Segurança e Gestão de Risco

2ºSem 2023/24

Information Security

and Applicable Standards

LUIS AMORIM

17 Fev 2024

Introduce yourself

- Name
- Provenance (local and school)
- Knowledge in Information Security
- Practical experience
  - In security (?)
- Expectations

Information About SGR UC

Objectives

- Learn to apply risk management techniques in order to manage risks, reduce vulnerabilities, threats and apply adequate safeguards / controls
- Learn how to determine appropriate strategies to ensure confidentiality, integrity and availability of information
- Learn how to design and guide the development of security policies in the organization

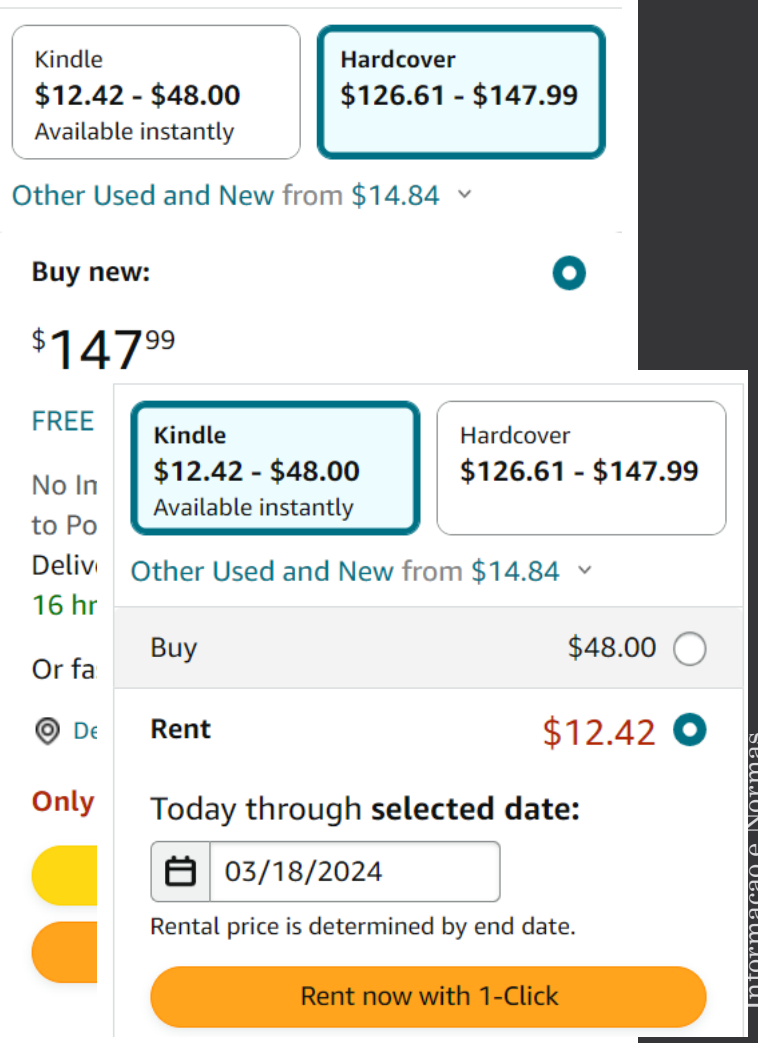
Information About SGR UC

- Bibliografia principal:
  - Information Security Risk Analysis, 3rd Edition, Thomas R. Peltier, Auerbach Publications, 2010, ISBN-978-1-4398-3956-0
  - Normas ISO 27001 e 27005
  - Publicações NIST

- Evaluation
  - Test/exam
  - Practical work on a real case

Information About SGR U

- Main bibliography:
  - Information Security Risk Analysis, 3rd Edition, Thomas R. Peltier, Auerbach Publications, 2010, ISBN-978-1-4398-3956-0



Information About SGR UC

- Schedule
  - Biweekly (TBC), on Saturdays
    - 1 - 17-02-2024 - Saturday
    - **2 - 24-02-2024 - Saturday**
    - 3 - 02-03-2024 - Saturday
    - **4 - 09-03-2024 - Saturday**
    - 5 - 16-03-2024 - Saturday
    - **6 - 23-03-2024 - Saturday**
    - 7 - 06-04-2024 - Saturday
    - **8 - 13-04-2024 - Saturday**
    - 9 - 20-04-2024 - Saturday
    - **10 - 27-04-2024 - Saturday**
    - 11 - 11-05-2024 - Saturday
    - **12 - 18-05-2024 - Saturday**
    - 13 - 25-05-2024 - Saturday
    - **14 - 01-06-2024 – Saturday**
  - Any changes will be communicated in advance
  -

Agenda/Objectives

- Capacities/Objectives to be acquired
  - **Understanding the underlying principles of security in Information Systems**
  - **Understand the concepts of threat, the assess of assets, information assets, physical, operational and information security and how they are related**
  - Understand risk analysis and risk management
  - Understand technical and administrative mitigation approaches
  - Understand the need for a global security model and its implications for the security manager
  - Understanding security technologies
  - Understand the basics of encryption, considerations about its implementation, and key management
  - Learn how to design and guide the development of a security policy in the organization
  - Learn how to determine appropriate strategies to ensure confidentiality, integrity and availability of information
  - Learn how to apply risk management techniques to better manage risk, reduce vulnerabilities, threats and apply appropriate safeguards/controls

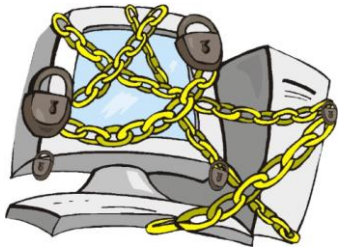
AGENDA

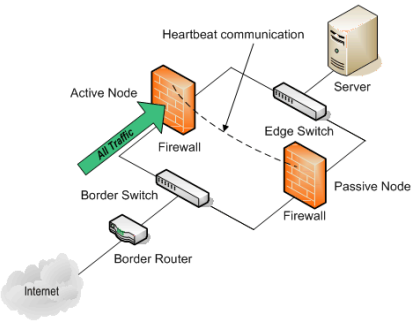
- **Information Security**

- Integrated approach to Security
- Applicable rules and legislation
- Introduction to ISO 27001
- Introduction to Risk Management

Information Security

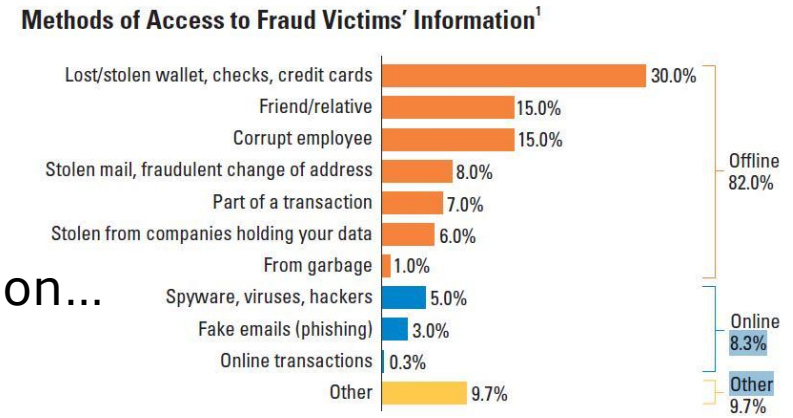
- Information Systems Security?





- Or Information Security?

- But, currently Systems are the basis of Information...

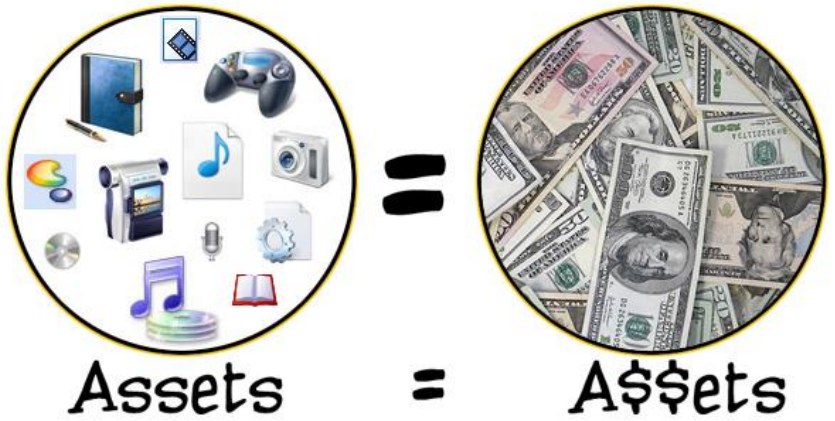


Information Security

- Data vs Information
  - Data by itself is not Information
  - What we want to effectively protect is information
  - However, we only have Information if we have data

Information Security

- Importance of **Information as an asset** for organizations
  - Banks (clientes patrimony)
  - Military forces (national defense)
  - Industry (industrial secrets)
  - Health (patients clinical records)
  - Security Forces (registration of violations)
  - Transportation (network operability)
  - ...



Information Security

- Identification of Information Forms

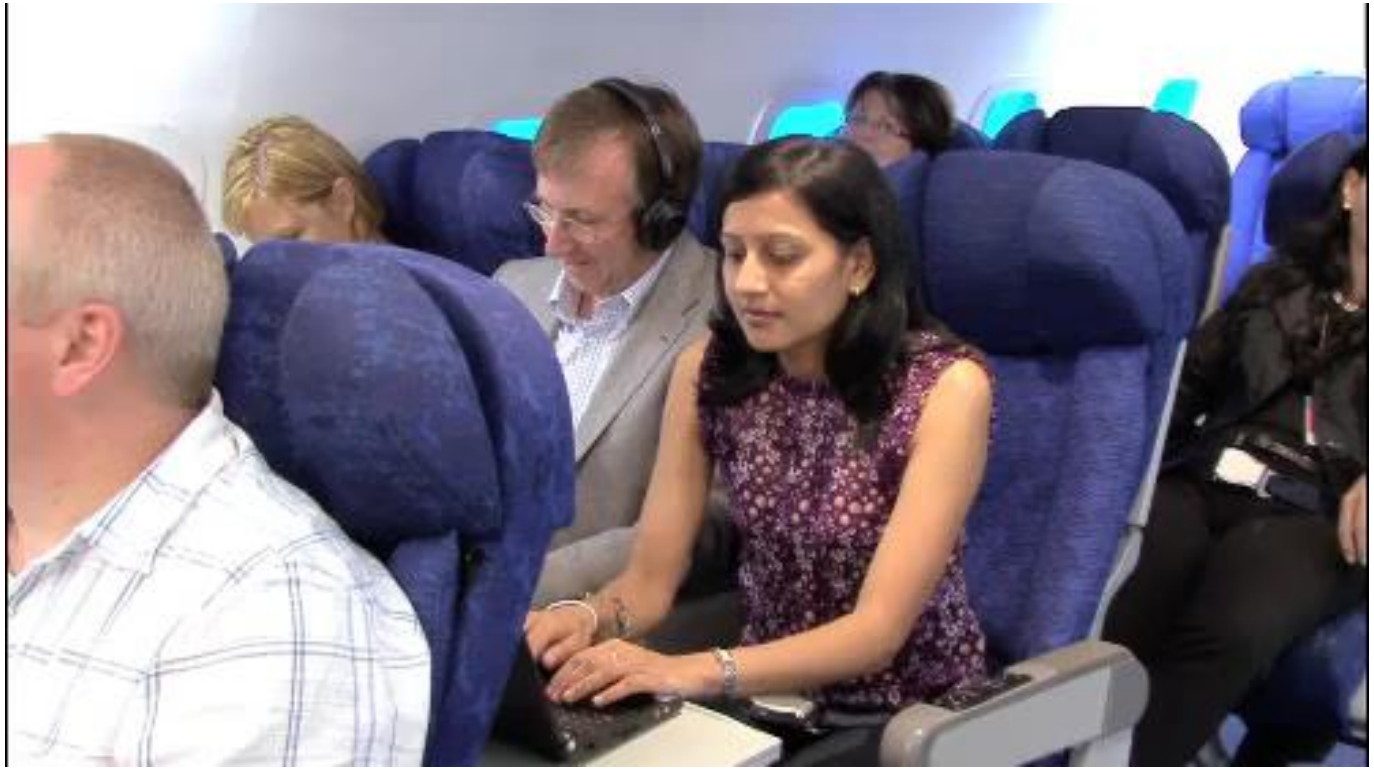
- To protect information we need to start identifying the ways in which this information is transmitted
  - Visual-image/video
  - Audio
  - Writing
  - ….
  - Electronics

INFORMATION SECURITY
- VISUAL/MULTIMEDIA INFORMATION

- Information captured by cameras
  - Increased care given the media coverage of certain events
  - And the proliferation of CCTV

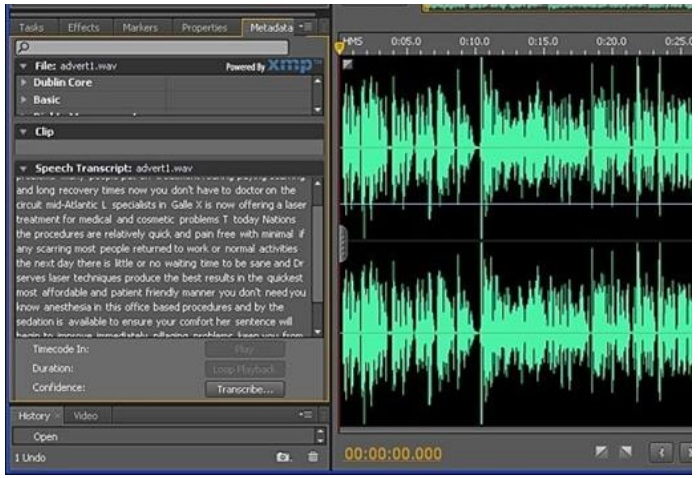
- Information in public places
  - Aircraft/Public transporation
  - Public places

INFORMATION SECURITY
- VISUAL/MULTIMEDIA INFORMATION



INFORMATION SECURITY
- ORAL/AUDIO INFORMATION

- Information analysis systems
  - Allow investigation
    (but they also allow you to spy)
  - They also allow authentication and
    access control

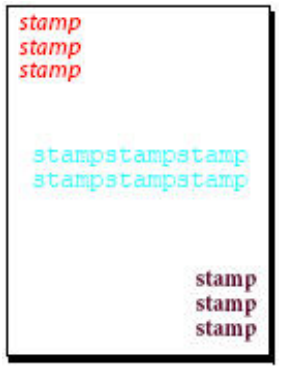


- Voice encryption system
  - To protect communication

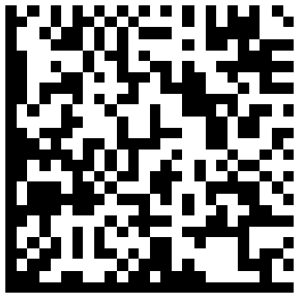
INFORMATION SECURITY
- THE PRINTED INFORMATION

- Print control
  - Secure printing

- Control of printed copies
  - Accounting
  - Document Stamping / Watermarking



- Protection of printed information
  - Sensitive information encrypted



INFORMATION SECURITY
- THE PRINTED INFORMATION

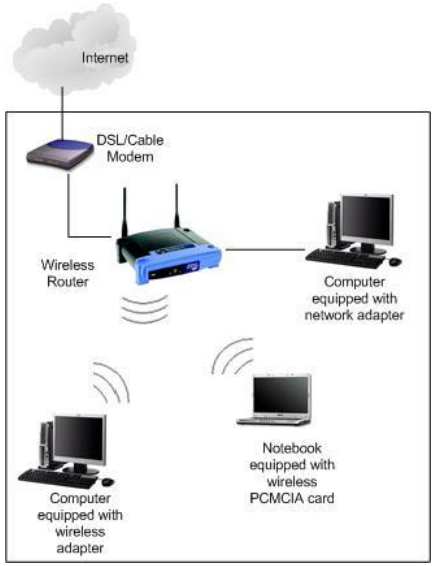
INFORMATION SECURITY
- THE PRINTED INFORMATION

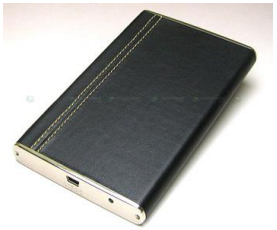
| INÍCIO | COMISSÃO | LEGI

COMISSÃO NACIONAL DE ELEIÇÕES

A CNE aprova novo cartão de Eleitor Biométrico

INFORMATION SECURITY
- INFORMATION IN DIGITAL MEDIA





- Some ways to protect
  - Encrypted discs (bitlocker)
  - Secure communication (VPN)
  - Network segregation (VLANs)

Information Security
- Information access control

- Scope of information
  - Internal
  - Partners
  - Clients
  - Public
  - …

- Classification
  - Unclassified
  - Reserved
  - Confidential
  - …

- Attention: Both scope and classification may vary over time <> requires a management process

Information Security

- Information Security [ISO/IEC 27001]

  "Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved"

Information Security

- C-I-A - The three essential characteristics for information security
  - C – Confidentiality
    "The property that information is not made available or disclosed to unauthorized individuals, entities, or processes"
  - I – Integrity
    "The property of safeguarding the accuracy and completeness of assets"
  - A – Availability
    The property of being accessible and usable upon demand by an authorized entity
- For each organization, each of these characteristics may have a different importance
  - Bank ≠ Utilities ≠ Transportation ≠ Health

Information Security

- **The management of Information Security in the Organization aims to**
  - Ensure the preservation of the confidentiality, integrity and availability of information;
  - Reduce risks for the business, by preventing and minimizing the impacts of security incidents;
  - Ensure the Continuity of the Organization's Business.

- **Information Security Management System (ISMS)**
  - "That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security"; [ISO/IEC 27001]
  - It's a management process;
  - It's not just about the technological component, but this is part of the security management process

Information Security

- **Concepts**
  - Threat

    A threat is anything (intentional or unintentional human act, or caused by nature), which has the potential to cause damage

  - Vulnerability

    Vulnerability is a weakness that can be used to endanger or cause damage to an information asset

  - Risk

    Risk is the probability of something bad happen and cause damage to an information asset

- **The likelihood that a threat explore a vulnerability to cause damage, is a risk to the organization.**

Exercise

- Found Threats to information security

- Found Vulnerabilities that can be explored by these vulnerabilities

Information Security

- Threats
  - Terrorism
  - Industrial espionagem
  - Unauthorized use of equipment
  - Fire
  - Flooding
  - Earthquakes
  - Power or Communications failure
  - Hardware or software failure
  - Unauthorized access
  - Information theft
  - Data corruption
  - Software bugs
  - Social engeneering
  - Virus attacks
  - Hacking

Information Security

- Vulnerabilities
  - Lack of fire detection and extinguishing systems
  - Lack of Flood detection systems
  - Non-existence of a BCM program
  - No power or communications redundancy
  - Weak software tests
  - Lack of intrusion protection systems (e.g. FW, IPS, ...)
  - Lack of physical access control systems (barriers, security, video, ID cards, ...)
  - Lack of logical access control systems (login/passwd, id management, tokens)
  - …

Information Security

- Risks
  - Information Theft
    - Or Theft of Information, left on the desk, by an external visit
    - – Why?
  - Information loss caused by Wrongly deleted data
  - ...

  But also the Risks associated with
  - Disclosure of documents in physical support (paper):
    - Left on desks;
    - In the trash;
    - On copiers/printers.

AGENDA

- Information Security

- **Integrated approach to Security**

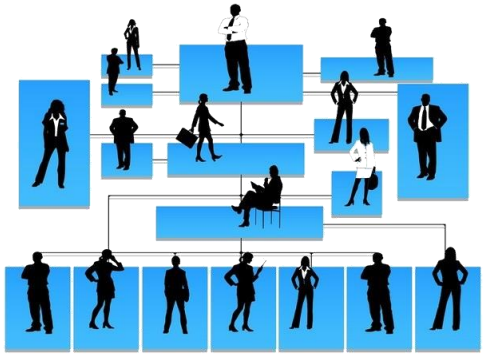
- Applicable rules and legislation

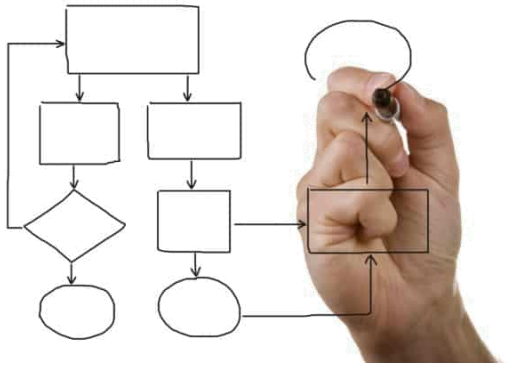
- Introduction to ISO 27001

- Introduction to Risk Management

Information Security

- We consider information security the implementation of a set of controls or measures that allow us to protect information, in a global and integrated way:
  - People
  - Processes
  - Products/Tools





Exemplification

- Information Security
-

Examples

- **Biggest data breaches (since 2000)**
  1. Yahoo, August 2013 > 3 billion accounts
  2. Alibaba, November 2019 >1.1 billion pieces of user data
  3. LinkedIn, June 2021 > 700 million users
  4. Sina Weibo, March 2020 > 538 million accounts
  5. Facebook, April 2019 > 533 million users
  6. Marriott International (Starwood), September 2018 > 500 million customers
  7. Yahoo, 2014 > 500 million accounts
  8. Adult Friend Finder, October 2016 > 412.2 million accounts
  9. MySpace, 2013 > 360 million user accounts
  10. NetEase, October 2015 > 235 million user accounts
  11. Court Ventures (Experian), October 2013 > 200 million personal records
  12. LinkedIn, June 2012 > 165 million users
  13. Dubsmash, December 2018 > 162 million user accounts
  14. Adobe, October 2013 > 153 million user records
  15. My Fitness Pal, February 2018 > 50 million user accounts

  (fonte: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html)

The New York Times

Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing

Dec. 11, 2018

WASHINGTON — The cyberattack on the Marriott hotel chain that **collected personal details of roughly 500 million** guests was part of a Chinese intelligence-gathering effort that also hacked health insurers and the security clearance files of millions more Americans, according to two people briefed on the investigation.

The **hackers**, they said, **are suspected of working on behalf of the Ministry of State Security, the country's Communist-controlled civilian spy agency**. The discovery comes as the Trump administration is planning actions targeting China's trade, cyber and economic policies, perhaps within days.

Those moves include indictments against Chinese hackers working for the intelligence services and the military, according to four government officials who spoke on the condition of anonymity. The Trump administration also plans to declassify intelligence reports to reveal Chinese efforts dating **to at least 2014 to build a database**

Examples

- Threat: Hacking

REUTERS®

World Business Markets Sustainability Legal More

Technology

U.S. government concludes cyber attack caused Ukraine power outage

By **Dustin Volz**

February 26, 2016 12:06 AM GMT · Updated 8 years ago

Aa

WASHINGTON (Reuters) - A December power outage in Ukraine affecting 225,000 customers was the result of a cyber attack, the U.S. Department of Homeland Security said Thursday, marking the first time the U.S. government officially recognised the blackout as caused by a malicious hack.

Security experts had already widely concluded that the downing of utilities in western Ukraine on Dec. 23 was due to an attack, which is believed to be the first known successful cyber intrusion to knock a power grid offline.

Examples

- Threat: Ransomware

A Colonial Pipeline facility in Pelham, Ala. The company said it had learned on Friday that it was the victim of a cyberattack. Jay Reeves/Associated Press

The New York Times

Cyberattack Forces a Shutdown of a Top U.S. Pipeline

The operator, Colonial Pipeline, said it had halted systems for its 5,500 miles of pipeline after being hit by a ransomware attack.



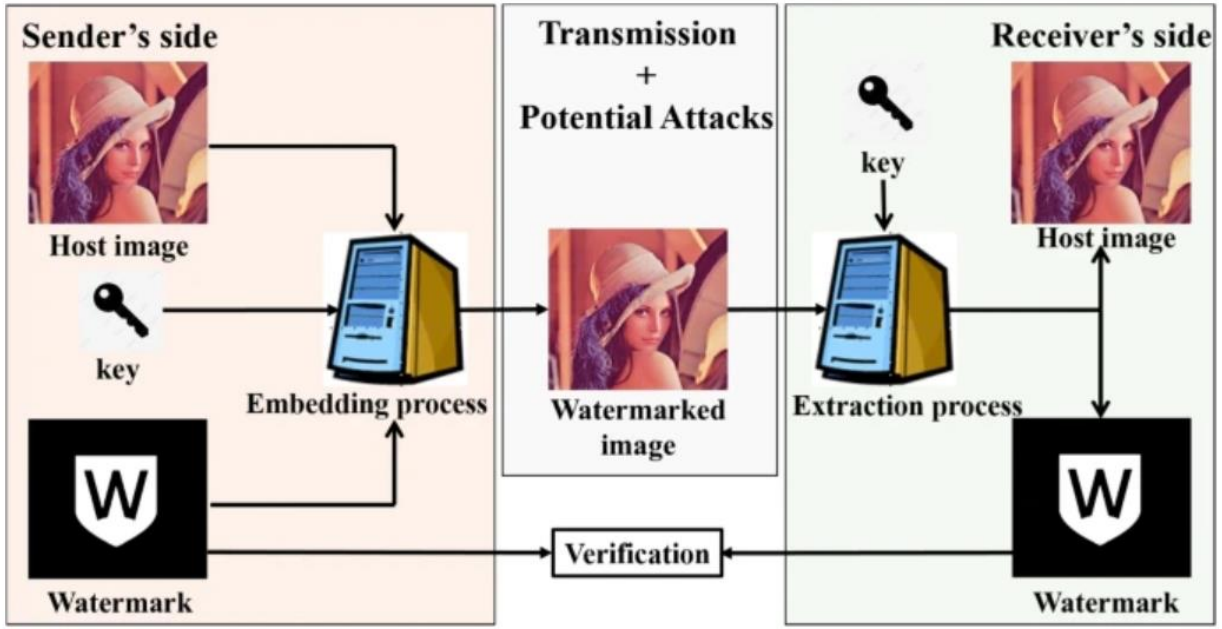
By David E. Sanger, Clifford Krauss and Nicole Perlroth

Published May 8, 2021 Updated May 13, 2021

Examples

- Threat: Terrorism

- But can also be used as a control



Planos de ataques da Al Qaeda escondidos em pornografia

Entre eles estavam sequestros de navios de cruzeiros e atentados na Europa semelhantes aos de Bombaim, em 2008

Por: tvi24 | 1-5-2012 0:37

Gosto 48 pessoas gostam disto.

Like 48 Send

Casino da Sorte Português Jogue sem necessidade de depósito Ou

A polícia alemã descobriu planos de ataques da Al Qaeda escondidos num vídeo pornográfico que um jovem austríaco tinha escondido na roupa interior.

Entre os alvos encontravam-se navios de cruzeiro e estavam previstos ataques na Europa ao estilo dos que ocorreram na cidade indiana de Bombaim, em Novembro de 2008, em que uma dezena de operacionais armados espalhou o terror durante três dias, matando 164 pessoas.

Esta descoberta só agora revelada foi feita já no ano passado. De acordo com a CNN, tudo começou quando as autoridades germânicas detiveram em Berlim Maqsood Lodin, um austríaco de 22 anos, que estivera recentemente no Paquistão e entrara na Alemanha por terra, depois de ter regressado à Europa através da Hungria.

Examples

- Threat: Documen
  theft

Expresso

Roubados documentos dos submarinos

Vários documentos foram "**cirurgicamente**" **roubados** de um carro ontem em Lisboa.

10:01 | Quarta feira, 3

O contrato entre o Estado e a empresa alemã Ferrostaal sobre as contrapartidas pela venda a Portugal de dois submarinos foi ontem roubado, segundo revela hoje o "Correio da Manhã".

Os documentos foram roubados do carro quando Christoph Mollenbeck, representante da Ferrostaal, jantava com um amigo em Lisboa, perto da Cinemateca.

Segundo o mesmo diário, o Audi A6 foi "cirurgicamente assaltado" e não tinha quaisquer "sinais de arrombamento". Só quando Mollenbeck e o amigo e compatriota Kai Jusec chegaram a casa é que deram pela falta da pasta e do portátil.

Às autoridades, Christoph Mollenbeck disse que as contrapartidas foram ontem renegociadas entre a empresa e o Estado. Do carro também desapareceu o memorando de entendimento entre a Ferrostaal e o Laboratório de Tecnologias de Informação.

O caso está a ser investigado pelo DIAP de Lisboa, liderado por Maria José Morgado.

AGENDA

- Information Security
- Integrated approach to Security
- **Applicable rules and legislation**
- Introduction to ISO 27001
- Introduction to Risk Management

Applicable rules and legislation

- The use of standards and good practices allows
  - Use of tested and proven methodologies
  - Incorporation of real knowledge (models/rules) at the level of an enlarged community
  - Possibility of measurement and comparison

- Knowledge and adoption of legal requirements allows
  - Compliance with the law, ensuring legality

Applicable rules and legislation

- (some) Standards related with security
  - ISO/IEC 27001:2022 (BS7799-2) - Information Security Management Systems - Requirements
  - ISO/IEC 27002 – ex ISO/IEC 17799- Code of practice for Information Security Management
  - ISO/IEC 27003:2010 - Information security management system implementation guidance
  - ISO/IEC 27004:2009 - Information security management - Measurement
  - ISO/IEC 27005:2008 (BS7799-3) - Information security risk management
  - ISO/IEC 27006:2007 - Requirements for bodies providing audit and certification of information security management systems
  - ISO/IEC TR 27015:2012 — Information technology — Security techniques — Information security management guidelines for financial services
  - ISO/IEC 27033-2:2012 Security techniques -- Network security -- Part 2: Guidelines for the design and implementation of network security
  - ISO/IEC 27035:2016 Information technology -- Security techniques -- Information security incident management
  - ISO/IEC 15408:2005 - Security techniques — Evaluation criteria for Itsecurity (Common Criteria)
  - ISO 24760 - A Framework for Identity Management -This has not yet been published.
  - ISO 22301:2019 (BS25999) – Business Continuity Management System - requirements

Applicable rules and legislation

- ISO/IEC 15408 - Security techniques-Evaluation criteria for ITsecurity
  - ISO/IEC 15408-1 - Part 1: Introduction and general model
    - defines two forms for expressing IT security functional and assurance requirements:
    - the protection profile (PP) construct allows creation of generalized reusable sets of these security requirements. The PP can be used by prospective consumers for specification and identification of products with IT security features which will meet their needs.
    - the security target (ST) expresses the security requirements and specifies the security functions for a particular product or system to be evaluated, called the target of evaluation (TOE). The ST is used by evaluators as the basis for evaluations conducted in accordance with ISO/IEC 15408
  - Part 2: Security functional requirements
    - defines the required structure and content of security functional components for the purpose of security evaluation. It includes a catalogue of functional components that will meet the common security functionality requirements of many IT products and systems.
  - Part 3: Security assurance requirements
    - defines the assurance requirements of ISO/IEC 15408. It includes the evaluation assurance levels (EALs) that define a scale for measuring assurance, the individual assurance components from which the assurance levels are composed, and the criteria for evaluation of protection profiles and security targets

Applicable rules and legislation

- ISO/IEC 18028 - Security techniques - IT network security
  - Part 1: Network security management
  - Part 2: Network security architecture
  - Part 3: Securing communications between networks using security gateways
  - Part 4: Securing remote access
  - Part 5: Securing communications across networks using Virtual Private Networks

Applicable rules and legislation

- But also other standards related to

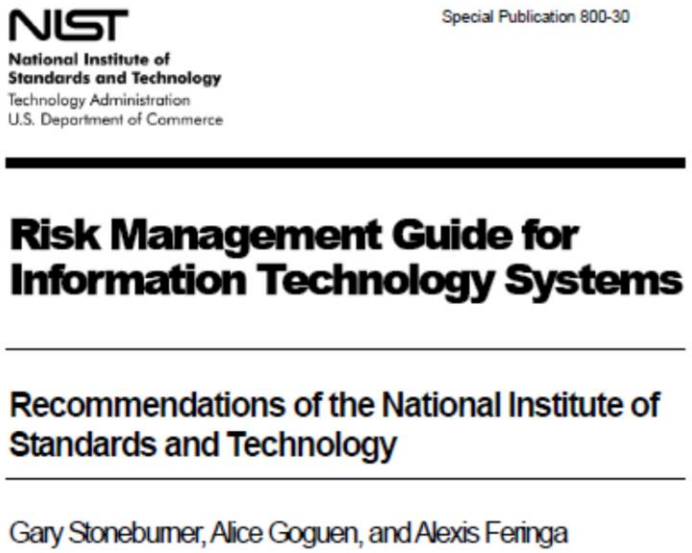
  - ISO/IEC 21559-1 - Telecommunications and information exchange between systems

  - ISO/IEC 25000:2014 - Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE

Applicable rules and legislation

- NIST Special Publication 800-30
- (different approaches)
  - The controls to be implemented can be grouped into
    - Technological
    - Non-technological: Management,

    Operating and Organizational


NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-30

Risk Management Guide for Information Technology Systems

Recommendations of the National Institute of Standards and Technology

Gary Stoneburner, Alice Goguen, and Alexis Feringa

Applicable rules and legislation

- Other standards and legislation with an implication for Security
  - IT Governance
    - ITIL (ISO/IEC 20000) – operating procedures, with regard to security
    - COBIT, in the implementation of controls

- Legislation
  - SEGNACs – GNS – Handling of classified matter
  - Law nº 109/ 2009 - Cybercrime Law
  - Law n.º 58/2019 – Personal Data Protection Act
  - Law n.º 46/2018 – Law establishing the legal regime of cyberspace security
  - DL n.º 65/2021- regulation of aspects related to security requirements and incident reporting rules

- Specific rules for certain sectors
  - Sarbanes-Oxley Act - aims to ensure the establishment of audit and security mechanisms
  - Basileia II - international agreement determining the risk management rules for banks
  - PCI DSS - Payment Card Industry Data Security Standard
  - HIPAA - Health Insurance Portability and Accountability Act

Applicable rules and legislation

- But, also standards related to the quality and processes of the organization
  - ISO9001 - Quality management systems - Requirements
  - ISO 14001 Environmental management systems - Requirements with guidance for use
  - OHSAS 1800 > ISO 45001 - Occupational health and safety management systems — Requirements with guidance for use
  - "NOTE: If an organization already has an operative business process management system (e.g. in relation with ISO 9001 or ISO 14001), it is preferable in most cases to satisfy the requirements of this International Standard within this existing management system." [ISO 27001]

Applicable rules and legislation

- Connecting Quality to Safety

- Can we have Quality without concerning about the Security of an Information System?

- Will we be able to achieve the right security levels, without having quality, at the product level and the development and maintenance process?

- Both Quality and Security must be present at the end of the entire life cycle of an Information System

Applicable rules and legislation

- The requirements to be considered may be
- Normative
- Legal

- +Contractual

Segurança e Gestão de Risco

2ºSem 2023/24

Information Security

and Applicable Standards

LUIS AMORIM

17 Fev 2024