Security and Risk: Quick Summary

Gabriel Rovesti

Contents

1. Disclaimer

Given the course has so much content, a complete notes file is available, basically an extended transcript of file, here I will give a full revised short summary to avoid the unreadable sets of slides of this course. Hope this could be useful, between all of my other works.

2. M1.1 - Basic concepts

2.1. aaa

3. M1.2 - Basic concepts

3.1. aaa

4. M2.1 - Planning for Cybersecurity

4.1. aaa

5. M2.2 - Planning for Cybersecurity

5.1. aaa

6. M3.1 - Cybersecurity Operations and Management

6.1. Human Resource Security

- Includes hiring, training, monitoring and handling employees
- Not only a technical challenge, also employees have to be aware of incidents and problems
- Harmful behaviors can occur, being both malicious and non-malicious

6.2. Hiring process

- ISO 27002 specifies "the hiring process ensures employees and contractors understand their responsibilities, suitable for their roles"
- They should be fully capable of perform the intended job, without making unfounded claims and avoiding "negligent hiring"
- Ask applicants as much detail as possible and in case get even criminal/credit record check, according to the country's law
- Employees should agree and sign the terms and conditions of contracts, including non-disclosure agreement and ensuring assets are confidential, agreeing to respect both the policy and confidentiality

6.3. During and after employment

- Each job should have specific cybersec tasks associated
- Employers and contractors should be aware of responsibilities, policy and training programs
- Several principles for personnel security:
  - Least privilege
  - Separation of duties
  - Mandatory vacations
  - Limited reliance on key employees
  - Dual operator policy
- During the termination of employment phase, organization's interests should be protected and all data/accounts/codes/assets regarding specific individuals will be removed

6.4. Security awareness

- Having a good security awareness and appropriate security training is as important as any other security countermeasure or control
- Activities that explain and promote security should develop into secure practices according to the specific role, accompanying good education/certification
- All employees have security responsibilities which the awareness program should constantly push, being focused on all people and categories
- A good program should include all aspects (e.g., communication, responsibility, help, security culture)

- According to ENISA we should have:
  - Plan/Assess/Design
  - Execute/Manage
  - Evaluate/Adjust
- Good communication materials should be available:
  - both in-house
  - and externally obtained
- Good education/certification programs should be also available, considering specialized training
- Role-based training also should encompass:
  - Manage
  - Design
  - Implement
  - Evaluate

6.5. Hardware management

- Hardware = any physical asset used to support corporate information or systems, including the software embedded within them and the operating systems
- Hardware Asset Management (HAM) deals specifically with hardware portion of IT assets, managing the physical components
- Its lifecycle is composed by:
  - Planning
  - Acquiring
  - Deploying
  - Managing
  - Disposing
- Destruction is important to handle data safely

6.6. Office equipment

- Every hardware inside an office, containing sensitive information processed by or stored inside of it
- Could be also multifunction devices (MFD)
- Each contains some processing power and each is an asset to protect opportunities for threat and protection
- Could be exposed to several threats:
  - Network services
  - Information disclosure
  - DoS attacks
  - Physical security

  - OS security
- They can have a checklist containing organization measures

6.7. Equipment disposal

- SOGP recommends sensitive information should be securely destroyed
- Three main actions:
  - Clear = sanitize storage locations
  - Purge = apply logical/physical techniques to destoy encryption key on devices
  - Destroy = renders target data recovery infeasible

6.8. Industrial Control System (ICS) security

- Used in control industrial processes, including Supervisory Control and Data Acquisition (SCADA)
- Consists of a combination of control components used to achieve industrial objectives
  - HMI - Human-Machine Interface
  - Remote diagnostics and maintenance
  - Sensors
  - Actuators
  - Control
- They are distributed in insecure locations, often with microcontrollers with limited processing power
- There could be several threats:
  - Blocked/delayed flow of information
  - Unauthorized changes to instructions
  - Inaccurate information
  - ICS software or settings modified
  - Interference with operation of equipment protection systems, safety systems and system settings

6.9. Mobile device security

- Mobile device = Portable computing and communications device
- Prior to the use of smartphones, user devices were clearly confined over defined perimeters
- Now devices are constantly connected and there's always the need for more
- Each has a full stack, from hardware/firmware/mobile OS/application, being an entire ecosystem
- Millions of apps are available and each should conform to the organization security requirements; some examples
  - Rooting/Jailbreaking
  - Sideloading
- Many vulnerabilities to list, given they are outside of the corporate perimeter

- *Bring Your Own Device (BYOD)* - many organizations find convenient to have such a policy, inspecting devices and their features
  - configuring devices in such a way it’s possible to access, protect and wipe data from them safely, even remotely

7. M3.2 - Cybersecurity Operations and Management

7.1. System access and its functions

- Capability that restricts access to business applications, denying or limiting access to specific users
- *Functions*:
  - Authentication
    - Verifying the identity of user
  - Authorization
    - Granting of access by a security administrator, based on a security policy
  - Access control
    - Granting or denying specifing access requests
- Functions to establish rules and privileges and moderate access to an object in the system
- Each user has to be authorized properly, defining access privileges

7.2. Authentication factors and means

- Simplest way to access, including an identification and verification step
- Authentication factors are methods
  - The user has (possession factor) - tokens/smart cards/wireless tags
  - The user knows (knowledge factor) - passwords/PINs/tokens
  - The user is or does (inherence factor) - biometrics

7.3. Authenticators

- Means used to confirm a user/process/device
- Can be:
  - Multi-factor: use of one or more authentication means
  - Password-based: use of an ID and a password

7.4. Vulnerability of a password

- Instead of using a file retrieved by ID, to avoid storing password one can use a one-way hash function of the password
- Different kinds of attacks exist
  - Dictionary attacks
  - Specific account
  - Popular password
  - Password guessing
  - Hijacking
  - Monitoring/Exploiting
- Rely on hardware/SSO/password managers to avoid problems
- Select password not too short or easy to guess, eliminating guessable passwords

7.5. Hashed password and salt

- Combine the password with a fixed length salt value using an hashing algorithm
- In verification, the ID is used to see if result matches, therefore password is accepted
- Salt usage
  - prevents duplicate password
  - increases difficulty for attacks
  - nearly impossible to use same password for more systems
  - is non-deterministic

7.6. Password cracking

- Process of recovering secret password stored in a system
- Many approaches like developing a dictionary to crack all words or precomputing hash values

7.7. Password file access control

- Deny the attacker access to the password file
- Allowing it only for a privieged user
- File can become readable or physical security might be a problem, to use a policy to force users selecting passwords difficult to guess

7.8. Possession-based authentication

- Object the user possess for user authentications = hardware tokens
- *Memory cards*: have an electronic memory, store but do not process data, used for physical access alone
  - May require specific requirements and can be lost
- *Smart tokens*: have some specific physical characteristics, user interface, electronic interface and authentication protocol
  - Have a smart card, a microprocessor and a processing circuit
- *Electronic identity cards*: also called eID, they provide stronger proofs of identity, given thy are verified by a government
- *One-Time Password (OTP) device*: it generates one time passwords, using a seed embedded

7.9. Biometric authentication

- Based on the specific individual characteristics
- Technically complex and expensive
- Nature and requirements should be considered, being universal, distinct, permanent and collectable
- Should meet some criteria:
  - Performance and accuracy
  - Difficulty of circumventing
  - Acceptability by users

7.10. Access control

- Gaining the ability to communicate or interact with a system. In other words, the process of granting or denying specific requests, via specific services and mechanisms

- ACCESS CONTROL = AUTHENTICATION + AUTHORISATION
- Has different inputs
  - Who issued the request
  - What is requires
  - What rules apply
- *System access* deals with moderating access to system objects via authentication (establishing user identity) and authorisation (defining user privileges)

7.11. Access control elements

- *Subject*
  - Entity capable of accessing objects
  - Typically considered accountable for their actions
  - Can be creators of resources, groups of users or every user possible to access
- *Object*
  - Resource which access is controlled and used to contain and/or receive information
- *Access rights*
  - The ways in which a subject can access an object

7.12. Access control policies

- Dictates what types of access are permitted
- Different categories exist:
  - *Discretionary access control (DAC)*
    - Based on requestor identity and on access rules, granting specific permissions
  - *Mandatory access control (MAC)*
    - Comparison between security labels (sensitiveness of resources) with security clearances (which resources to access)
    - Has to be mandatory, so not to enable user wishes
  - *Role-based access control (RBAC)*
    - Access control based on user roles
    - Role permissions can be inherited through an hierarchy
    - Can apply to a single or several individuals
  - *Attribute-based access control (ABAC)*
    - Access control based on attributes associated with and abot subjects and objects, combining attributes under which an access takes place

7.13. Access control structures

- Access matrix = using access control lists (ACLs) or capability tickets
- Governed by a set of rules granting the subject access

7.14. Customer access

- Each customer needs to be uniquely approved and identified, both indivodual and in groups, responding to organization’s business requirements
- Each one should be aware and trained
- Balance between customer satisfaction and meeting security requirements
- Subject to the same types of technical controls, defining access privileges and selecting an appropriate authentication procedure

8. M3.3 - Cybersecurity Operations and Management

8.1. Computer Security Incident Response Team (CSIRT)

- Responsible for rapidly detecting incidents
- Minimizing loss and destruction
- Mitigating the weaknesses that were exploited
- Restoring computing services
- Calculates the added value to invest in safety resources
- In small organizations can be the security team, in large ones they are two separate entities

8.2. Security Incidents

- Any action that threatens one or more of the classic security services
- Unauthorized access or modification
- Procedures to manage them
  - Sorting, detecting, identifying, documenting

8.3. Managing, detecting and responding to incidents

- Should be detected and reported
  - Manually (reports)
  - Automatically (with integrity/log tools)
- Triage
  - find the single point of contact for services and request additional information to categorize the incident and notify parts of the enterprise
- Documentation to respond to them
  - Detail/Describe/Identify categories, personnel, circumstances
  - Should immediately follow a response to the incidents
    - What
    - How
    - Details
    - Impact
  - Allows for reviewing the risk assessment and strengthening controls
- Once an incident is opened, has to go through a number of states until no further action is required and is considered closed

Security controls are in place throughout:

- Hardware
- Software
- Firmware

8.4. Malware and protection

- Program inserted into others compromising confidentiality, integrity, availability
- Many types and should be protected against them as much as possible
  - Clickless
  - Fileless
  - Adwares
  - Worms/Viruses, etc.
- Businesses are experiencing more and more
- Practical steps to take, avoiding attack and defending against different attack surfaces
- Protection software to use to protect against them, automating actions as much as possible, verifying all defenses and collecting results from all points of attack
  - Scanning
  - Monitoring
  - Identifying
  - Disinfecting
- Software has to be accompanied by other measures like whitelist, firewalls and virtualization

8.5. Intrusion Detection

- The sooner the intrusion is detected, the less damage can be done
- When an intrusion happens, confidentiality is lost on all levels and collecting informations can help assessing risks and other means of security
- No exact distinction between an attack and normal use of resource: some overlap might happen
- Identification between legitimate and new user
- Approaches
  - *Misuse detection*: take the strange behaviour and consider it as normal attack, via usage of patterns and signatures. It cannot detect novel/unknown attacks
  - *Anomaly detection*: detect activities different from normal behavior and be able to detect previously unknown attacks, having a trade-off between false positives and false negatives
- Intrusion Detection System
  - Sensors: collecting data and inputs
  - Analyzers: receive data from sensors and support evidence
  - User interface: give user output
- Techniques
  - Host-based
    - Layer of security to detect intrusions, events and send alerts
    - Detect thresholds and profiles

- Network-based
  - Monitor the traffic on the networks and see if packets match signatures
  - Can use sensors to gather data and feed information
  - It can see data inside the network but also outside of firewalls

8.6. Data Loss Prevention

- Information leakage can happen in an untrusted environment
- Monitor, and protect data in use and data at rest through deep content inspection
- Often includes unencrypted content
- Sensitive data should be precisely identified in an enterprise via different means
  - rule-based/fingerprinting/exact-partial file matching
- Data states
  - Data at rest = big risk with info stored throughout the enterprise
  - Data in motion = data trasmitted over enterprise networks, subject to active/passive monitoring of information across enterprise networks
  - Data in use = part of media and saved physically somewhere, controlling the movement in end-user systems