UiO : Institutt for informatikk

Datateknologi og sikkerhet

IN1020 – Introduksjon til datateknologi
09.11.2022 – Hvordan utnyttes datasystemer

Kristin Skar
kritisk@ifi.uio.no

Siste innspurt

- **9. november:** Hvordan utnyttes datasystemer
- **10. november:** Personvern og systematisk informasjonssikring
- **16. november:** «Læring i samvirket mellom mennesker og teknologi»
- **17. november:** Programmering med assemblerkode
- **23. november:** Oppsummering og info om eksamen

Oppgave:

I hvilke situasjoner benyttes gjerne kryptografi som sikkerhetstiltak?

Velg et eller flere alternativer

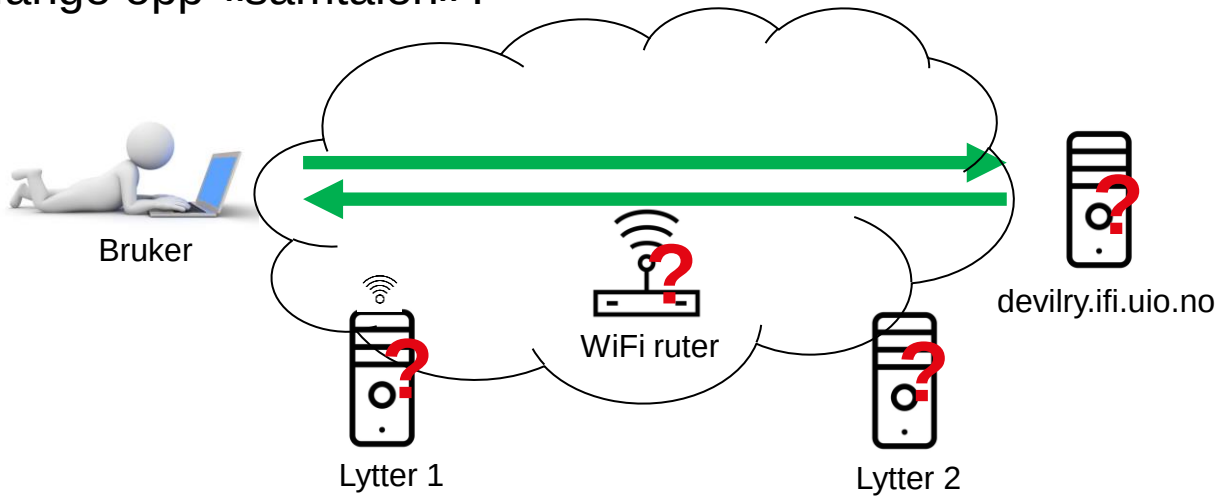
- [ ] For trygg lagring av informasjon på utrygge langringsenheter.
- [ ] For trygg overføring av informasjon i datanettverk.
- [ ] For å bidra til å detektere innbrudd i datasystemer.
- [ ] For å sikre korrekt sikkerhetskopiering av informasjon.

Sikkerhet i trådløse nett

Kommunikasjonskanal til devilry.ifi.uio.no

Ukryptert forbindelse (http) via ukryptert nett.

Hvem kan fange opp «samtalen»?

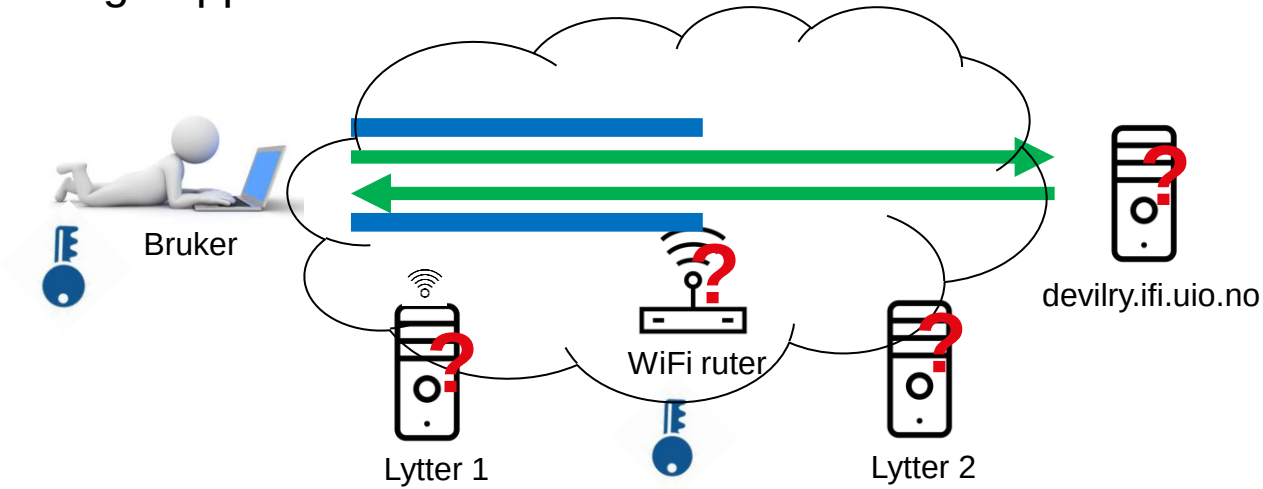


Sikkerhet i trådløse nett

Kommunikasjonskanal til devilry.ifi.uio.no.

Kryptert forbindelse til WiFi-ruter.

Hvem kan fange opp «samtalen»?

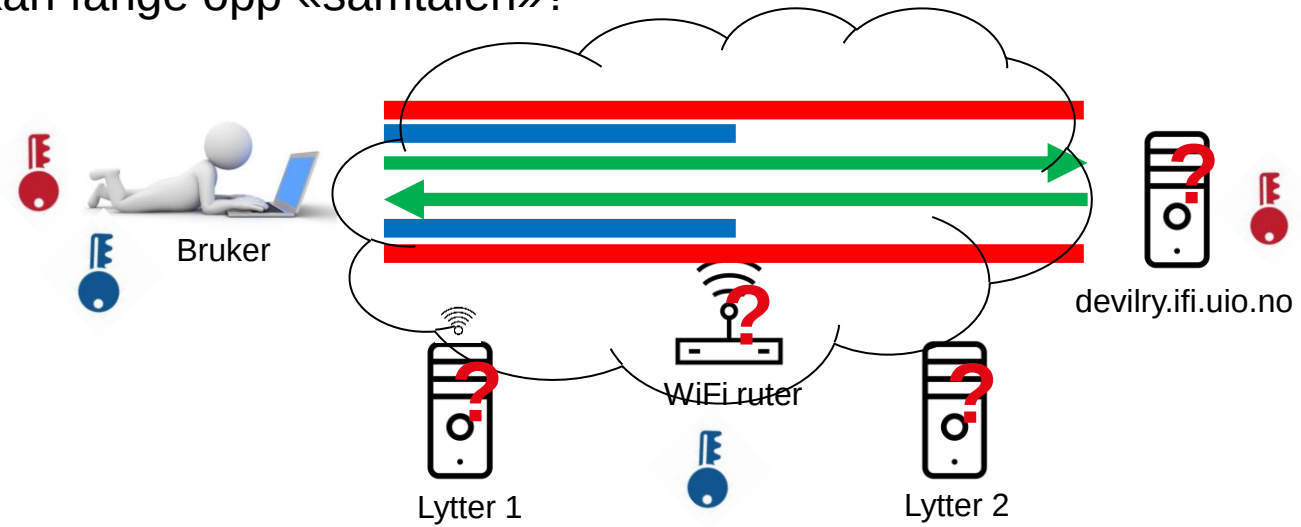


Sikkerhet i trådløse nett

Kommunikasjonskanal til devilry.ifi.uio.no.

Kryptert forbindelse til wifi-ruter og HTTPS til devilry.ifi.uio.no.

Hvem kan fange opp «samtalen»?



Tradisjonell sikkerhetsmodell:
Stoler på endesystemene, nettverket anses upålitelig.

Systemsikkerhet

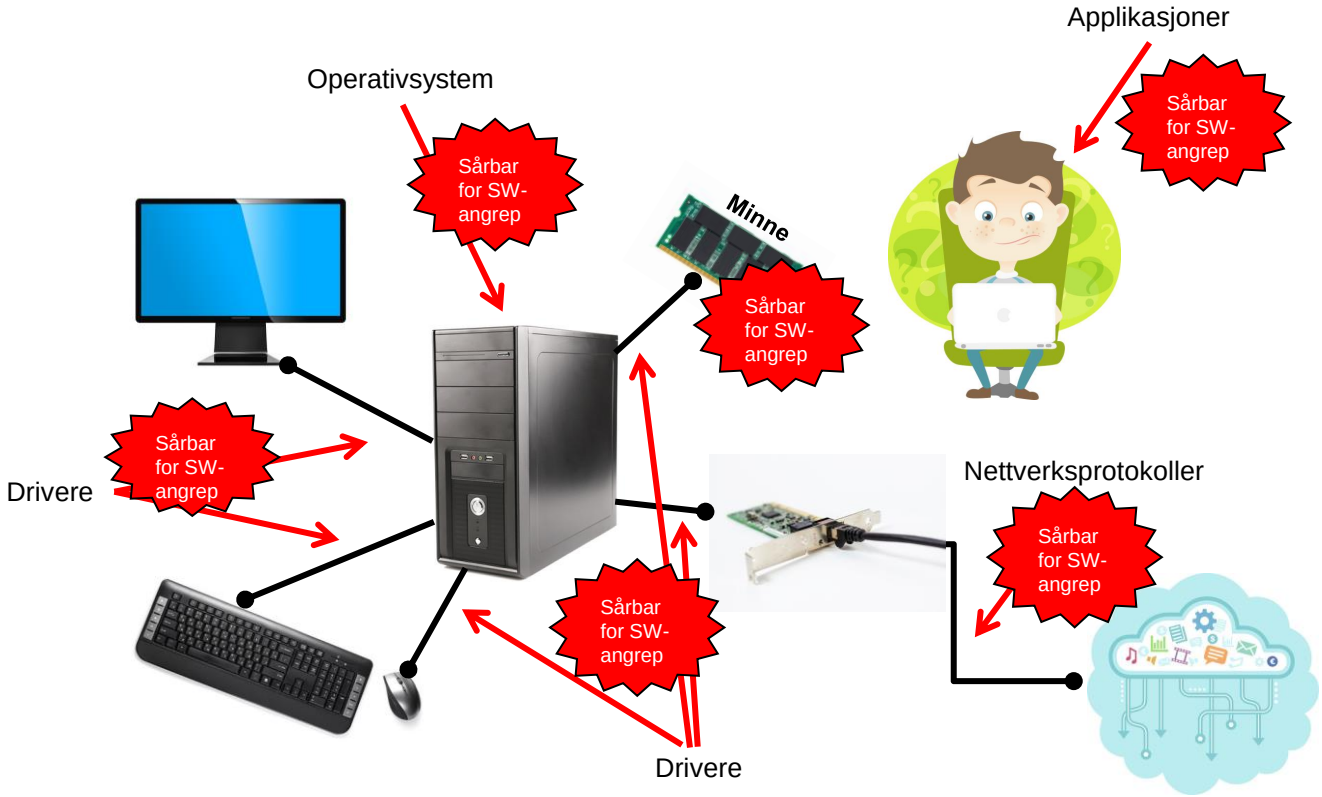
«Å bruke kryptering på internett tilsvarer å bruke en pansret bil for å levere kredittkortinformasjon fra en som bor i en pappkartong til en som bor på en parkbenk»

Gene Spafford

Programvare:

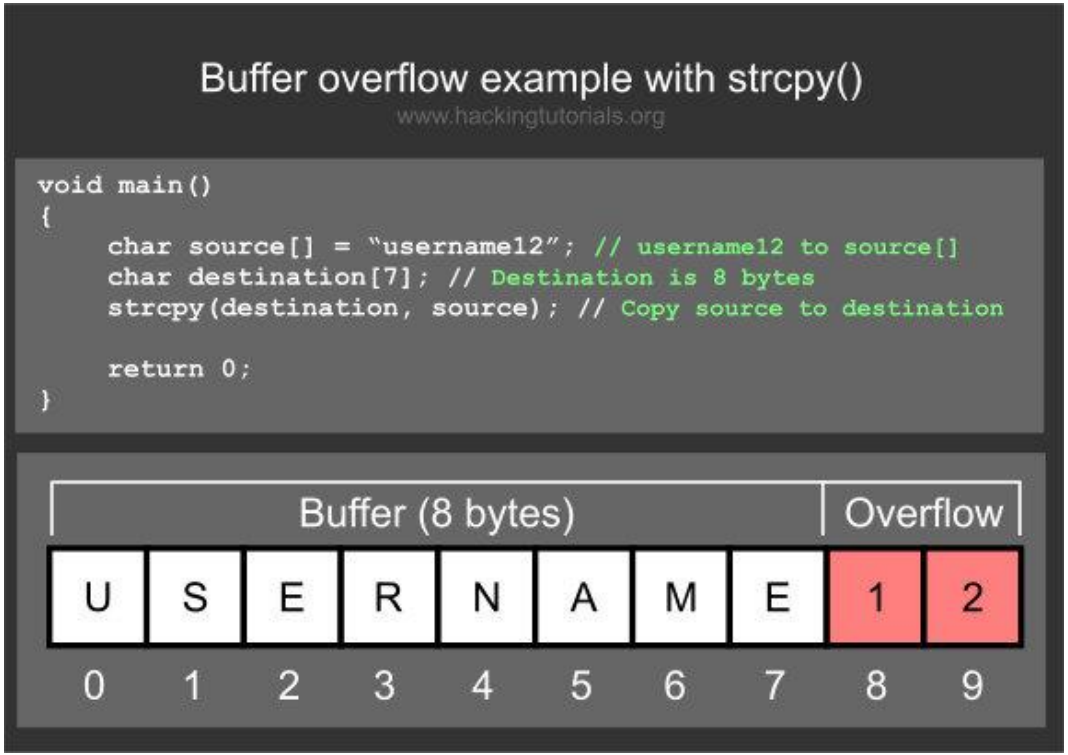
Applikasjonsprogramvare

Systemprogramvare


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

Kan man «hacke» minnet i en datamaskin?

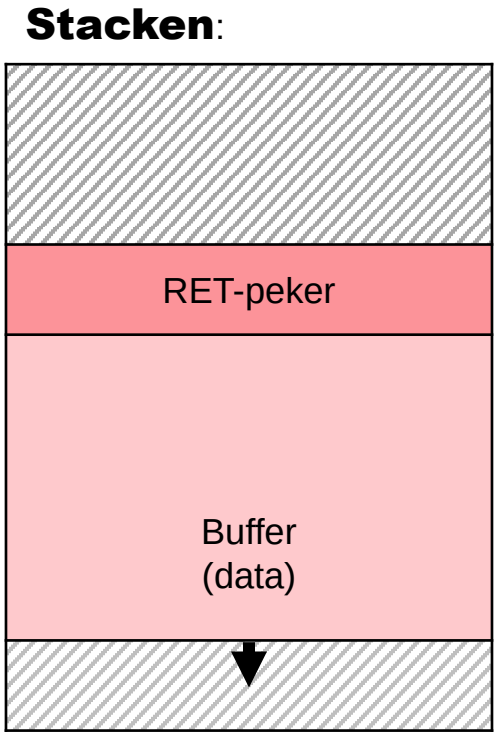
Et buffer er en sammenhengende seksjon i minnet i datamaskinen, avsatt til å inneholde data.



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 det være skadelig?

JA - brukes aktivt av hackere:

- Kan klare å kjøre egen programkode
- Kan starte andre programmer enn tiltenkt

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 «Brukere»:

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

Eksempel på brukerdialog:

Oppgi brukernavn: anneh Oppgi passord: xyxyxy OR 1=1

Dette kan resultere i følgende gyldige SQL-setning:

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

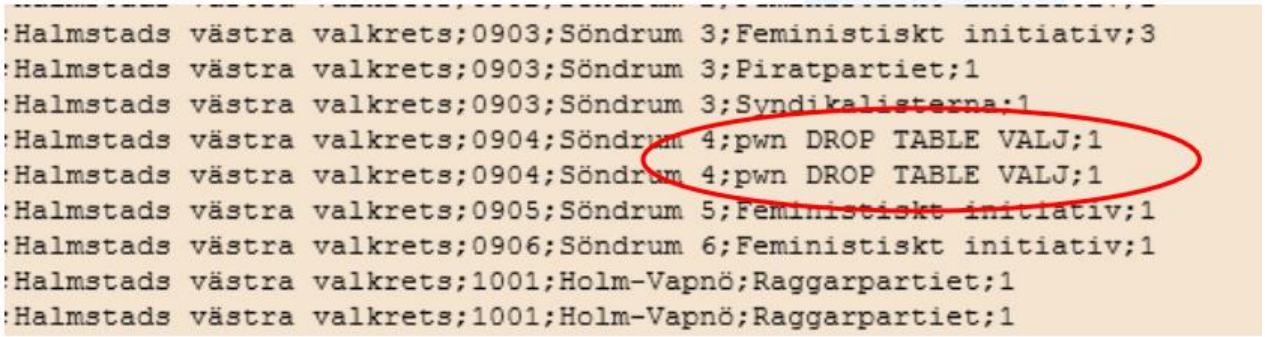
- For den interesserte (Computerphile): https://www.youtube.com/watch?v=ciNHn38EyRc

Svensk valgsabotasje

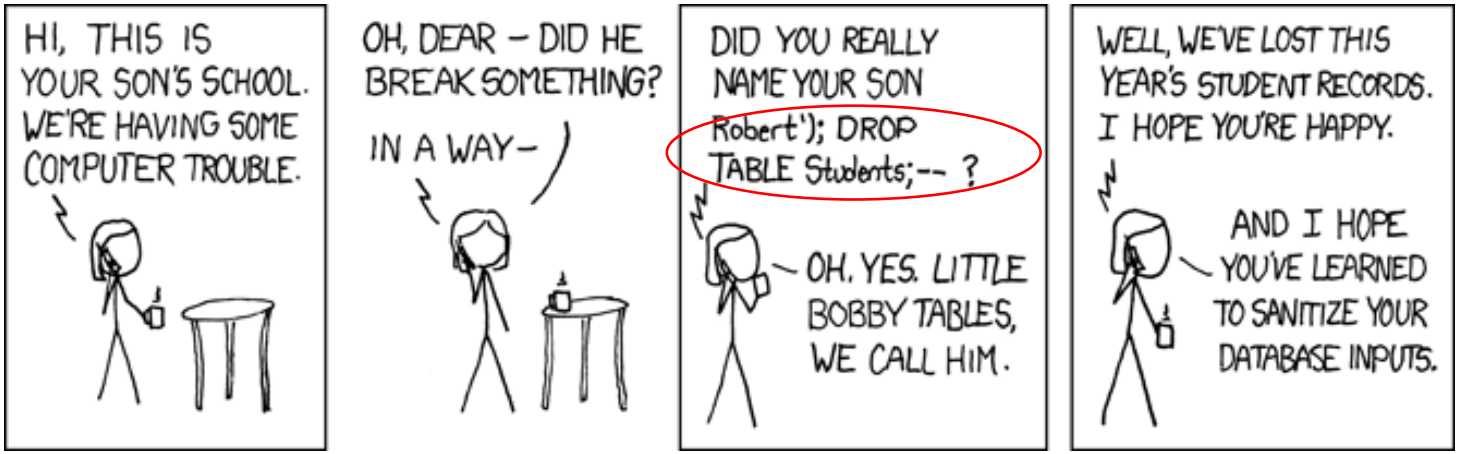
- Sabotasje ved å slette data/tabeller:

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

- «Hacking swedish election with pen and paper»:



Nerde-humor


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Cross Site Scripting (XSS)

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

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

3. Angriperen tar kontroll over brukerens maskin og/eller data via den injiserte koden.

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

Utgjør du og jeg en trussel?

Pakken №NO/2938456 er på vent

posten

Hallo j[redacted]

Pakkenummeret ditt 2938456 er i påvente på grunn av ubetalte leveringskostnader (27,50 NOK), vi har holdt pakken i vente til vi hører fra deg

Sporingsnummer : NO/2938456

Merk at ordren din blir returnert til avsenderen hvis ingen betaling mottas

Send pakken min

Med vennlig hilsen

©PostenNorge

S banken

Kjære kunde,

Vårt system gjenkjenner at mobilnummeret knyttet til din sbanken-konto ennå ikke er bekreftet.

Av sikkerhetsgrunner er vi tvunget til å begrense tilgangen til din sbanken-konto. Hvis du ikke oppgir opplysningene dine innen 28. oktober 2022.

https://secure.sbanken.no/

1. *Logg på med bankopplysningene dine.*
2. *Følg de obligatoriske trinnene for å fullføre den nødvendige prosessen.*

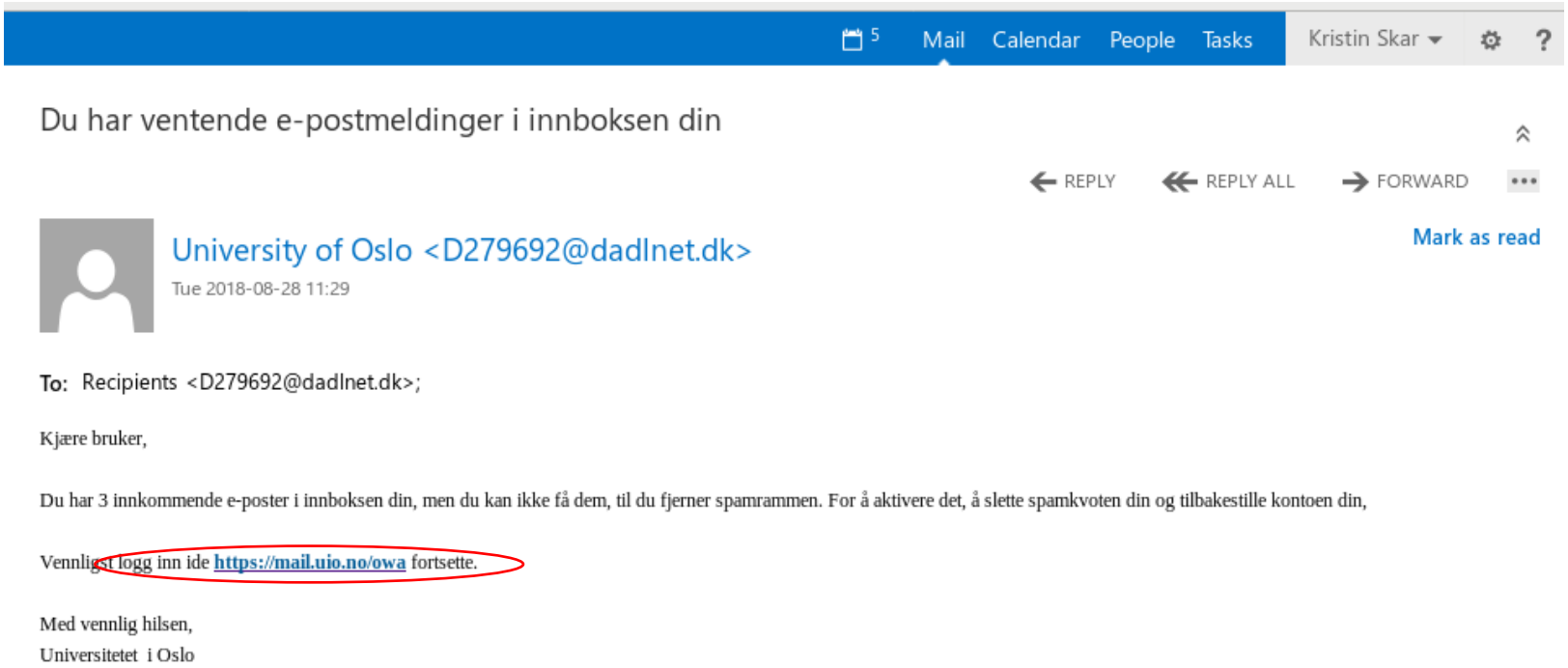
Vær oppmerksom på at denne meldingen genereres av en PLS. Ikke bruk Svar til-funksjonen.

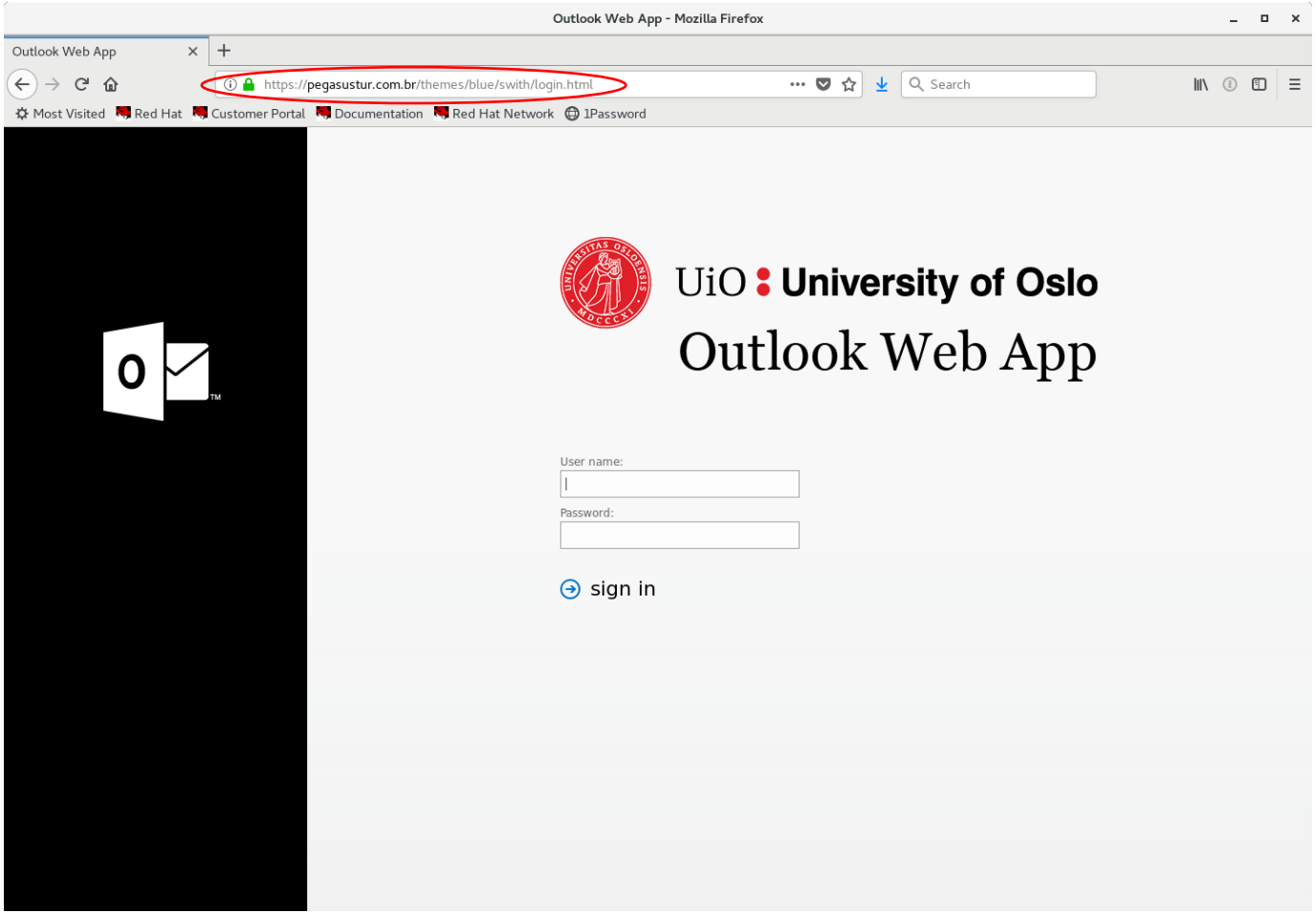
Takk for tilliten.

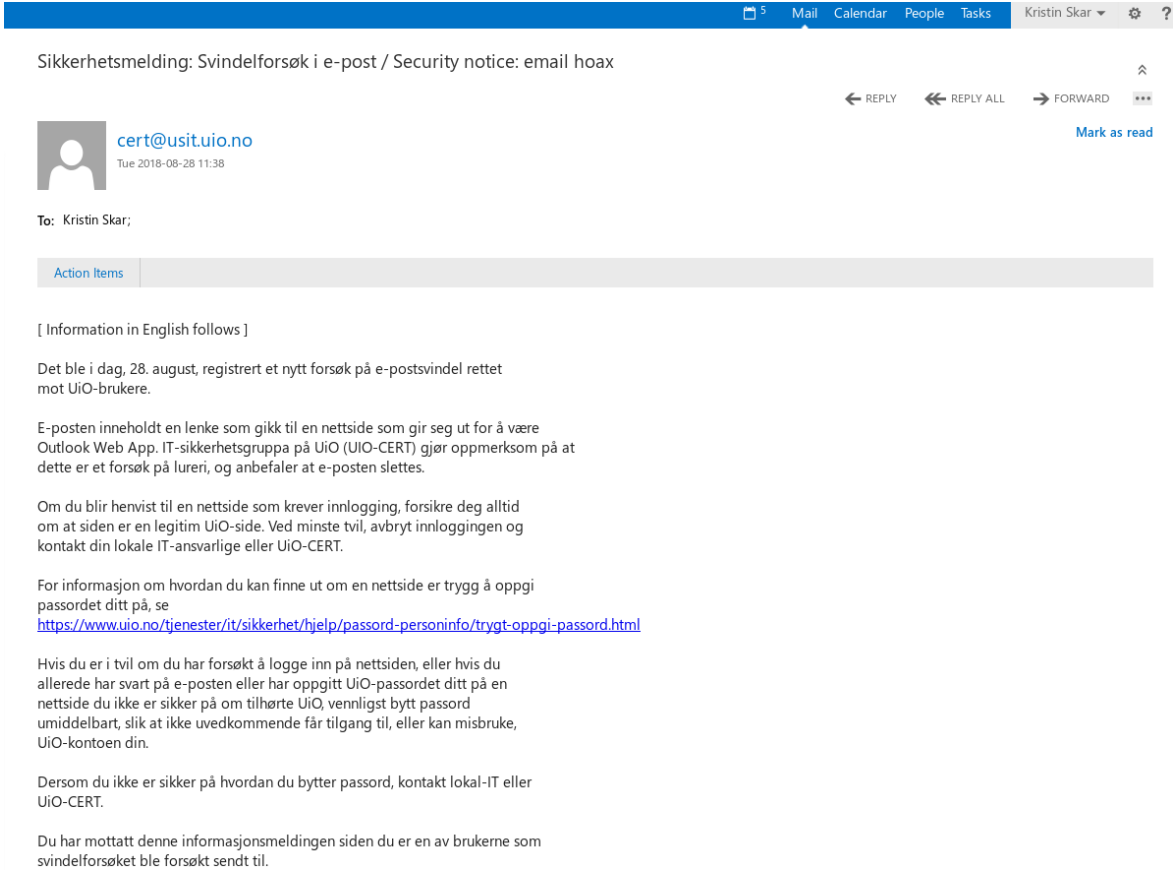
Sbanken Gruppe.

Detaljert!

Denne innovative og sikre sikkerhetstjenesten er basert på et forsterket autentiseringssystem for hver kunde.


5 Mail Calendar People Tasks Kristin Skar
Du har ventende e-postmeldinger i innboksen din
REPLY REPLY ALL FORWARD
Mark as read
University of Oslo <D279692@dadlnet.dk>
Tue 2018-08-28 11:29
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
Outlook Web App
https://pegasustur.com.br/themes/blue/swith/login.html
Search
Most Visited
Red Hat
Customer Portal
Documentation
Red Hat Network
1Password
UiO : University of Oslo
Outlook Web App
User name:
Password:
sign in



5 Mail Calendar People Tasks Kristin Skar

Sikkerhetsmelding: Svindelforsøk i e-post / Security notice: email hoax

REPLY REPLY ALL FORWARD

Mark as read

cert@usit.uio.no
Tue 2018-08-28 11:38

To: Kristin Skar;

Action Items

[Information in English follows]

Det ble i dag, 28. august, registrert et nytt forsøk på e-postsvindel rettet mot UiO-brukere.

E-posten inneholdt en lenke som gikk til en nettside som gir seg ut for å være Outlook Web App. IT-sikkerhetsgruppa på UiO (UIO-CERT) gjør oppmerksom på at dette er et forsøk på lureri, og anbefaler at e-posten slettes.

Om du blir henvist til en nettside som krever innlogging, forsikre deg alltid om at siden er en legitim UiO-side. Ved minste tvil, avbryt innloggingen og kontakt din lokale IT-ansvarlige eller UiO-CERT.

For informasjon om hvordan du kan finne ut om en nettside er trygg å oppgi passordet ditt på, se
https://www.uio.no/tjenester/it/sikkerhet/hjelp/passord-personinfo/trygt-oppgi-passord.html

Hvis du er i tvil om du har forsøkt å logge inn på nettsiden, eller hvis du allerede har svart på e-posten eller har oppgitt UiO-passordet ditt på en nettside du ikke er sikker på om tilhørte UiO, vennligst bytt passord umiddelbart, slik at ikke uvedkommende får tilgang til, eller kan misbruke, UiO-kontoen din.

Dersom du ikke er sikker på hvordan du bytter passord, kontakt lokal-IT eller UiO-CERT.

Du har mottatt denne informasjonsmeldingen siden du er en av brukerne som svindelforsøket ble forsøkt sendt til.

Bedragere lurte ansatt til å utbetale en halv milliard kroner

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

VG, 18.04.2016

nrk.no, 19.12.2019

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.

Nordlys, 21.05.2020

UiT advarer mot falsk e-post med virusinfisert vedlegg

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

DN, 20.09.2017

Er jeg en “sårbarhet”?

JA!

Men; Du er også en viktig forsvarsmekanisme.

Mennesker utnyttes – også digitalt

- Offer for svindelangrep
- Utpressing/overtalelser

«Sikkerhetskultur»

(God eller dårlig?)

DNS og sikkerhet – og et eksempel på en utnyttelse

- DNS: Navneoppslag, knytter *maskinnavn* til IP-adresse:
  - devilry.ifi.uio.no -> 129.240.65.20
  - En maskin forespør typisk en *navnetjener* om adresse.
  - Kommunikasjonen foregår i klartekst
- Fallgruver ved bruk:
  - DNS-forfalskning: Uvedkommende introduserer uriktige opplysninger i navnetjener
  - DNS-modifisering: Man in the Middle-angrep, forfalsker meldinger
  - DNS-kapring: Endre hvilke navnetjener offerets maskin benytter

➢ Stol aldri ubegrenset på et domenenavn. Vanskelig å oppdage feil.

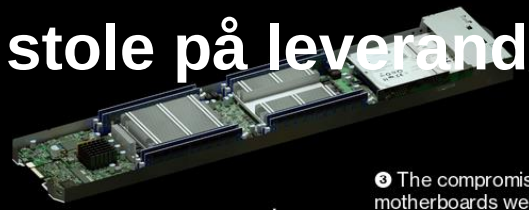
Kan maskinvare «hackes»?

Kan vi stole på leverandørkjeden?

How the Hack Worked, According to U.S. Officials

❶ A Chinese military unit designed and manufactured microchips as small as a sharpened pencil tip. Some of the chips were built to look like signal conditioning couplers, and they incorporated memory, networking capability, and sufficient processing power for an attack.

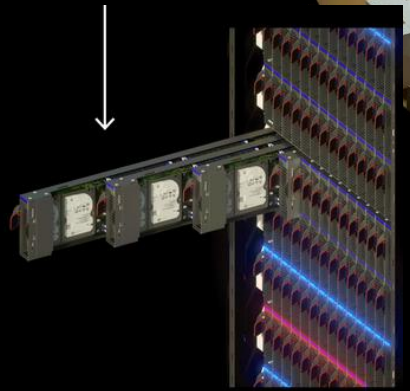
❷ The microchips were inserted at Chinese factories that supplied Supermicro, one of the world's biggest sellers of server motherboards.



❸ The compromised motherboards were built into servers assembled by Supermicro.

❹ The sabotaged servers made their way inside data centers operated by dozens of companies.

❺ When a server was installed and switched on, the microchip altered the operating system's core so it could accept modifications. The chip could also contact computers controlled by the attackers in search of further instructions and code.



Kilde:
https://www.digi.no/artikler/kina-kan-ha-infiltrert-nettverket-til-naermere-30-amerikanske-selskaper/447913

Læringsmål

- Angrepsvektor og sikre *datasystemer*:
  - Hva skal til for at vi skal kunne stole på datasystemet?
  - At ingenting er sikrere enn det svakeste ledd.
- Kjenne *applikasjonssikkerhet*, og vanlige sårbarheter i applikasjoner.
- Kjenne til sårbarheter knyttet til *systemprogramvare*.
- Mennesket som reell sårbarhet.

Takk for i dag!

mn.uio.no/ifi