

TDT4109

sikkerhet del 2

1

Dagens pensum

- Hva er risiko?
- Er bedrifter klar over risiko av denne typen?
- McCumbers kube – alt satt i sammenheng!
- Sikkerhetskultur
- Sårbarheter

2



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?

3



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.

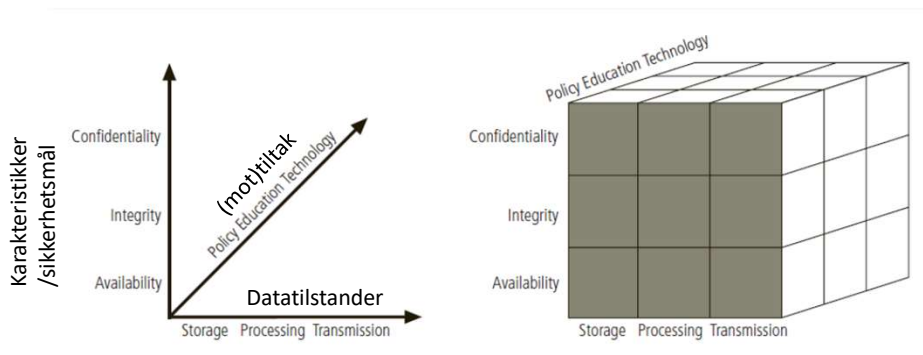
4

4



Cybersecurity Cube

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



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

5

5



Aksene i McCumber sin kube

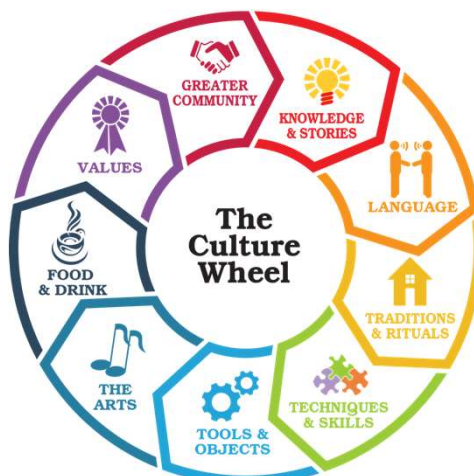
- Sikkerhetsmål
 - Konfidensialitet
 - Integritet
 - Tilgjengelighet
- Datatilstander
 - Storage: data er lagret
 - Processing: data kvernes i en prosess
 - Transmission: data overføres på én eller annen måte
- Mottiltak
 - Policy: retningslinjer/regler som sier noe om hva man skal gjøre/ikke gjøre
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

6

6



Kultur



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

7

7



Et par momenter Bjarte Malmedal beskrev

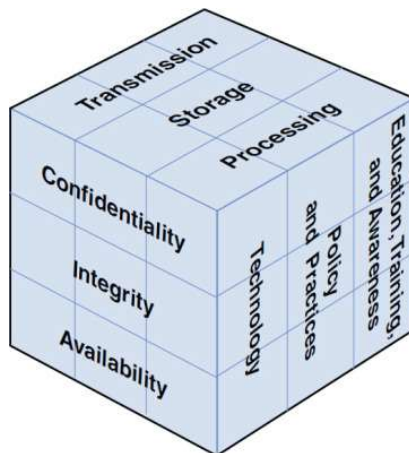
- Kultur er så mye mer enn det du kan se
- Digital sikkerhetskultur er også kultur!
- Digital sikkerhetskultur handler om menneskene
 - Hva gjør *du* hvis reglene er drakoniske, eller gjør det vanskelig å gjøre jobben?
 - Tør *du* si ifra hvis du plutselig har gjort noe galt, som kan gå ut over noe?
 - 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](#)

8

8



Oppsummering: alt henger sammen!



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

9

9



Sårbarheter

10

10



Læringsmål for denne delen

Forstå hva en (IKT-) sårbarhet er. Kjenne til ulike typer sårbarheter og hva vi kan gjøre for å redusere sårbarheten i egne systemer.

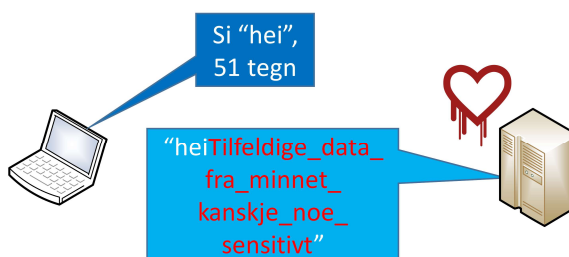
11

11



En sårbarhet er en svakhet som muliggjør at sikkerheten i et IKT-system kan bli brutt

- Tekniske
- Fysiske
- Prosedyremessige
- Organisatoriske
- Menneskelige



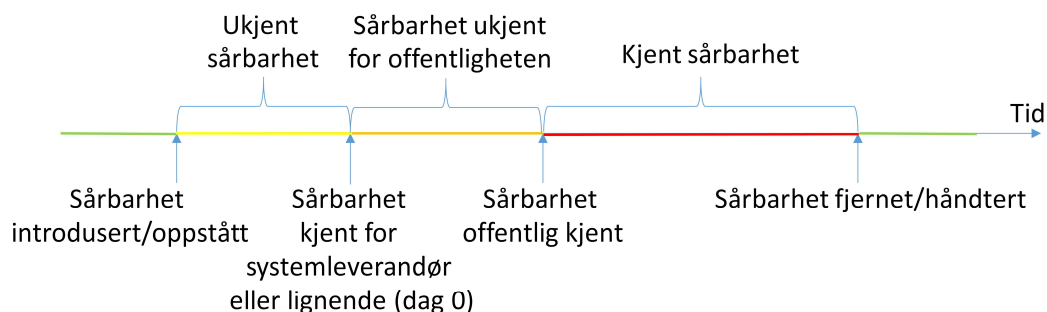
Trusselkapabilitet > motstandskapabilitet

12

12



En sårbarhet kan utnyttes fra den oppstår til den er fjernet - tidsvinduet fra den blir offentlig kjent er særlig kritisk

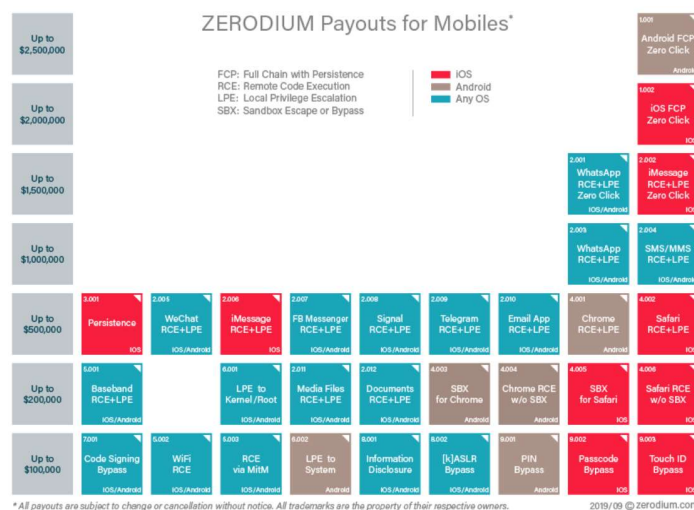


13

13



Alvorlige sårbarheter har potensielt høy verdi som salgsvare – i tillegg til at flere leverandører har belønningsprogrammer for informasjon om sårbarheter i egne produkter



Figur fra: ZERODIUM
<https://zerodium.com/solutions.html>

14

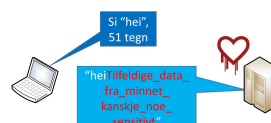
14



Common Vulnerability Scoring System (CVSS) er en standard for å uttrykke sårbarheters alvorlighetsgrad

- Score fra 0 til 10:
 - 0: Ingen
 - 0,1-3,9: Lav
 - 4,0-6,9: Medium
 - 7,0-8,9: Høy
 - 9,0-10: Kritisk
- Grunnscore som kan påvirkes av en tidsavhengig og en miljøavhengig score

Heartbleed (CVE-2014-0160)
Grunnscore: **7.5 Høy**



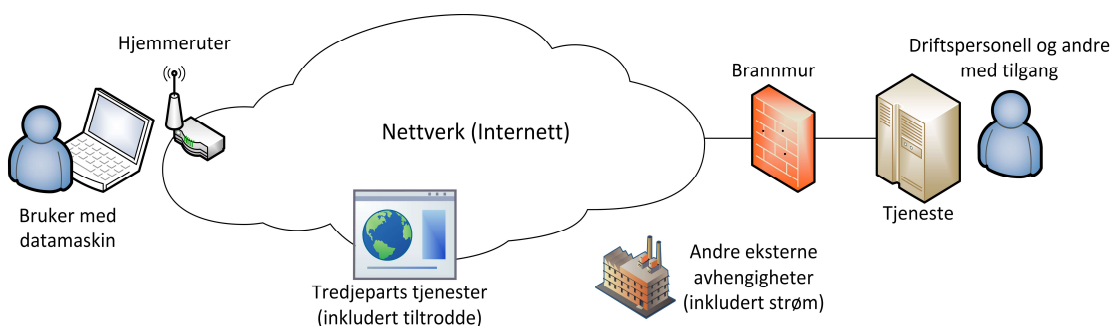
Kilde: <https://nvd.nist.gov/vuln/detail/CVE-2014-0160>

15

15



Mulige sårbarheter (fysiske, menneskelige, tekniske, organisatoriske og prosedyremessige) ved bruk av tjeneste over Internett



16

16



Sårbarheter

Hovedkategorier og eksempler

Hardware

- Hardware designfeil
 - RAM minnekomponenter er montert for nærme hverandre
 - Stadige endringer påvirker nabokomponenter
 - Rowhammer hentet data fra nærliggende minneceller, selv om de var beskyttet
- Intel II Pentium flyttallsdivisjonsfeil
 - Alle nye chipper har feil, debugging er en kontinuerlig prosess
- [https://en.wikipedia.org/wiki/Meltdown_\(security_vulnerability\)](https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability))
- Utnyttelse av hardwarefeil skjer gjerne i svært rettede angrep

Software/programvare

- Feil i operativsystemet eller programkoden
 - Fiks ved å oppdatere jevnlig, 'patche'
 - Følge med på komponenter du bruker, sikre at du bruker siste versjon

17



Vulnerabilities

Software vulnerabilities categories

- **Buffer overflow** – when data is written beyond buffer limits (allocated memory)
 - Leading to system crash, data compromise, or provide escalation of privileges
- **Non-validated input** – transferring invalid data to be processed further
 - An image file with invalid image dimensions could force the program to allocate buffers of incorrect and unexpected sizes
- **Race conditions** – when an output depends on other ordered/timed outputs
 - Creates problems when the ordered/timed events do not occur in the proper order/timing
- **Weaknesses in security practices** – when creating own security algorithms
 - Developers should use already tested and verified security libraries
- **Access-control problems** – controlling who does what
 - Many security vulnerabilities are created by improper use of access controls

18

18



<https://xkcd.com/327/>



19

19



Hvordan kan man redusere sårbarheten i egne systemer?

Unngå at sårbarheter blir utnyttet, f.eks.:

- Rask sikkerhetsoppdatering og utfasing av systemer
- Reduser angrepsflaten
- Særskilte tiltak for å avdekke sårbarheter
- Sårbarheter kan skyldes at vi ikke har gjort tilstrekkelige sikkerhetstiltak eller fordi utførte tiltak ikke fungerer som tiltenkt

Reduser konsekvensene av at sårbarheter utnyttes, f.eks.:

- Hver entitet bør ikke ha flere privilegier enn nødvendig
- Forsvar-i-dybden gjennom redundante sikkerhetstiltak
- Mindre avhengighet til systemene
- Rask deteksjon og effektiv hendelseshåndtering

20

20



Oppsummering

- En sårbarhet er en svakhet som muliggjør at sikkerheten i et IKT-system kan bli brutt.
- Sårbarheter har ulik alvorlighetsgrad. Mulighetene en angriper har til å utnytte en sårbarhet, og konsekvensene av dette, vil avhenge både av sårbarheten og omgivelsene sårbarheten befinner seg i.
- Rask sikkerhetsoppdatering, og utfasing av systemer som ikke lenger vedlikeholdes sikkerhetsmessig, er viktig for å redusere sannsynligheten for at sårbarheter blir utnyttet.
- Vi må ha en bevisst tilnærming for å finne og håndtere sårbarheter, siden mange sårbarheter ikke avdekkes gjennom vanlig bruk.
- Vi vil ikke klare å oppdage eller fjerne samtlige sårbarheter. Vi må derfor også gjøre tiltak for å redusere konsekvensene av at sårbarheter blir utnyttet.
- Synes du hacking ser litt artig ut? Test [noe slikt!](#)

21