (GDPR, RGPD in French)

6 steps to put GDPR in place

Step 1: Appoint a data protection officer

Step 2: Identify data processing operations

Step 3: Define corrective actions

Step 4: Analyze the risks

Step 5: Establish internal procedures

Step 6: Maintain documentation

See also: https://gdpr.eu/ and https://gdpr-info.eu/

Threat & fight

How to fight and protect you ?

- Technology and tools
  - Infrastructures
  - Services
  - Content and encryption
- Administrative and organisational measures
  - Information security policies (See lecture topic)
  - Documentation, know-how sharing
  - Acceptable use policies (AUP)

How to fight and protect you ?

- Which technologies and tools are available ?
- On which services and providers can I count ?
- With whom and competencies to work ?

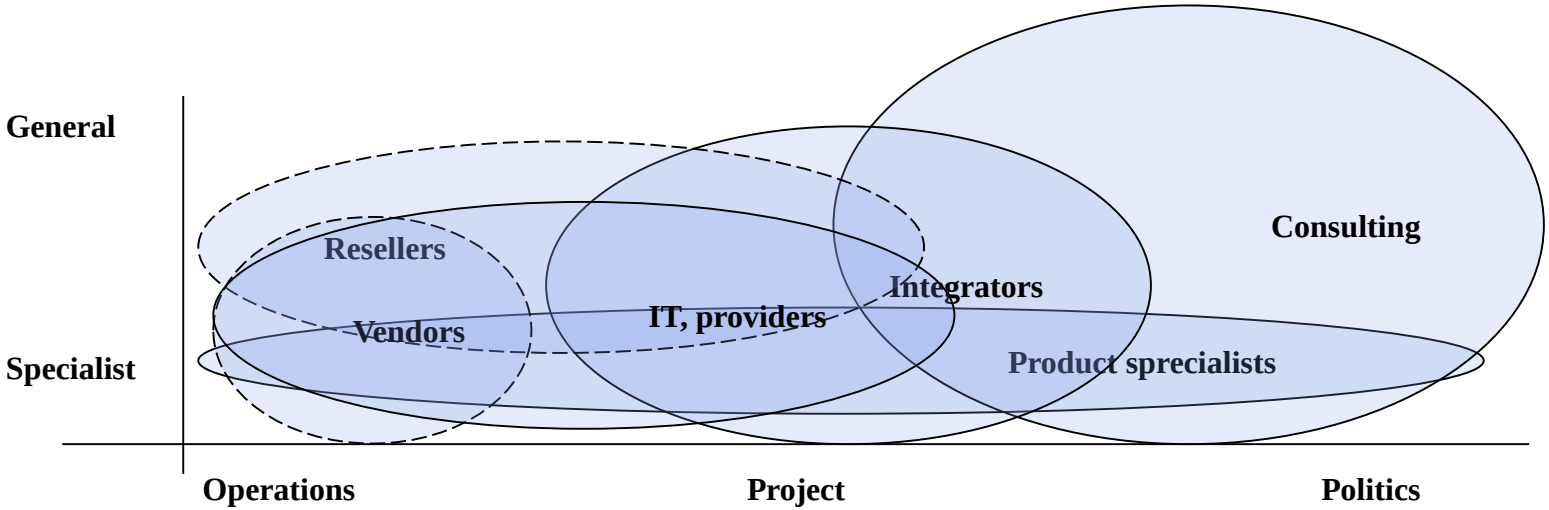
Unavoidable

- To be professional and have competency in IT/IS services and management (ITIL, ISO27001, security by design, code review, penetration and performance tests)
- To ask and obtain suitable financial means related to requirements
- Documentation and know-how sharing
- Training, responsibility and awareness of users
- Attacks and failure prevention (be proactive !)
- Fault tolerance (redondancy, critical components in spare, contract with supplier)
- Checklists and uptodate procedures
- Backup, frequent restore checks, and data archive

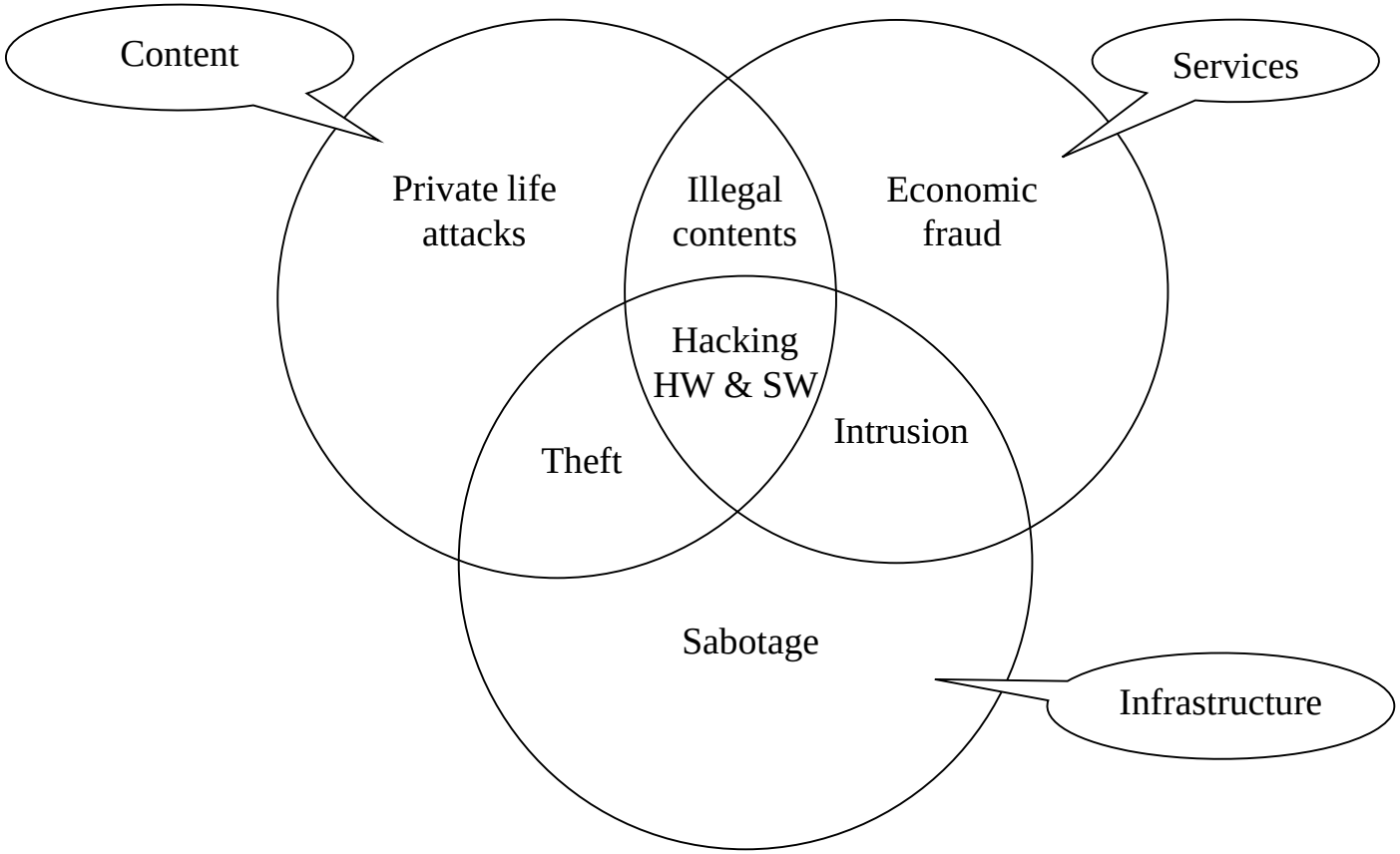
… and a touch of common sense !

Suppliers

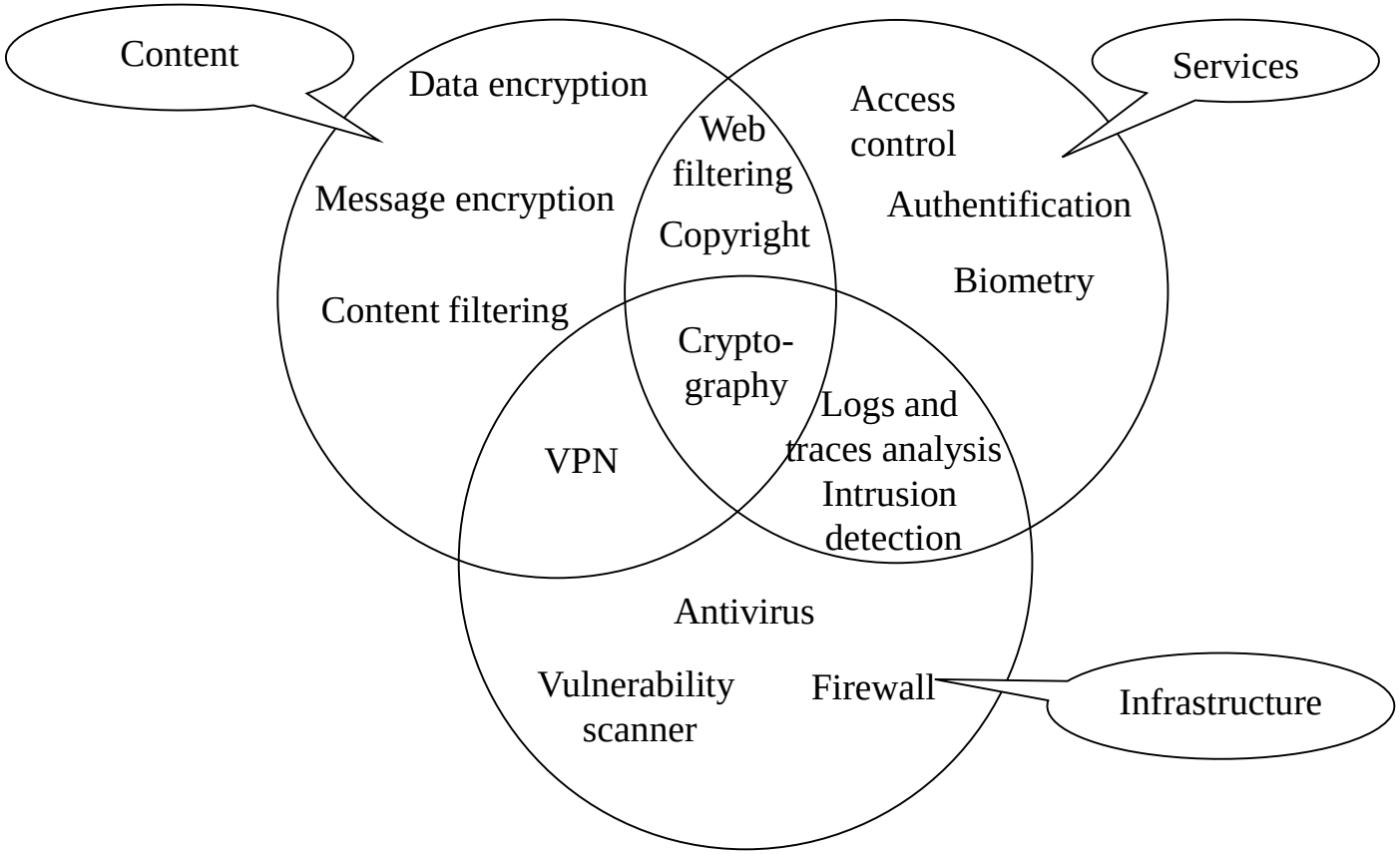
- Consultants
- Product specialists
- Integrators
- IT companies and providers
- Resellers



7 families of risks



7 responses


Content
Services
Infrastructure
Data encryption
Message encryption
Content filtering
Web filtering
Copyright
Access control
Authentification
Biometry
Crypto-graphy
VPN
Logs and traces analysis
Intrusion detection
Antivirus
Vulnerability scanner
Firewall

Infrastructure

Sabotage

- Direct operations, programmed or to damage a system or a network
- Side effect: attack to the image or business
- Usually indirect damages not quantifiable

Sabotage (Virus)

- A program able to auto-reproduce inside a system or piece of software
- types :
  - System : boot sector attack
  - Application: executable files attack, cryptolockers
  - Macro : linked to file document
  - Script : control of environment (javascript)
- Organisational consequences (identification of infected PC, disinfection, data loss)

Sabotage (Worm)

- Entire program able to reproduce and to spread inside networks
- Kind of « network virus » that doesn't need a host program
- Consequences : mailing service perturbations, LAN access from Internet, disclosure of information through attachments

Sabotage (Spam)

- Unsollicited email
- Bombing of messaging servers and filling of mailboxes
- Goal: to slow down or disrupt a provider and its customers

Sabotage (DoS)

- Saturation and Denial of Services
- Take remote control of a hundred of computers and schedule thousands requests at a given time and towards a given site simultaneously (Ddos – Distributed DoS)
- Forced to close the website
- Impact on busines is difficult to evaluate

Sabotage (Ping-of-the-death)

- Exploit of an IP protocol failure - weak implementation
- Ping command is used to know if a remote system is alive
- Abusive usage / forged packets «made» possible to crash the remote system

Sabotage (Defacement)

- To remotely modify the homepage of a website
- To use vulnerability of web/ftp servers
- Consequences on image (trade mark)

Sabotage (Logical bomb)

- Destructive program
- Pre-programmed rather than remote-contolled
- Dispute between customer/supplier, employee/employer conflict
- E.g. extortion or blackmail
- Can lead to data destruction

Intrusion

- An attack which is relatively easy to block
- Motivation : to prove that it is possible to enter inside a network / system
- Sometimes, in order to steal information
- Threat
  - Low level attack
  - Extremely strategic

Intrusion

- Hacking
  - To find and demonstrate software flaws/bugs
  - To publish them .. or to exploit
- Scanning
  - To try to see if ports are open or closed
  - To verify if closed ports and effectively well closed
- Trojan horse
  - A kind of virus that allows to execute operations from inside, without the knowledge of a user
  - To trap seized informations and send them backward

Intrusion

- Social engineering
  - To look for confidential information having the goal to gain entry to a system
  - Preliminary to intrusion
  - Identity usurpation

- Dictionary attack
  - To test all password combinations with or without a dictionary (brute force)

Information theft

- Intelligent services or/and economic warfare
- Contrary to theft of material, it is sufficient to read or make a copy of the information !

Information theft

- Theft of computers
  - To steal the laptop of a salesman, marketing director or manager
  - Reflex: to enhance value of the computer (container) and not its content ☺
  - Copy of sensitive data
  - Copy of information on a DVD or USB drive by your employees
  - Resale of marketing plans, projects, customers, …
- Shared printer, copier and fax
  - Remember : data often end on paper !

Information theft

- Sniffing
  - Analysis probe to sniff the network (LAN+WAN)
  - Almost undetectable, furtive
- Social engineering
  - to make believe that you are collegue or PC supporter in order to obtain a secret (by email or phone, …)
- Radiance
  - To capture electromagnetic perturbations generated by every system (screen, wifi)

Technology (infrastructures)

- Usage against
  - sabotage, intrusion, information theft
- Technics
  - Firewall
  - Intrusion detection
  - Antivirus
  - Vulnerability scanners
  - VPN
  - Traces analyser, event viewer

Firewall

- Network isolation (Internet, Extranet)
- 2 functionnalities
  - IP address filtering
  - Block low level attacks (spoofing, bad formed packets)

- 2 categories
  - Hardware (blackbox, router feature)
  - Software (dedicated server, desktop, WAF)

Antivirus

- To setup on
  - Desktop
  - Servers
  - Messaging systems
  - Gateway

- Specialized vendors and services
  - Worldwide alerts
  - Analysis of infected files
  - Support in case of heavy incident
  - Outsourced or internal management

Intrusion detection and vulnerability scanner

- Intrusion detection
  - Specific software detecting intrusion
  - Generate an alert

- Vulnerability scanner
  - Software controlling automatically applications flaws / bugs / old versions
  - Sofware applying automatically patches

Virtual private network (VPN)

- Data transmission over internet is at risk
- Usage of public infrastructure as an extension of the LAN
- How : configuration of encrypted channels (tunnels) between
  - desktop
  - servers
  - routers
  - firewalls

Virtual private network (VPN)

- 2 kinds: software and hardware

- Mecanism
  1. negociation of encryption keys between 2 components
  2. Flux encryption by sender
  3. Flux decryption by receiver

Traces analysis

- Traces analyses
  - Every attack leaves traces
  - To acquire proofs without alteration of original data
  - Authentication of proofs
  - Data analysis (sometimes post-mortem)

Traces analysis

- Tools
  - Logs Analyser
  - Recovery of HD data and analysis
  - Recovery of password, decryption

- Traces locations
  - Desktop and servers
  - Routers and firewalls
  - Messaging systems
  - Internet gateway/proxy
  - Application platforms

Services

Privacy

- you shall declare the treatment and storage of nominative data
- To misappropriate data
- Security default
- Cookies
- Online collection (websites)

Economic fraud

- Attack against business information
  - Revenues, sales, margins
  - Depending on activity sector
- Technically
  - Funds misappropriation
  - Payment means fraud
  - fraud(fake companies, products, services)
- Manipulations (stock exchange)
  - propagation of false information
  - operations without guarantee

Technology (services)

- Suited to services (applications)
  - Authentication
  - Access control
  - Biometry / Cards
  - Website filtering

Content

Authentication

- To proove your identity
  - To give an information known only by the user such as password, secret code, birthday, …
  - Individual hardware device, such as calculator, smartcard, …
  - Biometry such as fingerprints, eyeprint, …
- Limits
  - A password can be stolen, written or lended
  - 10 passwords are not unmanageable
  - 10 methods of password handling are unmanageable

Authentification

- New solutions …
  - Single authentication (single sign on)
  - Authentification calculator with one-time password (cyber-banking)
  - smartcard
  - biometry

- … but are complex to manage technically or for deployment (expensive too)

Access control

- Authentication is NOT access control !
- Partition logically workspace or data
- Many profiles combinations, role based
- Tied to work organisation (groups)

Smartcard

- Complex security technology (but safe!)
- CPU can run encryption algorithms
- Economically viable in case of multi-usage
  - authentication
  - storage of secret/personal data
- Distribution, replacement, loss, break generate costs

Website filtering

- Internet usage comes with abuse (as phone)
  - nature of visited sites
  - time spend to a private activity
- Control of visited websites
  - categorisation of websites (netiquette)
  - access configuration according to categories
- Many interests for groups, administration, universities
  - excessive and unappropriate usage (hacking, pornography)
  - companies responsibility regarding to accessed data

Illegal contents

- Injuries, defamation
  - By email, forum, site web
  - Unhappy employee, unsatisfied customer, rejected supplier , …
- Rumor & disinformation
  - Economic warfare
  - To damage concurrent

Illegal contents

- Race hatred, religious
  - victims and authors are employees
- Pornography with children
  - Company is responsible of every data treated on its computers/networks
  - witness, acomplice

Hacking HW & SW

- Goal : use tools or content without to pay for them
- Software hacking
  - intellectual property infrigement
  - victim : software editors / vendors
- Digital content hacking
  - Illegal copy
  - victims : industries like cinema and music
- Smartcard hacking

Technology (content)

- To maintain confidential information SECRET
- Encryption is the base solution
- New problems :
  - Control of Internet usage
  - Control of informations broadcasted outside the company (emails)
  - Protection of numerical contents with copyright or patents

Encryption

- To guarantee confidentiality of data
- To build an electronic safe under control of whom has the key (and only)
- example : automatic encryption of folders under modern operating systems
- Mobile computing
  - Encryption of local data
  - Secure remote access
  - VPN

Message encryption

- Information exchange using messaging
  - The message itself
  - Attached documents / pictures
- 3 types of solutions
  - Built-in functions of messaging systems (e.g. Exchange)
  - Dedicated commercial software / plugins
  - Dedicated open source or free software
- examples
  - S-Mime & PGP for messaging
  - SSL for electronic transactions over the Web

Control of content

- Cyber-surveillance (divulgation of confidential informations)
- Content analysis software based on keywords
- Questions :
  - Which keywords list ?
  - Which domain names (which competitors)?
  - Who will control ? How ?
  - How to guarantee the respect of private life of your employees ?

Copyright protection

- Any kind of digital content
  - music, movies, software, Web content, …
- A demand of economic nature
- Intellectual property related
- 2 kinds of answer
  - Legal and repression
  - Technology (watermark, digital signature, activation)