IT-Säkerhet Föreläsning 1

# Core

## CIA and AAA

# CIA:

### Confidentiality:

Ensure the data is seen by only the intended recipients

* Encrypting

### Integrity:

Ensure the data is not corrupted or altered

* Hashing

### Availability:

Ensure the data is available when necessary

* Clustering, failover

# AAA:

### Authentication:

Ensure the identity of the entity (user, equipment, object)

* Something that you know
* Something that you have
* Something that you are

### Authorization:

Ensure that the entity is restricted to it’s pre-defined right and privileges.

### Accountability:

Ensure non-repudiation

* Auditing (Logging & tracking)

# Risk Management

#### Asset:

Your data

#### Vulnerability:

A weakness or flaw that can either

#### Threat:

The possibility of an unwanted or harmful event occurring.

*Vulnerabilities pose threat to assets!*

#### Threat source/Agent:

Users, process or natural events that can materialize a threat.

#### Attack:

An action aiming to cause harm.

* Vulnerabilities are typical targets of attacks.
* Mechanisms that use vulnerabilities are called exploits.

#### Probability:

The chances that a threat can materialize.

#### Impact:

The consequence of a materialized threat.

#### Exposure factor:

Percentage of loss if a threat is materialized. ( How much you lost )

#### Controls;

Mechanisms that aim to mitigate threats ( Help against threats)

#### Total risk:

What is the total risk that a threat is happening.

#### Residual risk:

The risk even “after” controls are in place.

*Risk from unsecure coding are relatively lower than the risks that can be sourced from humans.*

* *Wikileaks*
* *Internal Employees*

### Handling Risk

#### Ignore the risk:

Not handling the risk and leave the software as is.

#### Avoid the risk:

Discontinue or retire the software that is subject to risk.

#### Mitigate the risk:

Implementation of security controls to reduce the risk.

#### Accept the risk:

* When the cost of controls outweighs the impact of the risk.

#### Transfer the risk:

Transferring the “liability” to a 3rd party.