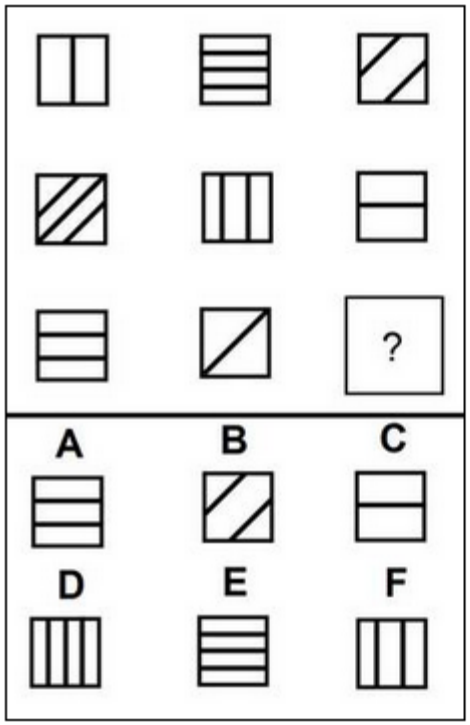
Spørsmål:

1: Hvilken figur skal inn i den siste ruten?



Svaralternativer:

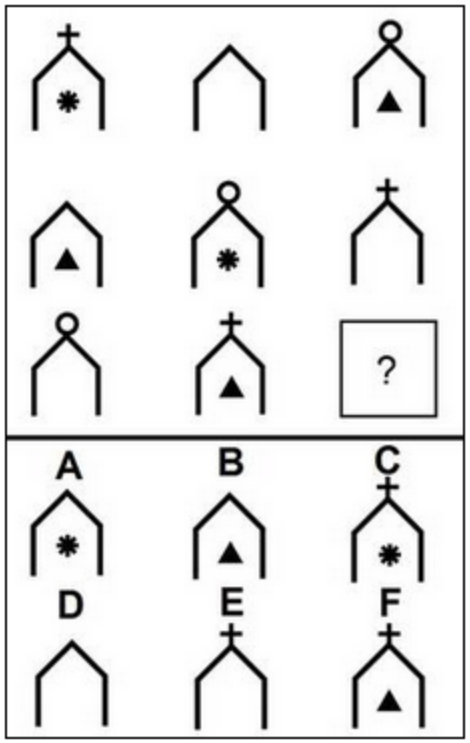
- A
- B
- C
- D
- E
- F

Spørsmål 1 av 10

Neste

Spørsmål:

2: Hvilken figur skal inn i den siste ruten?



Svaralternativer:

- A
- B
- C
- D
- E
- F

Spørsmål 2 av 10

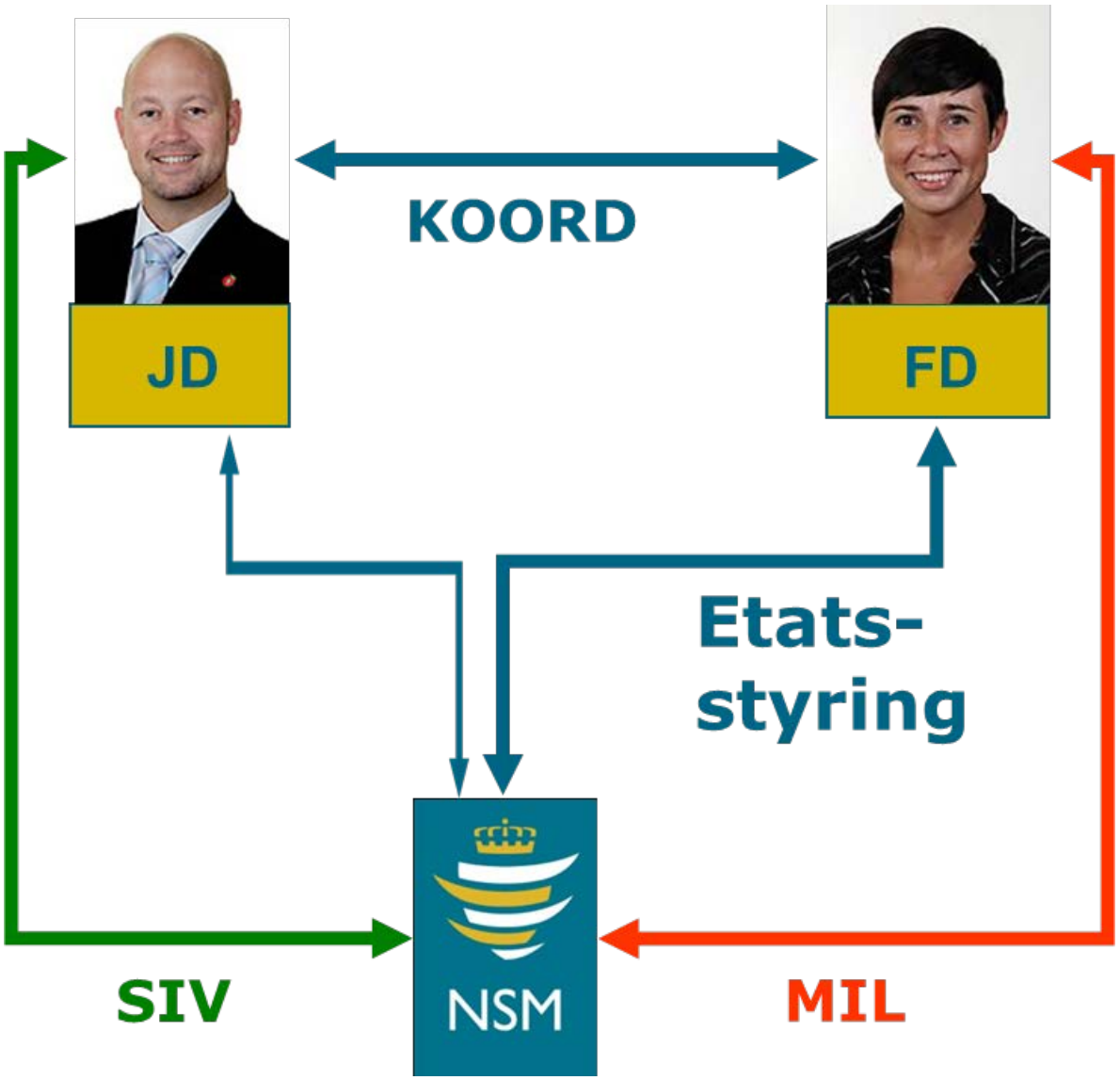
Neste

FORVENTNINGER TIL SIKKERHET I DEN DIGITALE VERDEN

Oslo , 27. mai 2015

Jørgen Dyrhaug
Nasjonal sikkerhetsmyndighet

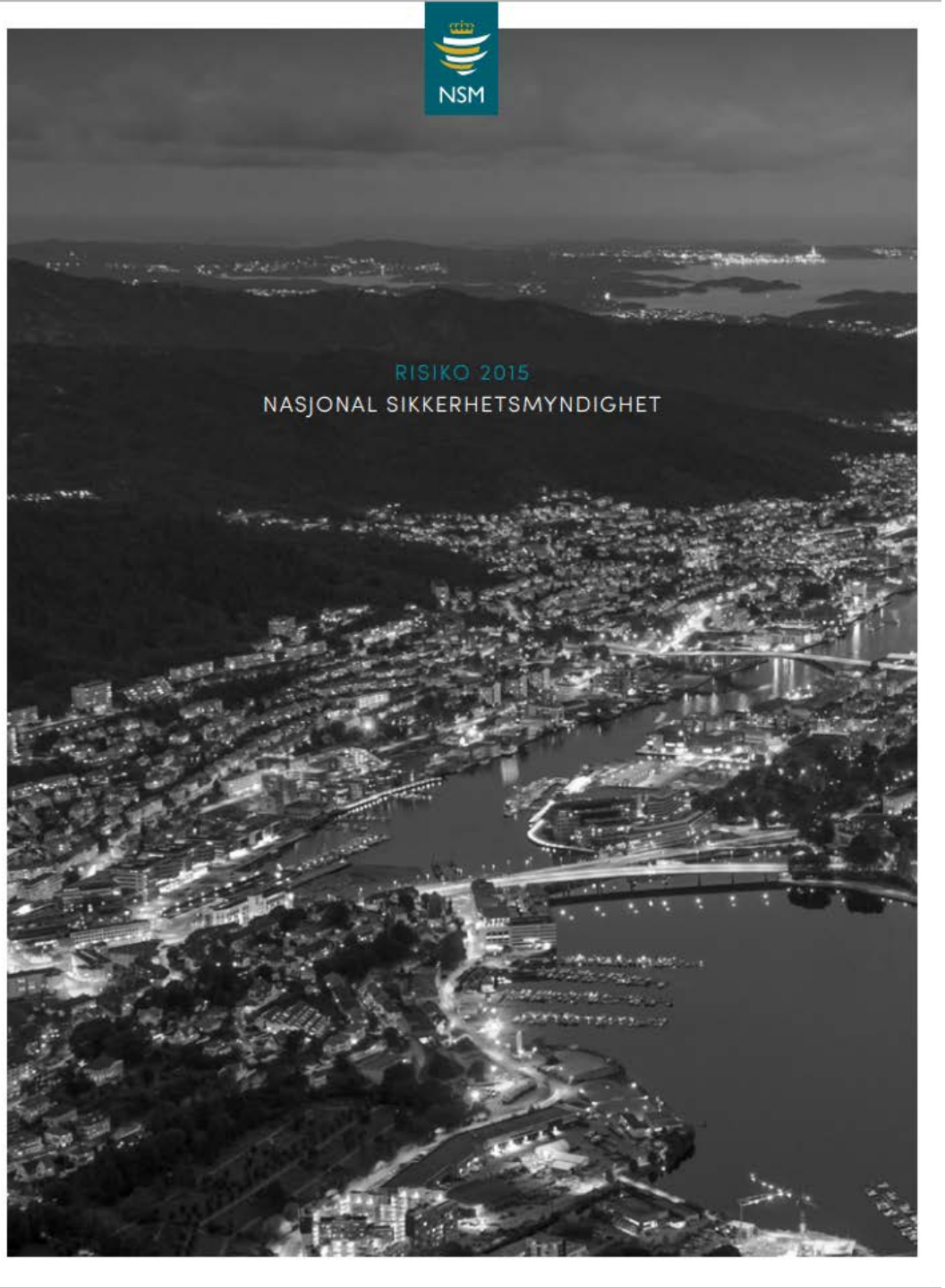
NSM | NØKKELINFORMASJON



Sikre samfunnsverdier

mot villede hendelser

(…til forskjell fra naturkatastrofer, ulykker og feil o.l)



NSM

HOVEDTRENDER

- Risikoen øker
- Vedvarende teknologiske sårbarheter
- Stort skadepotensiale
- Økt internasjonalisering
- Uoversiktlige leverandørkjeder
- Sikkerhetsarbeidet går fremover!

HVORDAN MØTER VI ET ENDRET RISIKOBILDE?

- Digitalt sårbarhetsutvalg
- Sikkerhetsfaglig råd
- Styrket nasjonal IKT beredskap
- Kurssenter for forebyggende sikkerhet

HVA MÅ DERE GJØRE?

- Forstå situasjonsbildet
- Erkjenne risiko
- Forstå sårbarhetene
- Skaffe kompetanse
- Gjøre noe med situasjonen!

2014 OPPSUMMERT

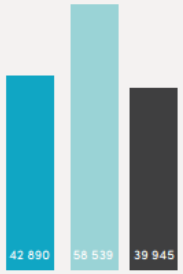
Her er noen utvalgte tall og fakta som sier noe om hva Nasjonal sikkerhetsmyndighet gjorde i 2

FOREBYGGING

42890

NØKLENE TIL NORGES HEMMELIGHETER

NSM produserer og distribuerer kryptonøklene som gjør det mulig å kommunisere sikkert i alt sikkerhetsgradert utstyr som blir brukt i Norge og internasjonalt. I fjor produserte vi 42 890 kryptonøkler. Reduksjonen fra året før skyldes reduserte internasjonale aktiviteter, samt en gjennomgang av det faktiske kryptobehovet.



41

SIKKERHETS-RAPPORTER

NSM leverte i løpet av 2014 41 ukentlige sikkerhetsrapporter til Justis- og beredskapsdepartementet og Forsvarsdepartementet.

1194

RÅDGIVNING OM OBJEKTSIKKERHET

Nasjonal sikkerhetsmyndighet gir råd om objekter som må sikres spesielt mot sabotasje og terror. I fjor gav våre fagfolk totalt 1194 rådgivningstimer til norske virksomheter.

655

NÅR STADIG FLERE

Den årlige sikkerhetskonferansen i Oslo kongressenter har på få år doblet antall deltakere til 655 i 2014.

400

KURSET 400 PERSO

I 2014 åpnet NSMs kurs for forebyggende sikke i Sandvika. I løpet av ha har vi i samarbeid med svaret kurset 400 perso forebyggende sikkerhe

257

KURSET HELE NORGE I SIKKERHET

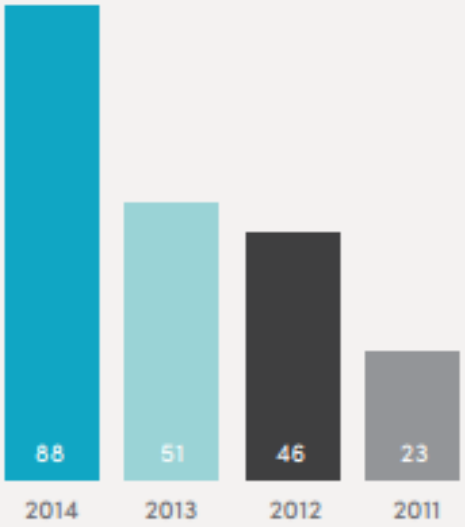
Oktober er Nasjonal sikkerhetsmåned i Norge. I fjor arrangerte vi sikkerhetsseminarer i sju norske byer, fra Lillesand i sør til Tromsø i fjor. Vi nådde totalt 257 deltakere.

HÅNDTERING

88

STADIG FLERE DATAANGREP

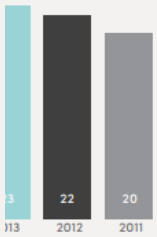
I fjor varslet og håndterte vi totalt 88 alvorlige dataangrep, mot 51 i hele 2013. Flesteparten av angrepene har som formål å stjele informasjon fra datasystemene til store eller viktige norske bedrifter.



ut har gjort at noen av tallene fra tidligere år har blitt revidert, men statistikken er sammenlignbar fra år til år.

TROLL

ktigste
ntallet tilsyn.
førte vi 27 tilsyn. Målet
ke antallet vesentlig.



121

GODKJENTE 121 DATASYSTEMER

Før et datasystem tas i bruk for sikkerhetsgradert informasjon, må det sikkerhetsgodkjennes av NSM. I fjor godkjente vi 121 datasystemer.

50

-SAKER

let NSM 2150 saker som
to fra luft. Alle som skal
ed droner og andre
for synsrekkevidde må
a NSM. Ny praksis av
er at færre trenger lisens.

22

LEVERANDØRER MÅ KLARERES

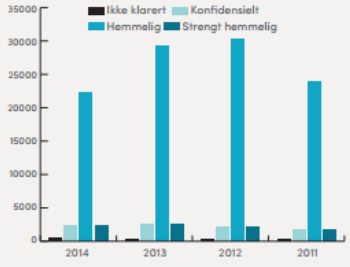
Alle leverandører som har behov for sikkerhetsgradert informasjon i forbindelse med leveransen, må klareres. I fjor fattet NSM totalt 22 vedtak om leverandørklareringer.

KERHETS-ER

r personopp-
le klarerings-
utført i Norge.
ene blir utført
rskjellige
digheter.

i registreringen av Strengt Hemmelig gjør at antallet trengt Hemmelig/ ret, fremstår som

tidligere års registreringspraksis hadde blitt lagt til grunn.



TRUSLER I DET DIGITALE ROM

Nettverksbaserte etterretningsoperasjoner er en betydelig trussel mot norske interesser. Slike operasjoner utføres mot en rekke mål i Norge. Fremmed etterretning angriper løpende norske myndigheter og virksomheter.

Den mest alvorlige etterretningstrusselen i fredstid er at aktører får innsyn i politiske vurderinger, militære forhold, kommersielle data og intellektuell eiendom. I en krise eller krig kan nettverksoperasjoner også benyttes til sabotasjeformål og til støtte for konvensjonelle militære operasjoner.

eller avskrekke trusselaktørene.

Aktører som truer norske interesser spenner fra statlige etterretnings- og sikkerhetstjenester, via tradisjonelle militære strukturer, kommersielle virksomheter, terrorist- og ekstremistgrupperinger, til organiserte hackergrupper. Etterretningstjenesten har primært fokus på statlige aktører og ikke-statlige aktører som operer på vegne av eller støttes av statlige myndigheter.

De alvorligste truslene i det digitale rom er fremmed etterretningsvirksomhet og mulighetene for sabotasjehandlinger. I likhet med tradisjonell etterretning er nettverks-baserte etterretningsoperasjoner knyttet til å skaffe informasjon om økonomiske, politiske og militære forhold. Nettverksbasert sabotasje hvor formålet er å påvirke eller stanse funksjoner eller prosesser innen kritisk

De fleste datasystemer bygger på teknologi og sikkerhetsprinsipper som er like på tvers av nasjonalstatlige grenser. Det gir en unik mulighet for etterretningsvirksomhet i det digitale rom. Aktører kan systematisk forberede angrep og relativt fritt velge mål, metode, forløp og tidspunkt. En rekke metoder kan benyttes for å trenge inn i et nettverk. E-post-vedlegg med skadevare er en enkel, men effektiv metode. Trusselaktøren kan også bruke såkalte "vannhullsangrep", det vil si å infisere en kjent internettside som hyppig besøkes av målet de ønsker å ramme. En annen metode er å utnytte tjeneste- og underleverandører som en indirekte vei til målet gjennom sammen-koblede nettverk eller gjennom felles brukere. Dersom en trusselaktør lykkes med å etablere flere typer skadevare i et system, er det relativt få begrensninger på videre aktivitet. I praksis kan all lagret informasjon kopieres, manipuleres eller ødelegges. Tilstedeværelsen i nettverket

(Foto: Shutterstock)

– Hackere er fem år foran oljenæringen

Petromagasinet | HMS og beredskap av Dan Arvid Bjørsvik - 26. mai 2015 0

Han var eneste nordmann som deltok i verdensmesterskapet for hackere, «NetWars Tournament of Champions», i Washington. Nå hjelper Chris Dale olje- og gasselskap med å bekjempe datainntrengere.

– På sikkerhetsfronten henger oljenæringen igjen fem år etter der de bør være. Samtidig sitter hackere med mye mer avansert verktøy som de samarbeider om å utvikle. Vi er nødt til å komme oss opp på et nivå der vi virkelig kan motkjempe hacker-angrep, sier Dale til Petro.no.

Februar i år gikk han fra å være sikkerhetssjef hos Sharecat Solutions AS til å jobbe som penetrasjonstester i sikkerhetsselskapet Netsecurity AS, som blant annet har BW Offshore på klientlisten. Ifølge askøyværingen omtaler han seg ikke som «hacker» i forretningssammenheng, fordi det forbindes med personer som har onde hensikter. Men i likhet med hackere er Dale hands-on på tastaturet hver dag. Det er der han trives best.

– Våre kunder ønsker å vite om produktene deres har åpne dører; er man nødt til å bruke motorsag og slegge for å komme seg inn i systemet eller kan man bare spasere rett inn? Min jobb er å tenke utenfor boksen når jeg ser på hvordan systemene er laget og hvor det er begått feil.

Hackere stod for 88 dataangrep i fjor – blir verre i år

Feil begås, skal vi tro Nasjonal Sikkerhetsmyndighet (NSM) rett. I fjor

Velkommen hjem, Goliat!

20. april 2015 0

Kongsberg Maritime sikrer Johan Sverdrup-kontrakt

26. mai 2015 0

Vestlandet arbeider mer med omstilling

26. mai 2015 0

Foto: colourbox.com

ØYSTEIN SUNDE SYNDROMET

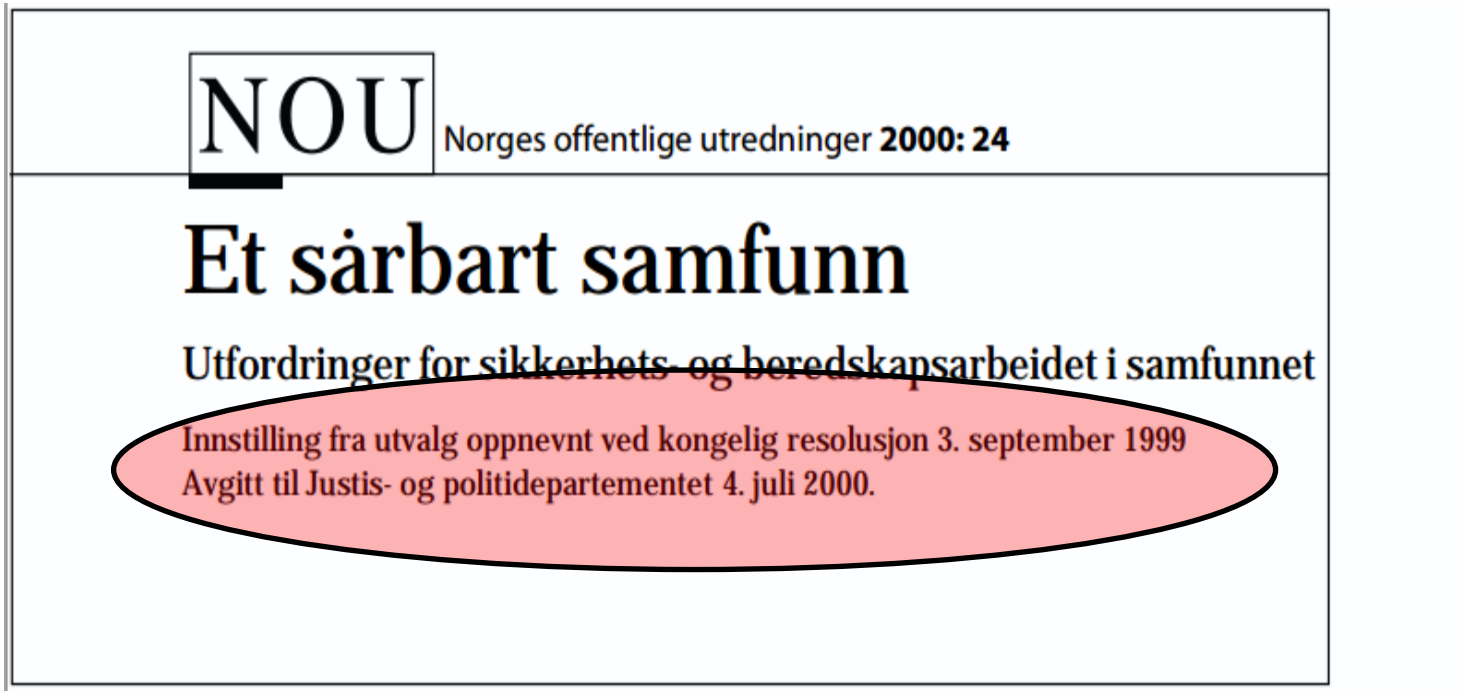
Illustrasjon: Skjermklipp fra NRK

Ulike typer elektroniske trusler:

Logiske angrep på komponenter som utgjør kritiske IKT-systemer kan skape store problemer for eierne av IKT-systemene. Det kan være snakk om spredning av virus [1] , trojanske hester [2] eller Ormer [3] . Den senere tid har vi sett flere store nettsteder blitt utsatt for det som kalles «distributed, coordinated denial-of-service attack». Det vil si at angriperne bruker flere kraftige datamaskiner til samtidig å sende formidable mengder forespørsler mot nettsiden de ønsker å angripe. Dette vil føre til at det angrepne nettstedets servere i verste fall vil bryte sammen, og i beste fall svært vanskelig for andre brukere å komme i kontakt med serveren.

Logiske angrep på komponenter som støtter opp om de kritiske IKT-systemer. Dette er indirekte angrep på støttefunksjoner som IKT-systemene er avhengige av for å kunne fungere. Det kan være ventilasjonssystemer, strømforsyning, vannkjøling m.m. På bakgrunn av dette er det ikke tilstrekkelig at bare IKT-systemene er sikret.

Bevisst utnyttelse av IKT-systemer for å tilegne seg informasjon som en i utgangspunktet ikke har rettmessig tilgang til, for eksempel knekking av koder for kryptering/passord for å tilegne seg andres krypterte informasjon. Elektronisk tyveri av dokumenter/informasjon samt spionasje, både industriell og statlig, er et stort problem som man ikke har oversikt over på grunn av store mørketall.



NOU Norges offentlige utredninger **2000: 24**

Et sårbart samfunn

Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet

Innstilling fra utvalg oppnevnt ved kongelig resolusjon 3. september 1999
Avgitt til Justis- og politidepartementet 4. juli 2000.

SIKKERHET?

HOLDER DET IKKE

BARE MED TEKNOLOGI?

Ny teknologi krever ny adferd!


There is always a WAY

FRISTENDE? En del nordmenn er naive, og går fem på når de får slike og lignende henvendelser. (Foto: BERIT B. NJARGA)

Nordmenn svindlet for 210 millioner i 2014

50

Publisert: Torsdag 22. januar 2015 kl 06:00

173 nordmenn ble i 2014 svindlet av bedragere med opprinnelse i Vest-Afrika, som de har truffet på nettet og på Facebook.

TWEETS 260 | BILDER/VIDEOER 48 | FØLGERE 16,5 K | Mer | Følger

Debit Card

@NeedADebitCard

Please quit posting pictures of your debit cards, people.

Registrerte seg mai 2012

Send en tweet til Debit Card

4 følgere du kjenner

48 bilder og videoer

Tweets | Tweets og svar

Retweetet av Debit Card

u mad i fuckd ya hoe @iChArnold · 6. jun.

My new debit card came today

34 | 13 | Vis flere bilder og videoer

Retweetet av Debit Card

amy feldsher @snaisy · 24. mai

Eugh Kelsey is bitching cos my bank card only has me and Lauren on it #firstworldproblems #jealous #thirsty

Folk å følge · Oppdater · Vis alle

U.S. Army @USArmy
Følges av Trond Lundberg o...
Følg

NGA @NGA_GEOINT
Følg

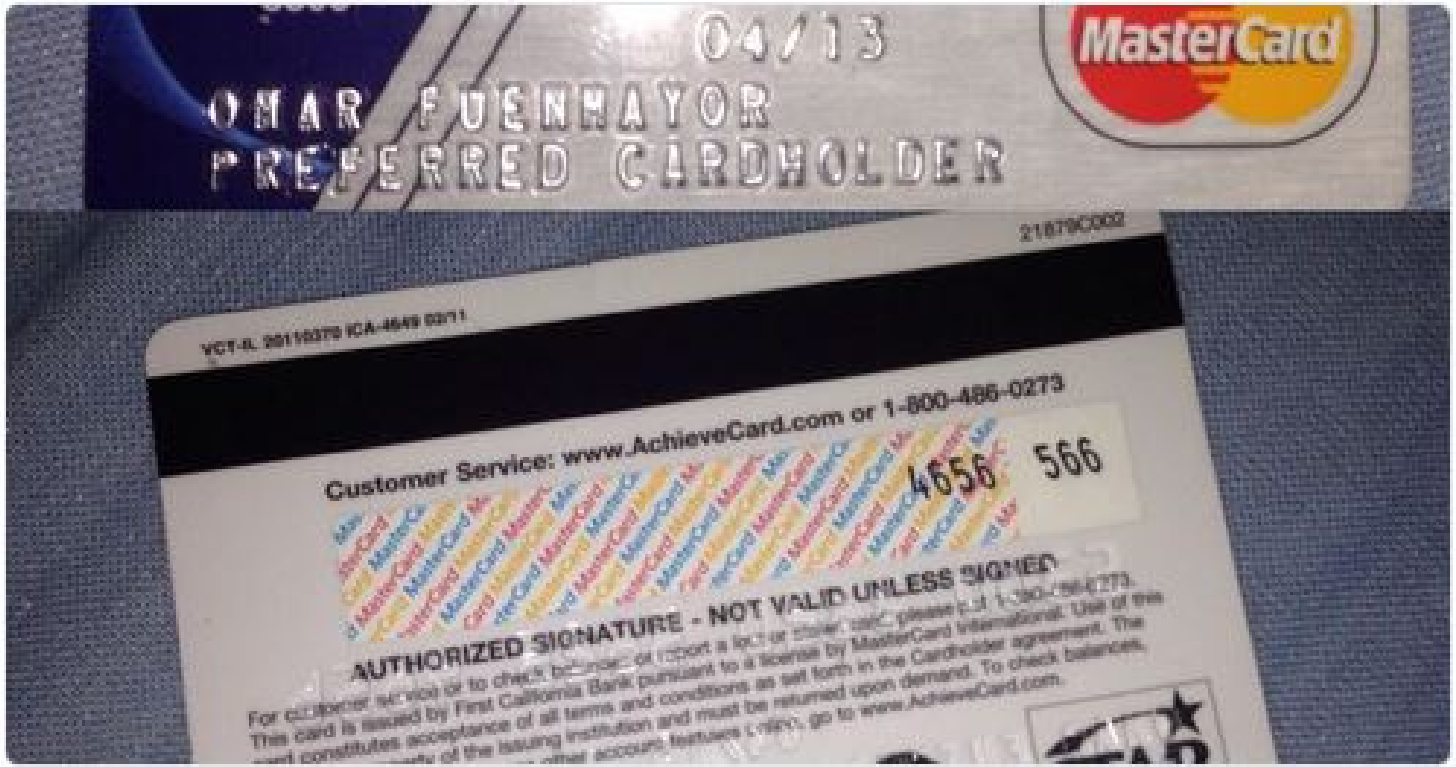
The White House @Whit...
Følg

Populære kontoer · Finn venner

Trender · Endre

#youandimusicvideo
#shawnsfirstsingle
The Fault In Our Stars
#TaylorTo1Mill
Takk
Trondheim
Tusen
Norway
Stavanger
Zucca

Got ma new credit card. its boring but it got 500 dollars
Ya'll broke niggas cant get on my level! #LikeABoss



197 67 Vis flere bilder og videoer

Dagbladet Null CTRL

Søk

Nyheter Sport Kultur Kjendis Reise Bil Meninger Magasinet Økonomi Pluss A-A eAvis NYT Været dbtv

Innenriks Utenriks Politikk Video Miljø Helse Teknologi Bil Sex og samliv Siste 48 timer Arkiv

Null CTRL

Meny

Farene Er du utsatt? Hvem er vi? Alle sakene

ER DU UTSATT?

Her kan du teste din datasikkerhet

Se selv!

Avslører demente med nøkkel i lomma, dialysepasienter og elever som skal stroppes fast

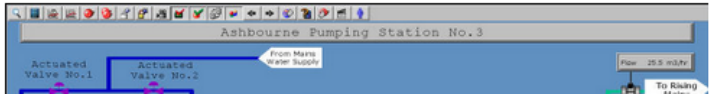
Taxi-leverandør lot «dørene stå åpne». Les mer

Dagbladet vant SKUP-prisen

dbtv For serien «Null CTRL». Les mer

Dagbladet vant «europeisk Pulitzer»

dbtv - For bidrag til journalistikkens framtid. Les mer



BBC Ukraine journalist Myroslava Petsa posted this screenshot from the VK page of Mikhail Chugunov (the original post, now deleted, is from July 11):

(Text in screenshot: “With Grads to Ukraine…”)


iBRABO
Follow @M_Taylor_Kiwi
Kiwi Jihadi @M_Taylor_Kiwi
@AbuPal1 Baqiya yes

Klipp fra VG

Klipp fra UKJENT KILDE

Tekno IT

Gir blaffen i datasikkerhet på jobb

Ansatte slumser med passord og bryter bevisst egne bedriftsregler for datasikkerhet. Antall nordmenn som motarbeider it-avdelingen er økende, ifølge sikkerhetsekspert.

Magnus Eidem
Publisert: 05.05.2015 – 21:53 Oppdatert: 05.05.2015 – 22:32

Les hele avisen

- Brudd på it-sikkerhetsreglene skjer i alle bedrifter. Som oftest aner ikke de ansatte at de bryter reglene, sier Sofie Nystrøm, direktør for norske CCIS - Center for Cyber and Information Security.

Uklare sikkerhetsregler og regler basert på forbud får mange ansatte til å se etter egne, enklere løsninger - uten at de skjønner konsekvensene.

- Frustrasjon er en viktig driver for å bryte reglene, sier CCIS-direktør Sofie Nystrøm. Foto: Gunnar Kopperud

- Det er lett å kjenne seg igjen. Man sender noen dokumenter man vil lese gjennom på kvelden til en privat epostadresse, eller lagrer dem på en ukryptert minnepinne eller i en gratis nettlagringstjeneste. Alle disse metodene betyr at man gjør dokumentene synlig for industrispionasje eller overvåkning, sier Nystrøm.

Minnepinner er enkle å miste og ukryptert e-post er som å sende postkort i vår fysiske verden.

En undersøkelse analyseselskapet VansonBourne har utført for it-selskapet Aruba Networks viser at 56 prosent av arbeidstagere har omgått eller kan tenke seg å omgå bedriftens sikkerhetsregler for å få noe gjort. Undersøkelsen er besvart av 12.000 arbeidstagere i 23 land. Kun 250 nordmenn er med i undersøkelsen, men

Har du husket å slå av stedstjenester på appene i mobilen?

Slik kan du bli overvåket på Twitter og Instagram uten å ane det

En rekke norske politikere har i årevis røpet sine egne bevegelser via sosiale medier. - Kan utnyttes av terrorister og fremmed etterretning, advarer sikkerhetsspesialist.

SLIK SKJEDDE KARTLEGGINGEN

Offentlige WiFi-nett er en større sikkerhetsrisiko enn falske basestasjoner

– Vi må erkjenne at vi kan bli overvåket

Justisminister Anundsen redegjør for Stortinget.

Norske forsikringer mot dataangrep er et nytt fenomen, der forskere ser flere utfordringer med å måle konsekvensene sammenlignet med tradisjonell forsikring.

DATAKRIMINALITET

Nå kan du forsikre deg mot dataangrep

Eksperter advarer mot å bruke det som en sovepute.

Av Espen Zachariassen (@ezach)

Publisert 23. mars 2015 kl. 15:14 - Oppdatert 23. mars 2015 kl. 15:41

Sammen med IBM har forsikringsselskapet If kjørt i gang det som skal være landets første forsikringsordning som rydder opp hvis bedriften blir utsatt for et dataangrep eller annen form for datakriminalitet.

Sintef har en ny forskningsgruppe på feltet og som ser mange uløste utfordringer.

Les også: Norske nettselskaper øver ikke på IT-angrep

Skade og tap

Forsikringen dekker skader og tap som følge av blant annet skadevare, virus, tjenestenektangrep og rene hacker-angrep.

Da er strategien at IBM vurderer hvert tilfelle


FLYBUSSEN
AIRPORT BUS
SAS
Flybussen.NO
SAS
tide
2352
Flybussen.NO
2352
SU 22505


Keep mum
she's not so dumb!
CARELESS TALK COSTS LIVES

PST ber arbeidsgivarar sjekke russiske tilsette etter spionforsøk

Fleire hundre russarar som har tryggleiksklarering er blitt utsette for press frå russisk etterretning om å gi frå seg sensitiv informasjon om norske forhold.

Arne Christian Haugstøyl i PST seier at tryggingsklarerte russiske statsborgarar er attraktive for russisk etterretning, som ønskjer intern informasjon om Noreg.
FOTO: NRK

Journalist
Katrine Nybø

Journalist
Tormod Strand
@tormodstrand

Publisert 21.05.2015, kl. 20:11

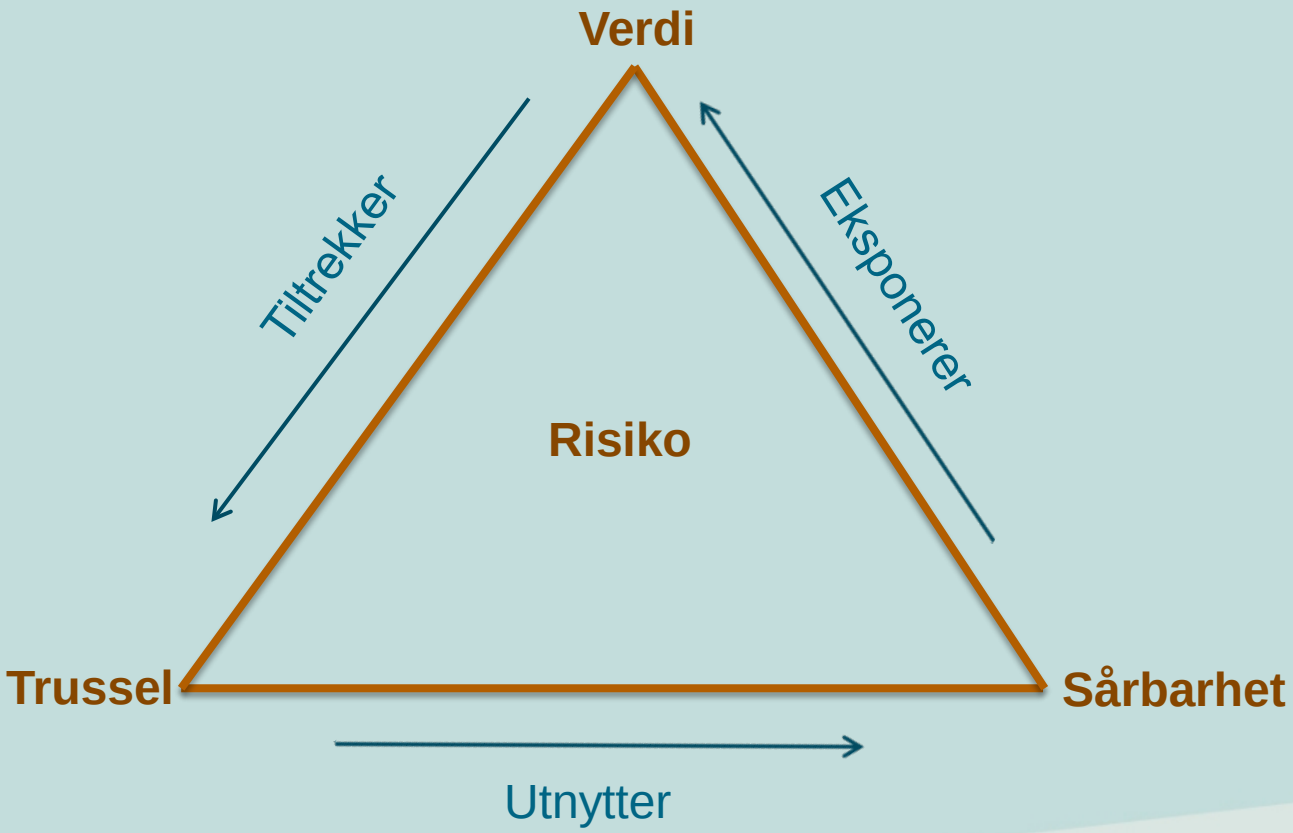
Den siste tida har fleire etniske russarar med tryggleiksklarering kome til PST og sagt at dei har vorte forsøkt pressa av russisk etterretning til å levere frå seg sensitiv informasjon.

Alle har jobbar som krev tryggleiksklarering på ulikt nivå. Desse tryggleiksklareringane er gitt i ei anna tryggleikspolitisk tid. Dei som sit i desse stillingane er utsette for press frå heimlandet.

– Vi har vore naive

Vises med tillatelse fra "www.caprino.no"

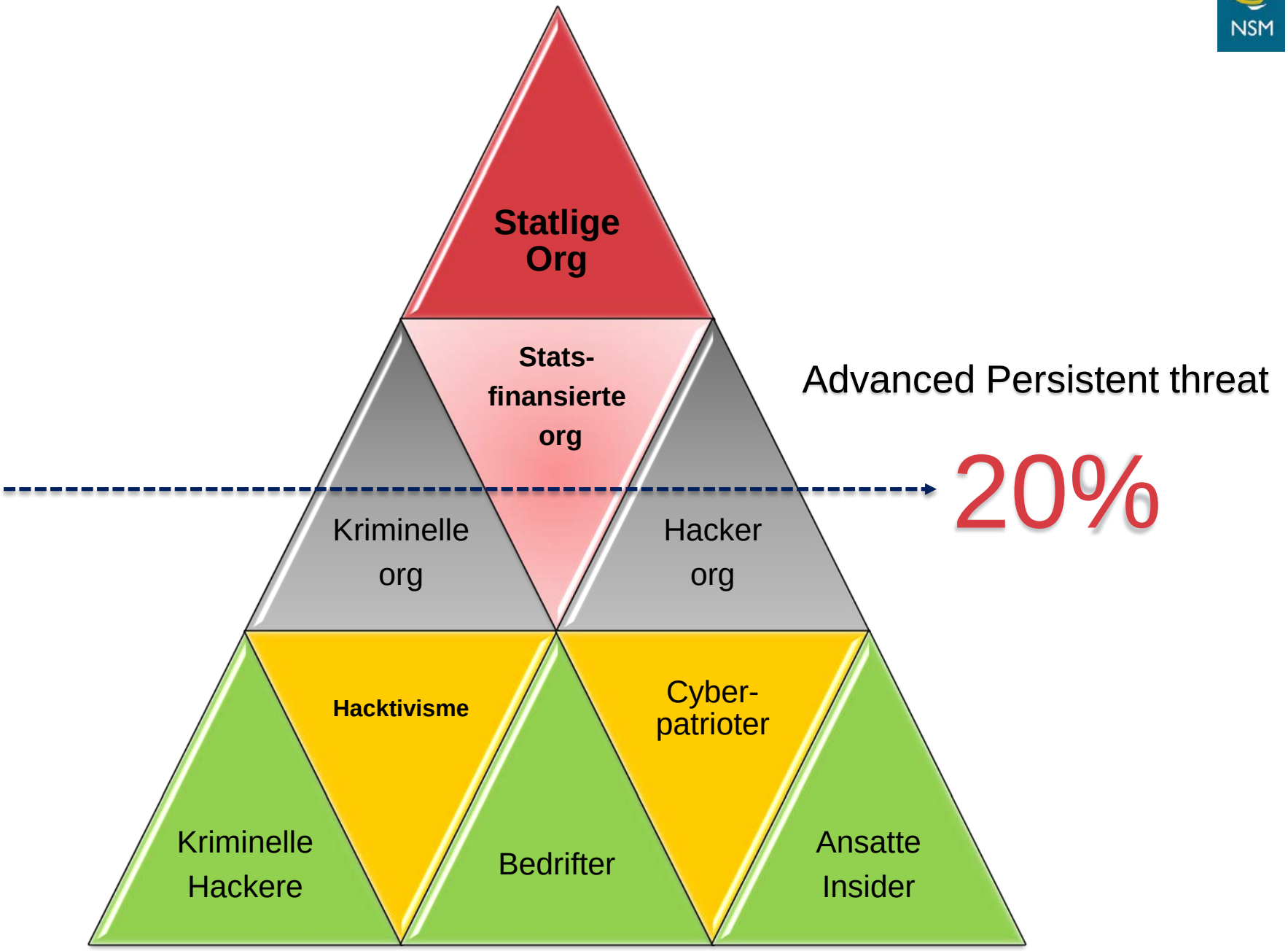
Risiko er funksjonen av…?



Hvordan ser en hacker ut?

Foto: colourbox.com

Foto: colourbox.com


Statlige Org
Stats-finansierte org
Kriminelle org
Hacker org
Hacktivisme
Cyber-patrioter
Kriminelle Hackere
Bedrifter
Ansatte Insider
Advanced Persistent threat
20%

«Det er en utfordring at mange ser ut til å tro at det er mulig å forebygge og forhindre uønskede hendelser i det digitale rom, på en slik måte at de selv ikke trenger å fokusere på egen sikkerhet»

Den norske drømmende, smånaive nissen

Den globale, kyniske varianten

Klipp: Ukjent kilde

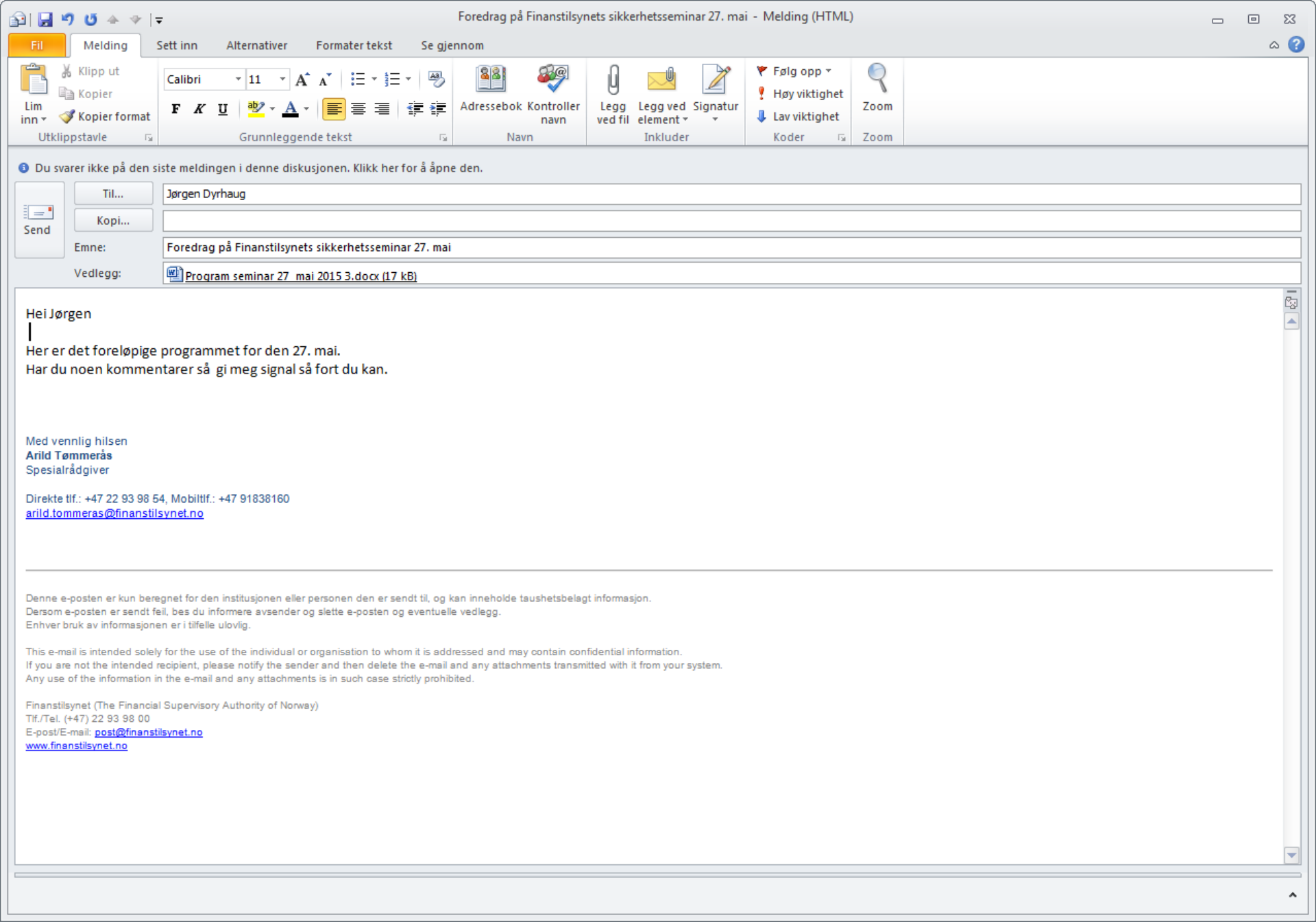
«Vi sloss daglig med å holde angriperen unna vår informasjon»

«Nei det har vi heldigvis ikke merket noe til»

«Vi får den sikkerhet vi er villig til å ha, og som vi fortjener»

Sikkerhetstiltak vil som oftest medføre en begrensning av en eller annen art, og da er spørsmålet om vi er villige til å akseptere begrensningene. Vi kan sannsynligvis ikke få i både pose og sekk.


«ÅPNE A DRE-POST,
VEDLEGG LINKER
FRA OLK
DERE IKKE KJENNER»


Foredrag på Finanstilsynets sikkerhetsseminar 27. mai - Melding (HTML)
Fil
Melding
Sett inn
Alternativer
Formater tekst
Se gjennom
Lim inn
Klipp ut
Kopier
Kopier format
Utklippstavle
Calibri
11
Grunnleggende tekst
Adressebok
Kontroller navn
Navn
Legg ved fil
Legg ved element
Signatur
Inkluder
Følg opp
Høy viktighet
Lav viktighet
Koder
Zoom
Zoom
Du svarer ikke på den siste meldingen i denne diskusjonen. Klikk her for å åpne den.
Send
Til...
Jørgen Dyrhaug
Kopi...
Emne:
Foredrag på Finanstilsynets sikkerhetsseminar 27. mai
Vedlegg:
Program seminar 27_mai 2015 3.docx (17 kB)
Hei Jørgen
Her er det foreløpige programmet for den 27. mai.
Har du noen kommentarer så gi meg signal så fort du kan.
Med vennlig hilsen
Arild Tømmerås
Spesialrådgiver
Direkte tlf.: +47 22 93 98 54, Mobiltlf.: +47 91838160
arild.tommeras@finanstilsynet.no
Denne e-posten er kun beregnet for den institusjonen eller personen den er sendt til, og kan inneholde taushetsbelagt informasjon.
Dersom e-posten er sendt feil, bes du informere avsender og slette e-posten og eventuelle vedlegg.
Enhver bruk av informasjonen er i tilfelle ulovlig.
This e-mail is intended solely for the use of the individual or organisation to whom it is addressed and may contain confidential information.
If you are not the intended recipient, please notify the sender and then delete the e-mail and any attachments transmitted with it from your system.
Any use of the information in the e-mail and any attachments is in such case strictly prohibited.
Finanstilsynet (The Financial Supervisory Authority of Norway)
Tlf./Tel. (+47) 22 93 98 00
E-post/E-mail: post@finanstilsynet.no
www.finanstilsynet.no


S-org
ORG
LEDELSE
TEKNOLOGI
BRUKERE

DET FINNES IKKE ÉN ENESTE VIRKSOMHET SOM ER ETABLERT I DEN HENSIKT Å VÆRE SIKKER!


Sikkerhet er ikke det viktigste
Hvilken risiko kan dere akseptere
Engasjement fra alle!
Kartlegg sårbarhetene deres
Ingen "one size fits all"!

Kjerne-
virksomhet

Ny teknologi krever ny adferd!

TV5 Monde røpet passord til egne kontoer på blant annet Youtube og Instagram i egne sendinger. (Skjermdump via 13 Heures) Illustrasjon:

KYBERANGREPET MOT TV5 MONDE

Hvordan kunne IS hacke en TV-stasjon?

Avslørte egne passord rett i TV-ruta.

Av Marius Jørgenrud

Publisert 13. april 2015 kl. 10:22 - Oppdatert 13. april 2015 kl. 11:31

Kvinnen skal ha mistet rundt ti hårlokker i møtet med robotstøvsugeren. FOTO: Changwon Fire Service Headquarters/YONHAP

Robotstøvsuger slukte håret til kvinne (52)

Den sør-koreanske kvinnen lå og sov og våknet da støvsugeren plutselig tok tak i håret hennes.

Øystein Kløvstad Langberg

Oppdatert: 10.feb. 2015 08:15

Robotstøvsugere som på egenhånd kan ta seg av husarbeidet, øker raskt i popularitet over hele verden.

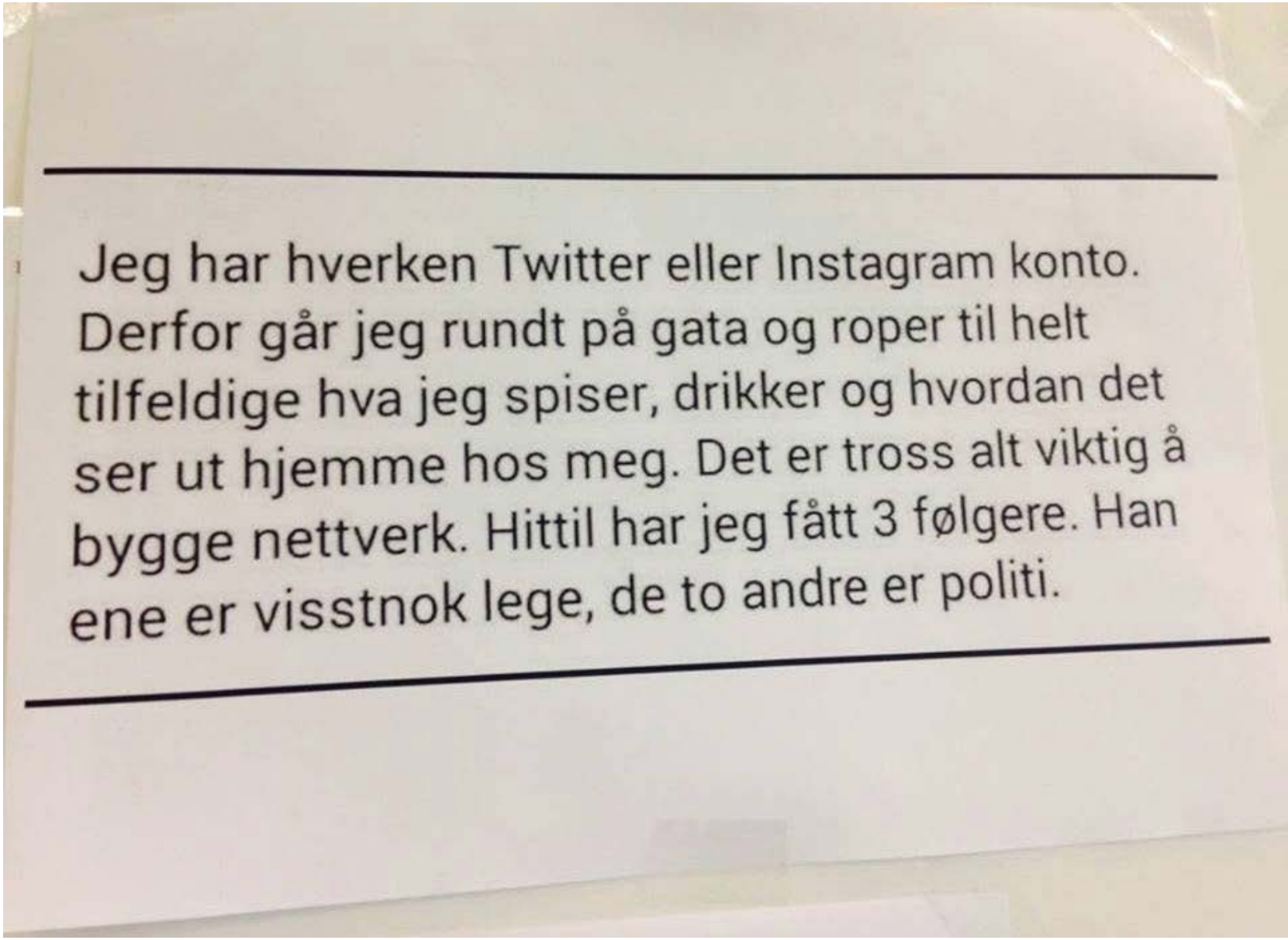
Men møtet med robotfremtiden ble ugjestmildt for en 52 år gammel kvinne fra byen Changwon i Sør-Korea.

Hun hadde satt på støvsugeren og lagt seg på gulvet for å sove.

Plusetlig våknet hun av noe som lugget kraftig. Støvsugeren hadde tatt tak i en stor bit av håret hennes og slukt den.

Fikk hjelp av ambulansepersonell

Hun klarte ikke å komme seg løs, og ringte lokale brannmannskaper med


Jeg har hverken Twitter eller Instagram konto. Derfor går jeg rundt på gata og roper til helt tilfeldige hva jeg spiser, drikker og hvordan det ser ut hjemme hos meg. Det er tross alt viktig å bygge nettverk. Hittil har jeg fått 3 følgere. Han ene er visstnok lege, de to andre er politi.

NSW