DIGITALE TRUSLER

TEKNISK WEBINAR
#SIKKERHETSMÅNEDEN

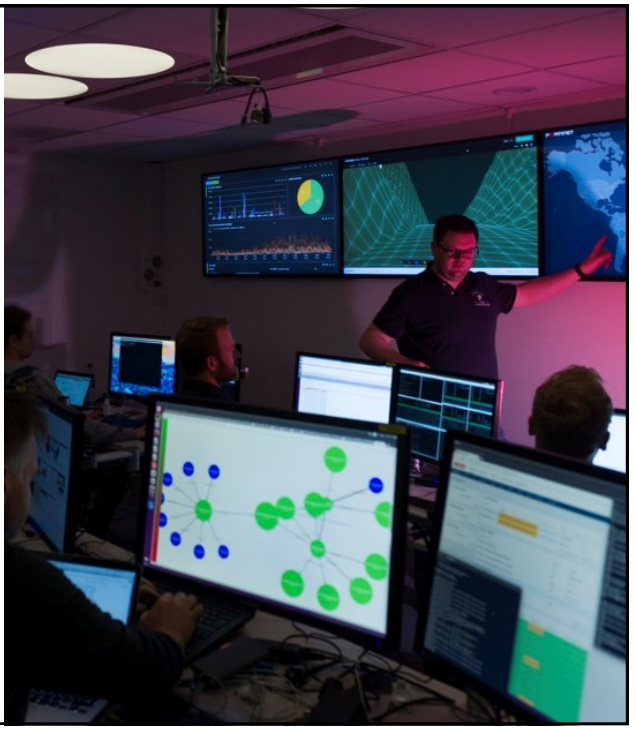
HÅKON LØNMO - BDO
THOMAS NORBECK - GLASSPAPER
24. OKTOBER 2018

BDO

BDO

BDO CERT

- Sikkerhetsovervåking
  - Oppdager, håndterer, forhindrer
- Sikkerhetstesting
  - Avdekker sårbarheter
- Bevisstgjøring styrker motstandsdyktighet
  - Teknisk
  - Strategisk



AGENDA

- Trusler og trender
- Tiltak
  - NSMs grunnprinsipper for IKT-sikkerhet
  - Overvåking og sikring av e-post

BDO

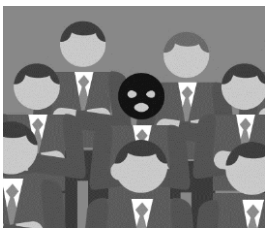
TRUSLER OG TRENDER

TRUSSELAKTØRER

Hacktivister

Kriminelle

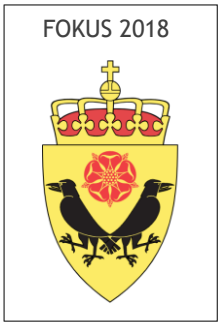
Statlig spionasje



Innsidere

ÅPNE KILDER: INTERNETT

ÅPNE KILDER: PUBLIKASJONER



DIREKTØRSVINDEL

NORGESHISTORIENS STØRSTE «BREKK»


VG NYHETER

< Nyheter | Innenriks | Utenriks | Siste 48t | Meninger

Bedragere lurte ansatt til å utbetale en halv milliard kroner

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

Kilde: vg.no 18.04.2016

- Andre eksempler på vellykket direktørsvindel i Norge
  - Mai 2017 – Fiskebåtrederi – **450.000 kr**
  - Juni 2017 – Festspillene i Nord-Norge – **770.000 kr**
  - Mai 2018 – Stavanger kommune – **500.000 kr**

8

NORCERT-VARSEL 25. JANUAR 2018

SENTRALT ANSATTE I HØYTEKNOLOGISKE NORSKE BEDRIFTER MÅL FOR E-POSTSVINDEL

- Majoriteten av virksomhetene benyttet Microsoft Office 365
- Videresendingsregel satt opp som en "Inbox Rule" på e-postkontoene
- Svindlerne benytter e-postkontoene til å sende falske e-poster som enten:
  - Reelle fakturaer med endret kontonummer
  - En melding om å endre kontonummer på en tidligere mottatt faktura
  - Falske fakturaer

NORCERT-VARSEL 25. JANUAR 2018

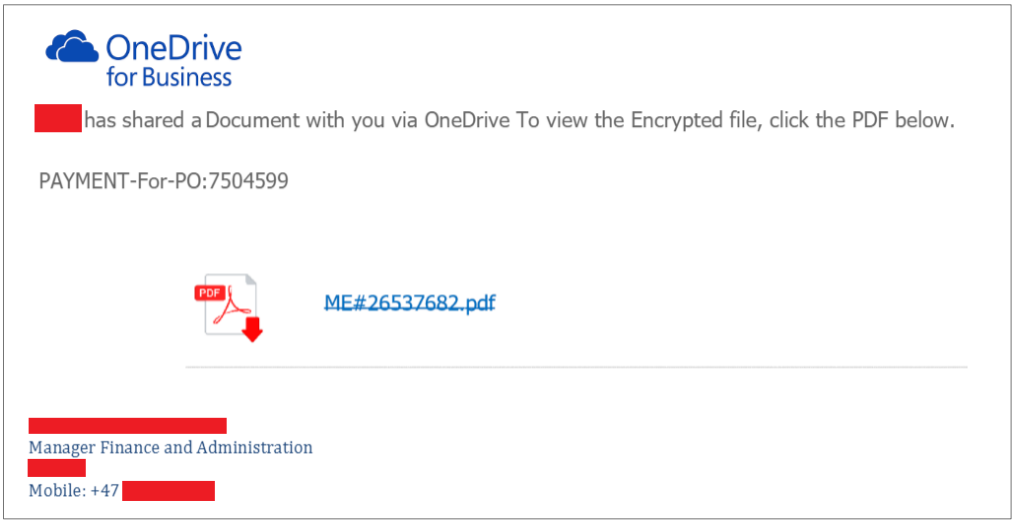
SENTRALT ANSATTE I HØYTEKNOLOGISKE NORSKE BEDRIFTER MÅL FOR E-POSTSVINDEL

- Majoriteten av bedriftene benytter Microsoft Office 365
- Videresendingsregel satt opp om en "Inbox Rule" på e-postkontoene
- Svindlerne benytter e-postkontoene til å sende e-poster som enten:
  - Reelle fakturaer med endret kontonummer
  - En melding om å endere kontonummer på en tidligere mottatt faktura
  - Falske fakturaer

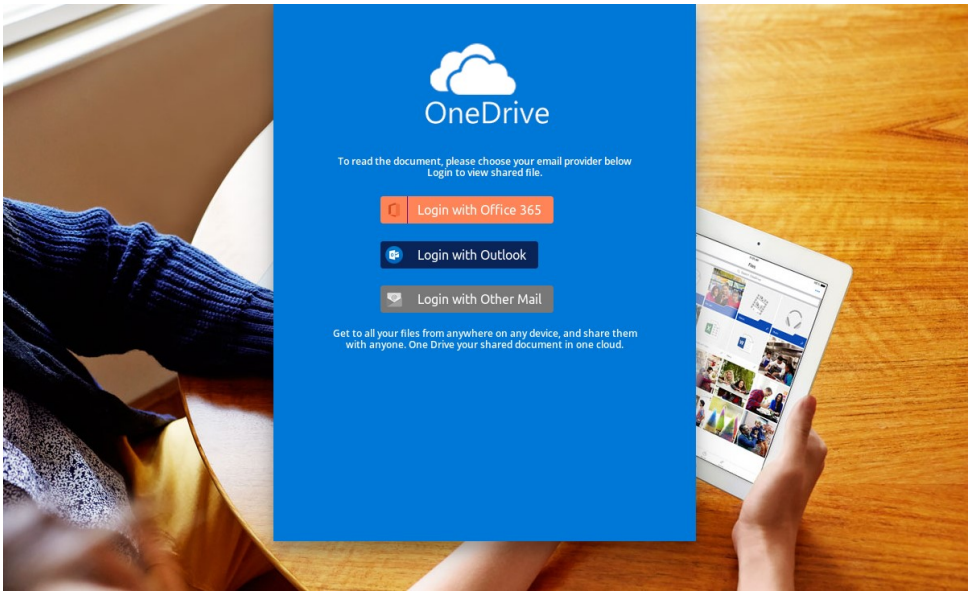
https://nsm.stat.no/norcert/norcertvarsler/e-postsvindel-trend/

BDO

E-POST ER DEN MEST UTBREDTE ANGREPSVEKTOREN

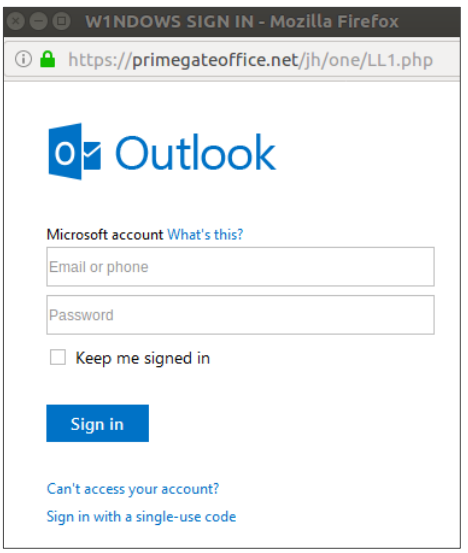


BDO



NETTFISKE

- Anbefaling: Aktiver tofaktor.



DATAINNBRUDD KAN GI STORE TAP

NOTPETYA

Mærsk tapte opptil 2,5 milliarder kroner på dataangrep

- Uten IT i 10 dager
- Volumene i shippingvirksomheten falt 2,5 prosent
- Enhetskostnadene for faste bunkerpriser økte med 3,9 prosent

Kilde: digi.no 07.11.2017

14

GLOBALISERING GIR ØKT SÅRBARHET

- Metabo Norge AS
  - 10 ansatte
  - Driftsinntekter 44 millioner (2017)
  - Heleid av tyske Metabowerke Gmbh

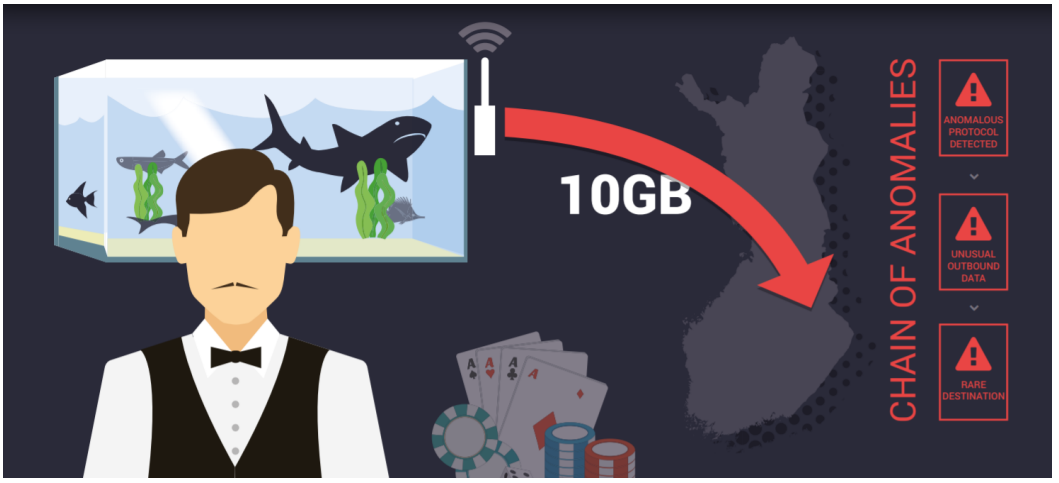
NOTPETYA RAMMET NORGESKONTOR

Det tok 12 dager før alt fungerte som normalt etter at systemene døde helt: – Angrepet kostet oss rundt 2 millioner kroner

Kilde: digi.no 14.07.2017

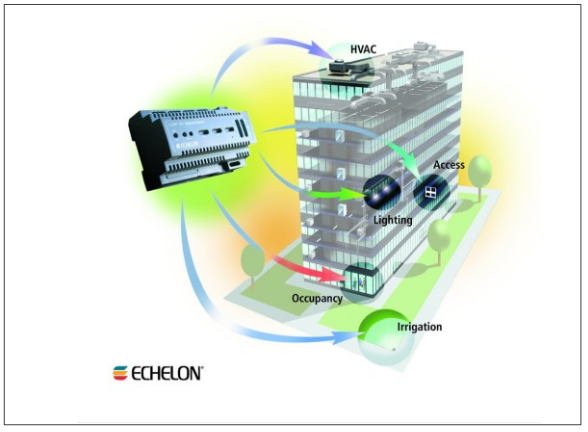
15

INTERNET OF THINGS



BDO

INTERNET OF THINGS



Johnson Controls

METASYS®

BDO

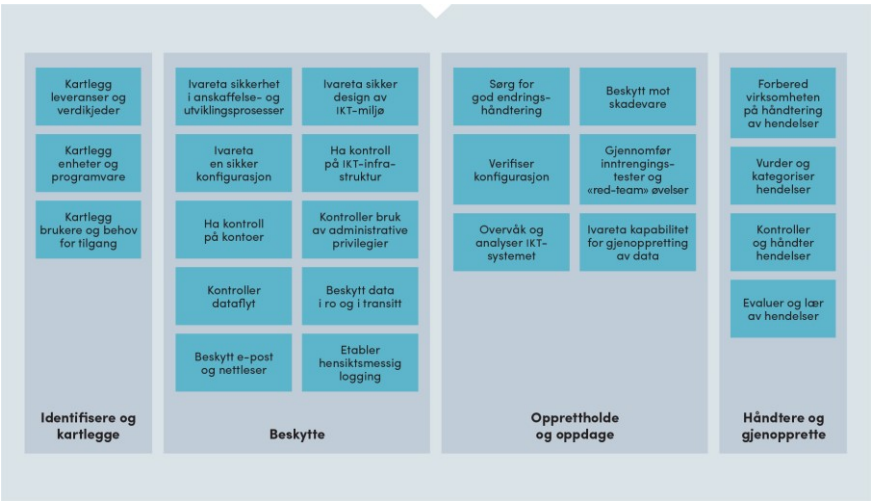
TILTAK

GRUNNPRINNSIPPER FOR IKT-SIKKERHET

NIST

GRUNNPRINNSIPPER FOR IKT-SIKKERHET

NASJONAL SIKKERHETSMYNDIGHET



SØK ETTER VIDERESENDING VIA **INNBOKS-REGLER**

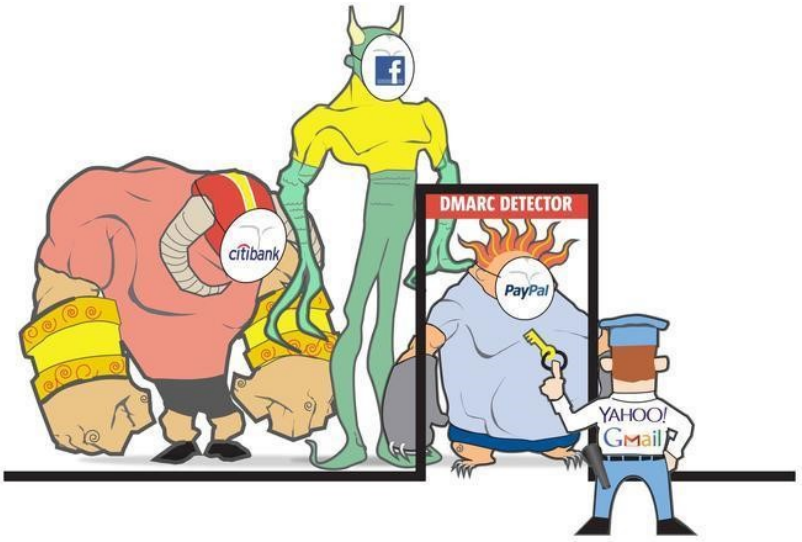
```
$Mailboxes = Get-Mailbox -ResultSize Unlimited
ForEach ($Mailbox in $Mailboxes)
{
$MailboxWithRule = Get-InboxRule -Mailbox $Mailbox.Alias |
where {($_.RedirectTo -ne $null) -or ($_.ForwardTo -ne $null) -or
($_.ForwardAsAttachmentTo -ne $null)}
if ($MailboxWithRule -ne $Null)
{
Write-Host "Postboksen $($Mailbox.PrimarySmtpAddress)
har følgende regler:"
$MailboxWithRule | fl Name, Identity, RedirectTo, ForwardTo,
ForwardAsAttachmentTo
}
}
```

SØK ETTER VIDERESENDING VIA **INNBOKS-INNSTILLINGER**

```
Get-Mailbox -resultSize unlimited |
Where {($_.ForwardingSMTPAddress -ne $null) -or
($_.ForwardingAddress -ne $null)} |
Select Name, ForwardingSMTPAddress, ForwardingAddress,
DeliverToMailboxAndForward
```

BDO

DMARC + SPF + DKIM => OPPDAGE OG BLOKKERE FORFALSKNING



BDO

DMARC

DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING & CONFORMANCE

- Beskyttelse av egne domener mot e-postforfalskning
- Blokkering av forfalsket e-post fra andres domener
- Automatisk rapportering av forfalsket e-post til eieren av domenet

- Flere tilbydere av DMARC-analyse
  - Agari
  - Dmarcian
  - DMARCAnalyzer
  - Proofpoint
  - Valimail

BDO

NOEN PRAKTISKE RÅD PÅ VEIEN TIL P=REJECT

- Start med alle domener, ikke bare hoveddomenet

- Start med monitorering for å få oversikt (p=none)

- Parkere domener som ikke benyttes til e-post
  - [domene.no.] TXT "v=spf1 -all"
  - [_dmarc.domene.no.] TXT "v=DMARC1; p=reject; rua=mailto:?; ruf=mailto:?«

- DKIM-signering er viktig fordi autoforwarding kan gjøre at SPF ikke validerer

BDO

NOEN PRAKTISKE RÅD PÅ VEIEN TIL P=REJECT

- Start med alle domener, ikke bare hoveddomenet
- Start med monitorering for å få oversikt (p=none)
- Parkere domener som ikke benyttes til e-post
  - [domene.no.] TXT "v=spf1 –all"
  - [_dmarc.domene.no.] TXT "v=DMARC1; p=reject; rua=mailto:?; ruf=mailto:?«
- DKIM-signering er viktig fordi autoforwarding kan gjøre at SPF ikke validerer
- Spørreundersøkelser og nyhetsbrev bør ikke sendes fra forfalsket e-post

BDO

- Link for sjekk av SPF og DMARC-oppføring av egne domener:

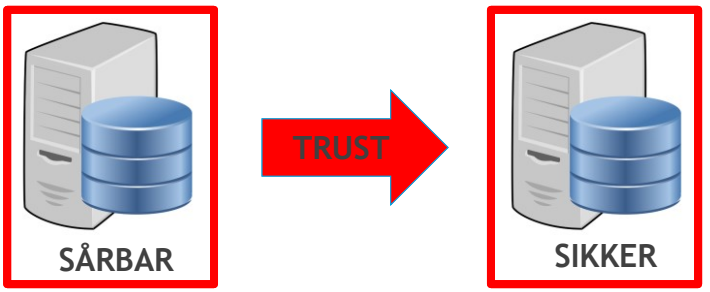
dmarc.no

27

BDO

TRUSSELAKTØRS PRIVILEGIUM

KAN VELGE LETTESTE VEI TIL MÅLET



EKSTERNE REFERANSER

https://www.nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/

https://www.nsm.stat.no/publikasjoner/rad-og-anbefalinger/temahefter/logging-okt-sikkerhet-i-ikt-systemer/

https://nsm.stat.no/norcert/norcertvarsler/e-postsvindel-trend/

https://www.nhn.no/helsecert/anbefalte-sikkerhetstiltak/dmarc/

https://researchcenter.paloaltonetworks.com/2018/08/clarifying-zero-trust-not/

https://www.usenix.org/node/194636 (Chief of NSA's TAO: Disrupting nation state hackers)

KONTAKT

+47 916 70 054
thomas.norbeck@glasspaper.no

+47 902 58 910
hakon.lonmo@bdo.no