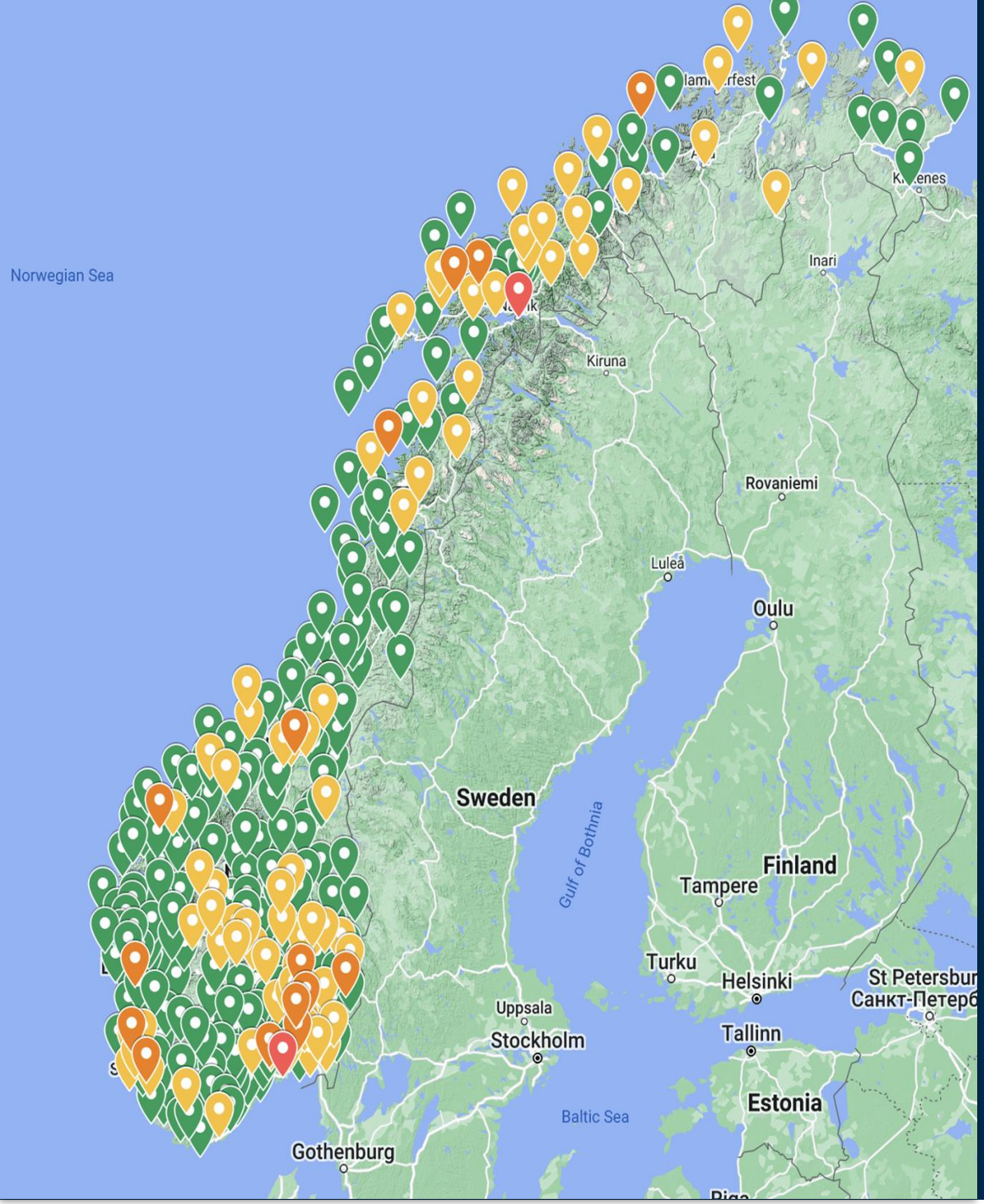


CYBER-X

DFØ/MPS,

Anskaffelseskonferansen 31. oktober 2023

André Årnes, Per Jakobsen

Direktoratet
for forvaltning og
økonomistyring

Markedsplassen for skytjenester skal bidra til styrking av sikkerhet i det offentlige Norge gjennom veiledning, digitale tjenester og skykontrakter.

Direktoratet
for forvaltning og
økonomistyring

Per Jakobsen

DFØ #mps, Seniorrådgiver Cybersikkerhet

Per Jakobsen er tidligere IT-leder med bakgrunn innen informasjonssikkerhet og personvern. Han har tidligere hatt ulike lederstillinger i IT-bransjen innen infrastruktur og web hosting, men har nå rollen som seniorrådgiver på markedsplassen for skytjenester. Der fokuserer han spesielt på cybersikkerhet i skytjenester. Per bidro til anskaffelsen av en public cloud skytjeneste i Narvik kommune som første offentlige virksomhet i Norge. Dette resulterte i en prinsippavgjørelse hos Datatilsynet om lovlig bruk av skytjenester
I offentlig sektor. Per har en sterk interesse for- og fokuserer på skykontrakter for verktøy og tjenester innen sikkerhet og personvern til bruk i offentlig forvaltning.

André Årnes

Partner Cyber Security @ WLC og Professor II @ NTNU

André Årnes er medeier og partner i White Label Consultancy og Professor II ved NTNU. Han har tidligere hatt rollen som SVP og Group Chief Security Officer (CISO/CSO) i Telenor Group (2015 – 2022), som CIO i Telenor Global Shared Services og som spesialetterforsker innen Digital Forensics og datakriminalitet ved Kripos / Økokrim. André har en sterk faglig interesse for sikkerhet, med fokus på sikkerhetsledelse og digital etterforskning. Han har redigert to akademiske lærebøker innen fletet. «Digital Forensics» (Wiley, 2018) og «Cyber Investigations (Wiley, 2022). Han har siden 2022 bistått DFØ og Markedsplassen for Skytjenester som strategisk sikkerhetsrådgiver.

White Label Consultancy

Direktoratet for forvaltning og økonomistyring

Om Markedsplassen for skytjenester (#mps)

- Markedsplassen er opprettet på bakgrunn av Nasjonal strategi for bruk av skytjenester
- Eies av Finansdepartementet. Styres av KDDs avdeling for IKT-politikk
- Tildelingsbrev fra Finansdepartementet
    - Veiledning, anskaffelse, informasjonssikkerhet og oversikt over markedet
- Fullmakt til å inngå statlige fellesavtaler ved kgl. res. av 3. september 2021

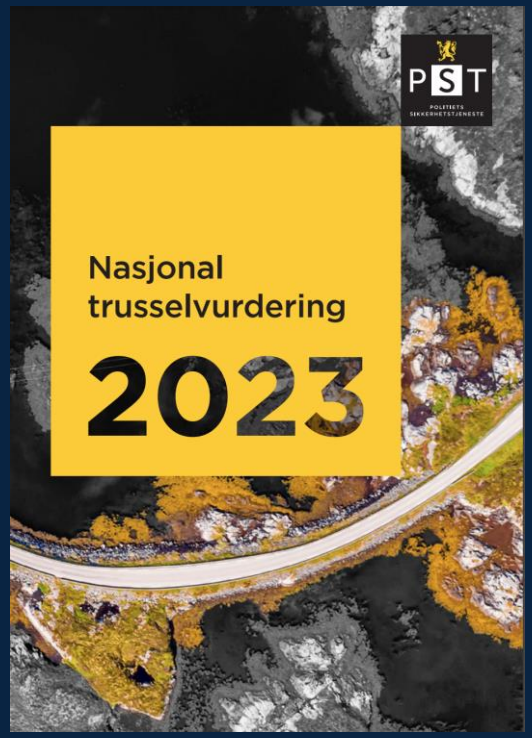
#mps | Markedsplassen for skytjenester – hva gjør vi?

Cybersikkerhet	Skykontrakter	Veiledninger, artikler
Portefølje av sikkerhetsprodukter og tjenester	Utarbeider skyavtaler til bruk i offentlig sektor	Nettsted, markedsplassen.anskaffelser.no
Utprøvinger med formål å etablere skykontrakter innen cybersikkerhet	CIPS (Cloud Infrastructure and platform services)	Artikler og informasjon innen anskaffelser og bruk av skytjenester

Direktoratet for forvaltning og økonomistyring

Norske myndigheter advarer om en rask økning av alvorlige cyberoperasjoner, økte og mer komplekse digitale sårbarhetsflater. Nettverksoperasjoner og etterretningsaktivitet fra Russland og Kina og bruk av verdikjedeangrep løftes frem som spesifikke trusler.

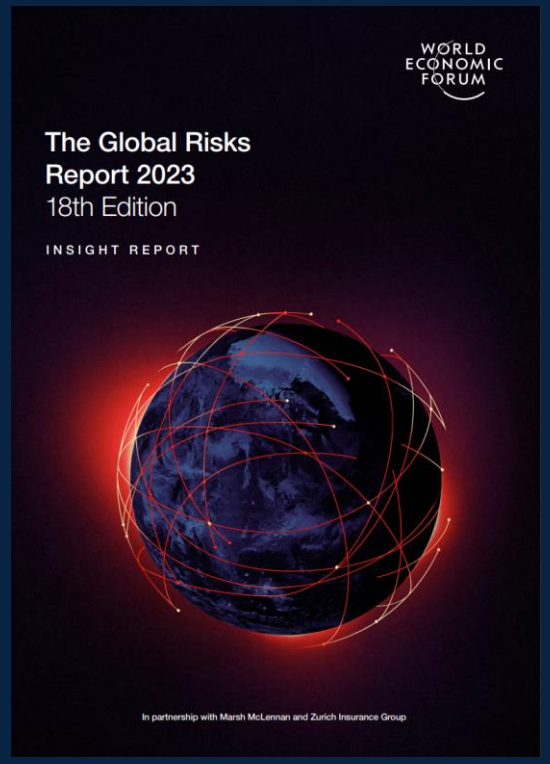
| Digital sårbarhetsflate utvikler seg | Lange og uoversiktlige leverandørkjeder | Tredobling av alvorlige cyberoperasjoner 2019 – 2021 | Kommersielt tilgjengelige brukerdata | Innsidevirksomhet | 5G og skytjenester | Kvantekappløpet | AI | (NSM 2023)



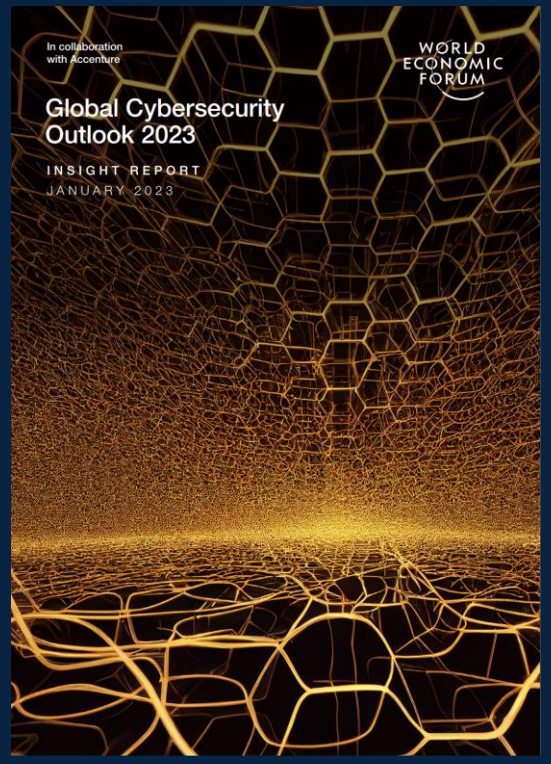
| Nettverksoperasjoner | etterretningsaktivitet | Avanserte digitale trusselaktører | Russland og Kina | Verdikjedeangrep | Operasjoner mot enkeltpersoner | (PST 2023)

| Mer enn 40 vellykkede destruktive nettverksoperasjoner fra Russland i Ukraina | Kina og cyberoperasjoner – myndigheter, forsvar, romforskning, helse, telekom og media | Kina og informasjonsdominans | (E 2023)

World Economic Forum løfter angrep mot kritisk infrastruktur, cyberkriminalitet og cyber-usikkerhet som globale risiko for de neste 10 årene, og toppledere forventer katastrofale cyber-hendelser i nær fremtid.



| Attacks on critical national infrastructure (CNI), widespread cybercrime, and cyber insecurity are highlighted as major risks throughout the next 10 years | Disruption of technology-enabled resources and services affecting society | (WEF Risk 2023)

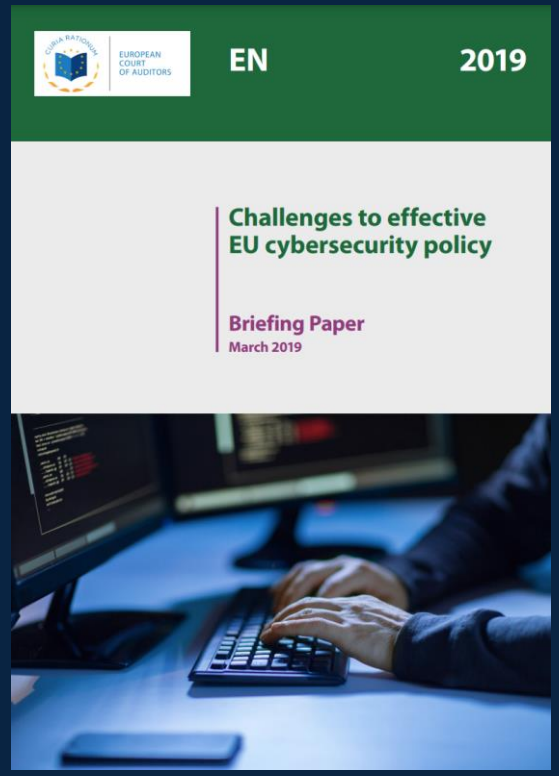


| Gap between business leaders and security leaders | Agreeing on how to best address cyber risk remains a challenge – business disruption and reputational damage | Cyberthreats have changed | Catastrophic cyber event is likely in the next two years | Dependency on supply chain | Balancing digital transformation and security | Regulations as an effective tool Cyber talent shortage | (WEF Cyber 2023)

Riksrevisjonens vurderinger av digital sikkerhet i Norge viser mangelfull oversikt, høyt sårbarhetsnivå og svak samordning. Dette er i tråd med ECA som peker på mangelfull motstandskraft mot digitale hendelser i EU.

| Svak samordning gjør arbeidet med digital sikkerhet krevende | Mangelfull informasjon om den nasjonale digitale tilstanden | Manglende oppfølging av nasjonal strategi | Mangelfull tilrettelegging for tverrsektoriell hendelseshåndtering | (Riksrevisjonen 3:7 2023)

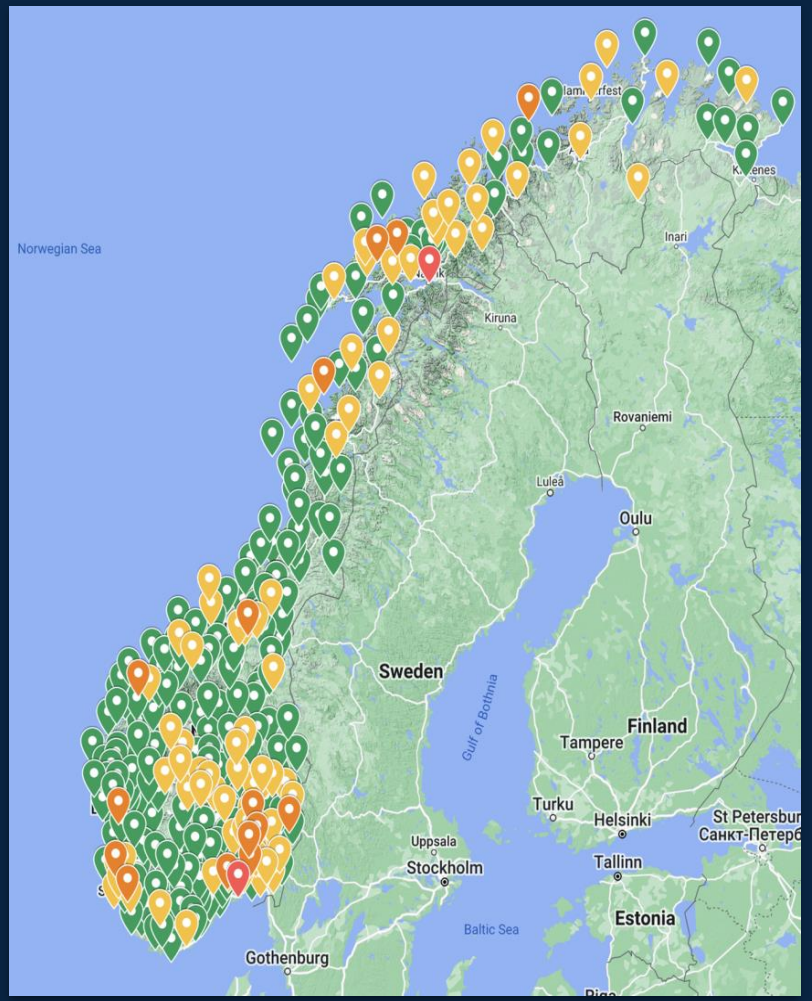
| Mangler i samvirket mellom kommando- og kontrollinformasjonssystemer | Sårbarheter I sikkerheten gir risiko for svekket operativ evne | Ikke greid å realisere effektive og sikre informasjonssystemer | (Riksrevisjonen 3:3 2023)

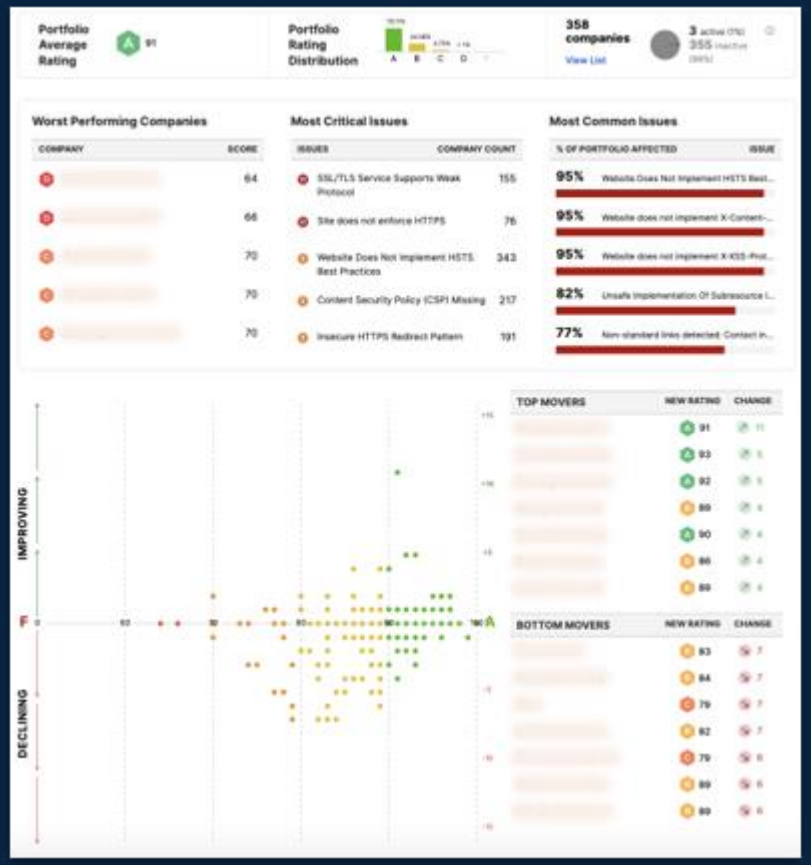


| Aligning investment levels with goals | Constraints in adequate resourcing | Weaknesses in governance | Skills and awareness | Information exchange and coordination | | Rapid detection and response | Protection of critical infrastructure and societal functions| Fragmentation – complex, multilayered landscape with many actors (ECA 2019)

| The number of attacks on EUIBAs is increasing sharply | Good practices not always implemented | Governance and strategy often lacking | Missing independent assurance | Level or preparedness inadequate | (ECA 2022)

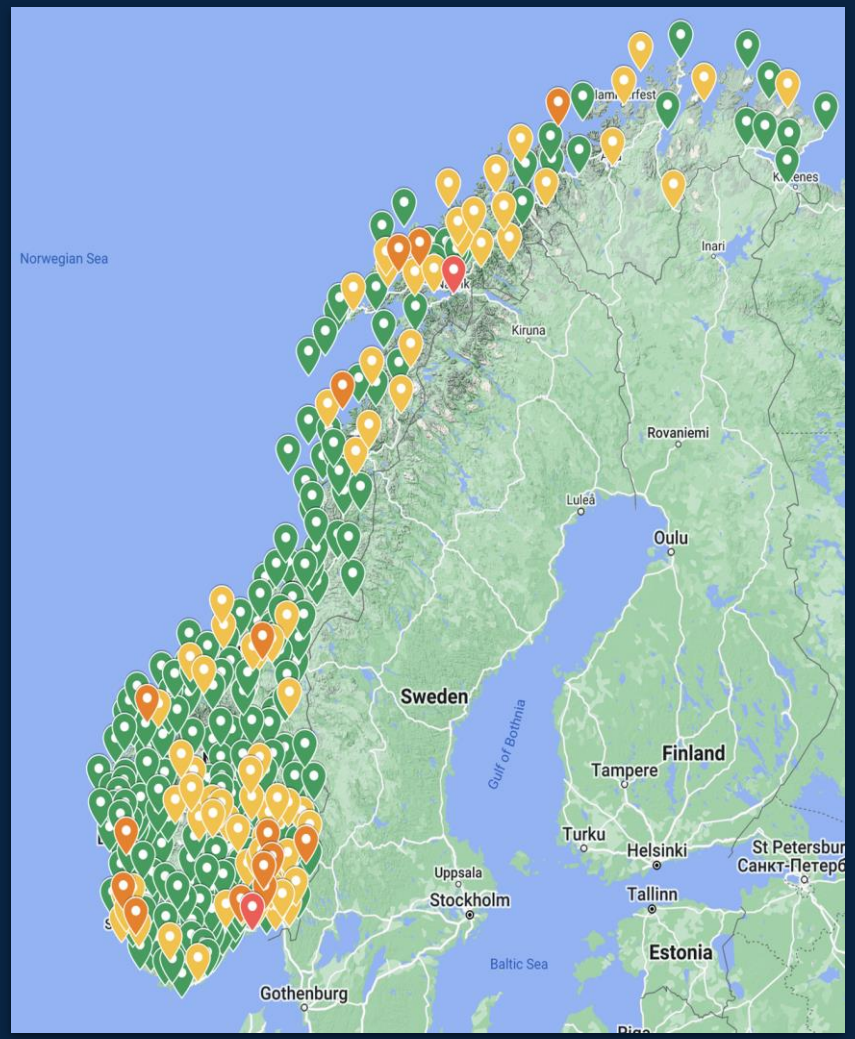
Et situasjonsbilde av sikkerhetsnivået i det offentlige Norge bekrefter et stort potensiale for å måle og forbedre sikkerhetshygienen på nasjonalt nivå.





Kilde: SecurityScorecard

Vi ser at en systematisk oppfølging basert på målbare indikatorer gir en positiv utvikling av sikkerhetsnivå. Manglende oppfølging fører gjerne til en negativ trend.



Kilde: SecurityScorecard

#mps | Cybersikkerhet - styrt eller tilrettelagt? MPS tar en tilretteleggingsrolle for skykontrakter og cybersikkerhetstjenester

Sikkerhetsledelse

- ✓ Nasjonal strategi og oppfølging av sikkerhet i det offentlige.
- ✓ Basert på premisser satt av og kontrollert av DigDir og NSM, med mandat å sikre en effektiv organisering av sikkerhetsarbeidet i det offentlige Norge.
- ✓ Basert på etablerte rammeverk, herunder ISO27001 og NIST Cyber Security Framework, samt krav fra NSM

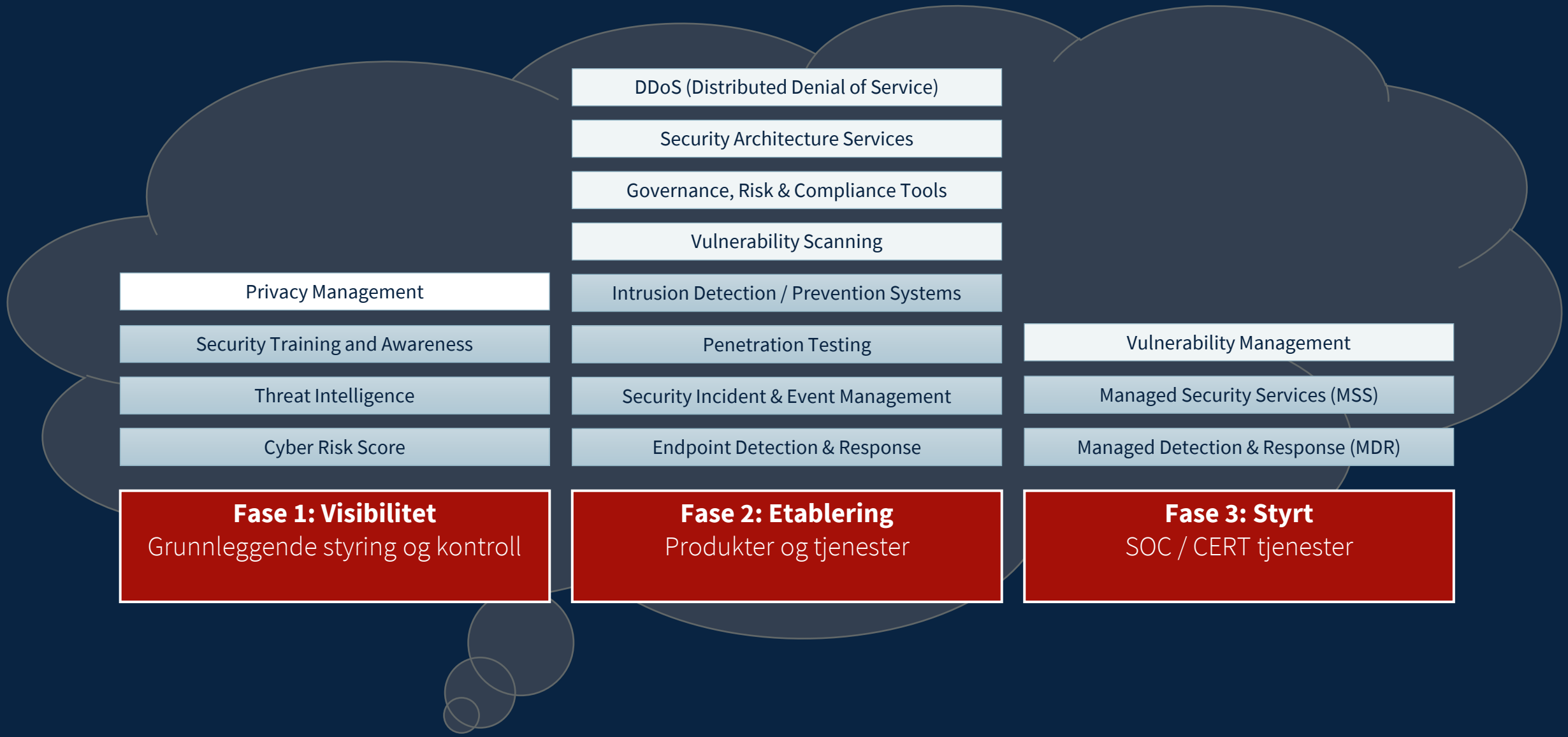
Kapasitetsbygging

- ✓ Referansearkitektur for forsvarbar sikkerhet (jf. "forsvarbar arkitektur", og "zero trust")
- ✓ Rammeavtaler med skyleverandører som sikrer et minimums sikkerhetsnivå for IKT-infrastruktur, og dermed vil bidra til sikkerhetsløft.
- ✓ Rammeavtaler med sikkerhetsleverandører som sikrer tilgang på basis- og avanserte sikkerhetsverktøy og tjenester.
- ✓ Nasjonalt konsept for Managed Security Services (SOC/CERT) med lokalt eierskap og sentral koordinering og oversikt

Strakstiltak

- ✓ **Etabler en totaloversikt over alle offentlige** enheter **og kommuner inkludert leverandørkjeden**
- ✓ **Oppfølging på tvers av departement basert på løpende rapportering og målbar fremdrift**
- ✓ **Etablering av basis sikkerhetstiltak iht ISO27001, NIST CSF og NSMs grunnprinsipper for IKT-sikkerhet 2.0**
- ✓ **Løfte statlige enheter, fylkeskommuner og kommuner med utdatert infrastruktur til forsvarbar arkitektur**

#mps | Portefølje av produkter og tjenester for offentlig sektor



#mps | Krav til portefølje av produkter og tjenester for offentlig sektor

- **Skybaserte**. Produkter og tjenester skal være skybaserte og må støtte anvendelse av skytjenester, men også støtte hybrid og on-site infrastruktur.
- **Automatisert**. Produkter og tjenester skal tilrettelegge for en høy grad av automatisering.
- **Nasjonal situasjonsforståelse**. Produkter og tjenester bør tilrettelegge for aggregert informasjon for sentrale funksjoner (f.eks. NSM og CERTer).
- **Flere leverandører**. Målbildet er, hvor relevant, å etablere avtaler med flere leverandører innenfor kategoriene og dermed tilrettelegge for fleksibilitet med hensyn på ulike modenhetsnivå.
- **Grunnleggende sikkerhetskrav**. Alle produkter og tjenester skal oppfylle sikkerhetskrav basert på NSM og NIST, ISO27001, samt lovpålagte krav og andre relevante standarder.

#mps | Rammeverk for sikker anskaffelse og bruk av skytjenester i offentlig sektor

Sikkerhet i skyen («security in the cloud»)	• Den største risikoen ligger i **feil bruk** av skytjenestene • Hvordan kan leverandørene hjelpe til? • Leverandørens sikkerhetsarkitektur, teknologi, verktøy og opplæring • Basert på beste praksis og etablerte referanserammeverk • Etterlevelse av lover og regler • Tilpasning til kundespesifikke krav gjennom opsjoner • Veiledning gjennom markedsplassen
Sikre skytjenester («security of the cloud»)	• Felles kontraktkrav og basiskrav for sikkerhet • Basert på anerkjente internasjonale standarder som ISO27001 og NIST CSF • Rammeverk for leverandøroppfølging og koordinering

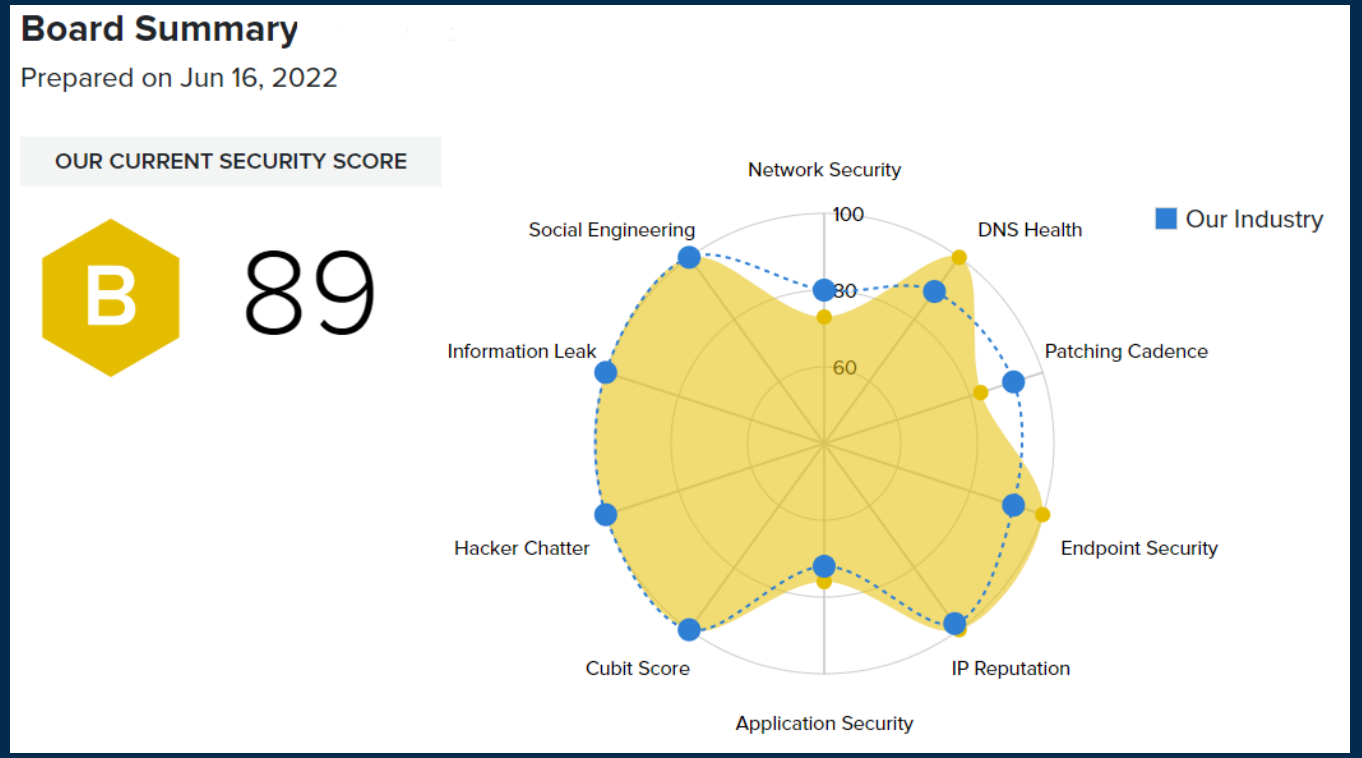
UTPRØVINGER FOR ANSKAFFELSER

PROSJEKT CYBERSIKKERHET

Direktoratet for forvaltning og økonomistyring

#mps | Hva er en Cyber Risk Score tjeneste?

Cyber Risk Score er en nettbasert tjeneste som gir en helhetlig vurdering av sikkerhetsnivået, sett fra internett og hjelper virksomheten med å prioritere tiltak for å beskytte seg mot potensielle trusler



Direktoratet for forvaltning og økonomistyring

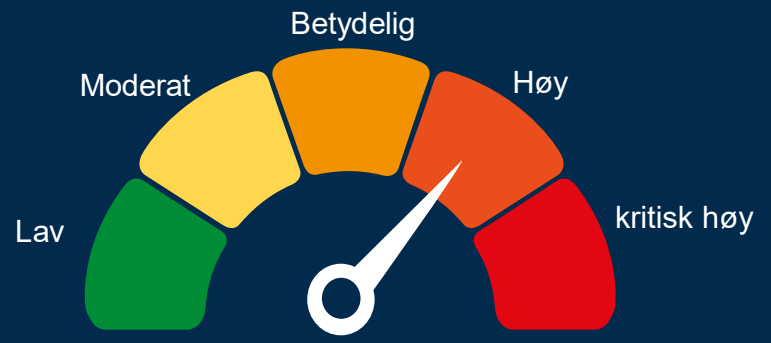
#mps | utprøving av en Cyber Risk Score tjeneste 2022

Formålet med utprøvingen - hvilken effekt kan bedre innsikt i egen sårbarhet på internett ha med hensyn på å treffe risikoreduserende tiltak.

Deltakelse: 26 statlige virksomheter og 4 kommuner

Hva er gjort?

- Informasjonsmøter med interessenter
- Webinar med KiNS
- Spørreundersøkelse
- Oppsummerende Workshops
- Gjennomgang - "Hva lærte vi?"



Direktoratet for forvaltning og økonomistyring

#mps | konklusjoner fra utprøvingen av en Cyber Risk Score tjeneste

- **Indikerer behov** for en cyber risk score tjeneste til virksomhet, IT- og sikkerhetsledelse.
- Kan benyttes som **styringsverktøy, operativt og for samhandling** i offentlig sektor innen cybersikkerhet

Utprøvingen bekrefter et stort potensiale for å måle og forbedre sikkerhetshygienen i det offentlige Norge.

- Må være **flere verktøy** i verktøykassa
- **Flere indikatorer** for sikkerhet kreves – kan **ikke være en hvilepute** for virksomhetsledelsen, men et mål på minimum sikkerhetshygiene på Internett
- **Relevant kompetanse** på IT- og sikkerhet kreves. MPS tilrettelegger for veiledning og samarbeid
- Behov for validering av **«digital footprint»** (IP-adresser og domenenavn) og sårbarbarheter
- Det er observert en **målbar positiv effekt** på risk score for de mest aktive deltakerne.

Direktoratet for forvaltning og økonomistyring

#mps | Fortsatt mulig for kommuner å delta på kommende avtale for Cyber Risk Score

Voldsom interesse for nytt skyprogram: – Kjipt å være flagget rødt når naboen er grønn, mener IT-sjef

Markedsplassen for skytjenester (MPS) er er i gang med å sjekke interessen for en ny skytjeneste som kartlegger cyberriskofaktorer i offentlig og statlig sektor. Styreleder i offentlig sikkerhetsforening mener programmet er et «must».

Torkjell Dahl er IT-sjef i Ringerike kommune. Her sammen med informasjonssikkerhetsansvarlig Axel Sjøberger. I tillegg til å være IT-sjef, er Dahl styreleder i sikkerhetsorganisasjonen KiNS, som har over 300 kommuner, fylkeskommuner og interkommunale selskaper som medlemmer. *Foto: Espen Ødegård, Ringerikes Blad*

Cyber Risk Score gir en helhetlig vurdering av sikkerhetsnivået sett fra internett og hjelper virksomheten med å prioritere tiltak for å beskytte seg mot potensielle trusler.

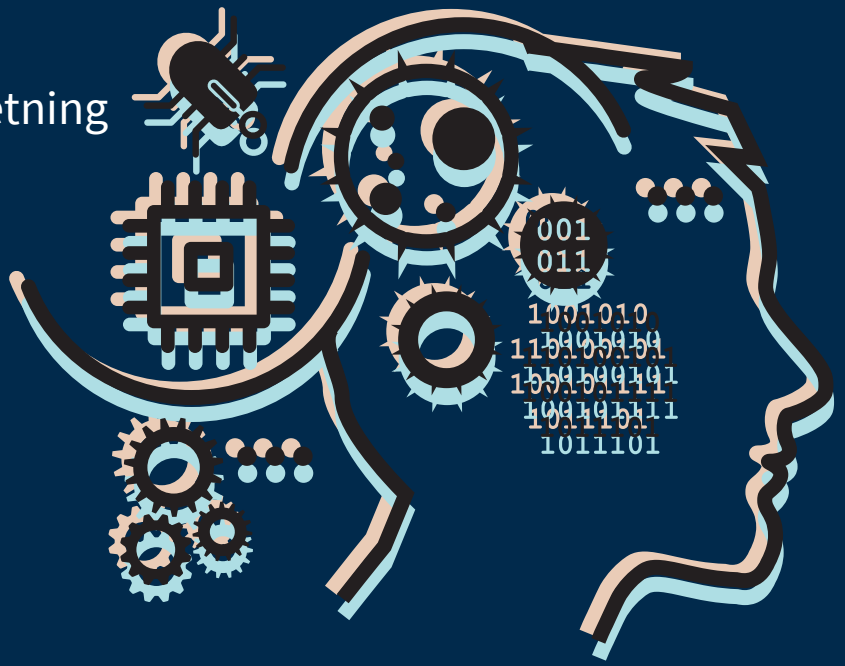
Mer informasjon finner du her:
Markedsplassen.anskaffelser.no

Direktoratet for forvaltning og økonomistyring

#mps | utprøving av en tjeneste for trusseletterretning 2023

Formål med utprøvingen

- Om **bedre kunnskap** i **trusselbildet** kan bidra til raskere og mer målrettet problemløsning innen Cybersikkerhet
- Vurdere behov for **økt utbredelse** av tjenester innen trusseletterretning gjennom fellesavtaler



Deltakelse

- Spesialisert tjeneste som **krever høy kompetanse** på brukersiden
- **Inviterte** utvalgte virksomheter til utprøving
- Inviterte til **drøftinger** med relevante interessenter innen stat og kommune

Hva er gjort?

- Utprøving fra mai til oktober er gjennomført
- Deltakende virksomheter **jobbet sammen** med leverandøren i perioden
- Utprøvingsaktiviteter med leverandør **avsluttet** 11. september

Direktoratet for forvaltning og økonomistyring

#mps| konklusjon trusseletterretning 2023

Deltakere med bakgrunn innen CISO/Sikkerhetsledelse, IT ledelse, sikkerhetsanalyse og trusselanalyse indikerer:

- **Virksomhetsledelsen** deltok aktivt

- Virksomhetsledelsen har i stor grad **forståelse** for trusselbildet og vilje og evne **til å agere** på risiki som avdekkes

- En tjeneste innen trusseletterretning **kan gi bedre innsikt** i trusselbildet hos organisasjoner som har tilstrekkelige ressurser og **spisskompetanse**

- Styrket informasjon om trusselbildet for virksomheten kan være et **nyttig verktøy** for **kommunikasjon** mellom sikkerhets-, IT- og virksomhetsledelse.

RecordedFuture: Linda Odin

Direktoratet for forvaltning og økonomistyring

#mps | utprøving av en tjeneste for personvern i leverandørkjeden

Kan bedre oversikt og innsikt i leverandørkjedenes personvern bidra til bedre og mindre ressurskrevende etterlevelse av GDPR for virksomhetene?

MPS har iverksatt en utprøving av en tjeneste som kan bidra til bedre styring og oversikt over leverandører og deres leveransekjeder

Deltakelse

- MPS har invitert 9 offentlige virksomheter til denne utprøvingen
- Virksomhetene vil få støtte fra leverandøren underveis

Hva skal gjøres?

- Virksomhetene som deltar har fått tilgang til tjenesten, og skal teste og evaluere nytteverdien gjennom utprøvingsperioden

Direktoratet
for forvaltning og
økonomistyring

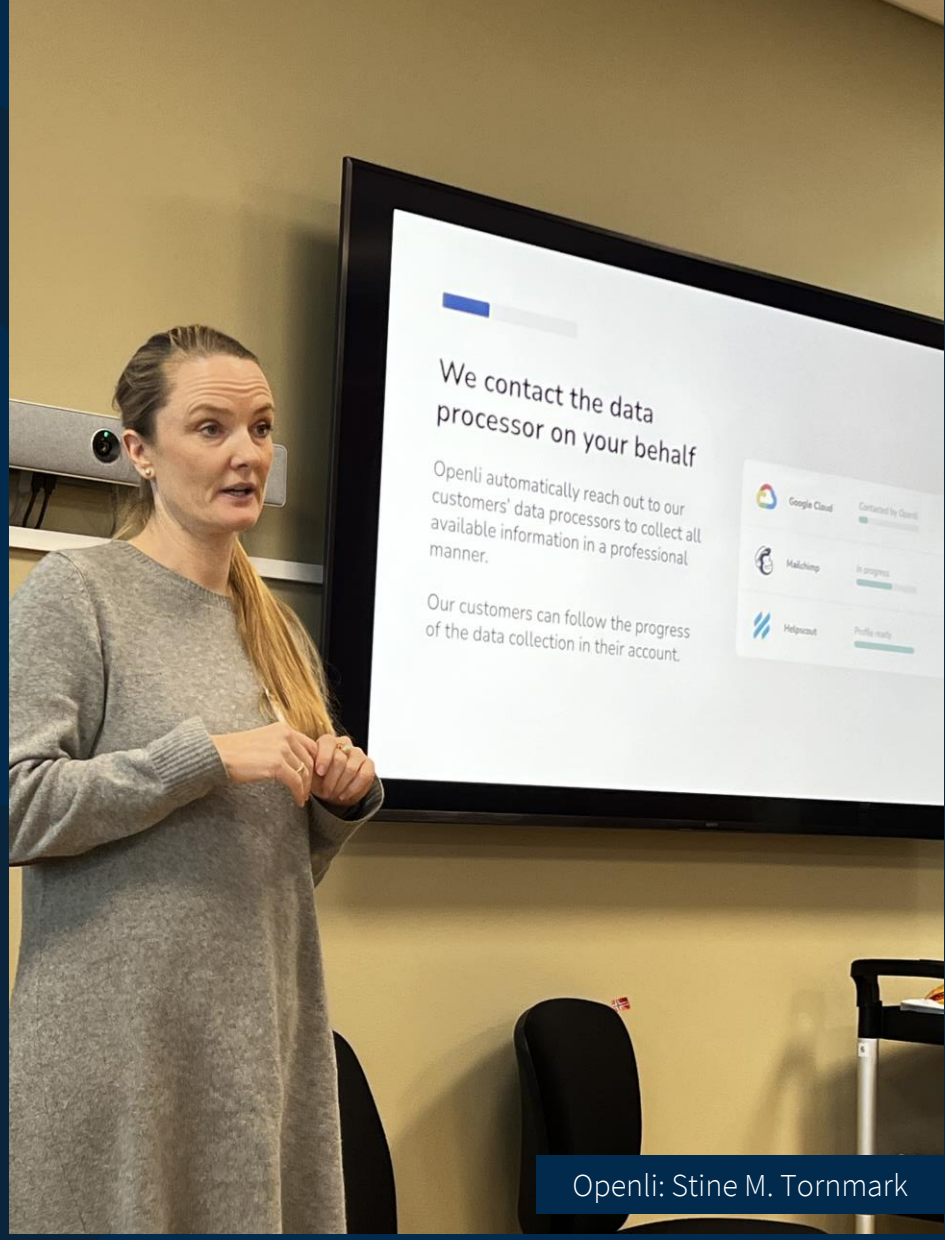
#mps | Personvern i leverandørkjeden – noen temaer vi ønsker å belyse:

- Komplekse leverandørkjeder - redusere risiko
- Fullmaktsbasert innhenting av opplysninger
- Mindre ressursbruk til oppfølging av krav til personvern

- Økt tillit til offentlige virksomheter ved synliggjøring av strategisk og operativt personvernarbeid

- Redusert ressursbruk for innsamling av GDPR informasjon fra virksomhetens databehandlere og oppfyllelse av lovmessige krav.

- Lavere ressursbruk til dokumentering ved tilsyn og revisjon.
- Bedre intern kommunikasjon til ledelsen og interessenter



Openli: Stine M. Tornmark

Direktoratet for forvaltning og økonomistyring

#mps | Hvor vil vi med aktivitetene innen cybersikkerhet og personvern?

- Tilrettelegge for et sikkerhetsløft i offentlig sektor, der trussel- og sårbarhetsbildet indikerer et betydelig behov for **større robusthet** innen sikkerhet og personvern i offentlig forvaltning

- Offentlige virksomheter har **behov for verktøy og tjenester** som kan måle egen sikkerhetshygiene og redusere risiko for cyberangrep fra trussel aktører ved bruk av en portefølje av verktøy og tjenester

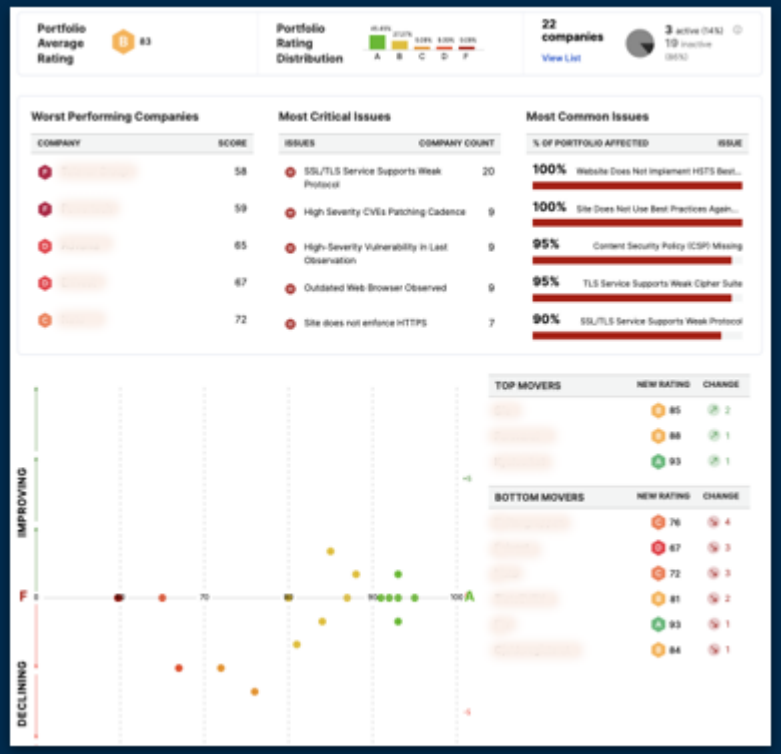
- **Undersøke behov og muligheter** ved å gjennomføre utprøvinger der kommuner, fylkeskommuner og statlige virksomheter deltar sammen med leverandører Hvis konklusjon fra utprøvinger tilsier **god nytteverdi**, vil det vurderes å gå videre med etablering av rammeavtaler

- For å bygge en robust motstandsdyktig virksomhet kreves det **flere ulike verktøy** som dekker behovet, men kompetanse og opplæring av ledelse og ansatte vil være minst like viktig.

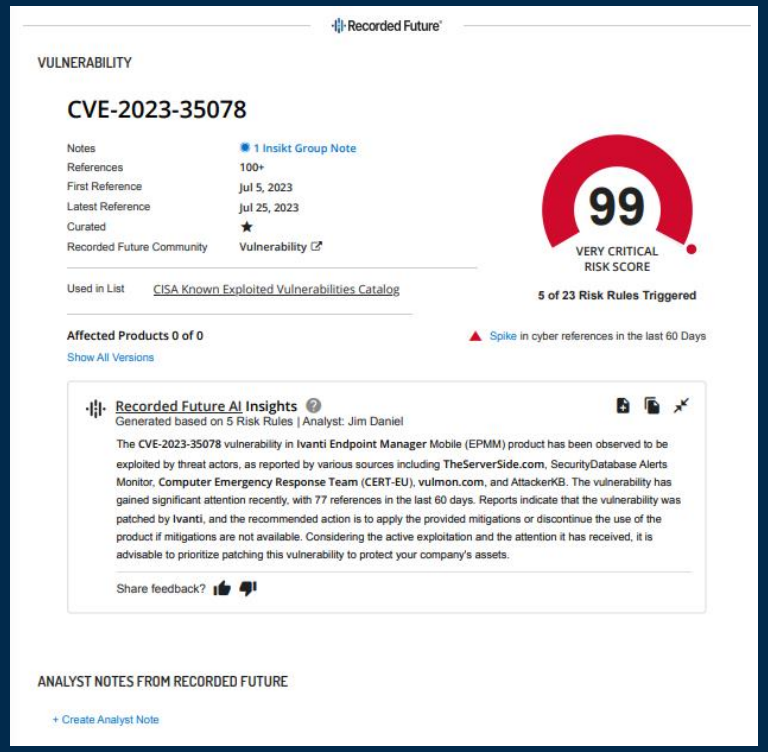
Hvilken effekt kan man oppnå ved å anskaffe flere ulike verktøy for Cybersikkerhet i virksomheten?

Direktoratet for forvaltning og økonomistyring

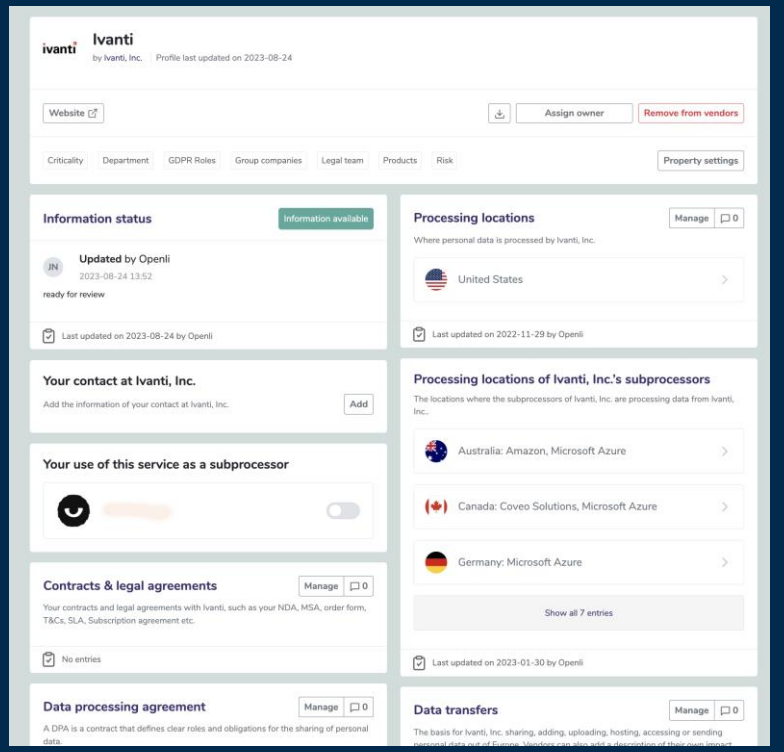
#mps | Eksempel på hvordan verktøyene samlet gir en bedre oversikt



Oversikt over sikkerhetsnivå over norske viksomheter med Ivanti EPMM



Detaljerte trusseloppdateringer om hendelsene og sårbarheten



Personverninformasjon for Ivanti fra et leverandørperspektiv

Kilde: SecurityScorecard, Recorded Future, OpenLi

Direktoratet for forvaltning og økonomistyring

Følg oss videre…

- Informasjonsmøte #MPS 14. desember
- Publisering av konklusjon etter utprøving av tjeneste for trusseletterretning
- Konkurranse for Cyber Risk Score tjeneste utlyses november 2023

- Kontakt oss på epost: markedsplassen@dfo.no
- Kontakt oss på linkedIn : https://www.linkedin.com/groups/9253192/

markedsplassen.anskaffelser.no

Markedsplassen for skytjenester skal bidra til styrking av sikkerhet i det offentlige Norge gjennom veiledning, digitale tjenester og skykontrakter.

Mange takk ☺

Direktoratet
for forvaltning og
økonomistyring