

UiO : Institutt for informatikk

Hvordan hackes vi?

IN1020 – Introduksjon til datateknologi
18.09.2025

Kristin Skar
kritisk@ifi.uio.no

Datateknologi og sikkerhet

Tema for tema:

1. Datasikkerhet - Er det så viktig? (20.aug)
2. Hvem er hvem på internett? Hvordan kunne stole på digitale aktører (27.aug)
3. Kryptografi – nøkkelen til (fungerende) digital samhandling (10.sept)
4. **Hvordan hackes vi? (18.sept)**
5. Å skape trygge digitale tjenester krever innsats (24.sept)

I dag: Hvordan hackes vi?

Ressurser:

- Forelesning 18.09.25
- Notat om sikkerhet uke 5
- Ukeoppgaver og pensumlitteratur (Kap. 5 (115-123), 7 (169-182 + 189-195), 15 (377 -389))

Nøkkelord:

- Sikker datalagring
- Nettverkssikkerhet
- Systemsikkerhet
- Applikasjonssikkerhet
- Sosial manipulasjon

Hackere er (stort sett) ute etter:

Hva:

- Tilgang til informasjon
- Endre/forfalske informasjon
- Utilgjengeliggjøre informasjon

Hvordan:

- ID-tyveri
- Utnytte sårbarheter i programvare
- Få noen til å gi deg det du vil ha









Beskytte *lagret* informasjon



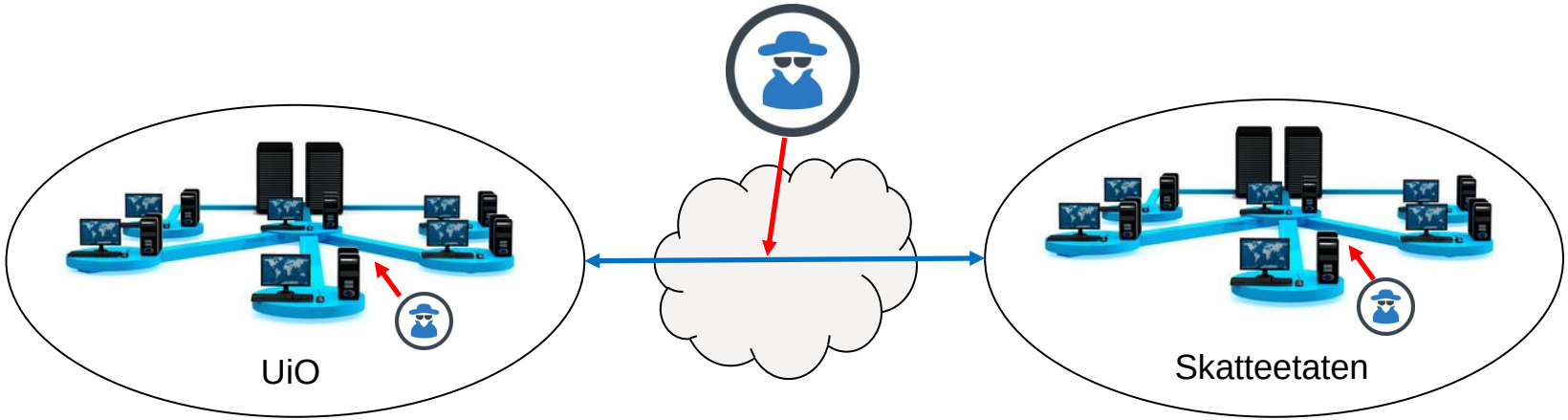




Beskytte lagret informasjon

- Å kryptere lagrede data er en strategi for å understøtte konfidensialitet og integritet:
  - Å sørge for at informasjon ikke kommer uvedkommende i hende ved å gjøre data uleselig/uforståelig for utenforstående.
  - Å sørge for at modifikasjon av data oppdages.
  - *Eksempel: Laptop mistes/stjeles, datainnbrudd på server/tjener der data lagres*.
- Sikkerhetskopiering er en strategi for å ta vare på informasjon over tid:
  - Bidra til økt tilgjengelighet ved å være i stand til å gjenopprette systemer og data ved uønskede hendelser som endrer eller sletter informasjon.
  - *Eksempel: Angrep med løsepengevirus, datainnbrudd der informasjon er slettet eller endret.*
- Gode retningslinjer for avhending av data:
  - Hvordan kvitte seg med fysiske enheter som inneholder data, uten å potensielt lekke data?

Beskytte informasjon under overføring



Kommunikasjonssikkerhet

Kommunikasjon i trådløse nett går via radiosignaler:

- «Hvem som helst» kan lytte til signalene.
- Signalforstyrrelser (tilsiktet eller utilsiktet) kan føre til utilgjengelighet
- Falske aksesspunkter: En trådløs enhet vil koble seg til aksesspunktet med sterkest signal.
- Kompromitterte aksesspunkter, spesielt åpne nett/aksesspunkter.

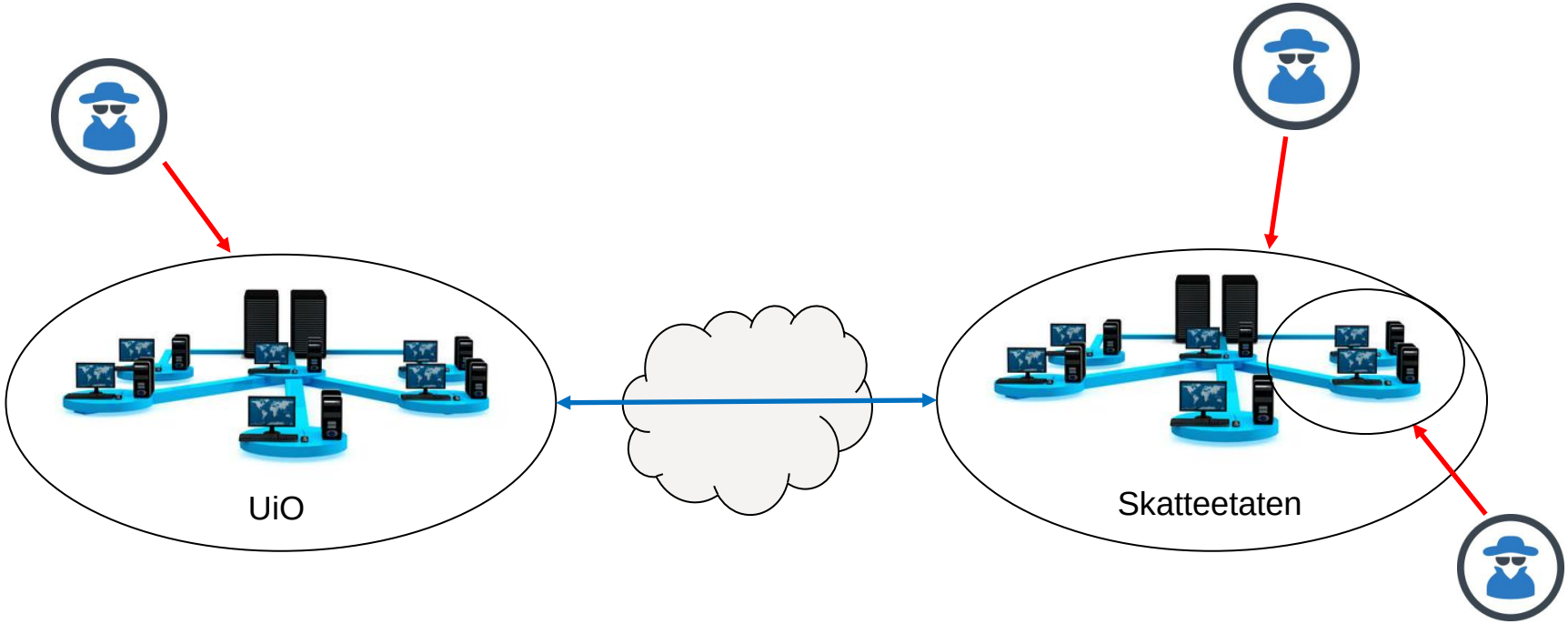


Kommunikasjon i kablede nett går via fysiske kabler:

- Avlytting krever fysisk tilgang, men er likevel fullt mulig.
- Ødelagt kabel (tilsiktet eller utilsiktet) kan føre til utilgjengelighet.
- Kompromittert nettverks-endepunkter (routere/switcher).
- Kompromitterte enheter på samme fysiske nettverk.



Beskytte systemer mot angrep



Datanettsikkerhet (skallforsvar/perimetersikring)

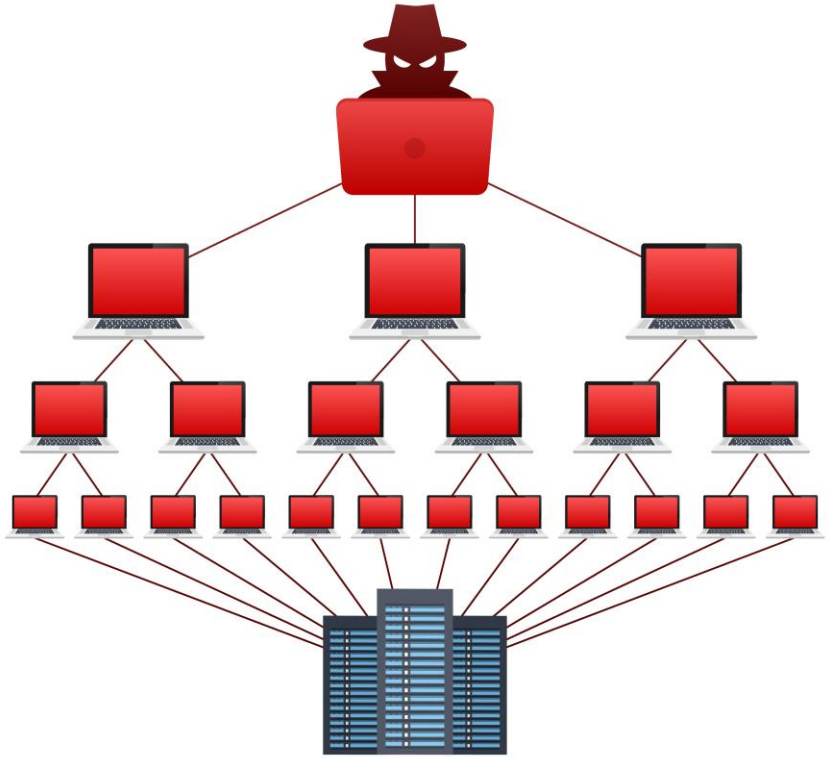


- Brannmur:
  - Slipper inn eller avvise trafikk inn i og/eller ut fra et nettverk basert på forhåndsdefinerte regelsett.
  - Brannmur fungerer som en *tilgangskontroll* for nettverket.
  - Kan være et dataprogram eller maskinvare laget for akkurat dette formålet.

- Inntrengningsdeteksjon

  Overvåker nettverkstrafikk, og kan detektere:
  - Både forsøk på og suksessfulle innbrudd
  - Datavirus og annen ondsinnet programvare
  - Tjenestenektangrep

Tjenestenektangrep (DoS eller DDoS)



Definisjoner

- Digital sårbarhet: En feil i et IKT-system som kan utnyttes
- Nulldags-sårbarhet: Sårbarhet som noen har kunnskap om, *før* produsenten/leverandøren eller brukerne av systemet/programvaren kjenner til den.
- Skadevare: Samlebetegnelse på programvare som har som mål å gjøre skade.
- Angrepsvektor: Metoden en angriper bruker for å utføre et angrep på en datamaskin, et nettverk eller et datasystem
- Sårbarhetsflate: Summen av (de potensielle) sårbarhetene i et system som kan nås og utnyttes av en angriper.

Angrepsvektor: Hvordan hackes datasystemer?

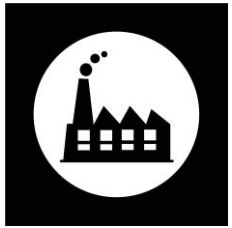
Aksessere ondsinnede eller infiserte nettsteder som inneholder ondsinnede script, eller laste ned og installere skadevare fra nettsteder.







Plugge inn eksterne enheter som er infisert med skadevare.



Infisering via *leveransekjeden*.





Kjøre vedlegg som kommer med e-post, som inneholder utnyttelser og skadevare.

Direkte angrep fra internet, som f.eks. utnytter sårbarheter i operativsystem eller applikasjoner som web-tjenere eller SQL-databaser.

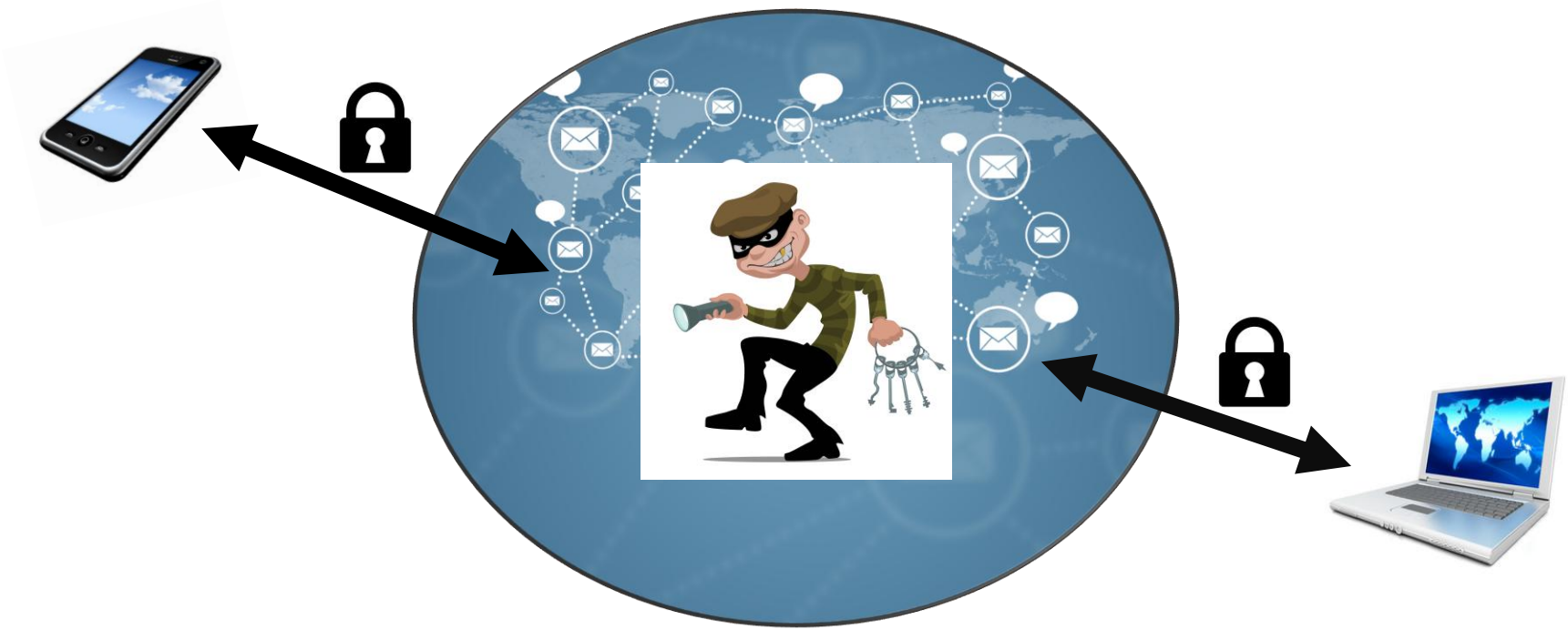


Et utvalg av typer skadevare:

Gruppene er til dels overlappende, og ikke alltid presist definert.

 Virus	Kjennetegnes ved at det sprer seg hver gang en fil med virus blir åpnet av bruker eller systemet.
 Dataorm	Skadevare som på egenhånd er i stand til å spre seg og finne nye ofre.
 Trojaner	Skadevare som utgir seg for å være et nyttig program.
Bakdør	En ubeskyttet og ukjent åpning inn i et datasystem, laget av en angriper.
 Spionvare	Programvare for å spionere på en bruker i håp om å få tak i f.eks. informasjon, passord, kontoinformasjon.
 Tastelogger (Keylogger)	En enhet eller programvare som er koblet til tastatur eller maskin og som lagrer eller videresender alle tastetrykk. En variant av spionvare.
Rootkit	Skadevare som endrer eller erstatter funksjoner i OS eller applikasjoner, med mål å ta kontroll over en maskin eller et system.
Exploit	Et program, en sekvens med data, eller en oppskrift på hvordan en sårbarhet kan utnyttes.

Tradisjonell sikkerhetsmodell:
Stoler på endesystemene, nettverket anses upålitelig.



Programvare:

Applikasjonsprogramvare:

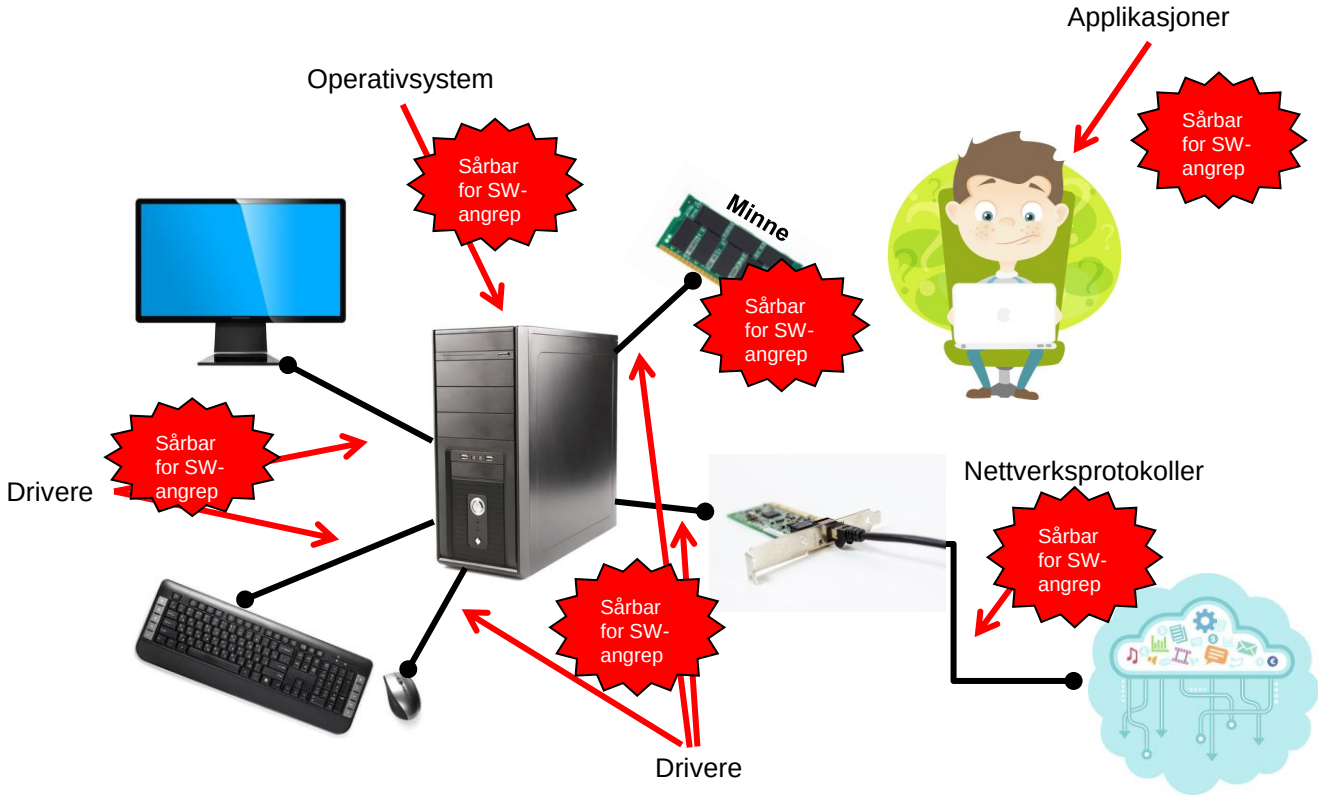


Applikasjonssikkerhet

Systemprogramvare:



Systemsikkerhet


Applikasjoner
Operativsystem
Sårbar for SW-angrep
Sårbar for SW-angrep
Minne
Sårbar for SW-angrep
Sårbar for SW-angrep
Drivere
Nettverksprotokoller
Sårbar for SW-angrep
Sårbar for SW-angrep
Drivere

Sikkerhet i operativsystemet

- OS styrer ulike brukeres tilgang til ressurser (prinsipp om *minste privilegium*)
- *Kjernen* i operativsystemet styrer alt.
- Kjernen kommuniserer med *periferenhetene* i datamaskinen gjennom *drivere*.
- Brukerprosesser kommuniserer via kjernen for å kunne benytte periferenhetene.
- Minnet i en datamaskin benyttes (bl.a.) til mellomlagring.

Sikkerhet i operativsystemet (forts)

1. Kjerne og drivere er dataprogrammer

- Kan inneholde sårbarheter

2. Kjernen kjører i *supervisor mode* og har tilgang til «alt»

- En sårbarhet i kjernen er kritisk

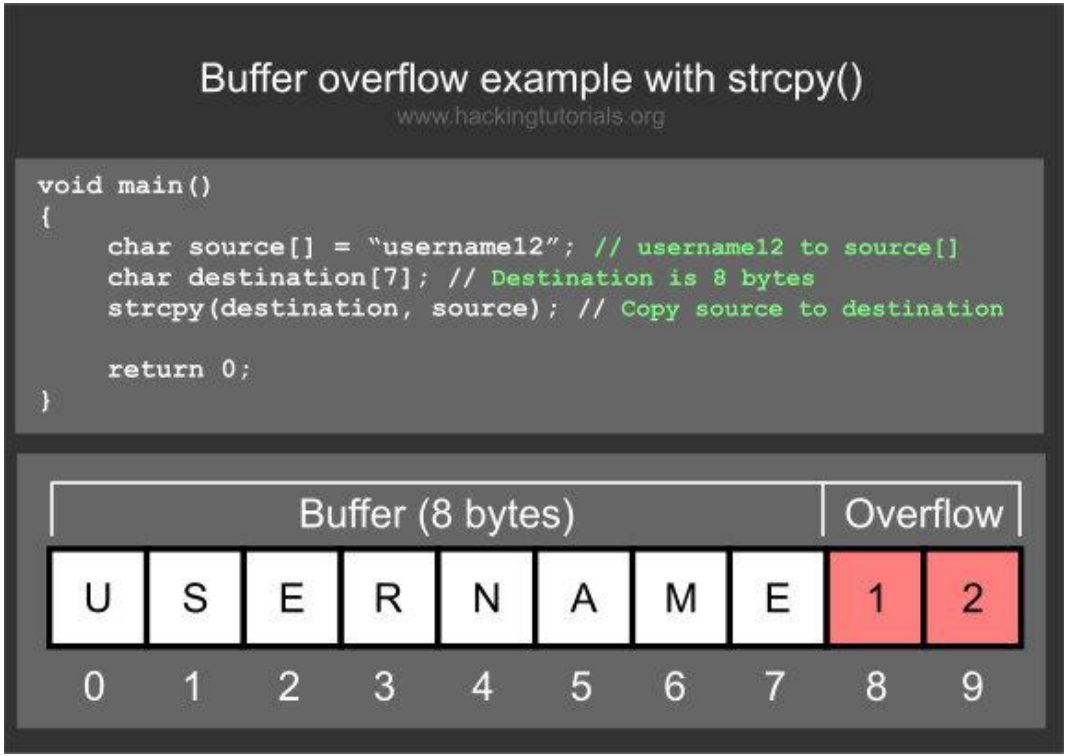
Ekstremt viktig å holde både operativsystem og drivere fri for sårbarheter:

- Sørge for trygg programvare
- Holde programvaren oppdatert vha. *sikkerhetoppdateringer*.



Kan minnet i en datamaskin «hackes»?

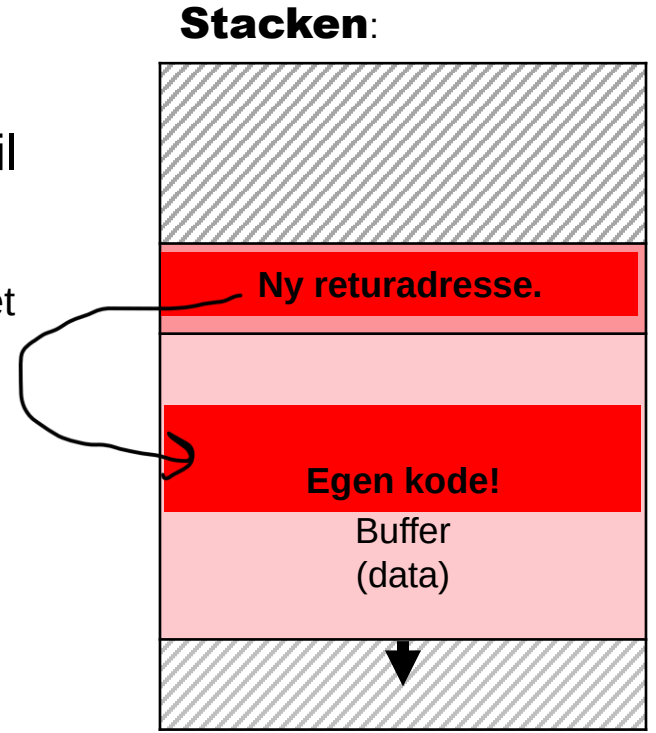
Et buffer er en sammenhengende seksjon i minnet i datamaskinen, avsatt til å inneholde data.



Kan dette brukes kreativt?

- JA – gjennom å kjøre slike sårbare programmer *kan* man skrive uhemmet til minnet i datamaskinen:
  1. Plassere egen programkode på steder i minnet hvor det ligger *kjørbar kode.*
  2. Endre en funksjons returadresse til å isteden peke til adressen i minnet der din kjørbare kode er plassert.

➢ For den interesserte (Computerphile): https://www.youtube.com/watch?v=1S0aBV-Waeo





Kan applikasjoner hackes?

Kjennetegn ved applikasjoner

Svært ofte:

- Dialog med bruker(e)
- Behandler input fra bruker(e)
- I bakkant av applikasjonen benyttes en *database* for lagring av informasjon.

SQL injisering

Eksempel: Tabellen «Bruker»:

BrukerId	Brukernavn	Passord	Fornavn	Etternavn	Kredittkort #
1001	anneh	ewtgfst45yh	Anne	Hansen	1609983275417533
1002	pederaa	67efg3ndfa	Peder	Aas	4586890148239766

Eksempel på brukerdialog:

Oppgi brukernavn: anneh Passord: xyxyxy OR 1=1

Dette kan resulte… …dige SQL-setning:

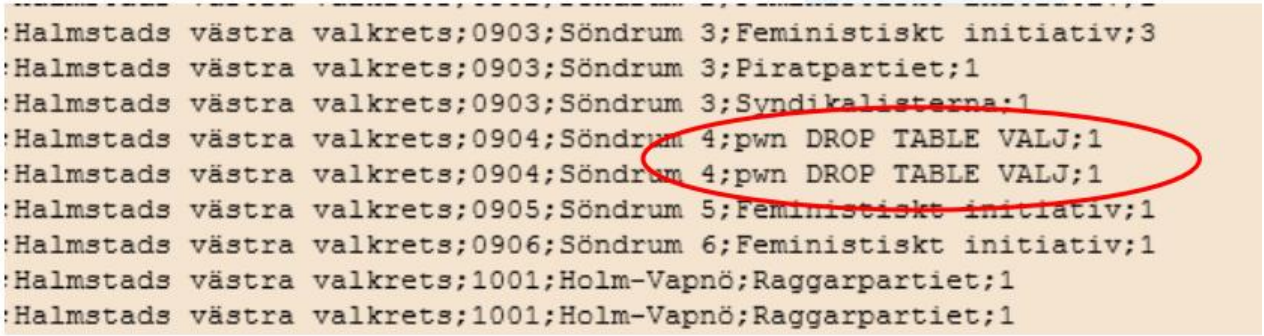
SELECT * FROM Bruker
WHERE Brukernavn = anneh and Passord = xyxyxy OR 1=1;

Filtrer all input !

- For den interesserte (Computerphile): https://www.youtube.com/watch?v=ciNHn38EyRc

Svensk valgsabotasje ☺

«Hacking swedish election with pen and paper»:



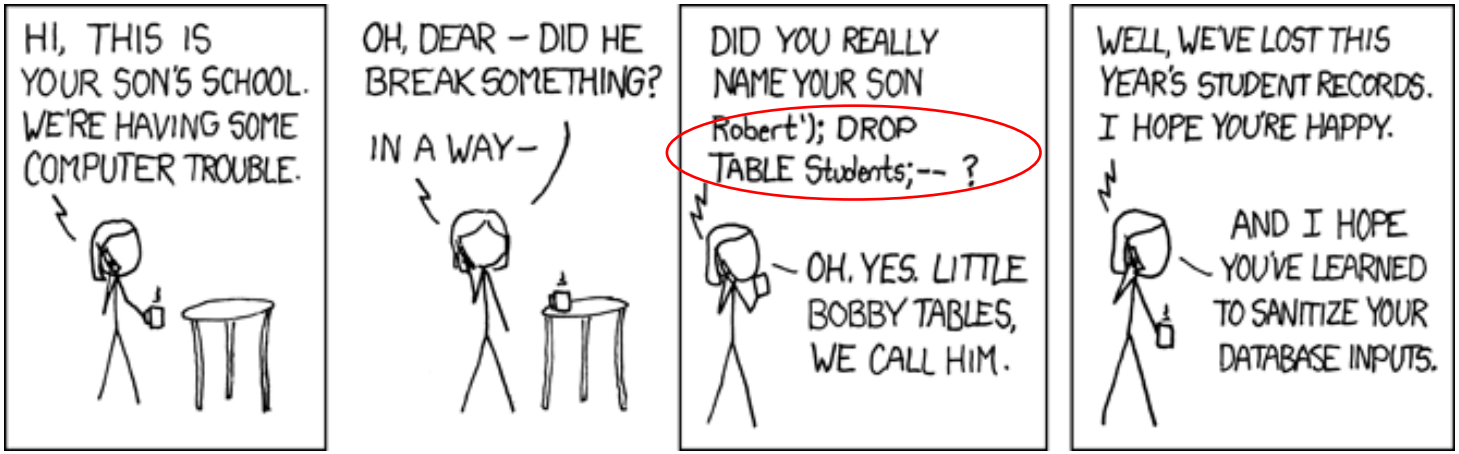
```
:Halmstads västra valkrets;0903;Söndrum 3;Feministiskt initiativ;3
:Halmstads västra valkrets;0903;Söndrum 3;Piratpartiet;1
:Halmstads västra valkrets;0903;Söndrum 3;Syndikalisterna;1
:Halmstads västra valkrets;0904;Söndrum 4;pwn DROP TABLE VALJ;1
:Halmstads västra valkrets;0904;Söndrum 4;pwn DROP TABLE VALJ;1
:Halmstads västra valkrets;0905;Söndrum 5;Feministiskt initiativ;1
:Halmstads västra valkrets;0906;Söndrum 6;Feministiskt initiativ;1
:Halmstads västra valkrets;1001;Holm-Vapnö;Raggarpartiet;1
:Halmstads västra valkrets;1001;Holm-Vapnö;Raggarpartiet;1
```

Forsøk på sabotasje ved å slette data/tabeller:

SELECT * FROM Brukere WHERE Brukernavn = anneh; DROP TABLE Valg;

- Mer info: https://www.wired.co.uk/article/sweden-election-hack

Nerde-humor: «Exploits of a Mom»



Kilde: https://xkcd.com/327/

Cross Site Scripting (XSS)



1. Angriper plasserer ondsinnede kode på en webside, kamuflert som innhold fra en bruker. Lagres på web-tjeneren.



Filtrer all input !

3. Angriperen tar kont
brukerens m
data via de

2. Intetanende bruker besøker websiden, og ondsinnet kode sendes tilbake til brukeren med innholdet.



- For den interesserte (Computerphile): https://www.youtube.com/watch?v=T1QEs3mdJoc

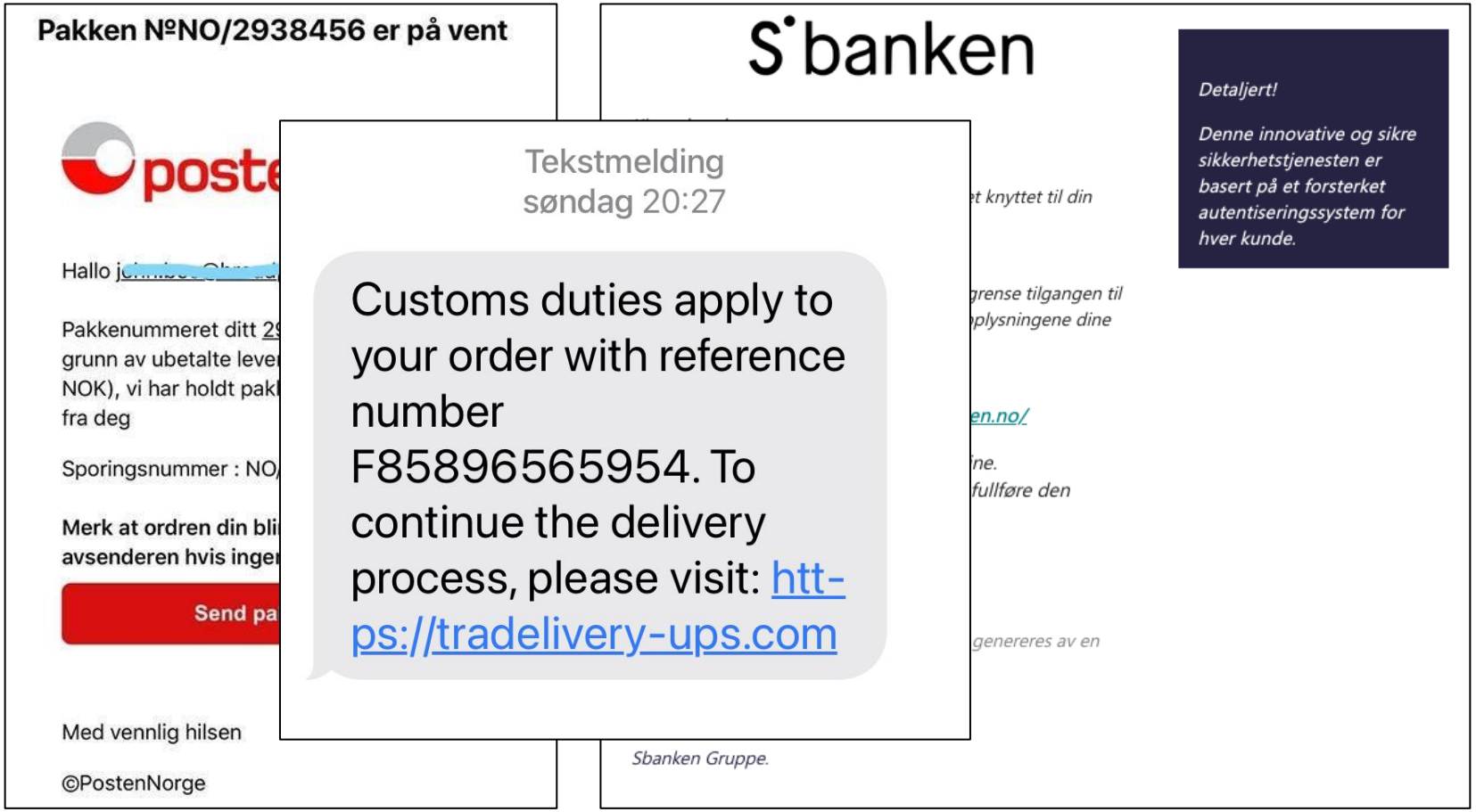
Sikre applikasjoner

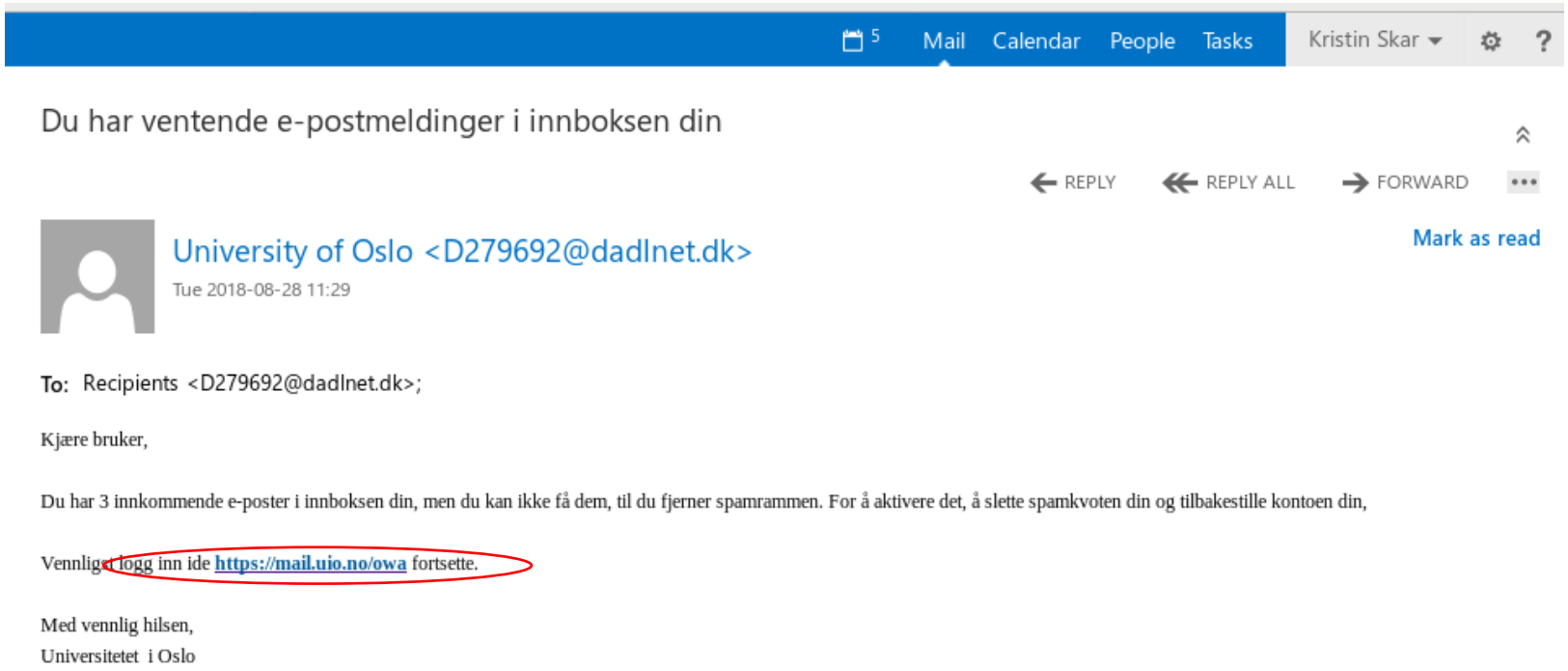
Design og utvikling med tanke på trygg bruk:

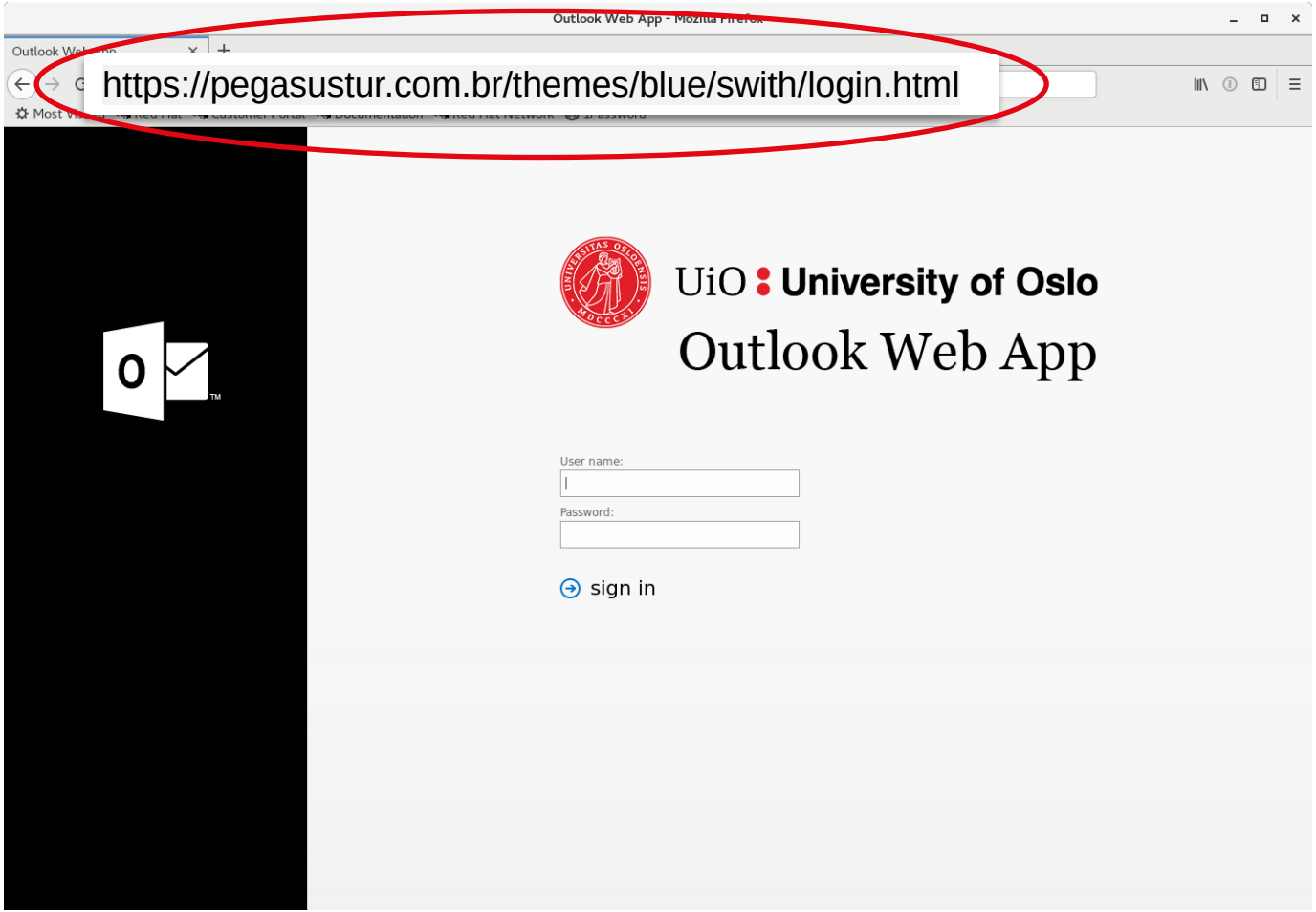
- I designfasen:
  - Kartlegge potensielle trusler
  - Identifisere tiltak som kan iverksettes for å motvirke truslene
- I programmeringsfasen:
  - Unngå å skape eller tilrettelegge for sårbarheter
- I produksjonsfasen:
  - Holde all programvare oppdatert

Utgjør du og jeg en trussel?




Pakken NºNO/2938456 er på vent
Hallo j
Pakkenummeret ditt 2
grunn av ubetalte leve
NOK), vi har holdt pak
fra deg
Sporingsnummer : NO
Merk at ordren din bli
avsenderen hvis inge
Send pa
Med vennlig hilsen
©PostenNorge
Tekstmelding
søndag 20:27
Customs duties apply to your order with reference number F85896565954. To continue the delivery process, please visit: htt-ps://tradelivery-ups.com
S banken
Detaljert!
Denne innovative og sikre sikkerhetstjenesten er basert på et forsterket autentiseringssystem for hver kunde.
et knyttet til din
grense tilgangen til
plysningene dine
en.no/
ine.
fullføre den
genereres av en
Sbanken Gruppe.


5 Mail Calendar People Tasks Kristin Skar
Du har ventende e-postmeldinger i innboksen din
REPLY REPLY ALL FORWARD
University of Oslo <D279692@dadlnet.dk>
Tue 2018-08-28 11:29
Mark as read
To: Recipients <D279692@dadlnet.dk>;
Kjære bruker,
Du har 3 innkommende e-poster i innboksen din, men du kan ikke få dem, til du fjerner spamrammen. For å aktivere det, å slette spamkvoten din og tilbakestille kontoen din,
Vennligst logg inn ide https://mail.uio.no/owa fortsette.
Med vennlig hilsen,
Universitetet i Oslo


Outlook Web App - Mozilla Firefox
https://pegasustur.com.br/themes/blue/swith/login.html
UiO : University of Oslo
Outlook Web App
User name:
Password:
sign in

Bedragere lurte ansatt til å utbetale en halv milliard kroner

- Oslo-politiet har samarbeidet med FBI
- Ingen pågrepet så langt

Politiet på bar bakke i Norfund-saken: 100 millioner borte etter digitalt angrep

Norfund bekrefter å ha tapt store summer i en avansert, digital svindel. Politiet har etterforsket saken i det skjulte.

UiT svindlet for 12 millioner

UiT betalte ut 12 millioner kroner til det som viste seg å være svindel. Pengene gikk til det som så ut som en faktura for en røntgenmaskin.

Etterbørs Musikk

Utenlandske «direktørsvindlere» stjal 770.000 kroner fra festspillene i Nord-Norge

Med falske epostadresser og god norsk klarte svindlere å få festspillene i Nord-Norge til å overføre store summer til kontoer i England og Tyrkia.

NTB
Publisert: 20.09.2017 – 06:38 Oppdatert: 20.09.2017 – 07:33

Vanskeligere og vanskeligere å ikke la seg lure.

Deepfakes utnytter kunstig intelligens for å lage videoer og lydinnhold det er svært vanskelig å avsløre som falskt.





Men; Du er også en viktig forsvarsmekanisme.

Mennesker utnyttes (også digitalt):

- Offer for svindelangrep
- Utpressing/overtalelser



«Sikkerhetskultur»

(God eller dårlig?)

Kan bankID hackes?





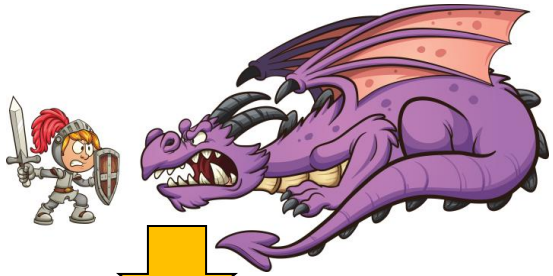
Eksempel: BankID som PKI

- BankID: Elektronisk identitet som kan brukes til autentisering og digital signering i offentlige og private tjenester.
- BankID-tjenesten: En PKI driftet av Stø AS, og selges som en tjeneste til virksomheter.
- Funksjon:
  - En bruker gis et offentlig nøkkelpar (privat + offentlig kryptografisk nøkkel), hvor offentlig nøkkel legges i et offentlig-nøkkel sertifikat som signeres av *tiltrodd sertifikatmyndighet.*
  - Utsteder og signerer av en BankID er banker/bank-samarbeider.
  - Strenge krav til å få utstedt BankID (legitimasjonskontroll) gir *Sikkerhetsnivå høyt* *(https://lovdata.no/pro/#document/NLX3/eu/32015r1502)*

Eksempel: BankID som PKI

- BankID autentisering med app, steg for steg:
  1. Identifikator: Fødselsnummer.
  2. Forespørsel sendes bankID-app på mobil.
  3. Bekrefter en forespørsel med app (Eks: Er det deg? Hvilke ordkombinasjon ser du?) + kode eller biometri på mobil.
  4. I mange tilfeller må du i tillegg bekrefte med ditt faste BankID-passord
  5. Hvis ok: Privat BankID-nøkkel brukes til autentisering (og/eller digital signering).
  6. Privat nøkkel verifiseres med tilhørende offentlig nøkkel.

Konklusjon: Helhet er nødvendig



Sikkerhet i applikasjonsprogramvare er ikke sikrere enn sikkerheten i datamaskinen den kjører på.

Sikkerhet i datamaskinen avhenger av sikkerhet i systemprogramvare, boot-prosess, maskinvare.

Læringsmål

- Kjenne til hovedprinsippene for nettverkssikkerhet
- Kjenne til sårbarheter knyttet til *systemprogramvare*.
- Kjenne *applikasjonssikkerhet*, og vanlige sårbarheter i applikasjoner.
- Menneskelig faktor som reell sårbarhet.
- Angrepsvektor og sikre *datasystemer*:
  - Ingenting er sikrere enn det svakeste ledd.

Takk for i dag!

mn.uio.no/ifi

