# Security essentials

## H1: Cybersecurity world

### What is cybersecurity:

It refers to a set of techniques used to protect the integrity of networks/programs/data from attacks/unauthorized acces.

### Where?:

* Applications
* Configuration
* Infrastructure
* Users

### Fix:

Identificeren 🡪 analyseren 🡪 behandelen

### Identiteit:

#### Persoons-identiteit:

* Identiteitskaart
* Financiele identiteit
* Online identiteit

#### Bedrijfsidentiteit:

* Toegang
  + Data
  + Kennis
* Human factor
  + Vertrouwen

### Cybersecurity for you:

* Unieke paswoorden:
  + Voldoende lengte
  + Verschillende cijfers/letters/random tekens
  + Paswoordmanager
* Two-factor authentication:
  + Sms
  + App/software
  + Hardware token
* Waar goede encryptie:
  + Harddrive/usb/gsm
  + Browsen/mails
  + Messaging

### Advantages of the attacker:

A picture containing graphical user interface

Description automatically generated

## Diagram Description automatically generatedH2: The security cube

### Dimensie 1: CIA Triad – Principles of security

The goals to protect the cyberspace.

* Confidentiality
  + (un)authorized users
  + Keeping secrets
  + Privacy
  + Acces control
    - Authentication
    - Authorization (wie mag er in)
    - Accounting
* Integrity
  + Data quality
  + Accuracy
  + Trustworthiness
  + Integrity check
    - Hash functions
    - Data validation check
* Availability
  + 24/7
  + Protected from attacks
    - Protected from natural disasters
    - Disaster recovery plans
  + Backups!
  + Maintenance

### Dimensie 2: Information states

* Data in transit
* Data at rest or in storage
  + Backups!
* Data in process

### Dimensie 3: Countermeasures

Skills and discipline of a cybersecurity professional.

* Technologies
  + Software based safeguards
    - Software firewall
    - Network and port scanner
    - antiVirus
    - IDS (intrusion detection scanners)
  + Hardware based safeguards
    - Firewall
    - IPS (intrusion prevention system)
    - Dedicated IDS
  + Network based safeguards
    - VPN (virtual private network)
    - NAC (network access control)
    - Wireless access point security
  + Cloud based safeguards
    - Saas
    - Iaas
    - Paas
* Policies, procedures and guidelines
  + Educating/training users/admin
  + Setting certain policies
* Users of cyberspace

### Security life circle & defense in depth:

Diagram

Description automatically generated

Diagram

Description automatically generated

## H3: The art of protection secrets

### Graphical user interface, diagram Description automatically generated with medium confidenceCryptography:

Techniek die data of informatie verstopt/beveiligd. Dit zodat hackers niet aan je informatie geraken.

#### Cryptology:

Het maken en ontcijferen van geheime codes.

### Symmetric encryption:

Zowel de encryption als decryption gebruikt dezelfde secret key.

Timeline

Description automatically generated

### Asymetric encryption:

Bij de encryptie word een publieke key gebruikt terwijl er bij de decryptie een private key word gebruikt.

Timeline

Description automatically generated

### Hashes:

Het verifieren dat een document niet is verandert. Een authenticatie de gebeurt dankzij een hexadecimale code.

### Classical cryptography:

#### Transposition:

Rearranging the order of characters.

* Fractionation: working with fractions of the plain tekst
* Substitution: Replacing characters by other characters
  + Simple: per character
  + Polygraphic: per group of characters

#### Caeser or shift cipher:

Alfabet + x = nieuwe letter

#### Substitution:

Lees hierboven.

Diagram

Description automatically generated

#### Enigma:

The thing the germans used.

### Modern cryptography:

* Symmetric
* Asymetric

#### DES (Data encryption standard):

* Key length: 64 bits
* Block cipher
* Not secure since 1995

🡪 Tripple des (3DES)

#### AES (advanced encryption standard):

* Key length: 128,192,256
* Block cipher 128 symmetric

## H4: Ensuring data integrity

### Hashing:

Ensuring data remains the same/is not compromised. Hashing can never be changed back. It’s basically an ID that is connected to a file in a certain state.

Hashing does not equal encryption/decryption.

#### How:

Using a tool that takes data and produces a fixed-length representation for that data called the hash value.

#### Rules:

The same input generates the same hash. If the input changes the entire hash changes.

The input can be any length. The hash has a FIXED length. The hash is irreversible.

### Broken Hashing algorithms:

* MD5:
  + 128 bit
  + Not used for passwords
  + Used to check integrity of files
* SHA: secure hash algorithm
  + Sha1:
    - 160 bit hash
  + Sha2:
    - 6 hash algorithms
    - SHA-224,SHA-256,…
  + Sha3:
    - Based on another cryptographic family
    - Not like md5

### Secure hashing algorithms:

* Bcrypt:
  + Based on symmetric encryption
  + Blowfish algorithm
  + Integrated salting
  + Uses KDF to protect against brute force
  + Attackers need way more RAM
* Argon2:
  + Alot more RAM/GPU needed
  + Customizable

### Salting:

Adding random data to the data before it enters a hash function.

Makes password hashing more secure!

Best practice word er gebruik gemaakt van een random salt generator. Hierdoor word salt never reused.

### Hashing and attacks:

#### Collision attack:

Trying to find two messages that produce the same hash value.

#### Brute force:

Attempts to determine a secret/password by trying every possible combination.

Dit kan van 2 sec tot 3+ jaar duren.

#### Dictionary attack:

Typically a guessing attack which uses precompiled list of options. Rather than trying every option, only try complete options which are likely to work.

🡺 Men gebruikt een ‘woordenboek’ van pre-defined woorden/namen.

#### Rainbow attack:

You actually work backwards from the hashed/encrypted text. The attacker will run through the algorithm to get every possible output given every possible input. The list of inputs may be brute force, dictionary, or hybrid. Based on the list of outputs, the attacker now has a reusable table mapping inputs to known outputs.

### Hashing applications:

Hashes are used everywhere: Passwords,crypto,fingerprints,ensuring data integrity.

Afbeelding met tekst, visitekaartje, schermafbeelding

Automatisch gegenereerde beschrijving

#### HMAC:

Checkt of een bericht is aangepast als het verstuurd word over een untrusted netwerk.

### Certificates:

Equal to a digital passport. Proves that the instance you are surfing to is legit.

#### Where do I get one?

At a certificate authority.

A CA functions as a licensing bureau.

Te controleren aan het slotje in je adresbalk.

Check PPT A

## H5: Protecting domains