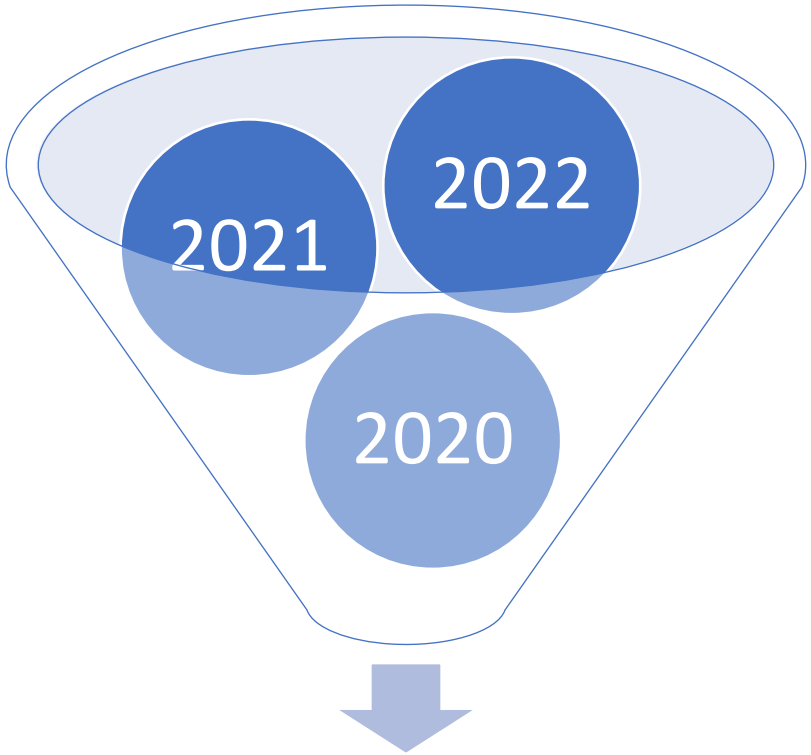
Information security

Sanita Meijere

09.11.2022

Why



Increase in attacks

Information security goals

Ensure uninterrupted availability of resources

Ensure compliance with policies and laws

Period of time during which an IS is not available

Costs of downtime vary depending on:	Industry
	Size of company

#1 cause of system downtime is hardware failure

Major causes of hardware damage

Natural disasters

Fires, floods, earthquakes, hurricanes, tornadoes, and lightning

Blackouts and brownouts

Blackout: total loss of electricity

Brownout: partial loss of electricity

- **Uninterruptible power supply (UPS)**: backup power for a short time

Vandalism

Data related risks

Data – most valuable asset

Data and applications subject to disruption, damage, theft

Cyber terrorism

Terrorist attacks on organizations' IS to:

- Disrupt network communication
- Implement denial of service attacks
- Destroy / steal information

Denial of service (DoS)

- Attacker launches large number of information requests
  - Slows down legitimate traffic to site

Distributed denial of service (DDoS)

- DoS attack from multiple computers
  - Usually from hijacked computers called “zombies”
  - There is no definitive cure for this
  - A site can filter illegitimate traffic

Hacking

= UNAUTHORIZED ACCESS

HONEYTOKEN: BOGUS RECORD IN NETWORKED DATABASE USED TO COMBAT HACKERS

Hijacking

Using some or all computer's resources without consent of its owner:

- for DDoS attack
- installing software **bot** (due to security hole in App or Operating System), usually installs email forwarding software

Main purpose of hijacking is to send spam

Some definitions

- **Honeypot**: server containing a mirrored copy of database / bogus database to educate security officers about vulnerable points
- **Virus**: spreads from computer to computer
- **Worm**: spreads in network w/o human intervention
- **Antivirus software**: protects against viruses
- **Trojan horse**: virus acting as legitimate software
- **Logic bomb**: software that is programmed to cause damage at a specific time

Other damage

Unintentional, non-malicious damage caused by:

- Poor training
- Lack of adherence to backup procedures
- Unauthorized downloading and installation of software
- Human error

Access Controls

Measures taken to ensure only authorized users have access to computer, network, application, or data

- Physical locks: secure the equipment in a facility
- Software locks: determine who is authorized

Access Controls

Types of access controls

- What you know: access codes, such as user ID and password
- What you have: requires special devices (cards)
- Who you are: unique physical characteristics (biometry)

Firewalls

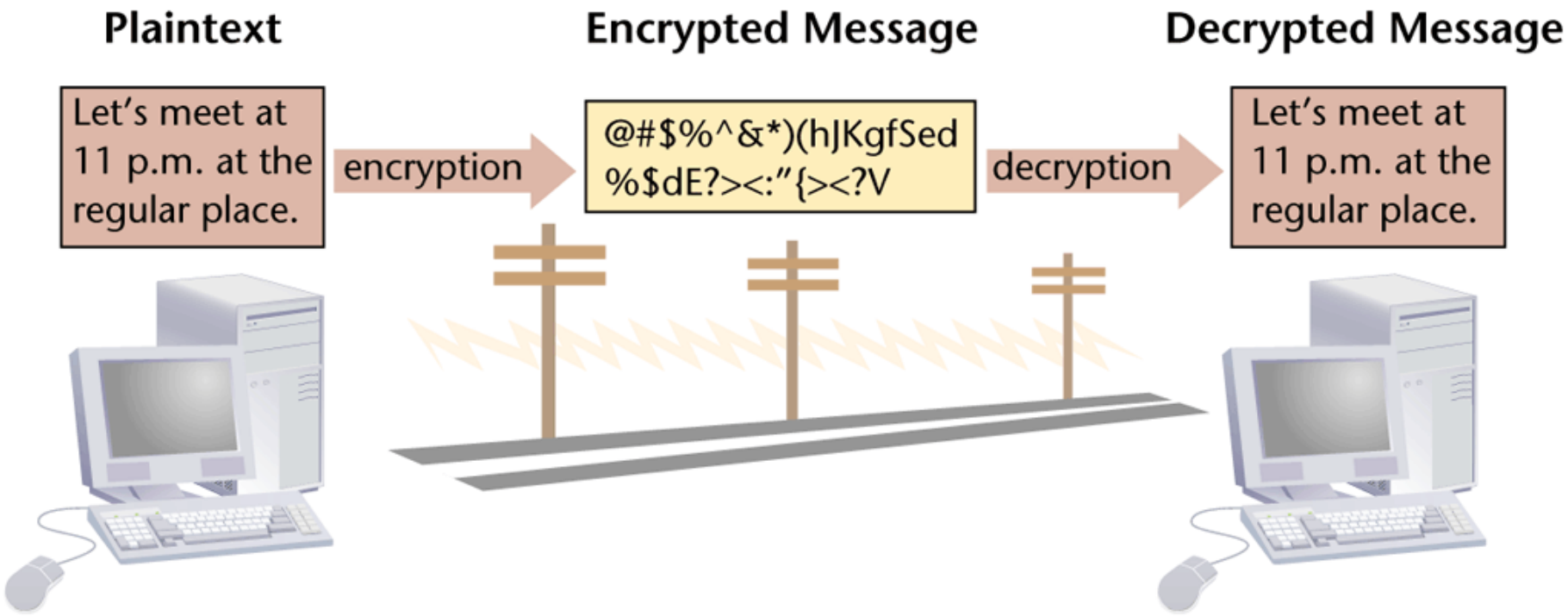
Hardware and software that blocks access to computing resources - the best defense against unauthorized access over the Internet

Encryption

Encryption: coding a message into unreadable form

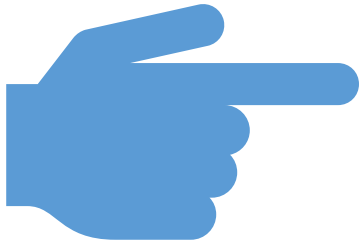
- Important when communicating confidential information

Encryption slows down communication - every message must be encrypted and then decrypted



Encrypting communications increases security

Single Sign On



User must enter name/password only once

Saves time

The Business Recovery Plan

Detailed plan about what should be done and by whom if critical systems go down

Also called:

- disaster recovery plan (DRP)
- business resumption plan
- business continuity plan

- Questions