Introduction to principles of cyber security

Hva er data/informasjon sikkerhet?

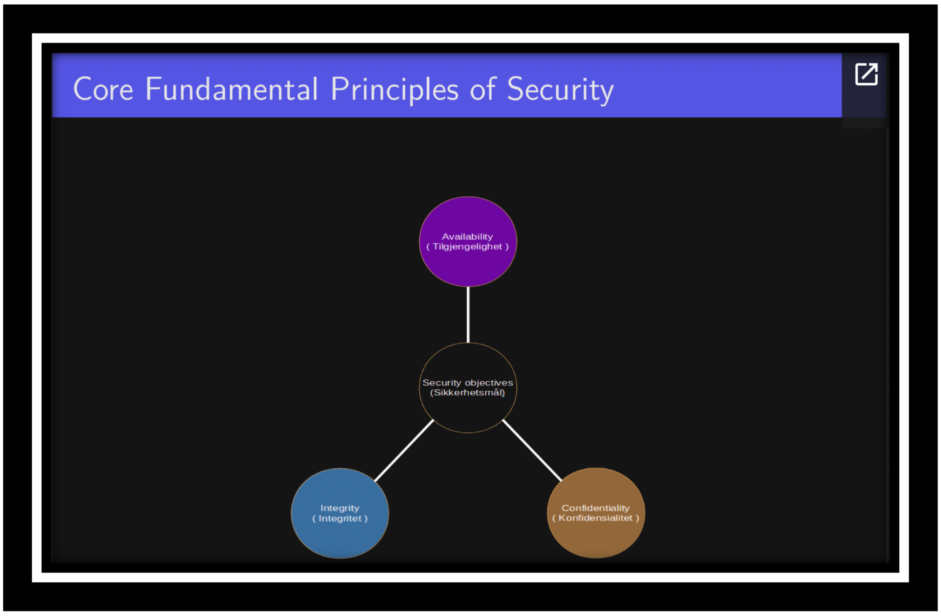
- Sikkerhet generelt handler om å beskytte viktig eller verdifulle ressurser mot uønsket handlinger. Dette refereres til datasikkerhet da de ressursene er data eller informasjon

Hva er det vi ønsker å beskytte/sikre?

- En ressurs kan være alt som har noe av en verdi for en organisasjon.
- Dette inkluderer maskiner, mennesker, software, rykte, informasjon osv.
    - Informasjon er typisk den mest verdifulle ressursen til en organisasjon og det ligger i hjertet til ethvert system.

Hvilke kjerneobjektiver søker vi for å beskytte ressursene våre?

1. konfidensialitet: et sikkerhets prinsipp eller gjenstand som fungerer for å sikre at informasjon ikke utdeles til brukere, prosesser eller gjenstander med mindre de har fått autorisert tilgang
2. integritet: Integritet innenfor datasikkerhet refererer til å sikre at dataene forblir nøyaktige, uforandrede og pålitelige gjennom hele lagrings- og overføringsprosessen.
3. tilgjengelighet: å kunne vite at man kan aksessere data og ressurser til autoriserte individer til en hver tid.



Core Fundamental Principles of Security

ADDITIONAL DESIRED PRINCIPLES OF SECURITY

Authenticity: a property achieved through cryptographic methods of being genuine and being able to be verified and trusted, resulting in confidence in the validity of a transmission, information or a message, or sender of information or a message.

Accountability/Non-repudiation: a property achieved through cryptographic methods to protect against an individual or entity falsely denying having performed a particular action related to data.

CHALLENGES OF COMPUTER SECURITY

Datasikkerhet er en kamp mellom en som ønsker å gjøre et inngrep og ønsker å finne hull og utvikleren som prøver å stenge dem alle igjen. Den store fordelen en inntrenger har er at de kun trenger å finne en svakhet mens designeren må finne og eliminere alle svakheter som må oppnås for maks sikkerhet.

De som bygger vegger tenker annerledes enn dem som forsøker å gå under, rundt, over eller gjennom dem.

IMPACT ON THE SECURITY OF OUR ASSETS

- a vulnerability is a weakness in the system that allows **threat** source to compromise its security. It can be a software, hardware (meltdown, spectre), procedural, or a human weakness that can be exploited.

We can find vulnerabilities through research, reported by the vendors, reported by hackers or individuals. There are public databases that contain discovered and reported vulnerabilities. There are also tools that can help us test our systems to check if they contain the reported vulnerabilities and we will learn some of those tools in this course.

A threat is any potential danger that is associated with the exploitation of vulnerability. If the threat that is someone will identify a specific vulnerability and use it against the company or individual, then the entity that takes advantage of a vulnerability is referred to as a threat agent.

THREATS TO COMPUTER/INFORMATION SECURITY

Interception

Unauthorized person, program or computer system gets access to resource.

Compromises the confidentiality.

Modification

Unauthorized person, program or computer system accesses and modifies the resource.

Compromises the integrity.

Interruption

Resource is lost, made inaccessible or unusable.

Compromises the availability.

Fabrication

Unauthorized person, program or computer system manufactures/produces fake objects and presents them as authentic.

Compromises the authenticity.

A threat agent/attacker is the person or mechanism that exploits the identified weakness to gain access to our assets. A threat agent could be an intruder accessing the network through a port on the firewall, a process accessing data in a way that violates the security policy.

An **employee** circumventing controls in order to copy files to a medium that could expose confidential information.

THREAT AGENTS AND METHODS THEY USE

When we identify the vulnerabilities that are inherent to our organization and its systems, it is important to also identify the sources that could attack them. The most obvious threat source is the malicious attacker who intentionally pokes and scan our systems looking for vulnerabilities to exploit. In the past, this was a sufficient description of this kind of threat source.

Increasingly, however, organizations are interested in profiling the threat in detail to more accurately determine:

Which attacks are likely to originate from each group based their capabilities as well as their tactics, techniques, and procedures (TTP).

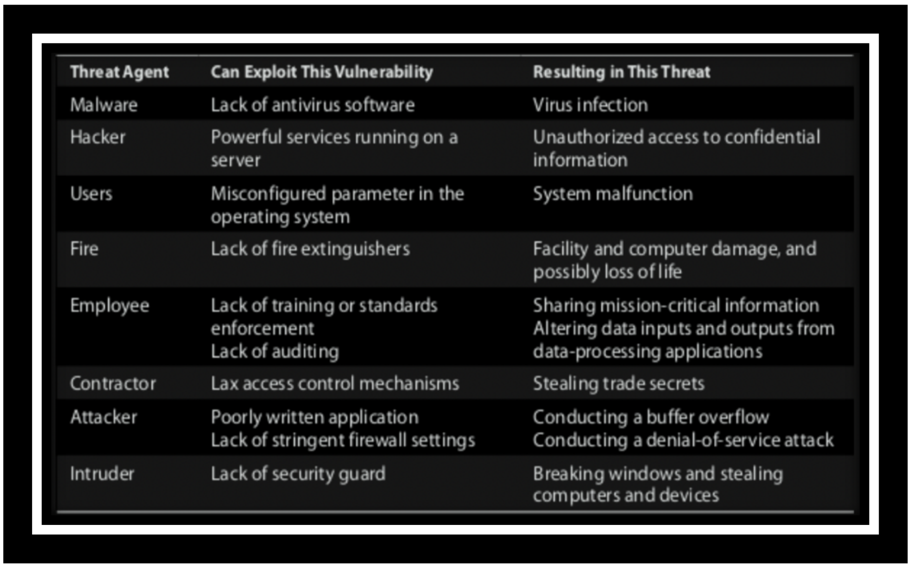
MITRE ATT&CK
(adversarial tactics, techniques, and common knowledge)

MITRE ATT&CK er et rammeverk som beskriver taktikker, teknikker og vanlig kunnskaper som cyberangripere bruker i sine angrep. Dette rammeverket ble utviklet av MITRE Corporation, en ideel organisasjon som arbeider innen teknologi- og sikkerhetsfelt.

MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on a real-world observation.

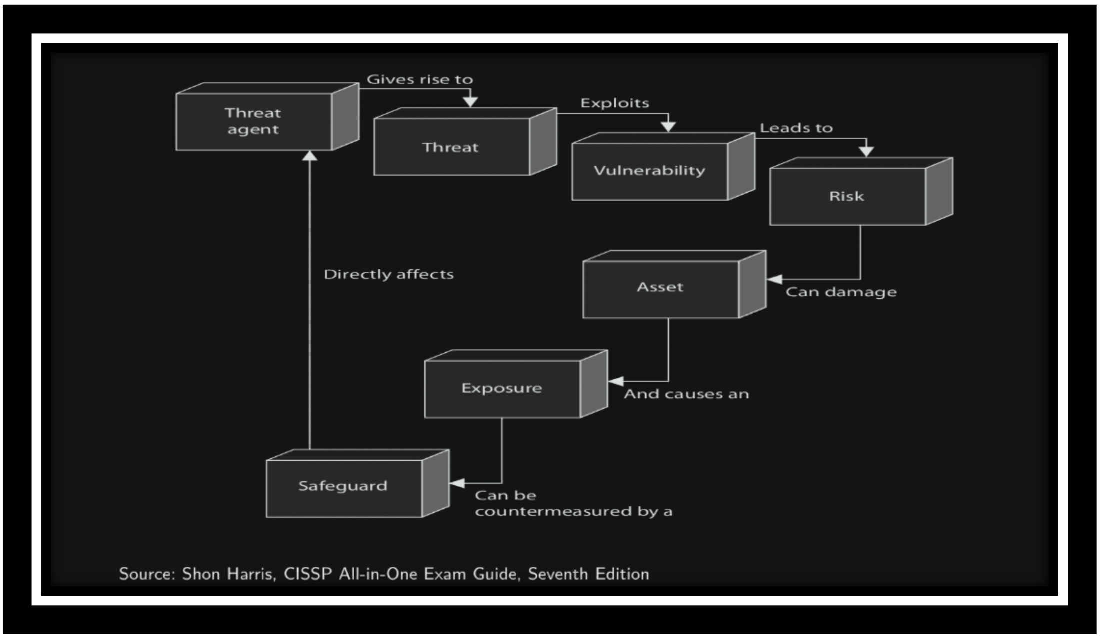
- Tactics represent the "why" of an ATT&CK technique or sub-technique.
- Techniques represent 'how' an adversary achieves a tactical goal by performing an action.
- Procedures are specific implementations of techniques.

THREATS AND VULNERABILITIES



Threat Agent	Can Exploit This Vulnerability	Resulting in This Threat
Malware	Lack of antivirus software	Virus infection
Hacker	Powerful services running on a server	Unauthorized access to confidential information
Users	Misconfigured parameter in the operating system	System malfunction
Fire	Lack of fire extinguishers	Facility and computer damage, and possibly loss of life
Employee	Lack of training or standards enforcement Lack of auditing	Sharing mission-critical information Altering data inputs and outputs from data-processing applications
Contractor	Lax access control mechanisms	Stealing trade secrets
Attacker	Poorly written application Lack of stringent firewall settings	Conducting a buffer overflow Conducting a denial-of-service attack
Intruder	Lack of security guard	Breaking windows and stealing computers and devices

A risk is the likelihood of a threat source exploiting a vulnerability. An exposure is an instance of being exposed to losses. A vulnerability exposes an organization to possible damages. A control or countermeasure is put into place to mitigate (reduce) the potential risk. A countermeasure may be a software configuration, a hardware device, or a procedure that eliminates a vulnerability or that reduces the likelihood a threat agent will be able to exploit a vulnerability.



Source: Shon Harris, CISSP All-in-One Exam Guide, Seventh Edition

SYSTEMATIC WAY TO SAFEGUARD OUR ASSETS

Identify

- Assets – (inventory system, asset management)
- Potential threats – (threat modeling, risk assessment)

Prevent

- Block attacks – (authentication, access control, encryption, firewall)
- Reduce vulnerabilities – (static/dynamic code analysis, software updates, vulnerability penetration testing)

Detect

- When an incident happens or shortly after – (monitoring systems, logs, malware scan, intrusion detection systems, integrity checksums/hashes, digital signatures)

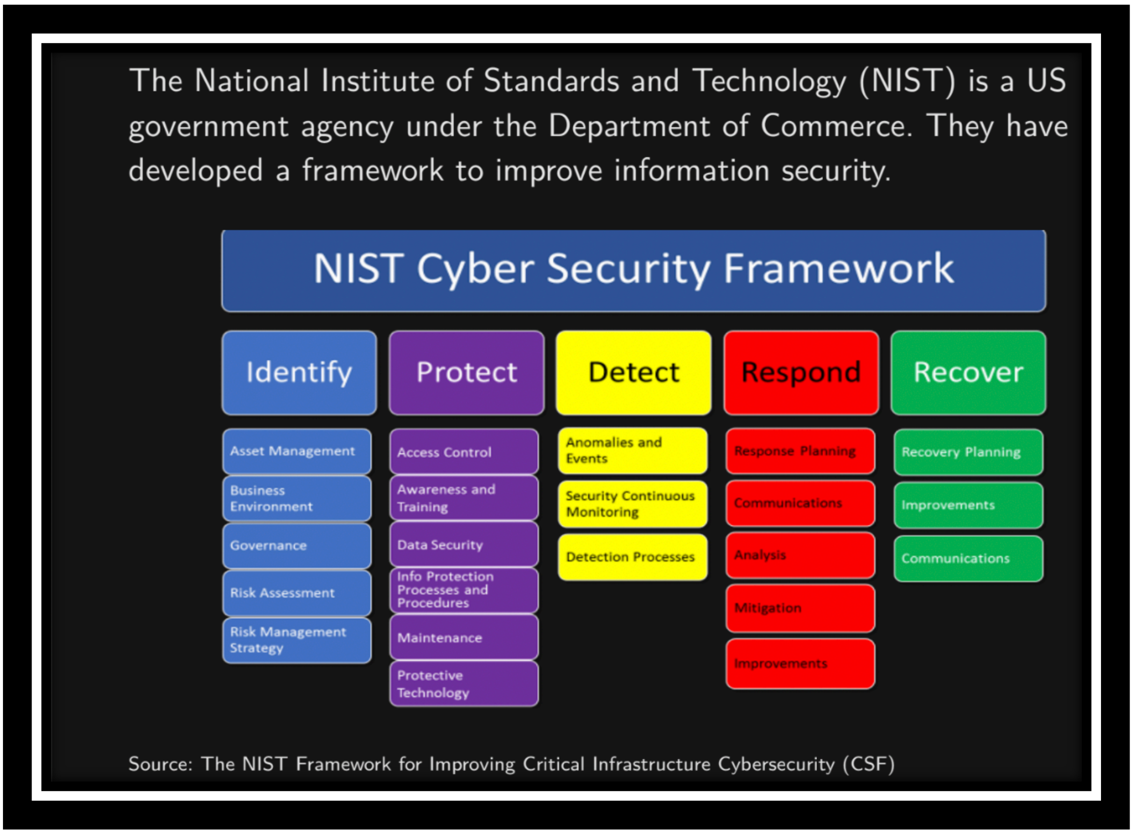
Respond

- Be able to respond to stop attacks and prevent further damage – (intrusion prevention systems, shutting down and rebuilding the system)

Recover

- Correct copy of the data can be reloaded from backup

NIST CYBER SECURITY FRAMEWORK



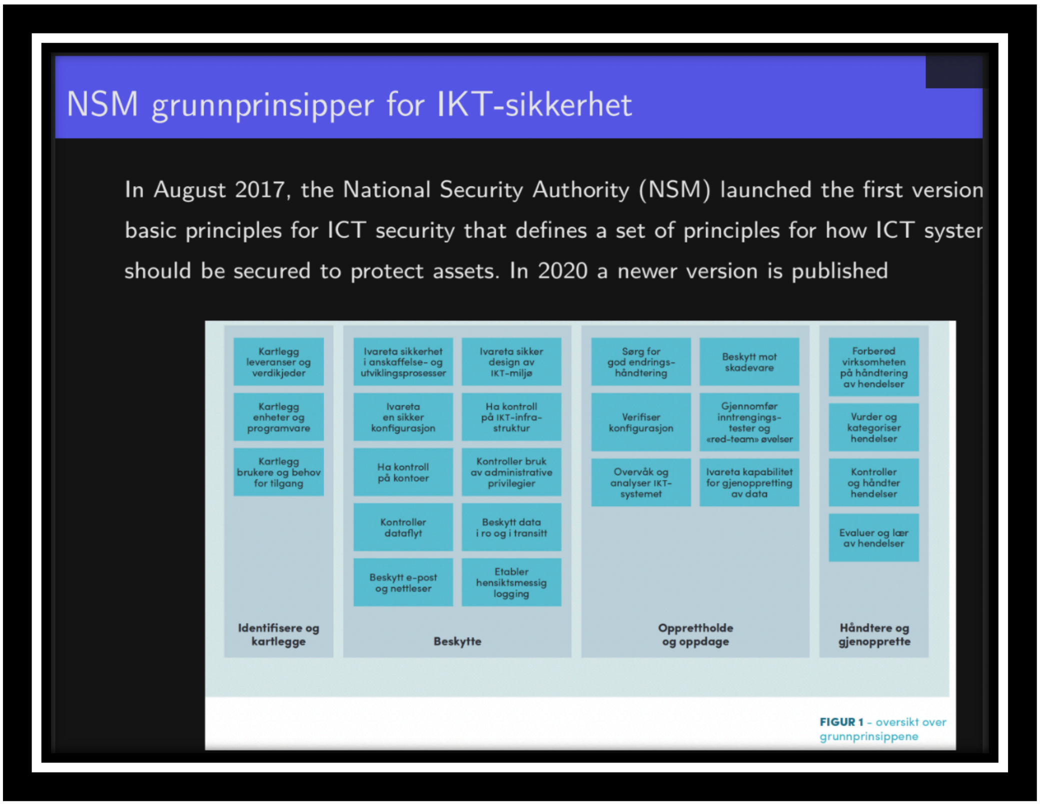
The National Institute of Standards and Technology (NIST) is a US government agency under the Department of Commerce. They have developed a framework to improve information security.

NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Source: The NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF)

NSM Grunnprinsipper for IKT-sikkerhet



NSM grunnprinsipper for IKT-sikkerhet

In August 2017, the National Security Authority (NSM) launched the first version basic principles for ICT security that defines a set of principles for how ICT syster should be secured to protect assets. In 2020 a newer version is published

Kartlegg leveranser og verdikjeder

Kartlegg enheter og programvare

Kartlegg brukere og behov for tilgang

Identifisere og kartlegge

Ivareta sikkerhet i anskaffelse- og utviklingsprosesser

Ivareta sikker design av IKT-miljø

Ivareta en sikker konfigurasjon

Ha kontroll på IKT-infra-struktur

Ha kontroll på kontoer

Kontroller bruk av administrative privilegier

Kontroller dataflyt

Beskytt data i ro og i transitt

Beskytt e-post og nettleser

Etabler hensiktsmessig logging

Beskytte

Sørg for god endrings-håndtering

Beskytt mot skadevare

Verifiser konfigurasjon

Gjennomfør inntrengings-tester og «red-team» øvelser

Overvåk og analyser IKT-systemet

Ivareta kapabilitet for gjenoppretting av data

Opprettholde og oppdage

Forbered virksomheten på håndtering av hendelser

Vurder og kategoriser hendelser

Kontroller og håndter hendelser

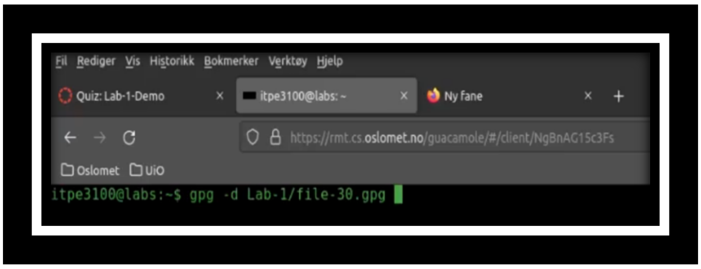
Evaluer og lær av hendelser

Håndtere og gjenopprette

FIGUR 1 – oversikt over grunnprinsippene

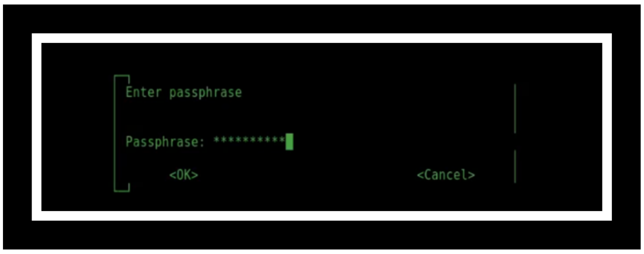
UKENTLIG ASSIGNMENT

GPG er et verktøy for å kryptere og dekryptere filer og mer. Vi legger til opsjonen -d for å dekryptere:

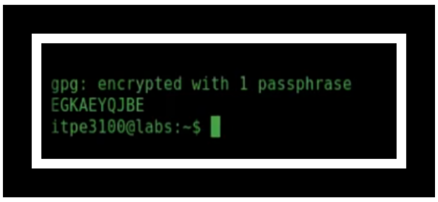

Fil Rediger Vis Historikk Bokmerker Verktøy Hjelp
Quiz: Lab-1-Demo
itpe3100@labs: ~
Ny fane
https://rmt.cs.oslomet.no/guacamole/#/client/NgBnAG15c3Fs
Oslomet
UiO

```
itpe3100@labs:~$ gpg -d Lab-1/file-30.gpg
```

Over kan vi se kommandoen for å dekryptere filen som heter file-30.gpg under mappa Lab-1. Under ser vi at det spørres etter passord:

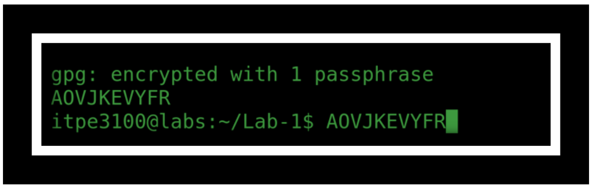


```
Enter passphrase

Passphrase: **********

     <OK>                          <Cancel>
```

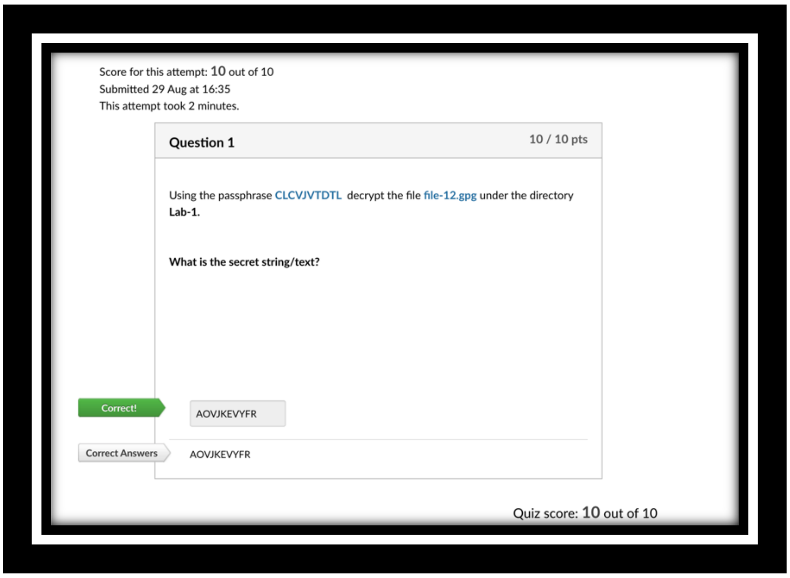


```
gpg: encrypted with 1 passphrase
EGKAEYQJBE
itpe3100@labs:~$
```

MITT RESULTAT:



```
gpg: encrypted with 1 passphrase
AOVJKEVYFR
itpe3100@labs:~/Lab-1$ AOVJKEVYFR
```



Score for this attempt: 10 out of 10
Submitted 29 Aug at 16:35
This attempt took 2 minutes.

Question 1 10 / 10 pts

Using the passphrase CLCVJVTDTL decrypt the file file-12.gpg under the directory Lab-1.

What is the secret string/text?

Correct! AOVJKEVYFR

Correct Answers AOVJKEVYFR

Quiz score: 10 out of 10