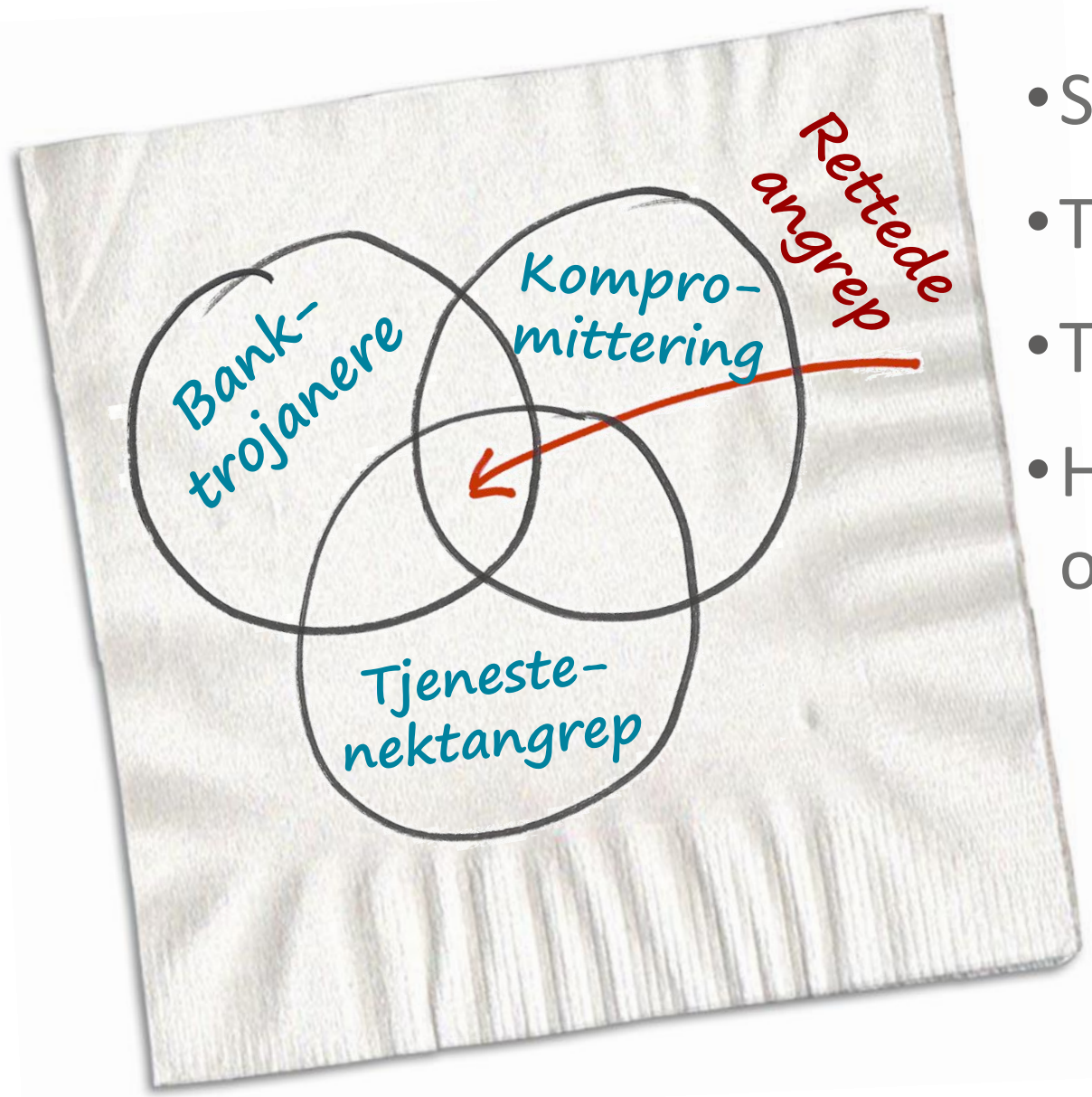
Det digitale trusselbildet – Sårbarheter og tiltak

EVRY

Agenda



- Sikkerhetsparadokset
- Trusler og trender
- Tall og hendelser
- Hvordan sikrer vi oss?

Sikkerhetsparadokset

Aldri hatt mer kunnskap

+

Aldri hatt mer ressurser

=

Aldri vært mer sårbare ?!

Hva står vi overfor?

78% økning i spionasje

NSM Rapport om sikkerhetstilstanden 2014

32% av alle bedrifter vil bli utsatt for Phisingangrep i 2015.

Symantech Treat report 2014

66% av alle norske organisasjoner har vært utsatt for hacking i 2014

Mørketallsundersøkelsen

Etterretningsaktiviteter fra Kina og Russland

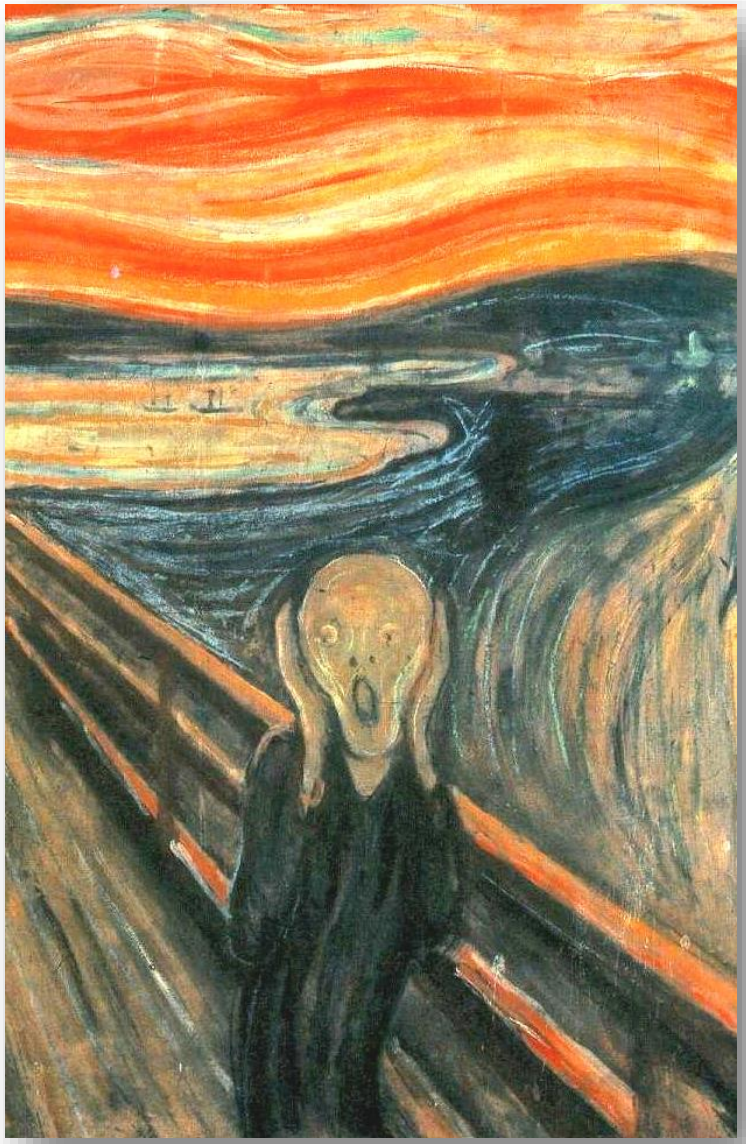
Kilde PST, FoE

Erkjennelser

- Vi må gå ut i fra at vi er kompromittert
- Vi må erkjenne at vi kommer til å bli rammet av en sikkerhetshendelse

- Spørsmålet er da – hvordan håndterer vi dette?

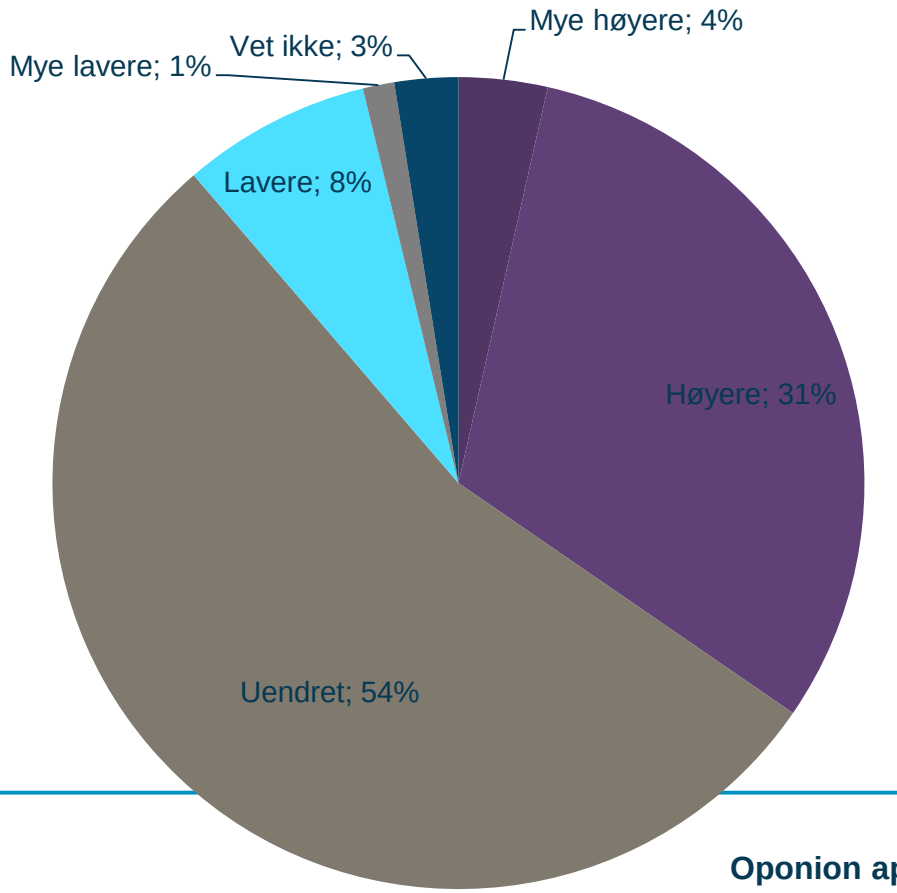
Målrettede angrep – Høy grad av suksess
Hvem er målet?



EVRY

35 prosent mener risikoen er blitt høyere

Opplever du risikoen for IT-innbrudd, datavirus og lignende i din virksomhet som endret det siste året? (n=200)

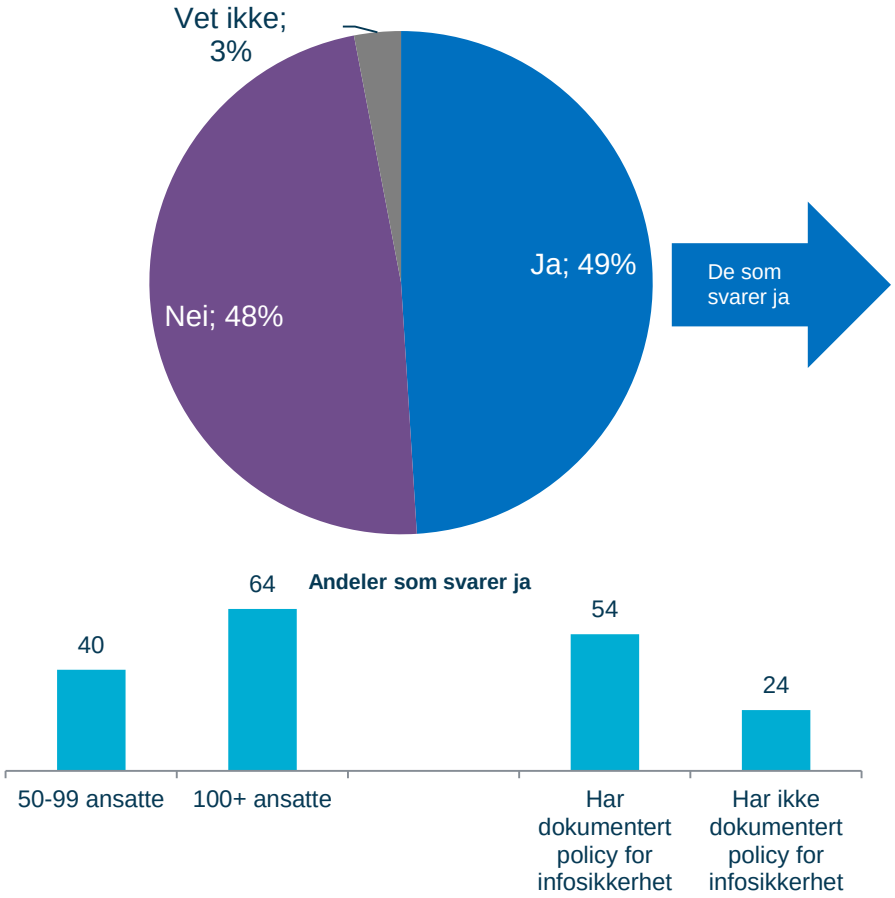


Nå vet altså Bjørn Ivroth at risikoen er høy!

Hva gjør Bjørn Ivroth?

Ledersikkerhet - Halvparten stiller ikke særskilte sikkerhetskrav

Stiller din virksomhet særskilte IT-sikkerhetskrav til kjernegruppen av ledere, IT-administratorer, primærinnsidere og styremedlemmer? (n=200)

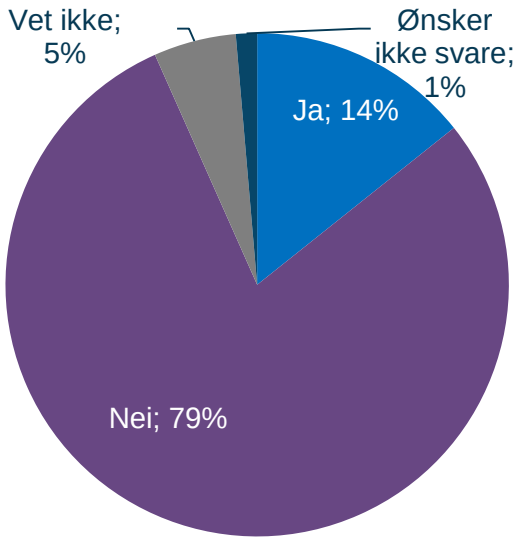


Hvilke særskilte IT-sikkerhetstiltak stilles til denne gruppen? (n=98)

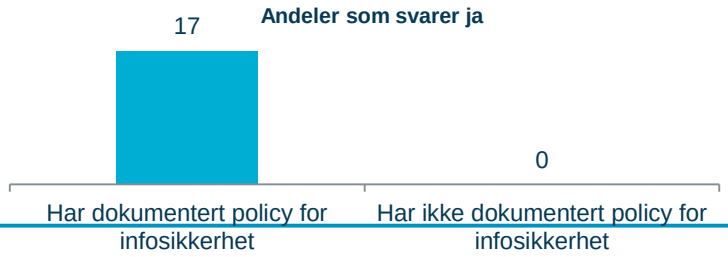
Oponion april 2015 for EVRY

8 av 10 har ikke praksis for å kontrollere for avlytting eller lekkasjer

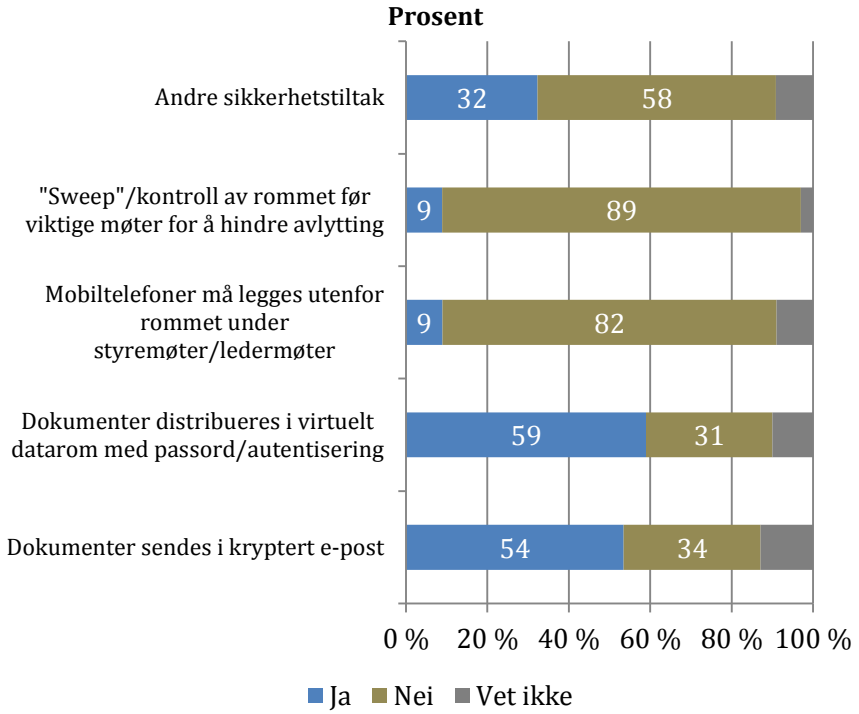
Har virksomheten policyer og/eller praksis for å kontrollere styrerom, møterom og styrepapirer mot avlytting eller lekkasjer? (n=200)



De som svarer ja



Gjøres noe av følgende for å forhindre at dokumenter kommer på avveie, samt hindre avlytting og lekkasje fra møterom for styre og toppledelse? (n=29)

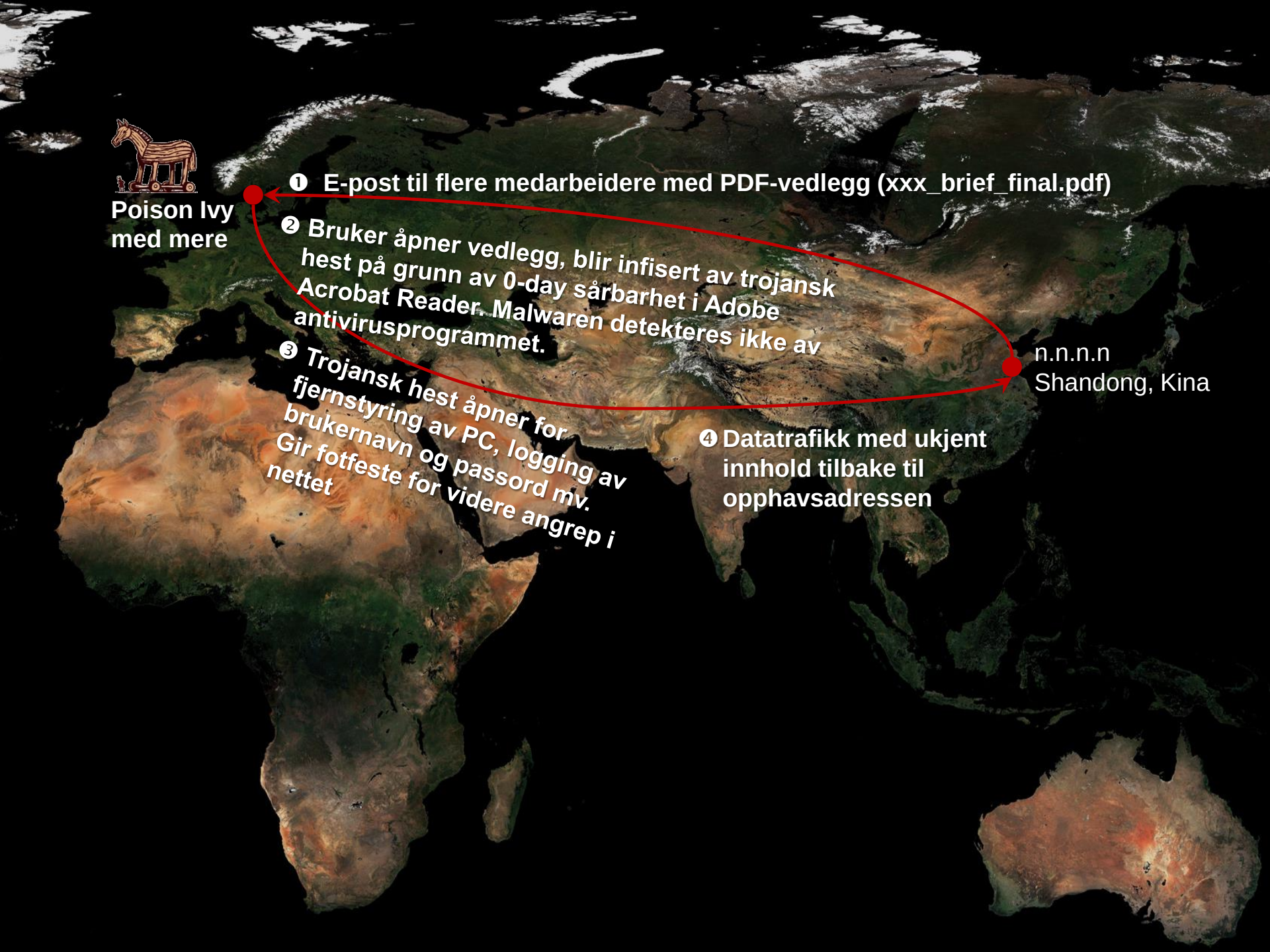


Sikkerhet i EVRY

- God forankring – høy fokus
- Koordinert sikkerhetsarbeid gjennom vårt Security Management Board
- Sikkerhetshendelser håndteres gjennom vårt Incident Response Team (IRT) og vårt EVRY Security Operation Center (ESOC)
- Sjekk av viktige møterom
- Risikovurdering av sikkerheten til våre toppledere
- Ekstra sikring av VIP utstyr

APT : Rettet angrep (kunde)

- **Rettet angrep mot en av våre kunder**
- Åpenbart designet for å stjele informasjon
  - Lignende angrep mot andre aktører i samme bransje, men unikt utformet for det aktuelle miljøet (subject og tittel på infisert PDF)
- **Initielt angrep via e-post til håndfull ansatte**
  - Infisert PDF utnyttet sårbarhet i Adobe Reader
    - Kjent i en måned før patch var tilgjengelig
  - Lastet ned «cocktail» av verktøy, inkl. **Poison Ivy**
  - Initielt ingen deteksjon av antimalwareverktøy
  - Estimert fotfeste på 10% av porteføljen
  - Tidspunkt (jul- og nyttår) for angrepet er neppe tilfeldig valgt


Poison Ivy
med mere
❶ E-post til flere medarbeidere med PDF-vedlegg (xxx_brief_final.pdf)
❷ Bruker åpner vedlegg, blir infisert av trojansk hest på grunn av 0-day sårbarhet i Adobe Acrobat Reader. Malwaren detekteres ikke av antivirusprogrammet.
❸ Trojansk hest åpner for fjernstyring av PC, logging av brukernavn og passord mv. Gir fotfeste for videre angrep i nettet
❹ Datatrafikk med ukjent innhold tilbake til opphavsadressen
n.n.n.n
Shandong, Kina

Sikkerhetshendelser får konsekvenser

#2	butikkkjede i USA
2000	butikker
#36	på Fortune 500
$73	milliarder i omsetning
361.000	ansatte (0.08% i infosec)

Target: Konsekvenser

70 millioner kunder berørt

40 millioner kort eksponert

Kostnad på >$148 millioner

Bytte av CEO, CIO

Tap av Omdømme

We're doomed!

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

EVRY

Forsvarerens dilemma

Partnere Brukere Apps Løsninger Sårbarheter Mål

Angripers mulighetsrom

Eneste mulige konklusjon:
"assume the breach"
og designe alt derfra

Partnere Brukere Apps Løsninger Sårbarheter Mål

“For lite” ihht. trusselbildet

Store, generiske rammeverk

(aka paralysis by analysis)

Minimum Viable Security

Security is not about doing a lot of smart things. It’s about not doing a few dumb ones. – Marcus J. Ranum

EVRY

EVRY Trusselmodellering

1. **Hva** ønsker vi å beskytte?
2. Hva ønsker vi å **beskytte det mot**?
3. **Hvordan** kan det angripes?
4. Hva er **sannsynligheten** for at det skjer?
5. Hva er **konsekvensene** om vi feiler?
6. Hvor mye er vi **beredt til å gjøre**?


EVRY
We bring information to life