Informasjonssikkerhet på jernbanen

- Sett fra et jernbaneforetak

Sjt konferansen 2022

Andreas Lumbe Aas
Direktør Sikkerhet og kvalitet, Vy tog

Kort om Vy

- Vygruppen - et av Nordens største transportkonsern
  - Norge og Sverige
- Fire virksomhetsområder:
  - Tog
  - Gods (tog)
  - Buss
  - Kundeopplevelse og innovasjon

Agenda

1. **Informasjonssikkerhetspolitikk**
2. **Verdier – Trusler – Sårbarheter**
3. **Sikkerhetskultur**
4. **Konsernstruktur – Mor / datter**

Dere skal få vite litt om hvordan vi jobber med informasjonssikkerhet i Vy

Informasjonssikkerhetspolitikk (utdrag)

Arbeidet med informasjonssikkerhet skal sikre at Vygruppens informasjon, herunder

- Personopplysninger (GDPR)
- Virksomhetskritisk informasjon (inkl togdrift)
- Skjermet informasjon (Sikringsforskriften)

Konfidensialitet
Integritet
Tilgjengelighet

er ivaretatt og beskyttet i henhold til den **verdi** den har for virksomhetene og de **lovkrav** som gjelder.

Verdier

Liv og helse

Passasjerer
Ansatte
3. person

Materiell & Miljø

Kjøretøy
Utstyr, Bygninger
Miljø, klima, natur

Transportfunksjon

Opprettholde rutetilbudet
Omdømme
Økonomi

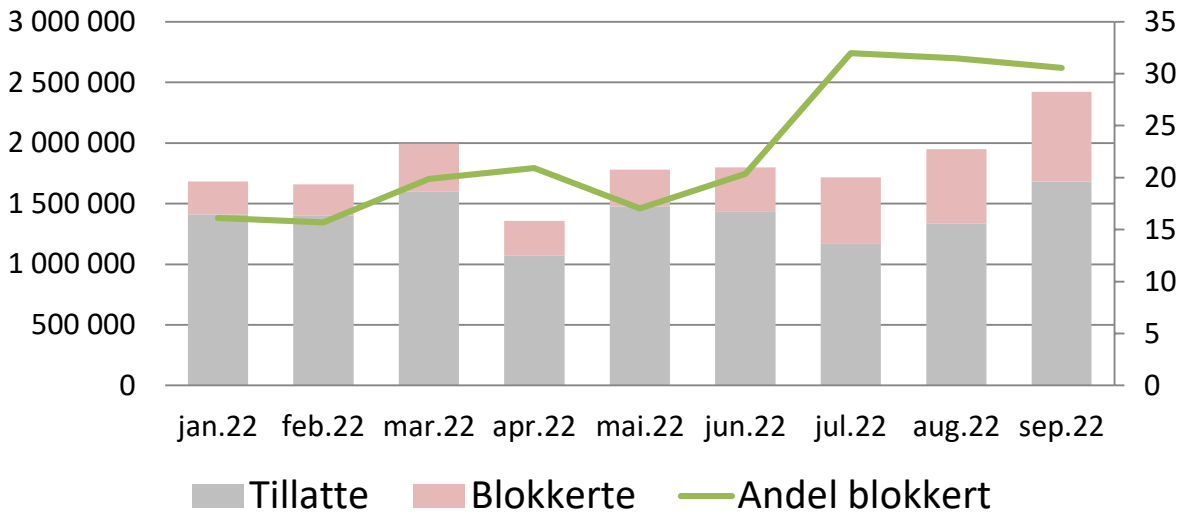
IT systemer og informasjon

Driftssystemer
Kundeinformasjon
Ansattinformasjon

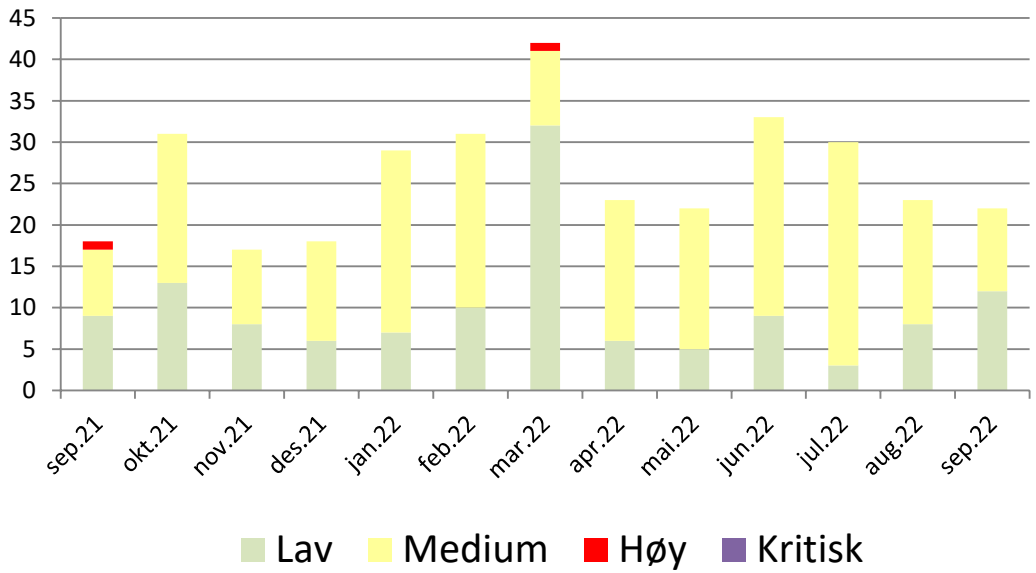
Trusler – eksempel med spam

Verdier
Trusler
Sårbarheter

E-poster



Kritikalitet i vurderte angrep



Trusselen er kontinuerlig til stede og håndteres av både oss og en sammensatt leverandørkjede

F eks:

- Microsoft stopper mye spam
- Telecom (Telenor, Telia etc) stopper mye tjenestenekt/DDoS
- NSM VDI - Varslingssystem for digital infrastruktur

Vi vurderer hvor alvorlige truslene er.

Flest i de minst alvorlige kategoriene, tilsvarende som for Uønskede hendelser.

Sårbarheter

Eksempler fra NSM - Nasjonalt digitalt risikobilde 2022

Gamle systembrukere

Det kan være mange grunner til at systembrukere er inaktive, som at folk slutter, at systemer ikke brukes lenger, at leverandører byttes ut. Ofte henger disse brukerne igjen i systemet, og ofte har de passord som enkelt kan knekkes.

Anbefalt tiltak: Kontoer som ikke benyttes, bør deaktiveres (GP-IKT 2.6.2 b)).

Dårlige passord

Mange brukere av systemet velger dårlige passord som det er lett for NSM å gjette/knekke. En trusselaktør trenger kun å knekke ett av hundre- eller tusenvis av passord for å få tilgang, avhengig av virksomhetens størrelse.

Anbefalt tiltak: Bruk et sentralt verktøy til å kontrollere passordkvaliteten opp mot virksomhetens sikkerhetskrav (GP-IKT 2.6.3 e)). Bruk multi-faktor autentisering, om mulig (2.6.7 e)).

Eksempel: Trenitalia ble rammet av ransomware-angrep i mars 2022. 5-10 mill USD
Påvirket billettsystemer, kundeinformasjon og togpersonalets sine tablets.

De klarte å opprettholde trafikken!

Leverandører og leverandørstyring

Krav til informasjonssikkerhet i kontrakter og følg opp.

Perimeterbasert (brannmur) → Identitetsbasert (sky)

Hvilke tilganger har leverandørene hos deg?

Sikkerhetskultur

Innmeldinger - informasjonssikkerhet

Er vi gode på det?
Når skal du melde?
Hvor skal du melde?
Tør du melde fra?

Beredskap

Øvelser! Øv også strategisk og for kontinuitet
Varsling – når IT-systemene er nede

Kulturbygging i beredskapen. UH → IT

Sikring

Grunnsikring – God praksis, sentralstyrt, dekker alle
Toppsikring – Verdier der skade/tap er alvorlig

Aktsomhet - bygge det inn i sikkerhetsstyringen og sikkerhetskulturen

Barrierer - MTO

Menneske
Teknologi
Organisasjon

Konsernstruktur – Mor / datter

Informasjon skal være ivaretatt og beskyttet i henhold til **verdien** den har og de **lovkrav** som gjelder.

Og husk sikkerhetskulturen!