

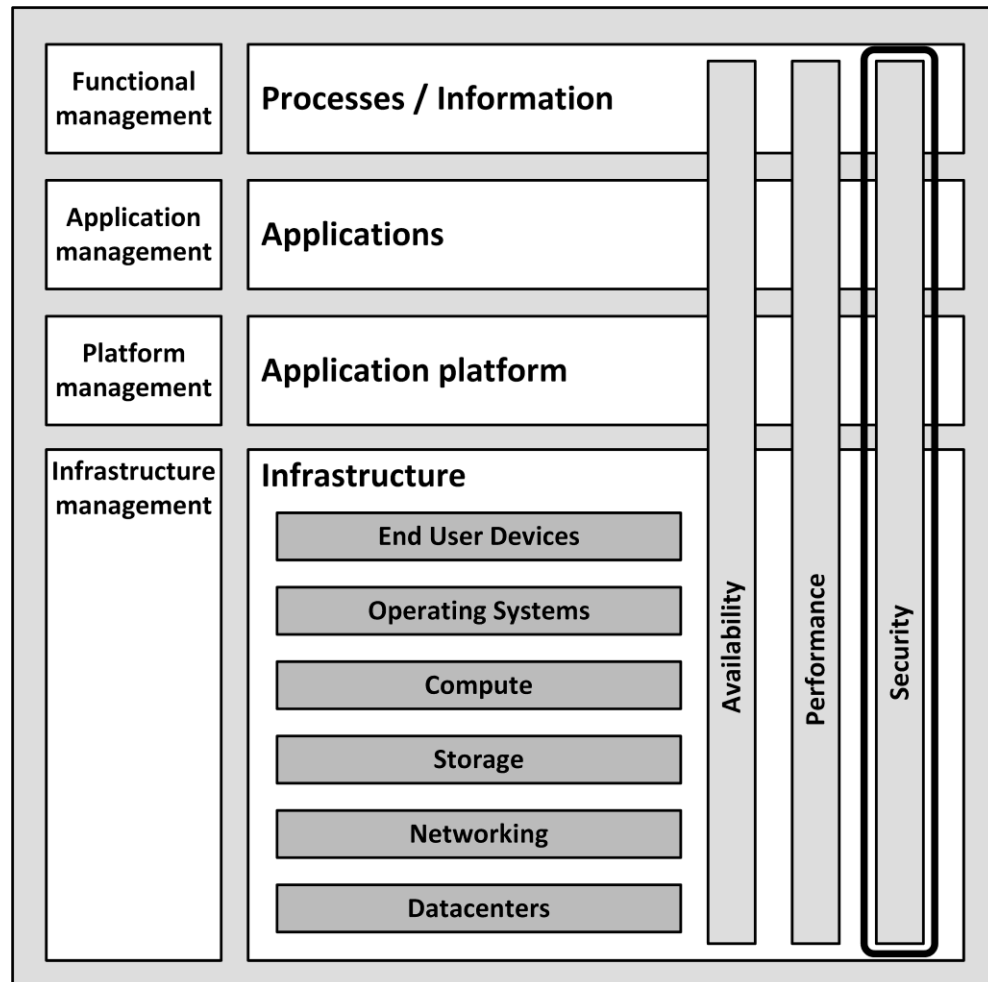
# IT Infrastructure Architecture

Infrastructure Building Blocks  
and Concepts

Security Concepts

# Introduction

- Security is the combination of:
  - Availability
  - Confidentiality
  - Integrity
- Focused on the recognition and resistance of attacks
- For IT infrastructures availability is a non-functional attribute in its own right



# Computer crimes

- Reasons for committing crime against IT infrastructures:
  - Personal exposure and prestige
  - Creating damage
  - Financial gain
  - Terrorism
  - Warfare

# Risk management

# Risk management

- Managing security is all about managing risks
- The effort we put in securing the infrastructure should be directly related to the risk at hand
- Risk management is the process of:
  - Determining an acceptable level of risk
  - Assessing the current level of risk
  - Taking steps to reduce risk to the acceptable level
  - Maintaining that level

# Risk list

- A risk list can be used to quantify risks
- Risk is calculated based on:
  - Asset name - component that needs to be protected
  - Vulnerability - weakness, process or physical exposure that makes the asset susceptible to exploits
  - Exploit - a way to use one or more vulnerabilities to attack an asset
  - Probability - an estimation of the likelihood of the occurrence of an exploit
  - Impact - the severity of the damage when the vulnerability is exploited

# Risk list

- P=Probability
- I=Impact
- R=Risk

<b>Asset</b>	<b>Vulnerability</b>	<b>Exploit</b>	<b>P</b>	<b>I</b>	<b>R</b>
Laptop	Laptop gets stolen	Sensitive data on hard disk is exposed	5	3	15
Printer	Printer hard disk contains sensitive data	Repair man could swap hard disk and the hard disk could get on the market with sensitive data	1	3	3
Work-stations	Virus attack unknown to virus scanner	Unavailability or disclosure of data	2	3	6
SAN storage system	Data protection via LUN masking contains error	Data could get exposed to wrong server	1	2	2

# Risk response

- There four risk responses:
  - Acceptance of the risk
  - Avoidance of the risk - do not perform actions that impose risk
  - Transfer of the risk - for instance transfer the risk to an insurance company
  - Mitigation of the risk and accepting the residual risk



# Exploits

- Information can be stolen in many ways
- Examples:
  - Key loggers can send sensitive information like passwords to third parties
  - Network sniffers can show network packages that contain sensitive information or replay a logon sequence
  - Data on backup tapes outside of the building can get into wrong hands
  - Disposed PCs or disks can get into the wrong hands
  - Corrupt or dissatisfied staff can copy information
  - End users are led to a malicious website that steals information (phishing)

# CIA

- Three core goals of security (CIA):
  - Confidentiality - prevents the intentional or unintentional unauthorized disclosure of data
  - Integrity - ensures that:
    - No modifications to data are made by unauthorized staff or processes
    - Unauthorized modifications to data are not made by authorized staff or processes
    - Data is consistent
  - Availability - ensures the reliable and timely access to data or IT resources by the appropriate staff

# CIA

- Example of confidentiality levels

Confidentiality Level	Description
1	Public information
2	Information for internal use only
3	Information for internal use by restricted group
4	Secret: reputational damage if information is made public
5	Top secret: damage to organization or society if information is made public

# CIA

- Example of integrity levels

<b>Integrity Level</b>	<b>Description</b>
1	Integrity of information is of no importance
2	Errors in information are allowed
3	Only incidental errors in information are allowed
4	No errors are allowed, leads to reputational damage
5	No errors are allowed, leads to damage to organization or society

# CIA

- Example of availability levels

Availability Level	Description
1	No requirements on availability
2	Some unavailability is allowed during office hours
3	Some unavailability is allowed only outside of office hours
4	No unavailability is allowed, 24/7/365 availability, risk for reputational damage
5	No unavailability is allowed risk for damage to organization or society

# Security controls

- Controls mitigate risks
- Security controls must address at least one of the CIA
- Information can be classified based on CIA levels
- Controls can be designed and implemented based on the identified risk level for CIA

# Security controls

- Example

[illegible]

# Attack vectors

- Malicious code
  - Applications that, when activated, can cause network and server overload, steal data and passwords, or erase data
- Worms
  - Self-replicating programs that spread from one computer to another, leaving infections as they travel
- Virus
  - Self-replicating program fragment that attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels
- Trojan Horse
  - Appears to be useful software but will actually do damage once installed or run on your computer



# Attack vectors

- Denial of service attack
  - An attempt to overload an infrastructure to cause disruption of a service
  - Can lead to downtime of a system, disabling an organization to do its business
  - In a Distributed Denial of Service (DDoS) attack the attacker uses many computers to overload the server
  - Groups of computers that are infected by malicious code, called botnets, perform an attack

# Attack vectors

- Preventive DDoS measures:
  - Split business and public resources
  - Move all public facing resources to an external cloud provider
  - Setup automatic scalability (auto scaling, auto deployment) using virtualization and cloud technology
  - Limit bandwidth for certain traffic
  - Lower the Time to Live (TTL) of the DNS records to be able to reroute traffic to other servers when an attack occurs
  - Setup monitoring for early detection

# Attack vectors

- DDoS countermeasures:
  - Immediately inform your internet provider and ask for help
  - Run a script to terminate all connections coming from the same source IP address if the number of connections is larger than ten
  - Change to an alternative server (with another IP address)
  - Scale-out the public facing environment under attack
  - Reroute or drop suspected traffic

# Attack vectors

- Social engineering
  - Social skills are used to manipulate people to obtain information which can be used in an attack
    - Like passwords or other sensitive information
  - By nature, people want to help other people

# Attack vectors

- Phishing
  - A technique of obtaining sensitive information
  - The phisher sends an e-mail that appears to come from a legitimate source, like a bank or credit card company, requesting "verification" of information
  - The e-mail usually contains a link to a fraudulent web page

# Attack vectors

- Baiting
  - Baiting uses physical media, like an USB flash drive, left to be found
  - It relies on the curiosity of people to find out what is on it
  - The attacker hopes some employee picks up the device and brings it inside the organization
  - When the device is put into an organization owned PC, malicious software is installed automatically