fundamentals; class 1

16/01/2019

What is it ?

Technical, organizational, legal and human means to prevent unauthorized use of the IS.

It is the protection of the assets and of the data.

Why ?

Crucial and critical

Security issues are caused by people wanting to:

* Gain benefits
* Get attention
* Harm someone

90/10 Rule:

10% of security is technical

90% rely on user to follow good practises

Data Leakage releases passwords, tokens, emails and private informations for sale on the internet

Marriott

Equifax

Yahoo

RSA security

GDPR - General Data Protection Regulation (Effective since 25th of May 2018)

* Standardize data protection regulations at European level
* It must be something common between companies
* Empowering businesses by developing self-control
* DPO : Data Protection Officer; was created because of the GDPR, responsible for overseeing data protection strategy (in compliance with the GDPR)
* Strengthen the right of people ( right to access, right to be forgotten, to portability…)

Investment in cyber security is growing more and more every year (101 billion dollars (??) spent in 2019 in cyber security related technologies)

Security violations:

Integrity of confidential information

Data corruption

Loss of valuable information

Loss of trust

Costly reporting in case of data compromises

Awareness :

* Phishing
* Social Engineering
* Browsing safe online

Objectives:

* Confidentiality
* Integrity
* Availability
* Non-repudiation

Process :

* Identify actives
* Identify responsibilities
* Identify vulnerabilities
* Identify consequences
* Identify damages
* Estimate the level of the risk
* Deploying risk measures
  + Access control mechanism
  + Network control
  + Application security
  + Authentication
  + DRP (Disaster Recovery Plan)
* Using standards and strategy processes
  + ITIL
  + ISO
  + …
* Corrective actions : it is necessary to act on the dysfunction and to remove its effect
* Preventive actions
* Improvement actions

Motivation and profile of attackers

|  |  |
| --- | --- |
| Student | Snooping around email |
| Cracker | Test secu, steal data |
| Sales rep | Claim to represent more than actually |
| Businessman | Discover competitor strategy |
| Ex-employee | Being fired |
| Accountant | Embezzle money from a company |
| ... | … |

List of most common attacks:

* DoS
* MinM
* Phishing
* SQL injection
* Drive-by: attack server
* Password
* XSS
* Eavesdropping
* Birthday attack: hash manipulation
* Malware attack

Virus: man made piece of code

Worm: self-replicating program spreading without user interaction

Trojan: make unexpected changes

Viruses / worms

* ILOVEYOU
* PETYA
* HeartBleed
* Freak
* Stuxnet

Cryptography:

Secrete communication with selective recipient.

Caesar shift cipher : shift by an agreed number each letter of the message by the sender and then the other way around by the receiver

Symmetric key cryptography : AES, simpler & faster than the asymmetric ones.

Asymmetric key cryptography (= Public key cryptography)

Digital certificates are important but need to come from a recognized source, because anyone can create a certificate. What matters in the owner of it.