

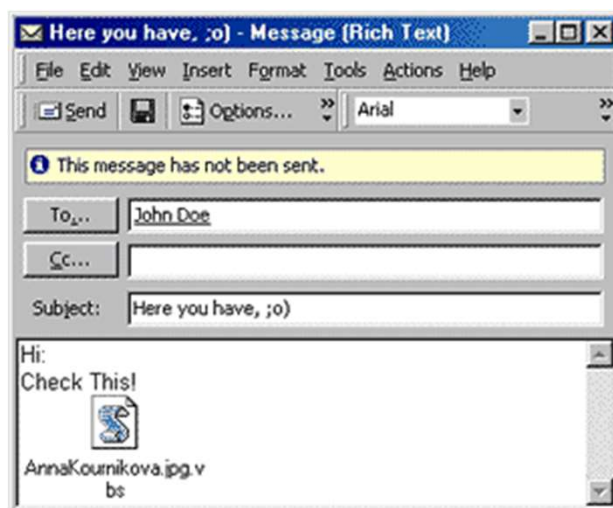
TDT4109

sikkerhet del 1

1



2001: “Here you have, ;0)”



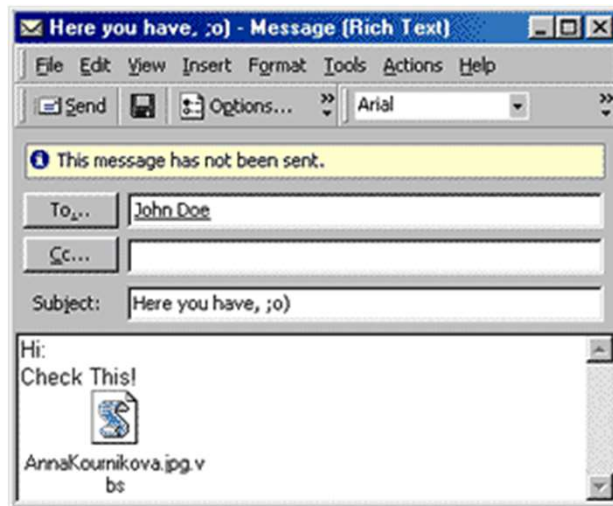
- Anna Kournikova.jpg.vbs
- Epost sendt fra en person som har deg i kontaktlisten.
- Vedlegg som benytter seg av godtroenhet, nysgjerrighet og... menneskelighet.
- Hvordan ser filnavnet ut? Hva er det egentlig?
- Hva skjer når det kjøres?
- En annen hacker (senere) som sonet tid for å ha laget Melissaviruset hjalp FBI med å finne ut hvem som laget AK.
- 150 timers samfunnstjeneste. Flaks, ganske ufarlig (i motsetning til ormen ILOVEYOU som kom året før). Mange millioner maskiner fikk det. Servere knelte.

2

2



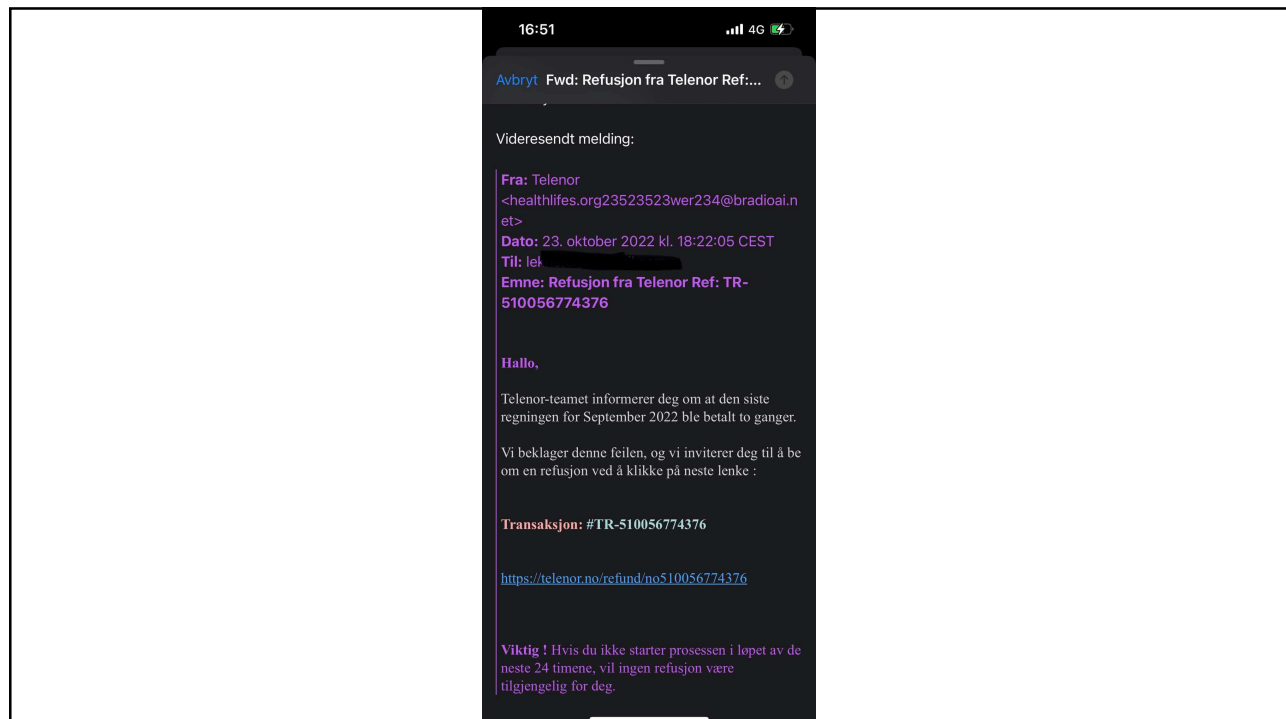
2001: “Here you have, ;0)”



- Anna Kournikova.jpg.vbs
- Epost sendt fra en person som har deg i kontaktlisten.

3

3



4

Målene med å undervise cybersikkerhet

- Elementer ved cybersikkerhet påvirker alle former for programvareutvikling
- Den store fordelene med datasystemer er [jo hvis](#) de er [på nett](#), sant
- Sette navn på ulike aspekter
- Sette disse i en kontekst
- Målet er ikke å lære dere opp til alt mulig på to timer, men å gjøre dere i stand til å kjenne igjen elementer når dere ser dem!
- Kjenne igjen trusler...

5

Termer brukt i disse to ukene

- Cybersikkerhet
- CIA-triangelet /sikkerhetsmål
 - Konfidensialitet
 - Tilgjengelighet
 - Integritet
- McCumbers kube
- Datatilstander
- Sårbarheter
- Trusler
- Sikkerhetskultur
- Risiko

6



Samfunnet

- Vi gir mer og mer ansvar til stadig mer avansert teknologi
 - Autonome biler, fjernstyrte oljeplattformer, elektroniske penger
 - Medisin, økonomi, utdanning
 - Personlig informasjon OG bedriftsinformasjon
- -> alt er koblet til alt
 - Vi samler, prosesserer, lagrer og deler enorme mengder digitale data
- Fantastiske muligheter, men nye risikoer
 - Vi må passe på data!
- Hvordan skal du og bedriften du jobber i forholde dere til dette?
 - Risikoaversjon, risikoblindhet eller risikohåndtering? Hva er risikoapetitten, og hvorfor?

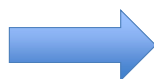
7

7



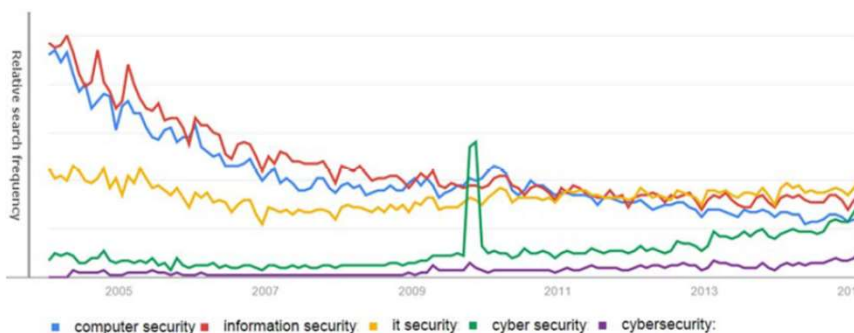
Litt historie

Computer security
Information Security
IT security



Vanlige termer
om å sikre
digital info

May 2009 [Obama speech on Cybersecurity](#)



8

8



En god definisjon av cybersikkerhet:

- *Collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices assurance and technologies that can be used to protect the cyber environment and organization and assets*

Cybersecurity Policy of South Africa, 2010

*Verktøy, retningslinjer, sikkerhetskonsepter, risikotilnærmingsmåter, handlinger, trening, teknologi
Cyberomgivelse – organisasjon og dets verdier*

9

9



La oss bryte ned cybersikkerhet

- Datasikkerhet: Å beskytte en datamaskin (og innholdet) fra seg selv, brukeren, og eksterne ting
- Dette gjelder jordskjelv såvel som ransomware eller spionasje
- **Cybersecurity er det pågående arbeidet med å beskytte nettverket og data fra *u*autorisert bruk eller skade.**

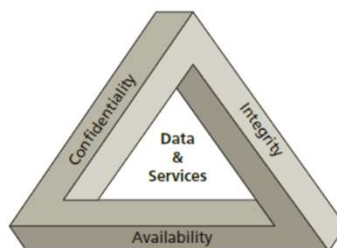
10

10



Cybersecurity-prinsipper

- **CIA triad**, industristandard i mange år
- Standarden er basert på tre typer behov ved et system:
 - Konfidensialitet
 - Integritet
 - Tilgjengelighet



11

11



Konfidensialitet

- Informasjon er **konfidensiell** når den er beskyttet slik at uautoriserte personer eller systemer ikke får tilgang
- Passer på at bare brukere med rettigheter og behov for tilgang har mulighet til å få det
- Mål på konfidensialitet
 - Informasjonsklassifisering
 - Sikker datalagring
 - Bruk av generelle sikkerhetsinstrukser
 - Opplæring av informasjonstilsynsfolk og sluttbrukere
- Tett knyttet til personvern (privacy)
- Et høyt nivå av konfidensialitet er nødvendig for personlig informasjon (GDPR)

12

12



Integritet

- Informasjon har **integritet** når den er komplett og ikke korrupt
 - Kan korrumpes ved ormer, virus etc.
- Se etter endringer i filintegritet for å se korrupsjon
 - Alternativ metode: file hashing (lab neste uke)
- Integritet er grunnsteinen i informasjonssystemer
 - Ingen verdi eller bruk hvis brukerne ikke kan stole på integriteten
- Filkorrupsjon, ikke bare fra hackere
 - Eksempelvis støy i overføringsmedia
- Bitsjekk, hashverdier og liknende brukes for å kontrollere integritet

13

13



Tilgjengelighet

- **Tilgjengelighet** gir autoriserte brukere tilgang til informasjon uten mye innblanding eller hindring, i et passende format
- Når man krever høy tilgjengelighetsgrad designes systemer for å hindre nedetid, gjennom
 - Fjerne 'single points of failure'
 - Støtte for 'reliable crossover'
 - Finne feil når de oppstår
- Hovedmål: operere i ekstreme situasjoner
 - De fem niene: 99.999% oppetid
 - Det er mindre enn 5.26 minutter per år!

14

14



Sårbarhet

- En sårbarhet (vulnerability) er en egenskap eller feil ved systemet (HW eller SW)
 - Dette kan angripe **konfidensialitet**, **integritet** og **tilgjengelighet**, enten ved at noen utnytter det eller at feil oppstår

15

15



Trusler



16

16



Hva er en trussel?

ISO 27002

Threat - a potential cause (årsak, handling) of an unwanted incident that may occur to an asset or organization

Incident – A single or a series of unwanted or unexpected events that have a significant probability of compromising business operations and threatening information security

Event– An identified occurrence of a system, service or network state indicating a possible breach of policy or failure of controls, or an unknown relevant situation

Asset (informasjonsverdi) – Anything that has value to the organization

17

17



Litt andre definisjoner? Gjør det oss klokere?

Any circumstance (omstendighet) or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

NIST

Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

ENISA

A threat can be anything, whether physical or abstract, if it has the potential to adversely affect an object or system.

DS2020

18

18



Threat actors - categories

- **Amateurs**, limited skills, use existing tools to attack
 - **Script kiddies** - just curious, or try to demonstrate their skills
- **Hackers**, break into computers/networks to gain access
 - **White hats** aim to discover weaknesses in the system
 - They take prior permission and results are reported to the owner
 - **Black hats** take advantage of any vulnerability for illegal personal, financial or political gain.
 - **Gray hats** are between white and black hat attackers.
 - Some may report the vulnerability to the owners, others publish it online so that other attackers can exploit it

19

19



Threat actors - categories

- Organized hackers
 - **Cyber criminals** - groups of professional criminals focused on control, power, and wealth.
 - Highly sophisticated and organized, cybercrime as a service
 - **Hactivists** make political statements to create awareness to issues that are important to them.
 - **State-sponsored** attackers gather intelligence or commit sabotage on behalf of their government.
 - Espionage, sabotage
 - Highly trained and well-funded
 - Their attacks are focused on specific goals beneficial to their government.

20

20



Risikovurdering – det er vanskelig, det...

- *Sannsynligheten* for at en sårbarhet blir utnyttet
- *Konsekvensen*: hvilken effekt har det hvis en sårbarhet blir utnyttet / uhell skjer
- *Risk*: kombinasjonen av sannsynlighet og konsekvens.
- Dette er vanskelig å gjøre. Hvordan måler man eksempelvis en angrippers målrettethet?

21



Situasjonsbilde - Ledelse og styring

Mangelfull risikoforståelse og verdivurdering.

- NSM erfarer at mange virksomheter mangler oversikt over sine egne verdier og egen sikkerhetstilstand. Sikkerhetsmessige utfordringer er ikke dokumentert og virksomheten har ikke formulert konkrete mål for sikkerhetsarbeidet. Ofte mangler det bevissthet omkring sikkerhetsmessig risiko og erkjennelse av at virksomheten kan være utsatt.
- Mange virksomheter har verken innhentet eller etterspurt trusselinformasjon som grunnlag for å utarbeide risiko- og sårbarhetsvurderinger.
- Virksomheter synes å være villig til å akseptere en sikkerhetsmessig risiko som NSM vurderer som uakseptabel for samfunnet som helhet.

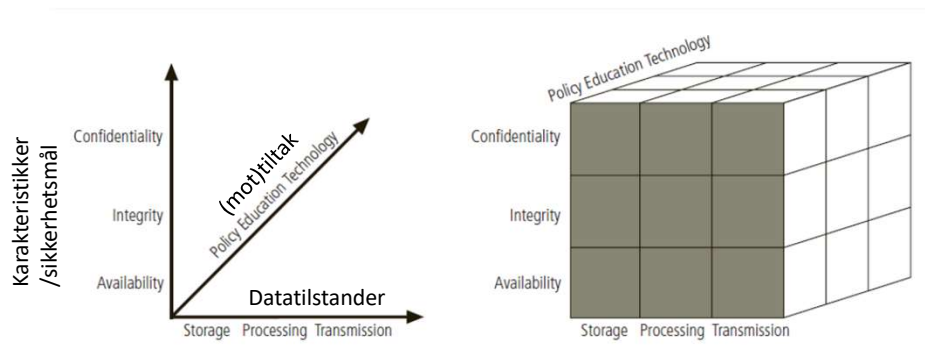
22

22



Cybersecurity Cube

- McCumber's Cube
 - En grafisk representasjon av et arkitekturvalg som brukes mye
 - 3x3x3 celler, lik Rubik's cube



The McCumber's cube (Whitman & Mattord, 2017)

23

23



Aksene i McCumber sin kube

- Sikkerhetsmål
 - Konfidensialitet
 - Integritet
 - Tilgjengelighet
- Datatilstander
 - Storage: data er lagret
 - Processing: data kvernes i en prosess
 - Transmission: data overføres på én eller annen måte
- Mottiltak
 - Policy: retningslinjer/regler som sier noe om hva man skal gjøre/ikke gjøre
 - Education: ryggmargsrefleksen. Kulturen, det du gjør når folk ikke ser på
 - Teknologi: brannmuren, og de andre tekniske løsningene

24

24



Kultur



(Stjålet fra <https://www.bridgestogether.org> – er det bra kultur da?)

25

25



Et par momenter Bjarte Malmedal beskrev

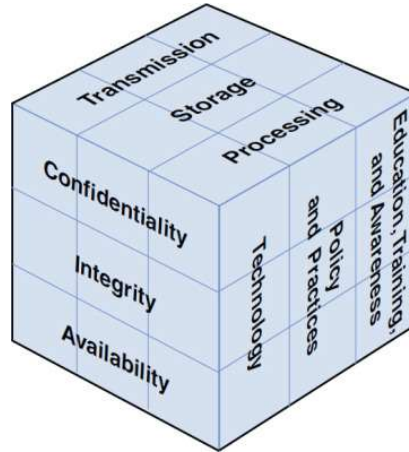
- Kultur er så mye mer enn det du kan se
- Digital sikkerhetskultur er også kultur!
- Digital sikkerhetskultur handler om menneskene
 - Hva gjør *du* hvis reglene er drakoniske, eller gjør det vanskelig å gjøre jobben?
 - Tør *du* si ifra hvis du plutselig har gjort noe galt, som kan gå ut over noe?
 - Kultur skapes av mennesker, men former også menneskene!
- Bjarte har jobbet fryktelig lenge og mye med sikkerhet, og vært med å skrive [veileder for kartlegging av digital sikkerhetskultur](#)

26

26



Oppsummering: alt henger sammen!



Figuren er hentet fra
<https://www.pearsonitcertification.com/articles/article.aspx?p=2990398&seqNum=6>

27