volue

En digital hverdag i vannbransjen – er sikkerheten på plass?

Jon Røstum, sjefstrateg Volue Infrastructure

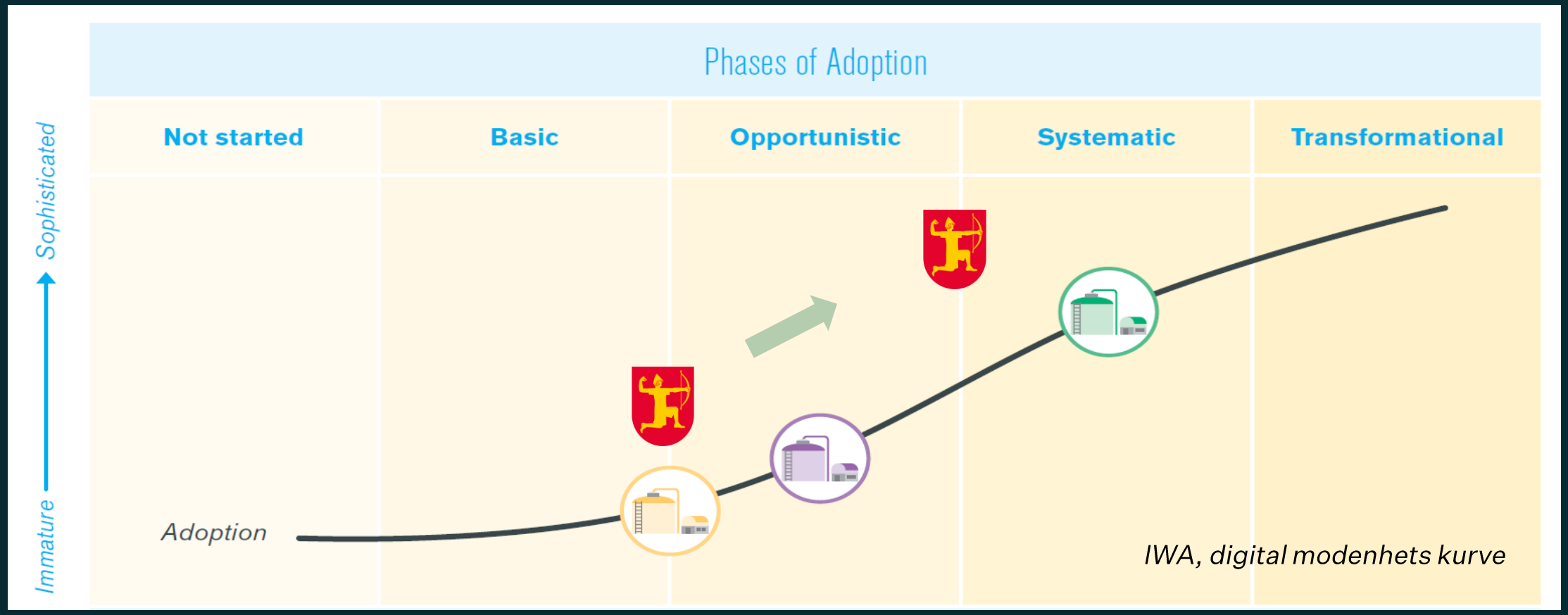
volue

Hvem av dere er det som jobber med informasjonssikkerhet til daglig?

Svar i SLIDO


volue

Vannbransjen digitaliseres



..men vi må tenke på informasjonssikkerhet! Må unngå at dagens nye løsninger blir fremtidens sårbarheter!

NRK – hot from the press

Ukraina utsatt for massivt dataangrep

nrk TV nrk RADIO nrk

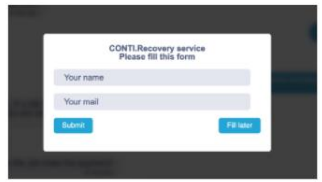
Dataangrep og hacking

Frykter personopplysninger er på avveie: 18.000 kan være rammet

Dataangrepet mot Nordland fylkeskommune kan ha rammet tusenvis av skoleelever og ansatte. Både Datatilsynet og politiet er varslet.

Hør svindlerne i aksjon: Ble svindlet for 600 000 kroner

Så proft gjennomført at selv ansatte hos Telenor kunne latt seg lure. Nå etterforskes saken hos politiet.



Dette møter deg når hackerne har fått tak i din personlige informasjon

Ny rapport peiker på svakaste punkt: – I verste fall så sit me der utan straum

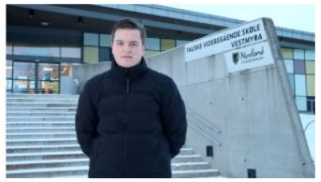
Både NVE og bransjen bør ta grep for å sikra kraftnettet best mogleg mot dataangrep. Det er konklusjonen i ein ny rapport.

Amedia-hackingen: Personopplysninger kan være på avveie

Konsernet ber abonnenter være ekstra oppmerksom på mistenkelige tekstmeldinger, telefonhenvendelser og e-poster.

Trente på dataangrep – måneder senere ble de hacket

I sommer øvde Nortura på digitale trusler. Det kan ha reddet selskapet da de ble utsatt for hacking rett før jul.

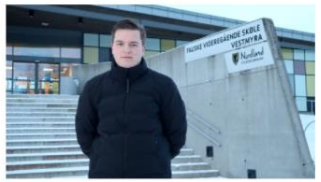


Elever må finne fram penn og papir etter dataangrep: – Synes synd på læreren

Bønder hardt rammet – Nortura avlyser all henting av dyr nyttårshelgen

Hacking

Mange av hackerne, som angriper bedrifter, har det som en helt vanlig dagjobb. Eksperter mener det er umulig å helgardere seg mot slike dataangrep.



Mats og 8.000 elever står uten datatilgang rett før skolestart

Dataangrep har slått ut en rekke aktører over hele landet i jula. – Det er kontinuerlig noen som prøver, og noen vil lykkes, sier IT-ekspert.

Amedia på pressekonferanse: Vil ikke kunne gi ut alle papiravisene i morgen

Tror rundt 20

+ Vis flere

Kommunens 16 krisescenarioer: Disse katastrofene kan ramme Oslo

En av dem er mer sannsynlig enn en pandemi.

Østre Toten – januar 2021

NRK Nyheter Sport Kultur Humor Distrikt Mer

Innlandet Tips oss Langlesing Radio TV

Varsel sendt: Østre Toten kommune får fire millioner i bot etter dataangrepet

Aldri før har Datatilsynet gitt ut så store bøter til en kommune.

Marte Iren Noreng Trøen
Journalist
Ragnhild Moen Holø
Journalist
Mette Vollan
Journalist

Publisert i går kl. 14:10
Oppdatert i går kl. 15:39

KUNNE VÆRT VERRE: Ordfører i Østre Toten, Bror Helgestad, sier de tar bota til etterretning. – Vi frykta et enda høyere beløp, sier han.
FOTO: LARS ERIK SKREFSRUD / NRK

- Alt av data kryptert (løsepenge virus)
- Penn & papir
- Løsninger i sky ikke berørt!
- Granskningsrapport bør leses, Husk: «NSM sine grunnprinsipper»

Drammen kommune februar 2021

HACKERANGREP MOT DRAMMEN KOMMUNE

Politiet etterforsker hackerangrep mot vann- og avløp i Drammen kommune

Ukjente gjerningsmenn skal ha forsøkt et hackerangrep mot deler av infrastrukturen for vann og avløp i Drammen kommune. (Foto: By Peulle - Own work, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=82256354)

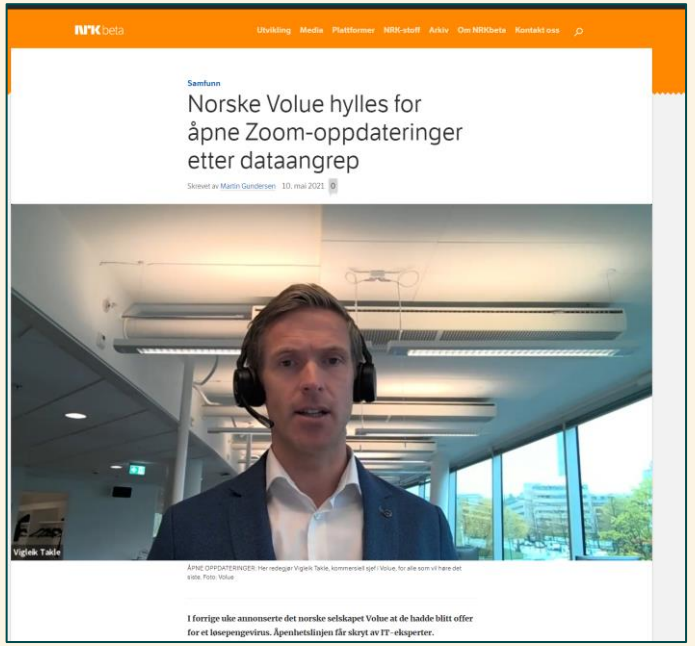
MARIUS B. JØRGENRUD SIKKERHET 22. FEB. 2021 - 11:24

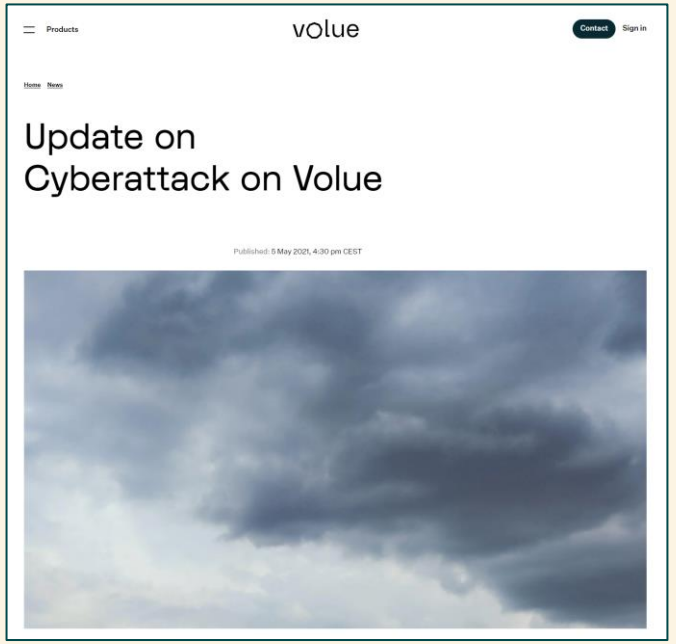
- Hacking av SCADA systemet
- Alle vann- og avløpssystemer fungerte som normalt, ingen av kommunens innbyggere ble berørt av situasjonen og ingen personopplysninger er på avveie.
- Politi etterforskning

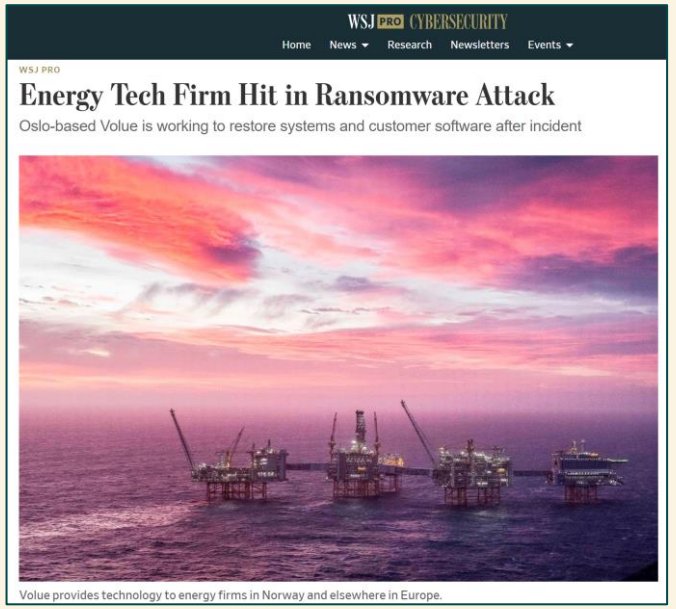
volue

Volue mai 2021

- Ryuk løsepengevirus
- Ulike løsninger påvirket
- Tett dialog og samarbeid med nasjonale sikkerhetsaktører (Datatilsynet, KraftCert)
- Daglige åpne webinar med mulighet for spørsmål og svar
- Pressemeldinger, media (NRK, Adressa, WSJ)
- Betalte ikke løsepenger

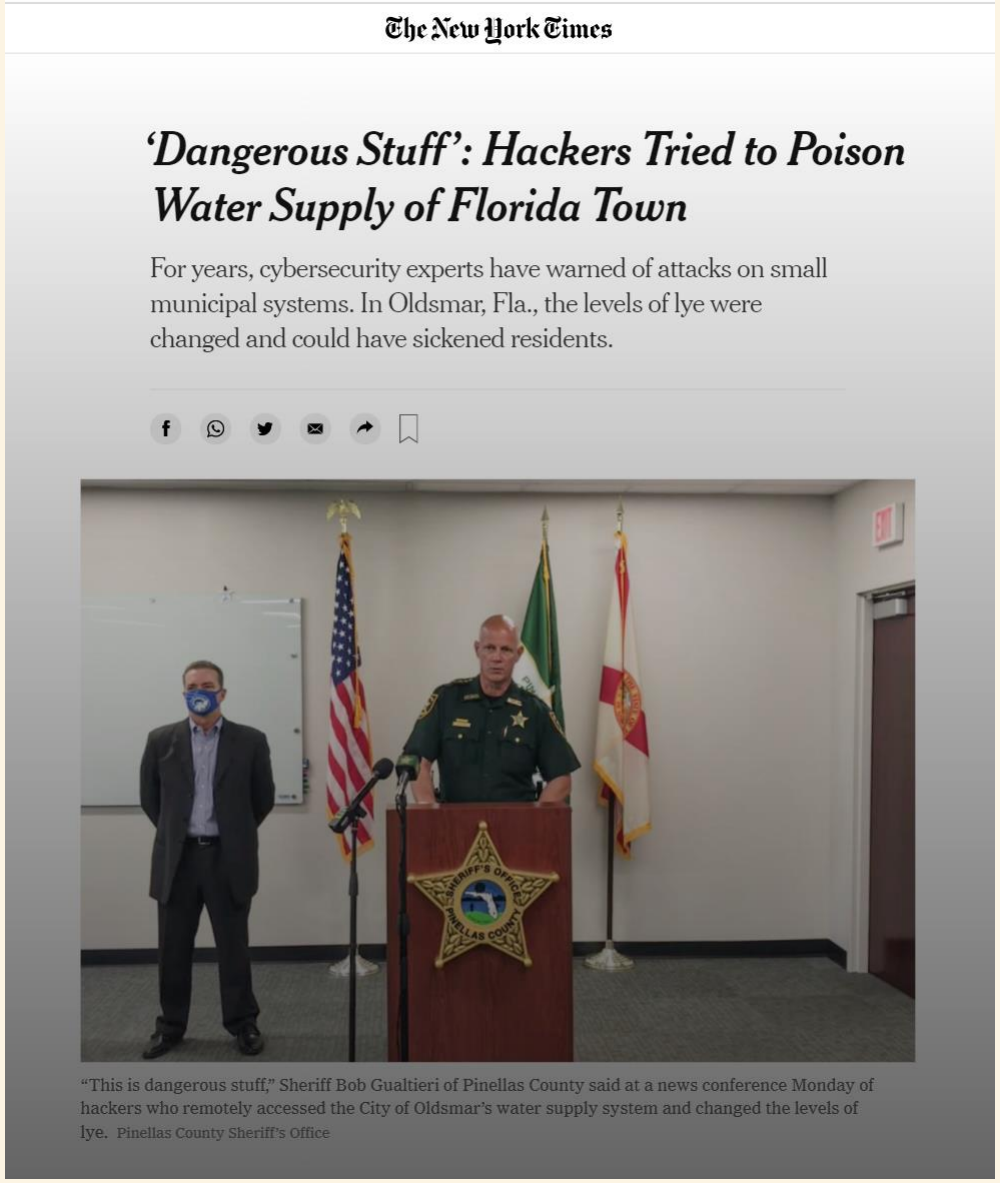






volue

5.Februar 2021 Florida



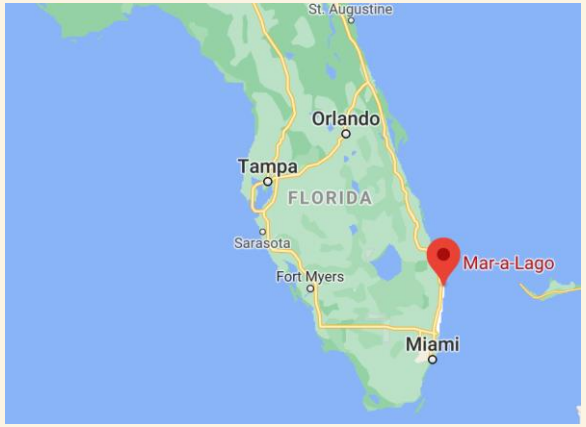
The New York Times

'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town

For years, cybersecurity experts have warned of attacks on small municipal systems. In Oldsmar, Fla., the levels of lye were changed and could have sickened residents.

"This is dangerous stuff," Sheriff Bob Gualtieri of Pinellas County said at a news conference Monday of hackers who remotely accessed the City of Oldsmar's water supply system and changed the levels of lye. Pinellas County Sheriff's Office

- Manipulering av driftskontrollsystemet for dosering av NaOH (lut)
- Operatøren så musen bevege seg dosen ble endret fra 100 til 11000 ppm
- Inngang via TeamViewer
- Felles bruk av svakt passord



Trump Suggests Injecting Disinfectant as Potential Coronavirus Treatment

By Matt Stieb

volue

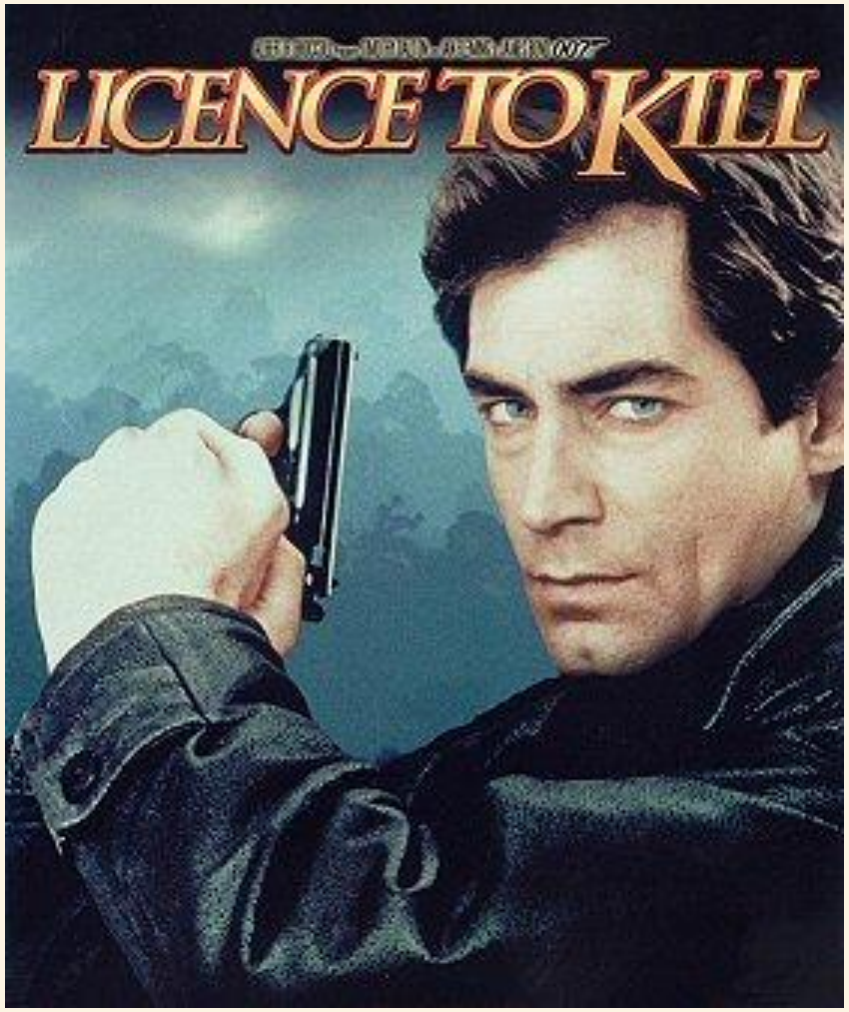
HAR DERE HØRT HISTORIEN OM VESTLENDINGEN SOM BLE OPPRINGT AV ØSTLENDINGEN?

Vannverkene skal tenke på alle farer som kan oppstå - også de digitale!

§ 6.*Farekartlegging og farehåndtering*
Vannverkseieren skal identifisere farene som må forebygges, fjernes eller reduseres til et akseptabelt nivå for å sikre levering av tilstrekkelige mengder helsemessig trygt drikkevann som er klart og uten fremtredende lukt, smak og farge.
Vannverkseieren skal sikre at tiltak som forebygger, fjerner eller reduserer farene til et akseptabelt nivå, identifiseres og gjennomføres.
Farekartlegging og farehåndtering skal danne grunnlag for beredskapsforberedelser som er beskrevet i § 11.
Vannverkseieren skal sikre at farekartleggingen og farehåndteringen er oppdatert.

§ 11.*Beredskap*
Vannverkseieren skal sikre at det gjennomføres nødvendige beredskapsforberedelser og utarbeides beredskapsplaner i samsvar med helseberedskapsloven og forskrift om krav til beredskapsplanlegging.
Vannverkseieren av vannforsyningssystemer med produsert vann per døgn på minst 10 m³ drikkevann, eller som forsyner en eller flere sårbare abonnenter, skal utarbeide en plan for beredskapsøvelser i samsvar med § 7 i forskrift om krav til beredskapsplanlegging. Vannverkseieren skal sikre at denne planen er oppdatert og følges.

Hvis det skulle mangle på motivasjonen – husk Matloven § 23! ☺



"Mattilsynet fører tilsyn og kan fatte nødvendige vedtak for gjennomføring av bestemmelsene gitt i eller i medhold av denne loven, herunder forby import, eksport og omsetning eller pålegge tilbaketrekning fra markedet, isolasjon, **avlivning**, destruksjon, kassasjon, båndlegging, merking eller særskilt behandling."


volue

Utviklingen de siste 5 år

07.04.2017

SLUTTRAPPORT

Statens tilsyn for planter, fisk, dyr og næringsmidler

Mattilsynet

Nasjonalt tilsynsprosjekt 2016

DRIKKEVANN:

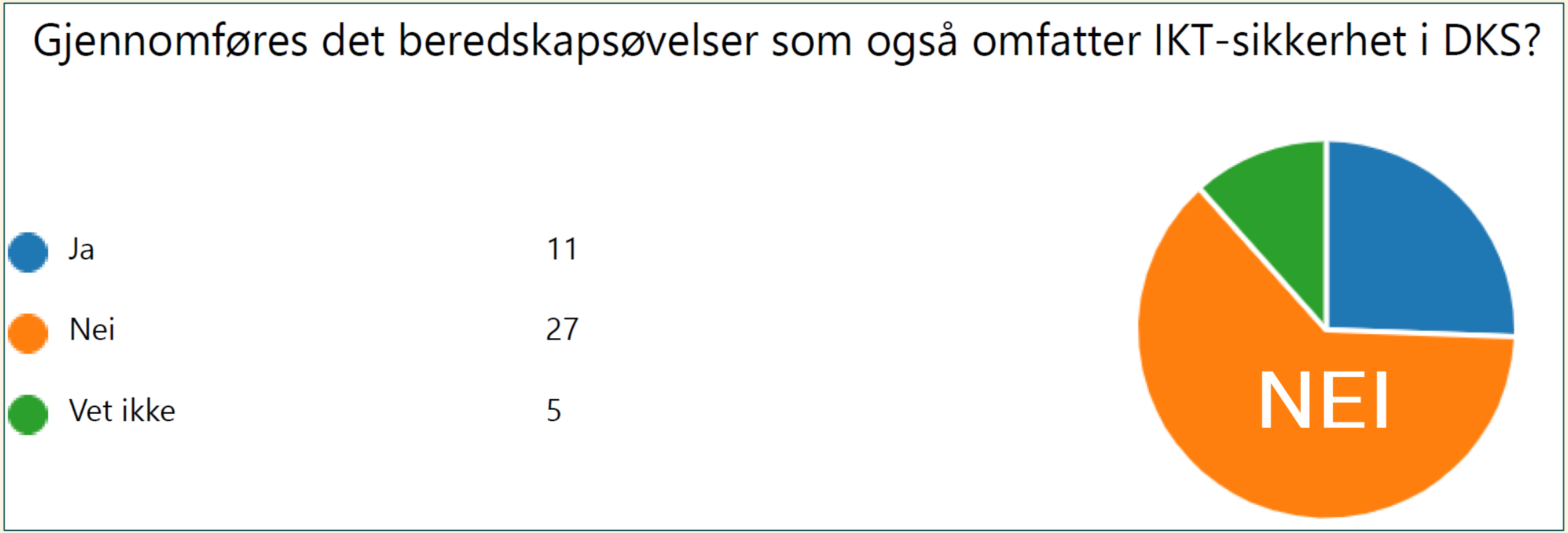
TILSYN MED VANNVERKENES BEREDSKAP

Vi skjønner ikke at vi ikke skjønner!

NSM, Norsk Vann Årskonferanse 1.september 2015

Skjønner vi mer nå?

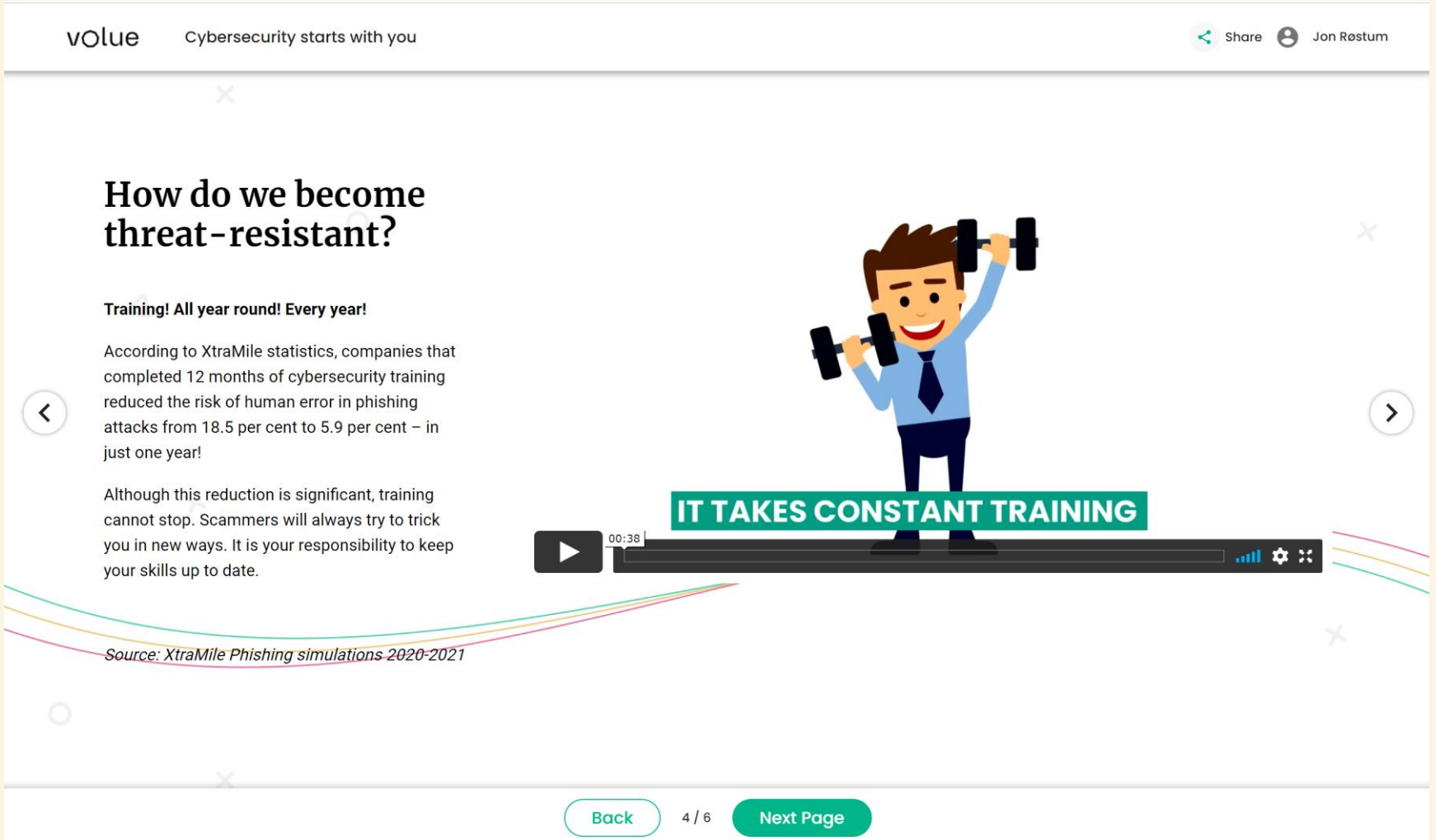
Beredskap og IKT-sikkerhet



Kilde: Spørreundersøkelse STOP-IT 2020, presentert på Norsk vann sin årskonferanse (Røstum, Jaatun, 2020)

Konklusjon: Vi skjønner mer og mer, men trusselbildet er i konstant bevegelse og vi blir aldri ferdig utlært!

volue



Relevante Norsk Vann rapporter

- Leses rapportene?
- Snart behov for oppdatering?

NSMs grunnprinsipper for IKT-sikkerhet

Norsk Vann 238/2018 ihht NSM sine anbefalinger

1. Identifisere og kartlegge	2. Beskytte og opprettholde		3. Oppdage	4. Håndtere og gjenopprette
1.1 Kartlegg styringsstrukturer, leveranser og understøttende systemer	2.1 Ivareta sikkerhet i anskaffelses- og utviklingsprosesser	2.2 Etabler en sikker IKT-arkitektur	3.1 Oppdag og fjern kjente sårbarheter og trusler	4.1 Forbered virksomheten på håndtering av hendelser
1.2 Kartlegg enheter og programvare	2.3 Ivareta en sikker konfigurasjon	2.4 Beskytt virksomhetens nettverk	3.2 Etabler sikkerhets-overvåkning	4.2 Vurder og klassifiser hendelser
1.3 Kartlegg brukere og behov for tilgang	2.5 Kontroller dataflyt	2.6 Ha kontroll på identiteter og tilganger	3.3 Analyser data fra sikkerhets-overvåkning	4.3 Kontroller og håndter hendelser
	2.7 Beskytt data i ro og i transitt	2.8 Beskytt e-post og nettleser	3.4 Gjennomfør inntrengings-tester	4.4 Evaluer og lær av hendelser
	2.9 Etabler evne til gjenoppretting av data	2.10 Integrer sikkerhet i prosess for endringshånd-tering		

«Virksomheter bør ta utgangspunkt i NSMs grunnprinsipper for IKT-sikkerhet. All erfaring tilsier at de er bedre rustet mot uønskede digitale hendelser hvis de følger rådene som blir gitt her»

NSMs fagdirektør, Roar Thon.

volue

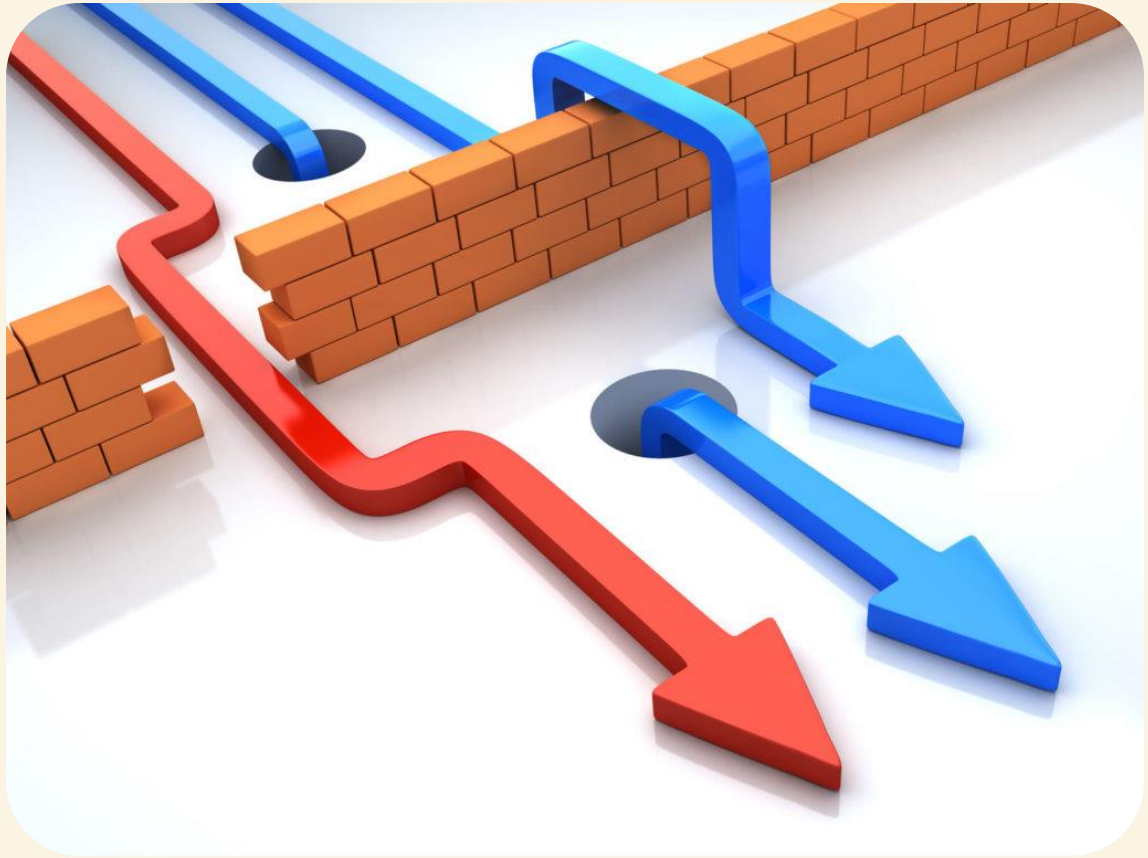
NSM: eget støtteark for å jobbe systematisk

NSMs grunnprinsipper for IKT-sikkerhet v2.0

Nr.	Kategori	GP. ID	Grunnprinsipp	Spesifisering	Tiltak ID	Tiltaksoverskrift	Tiltaksbeskrivelse
1	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer		1.1.1	Identifiser virksomhetens strategi og prioriterte mål	**Identifiser virksomhetens strategi og prioriterte mål**, samt regelverk, bransjenormer og avtaler som kan ha innvirkning på sikring av informasjonssystemer.
2	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer		1.1.2	Identifiser virksomhetens strukturer og prosesser for sikkerhetsstyring.	**Identifiser virksomhetens strukturer og prosesser for sikkerhetsstyring.** Dette inkluderer normalt **a)** policyer fra ledelsen, **b)** ledelsesstruktur med veldefinert ansvar og ansvarslinjer, **c)** prosesser for risikostyrin (se 1.1.3) **d)** fastsatte toleransegrenser for risiko (se 1.1.4), **e)** tilføring av tilstrekkelige ressurser og fagkompetanse for å støtte ledelsen i arbeidet. **f)** Etabler strukturer og prosesser for sikkerhetsstyring dersom dette mangler. Sørg for at det tilpasses virksomheten og er en inkludert del av virksomhetsstyringen. Se «Utdypende informasjon» for ytterligere informasjon.
3	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer		1.1.3	Identifiser virksomhetens prosesser for risikostyring knyttet til IKT	**Identifiser virksomhetens prosesser for risikostyring knyttet til IKT.** Dette inkluderer normalt **a)** verdivurdering, **b)** trusselvurdering, **c)** kartlegge eksisterende sikkerhetstiltak, **d)** risikoidentifisering, **e)** risikovurdering, **f)** risikorapportering, **g)** risikohåndtering, **h)** etablere eller justere sikkerhetstiltak for å redusere risiko **i)** verifisere at sikkerhetstiltakene fungerer etter hensikt. **j)** Etabler prosesser for risikostyring dersom dette mangler. Sørg for at prosessene tilpasses virksomheten og er en inkludert del av virksomhetsstyringen og sikkerhetsstyringen. Se «Utdypende informasjon» for ytterligere informasjon.
4	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer		1.1.4	Identifiser virksomhetens toleransegrenser for risiko knyttet til IKT	**Identifiser virksomhetens toleransegrenser for risiko knyttet til IKT.** Ledelsen må fastsette hvilke grenser fo risiko virksomheten aksepterer og hva som er uakseptabel risiko. Dette må kommuniseres på tvers i organisasjonen. Det er vanlig å fastsette risikogrenser basert på konsekvens for virksomheten ved tap av konfidensialitet, integritet og tilgjengelighet for informasjon og informasjonssystemer. Se 4.1.1, 4.1.2 og «Utdypende informasjon» for ytterligere informasjon.
5	Identifisere og kartlegge	1.1	Kartlegg styringsstrukturer, leveranser og understøttende systemer		1.1.5	Kartlegg virksomhetens leveranser, informasjonssystemer og understøttende IKT-funksjoner	**Kartlegg virksomhetens leveranser, informasjonssystemer og understøttende IKT-funksjoner**. Kartlegg **a)** IKT-systemer, data og tjenester, inkludert eierskap, **b)** kritiske forretningsroller og **c)** interne og eksterne IKT-avhengigheter. **d)** Gruppér i henhold til virksomhetens risikoaksept (1.1.4) og bruk resultatet som grunnlag for etablering av en sikker IKT-arkitektur, se prinsipp 2.2 - Etabler en sikker IKT-arkitektur.

00 INTRODUKSJON | 01 NSM GP-IKT 2.0 | 02 OM PRIORITERING AV TILTAK | 03 OM KOBLING MOT ISO 2700 ...

Gjennomføre inntrengingstester for å avdekke sårbarheter



«Hvit hatt» hacker:

- Er sikkerhetsbarrierene gode nok?
- Er det noen bakdører?
- Er det noen sårbarheter?

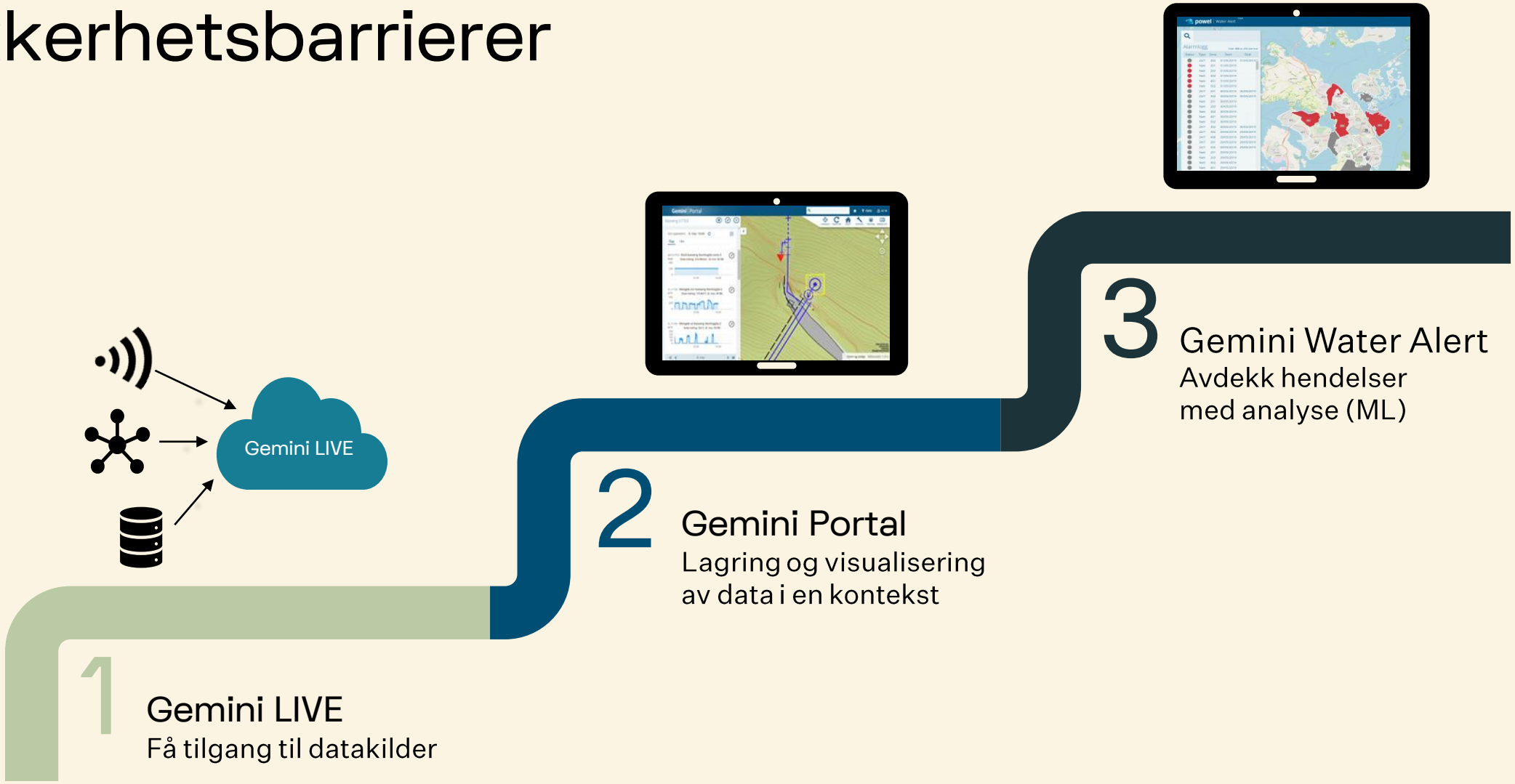
Tester:

Innside test (man er på innsiden av løsningen, hva kan man få til?)

Utside test (Kommer man gjennom fra utsiden via nett?)

volue

Eksempel fra Volue på sikkerhetsbarrierer



Informasjonssikkerhet og sanntidsdata

volue

SCADA system
DKS (Citect, ABB, Guard osv) etc

IoT Sensorer

Gemini LIVE

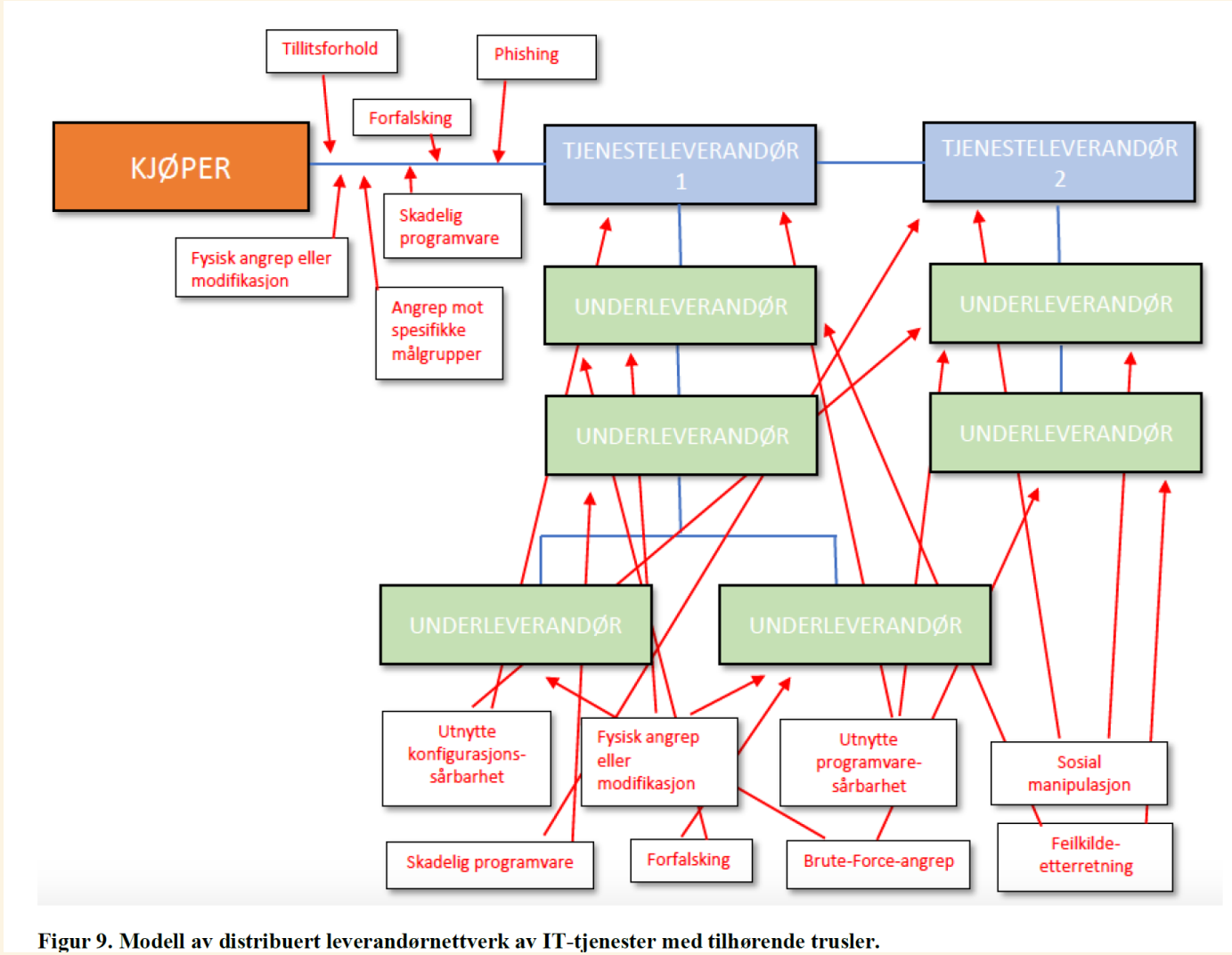
(unik kunde konto)

Cybersecurity:

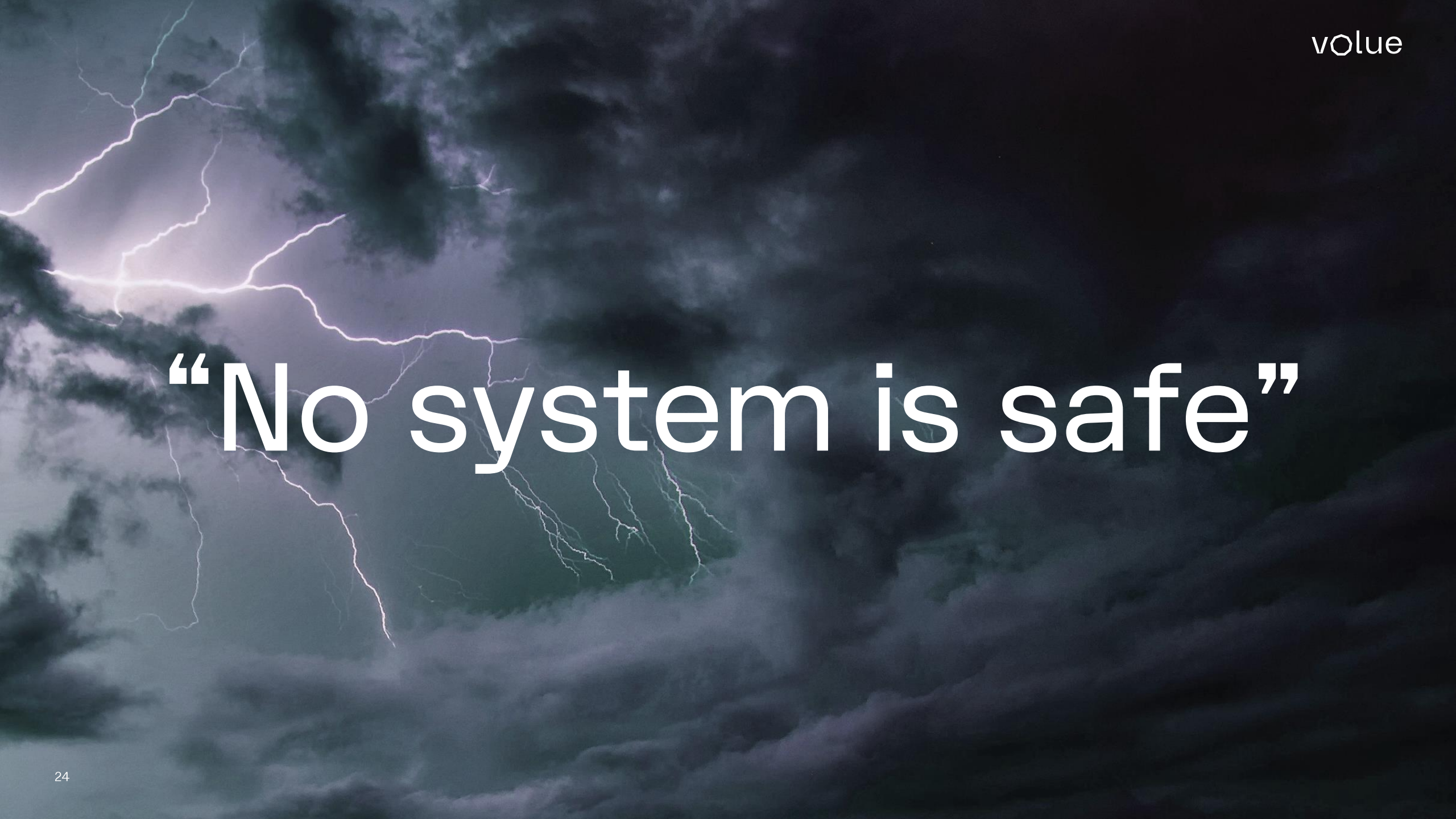
Moderne overføring av data (kryptert)	En veg - data skyves til Volue skyen	En dør- lettere å sikre (https), «mottakskontroll»	Skysikkerhet – »forsvar i dybden», flere barrierer	Kommunen selv bestemmer hva som skal vises av data	Bare innsyn- ikke styring

volue

Sårbarheter i leverandørkjeden



Figur 9. Modell av distribuert leverandørnettverk av IT-tjenester med tilhørende trusler.


volue
“No system is safe”