Introduction to Security

There is no 100% secure system!!!

Security History
- 1980s evolution of network interconnections
- increase in the extension of networks

The home environment
- Broadband
- Internet Banking

The corporate environment
- Transactions between corporations
- - Confidentiality of information

The need for security
- protection of assets (in this case, information)
- credibility and competitive advantage
- fulfillment of responsibilities
- continuity of operations and activities

Relative security
- cost of security X value of information
- cost of security X information time

Risk analysis
- identify the system's security "holes"
- determination of the need for security
- Transactions between corporations
- Confidentiality of information

HACKER AND CRACKER

When the subject is “information security”, “system invasion”, “data loss”, or “information theft”, it is very
It is common to hear the term Hacker as the causative agent of that fact. It's very important, before we start studying
about “information security”, we know how to differentiate a Hacker from a Cracker.

HACKER

Contrary to what many people think and say, they are individuals endowed with wisdom and skill, capable of developing computer systems or altering and developing computer system functionalities.

CRACKER

It's an underused term, precisely because many people refer to them as hackers. Crackers, like Hackers, are individuals with the wisdom and ability to develop or change systems, but there is a crucial difference between them:
Crackers use their wisdom to perform attacks on computer systems, program viruses, steal bank details, information, among other malicious actions.

SOCIAL ENGINEERING

It is a form of attack in which the attacker abuses the user's ingenuity or trust to obtain information or install software that will allow unauthorized access to your computer.

A very classic type of Social Engineering is an email message supposedly sent from the victim's bank where they are asked to click on the link to update their data. When you click, you will be directed to a site identical to your bank's website and end up entering your confidential data such as your account number

and password.

Policies Privacy Data

United States Privacy Act:
→ express written permission from the user. Canadian Privacy Act:
→ criminal offenses relating to invasions of privacy.
In Europe:
→ the most complete set of privacy laws today, GDPR.
In Brazil:
→ November 2012 - The so-called 'Caroline Dieckmann Law' is approved, Marco Civil da Internet, General Law for the Protection of Personal Data (LGPDP) 2018.

General Data Protection Regulation

Some Questions - GDPR
• Application management
• BIG DATA
• Internet of Things
• Drones
• Other solutions that are emerging in different contexts and scenarios

Cybersecurity Speeches

Internal security
• Fighting cybercrime
• Protection of critical infrastructure
National defense
• Militarization of cyberspace
• National sovereignty
Digital market
• Trust of users
• Condition for technological innovation and development
Freedoms and guarantees
• Privacy
• Rule of law

Articulation between domains

Strategic plan
• National Cybersecurity Strategy
• National Information Security Structure
Operational plan
• Common taxonomy
• Information sharing
• Situational awareness
• Escalation processes
• Variable geometry
• Mutual validation of processes and procedures

Cybersecurity Public Policies

Intervention axes (Simple Protection)
➢ Standardization and certification
➢ Training and awareness
➢ Alert and Incident Reaction
➢ Critical Infrastructure Protection
➢ Research and development
➢ Cooperation

Standardization and certification
• Common measurement framework and taxonomy that allow for assessment and certification
• Defines expectations of partners
• Allows for interoperability and cooperation
• Promotes trust

Fighting cybercrime
• Protection of property and people through criminalization of attacks against computer systems and the information contained therein
• Ensure an adequate level of security for ICT users
• Legislative update
• Idiosyncrisies of criminal prosecution in cyberspace
Training and awareness
• Cybersecurity is a shared responsibility

- We all need to be aware:
- Citizens, technicians, managers, legislators, politicians, researchers
- OECD: Guide for the Security of Information Systems and Networks: Towards a Culture of Security
- Ongoing training for different actors

Critical Infrastructure Protection

- Protection of IC vs. IIC protection
- 4-step methodology:
- definition of CI;
- identification of the infrastructures that fit within this definition;
- carrying out risk analysis in CI and identification of improvements;
- definition and implementation of appropriate protective measures
- Interdependence between sectors

Investigation and development

- Essential for national autonomy and capacity building
- Not only in technical components
- Economic development vehicle
- Axis of action present in all known National Cybersecurity Strategies