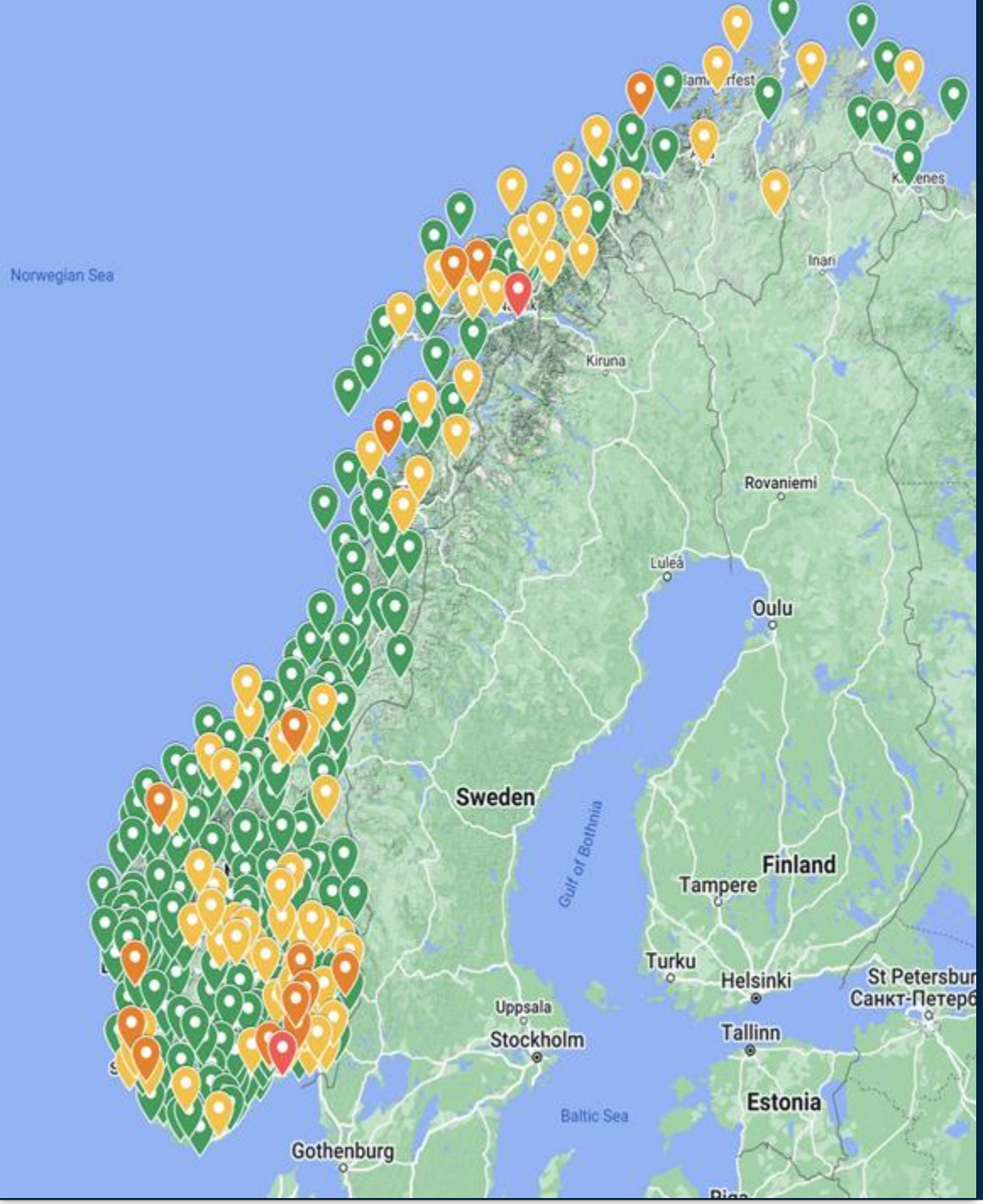


CYBER-X

DFØ/MPS,
Sikkerhetsfestivalen september 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 en erfaren IT-leder med bakgrunn innen informasjonssikkerhet og personvern. Han har tidligere jobbet i ulike lederstillinger i IT-bransjen, men nå jobber han på statens innkjøpssenter på markedsplassen for skytjenester. Der fokuserer han spesielt på cybersikkerhet i skytjenester. Per Jakobsen bidro til anskaffelsen av en public cloud skytjeneste i Narvik kommune kommune, som første offentlige virksomhet i Norge. Dette resulterte i en prinsippavgjørelse hos Datatilsynet om lovlig bruk av skytjenester i norsk offentlig forvaltning. Per Jakobsen fokuserer nå på anskaffelse av verktøy og tjenester innen sikkerhet og personvern for strategisk og operasjonell bruk i offentlig forvaltning.

– **Strategisk og operativ håndtering av cybertrusler krever bedre innsikt, verktøy og tjenester**

André Årnes

Partner @ WLC and Professor II @ NTNU

André Årnes is a Co-owner and Partner of White Label Consultancy and a Professor II at the Norwegian University of Science and Technology (NTNU). He has previously served as the SVP and Group Chief Security Officer of Telenor Group, as the CIO of Telenor Global Shared Services, and as a Special Investigator in Digital Forensics and Cyber Crime at the Norwegian Criminal Investigation Services (Kripos). André has a keen interest in cyber security, with an emphasis on security leadership and digital investigations, and he has published two edited books "Digital Forensics" (Wiley, 2018) and "Cyber Investigations" (Wiley, 2022).

– **Strategisk og operativ håndtering av cybertrusler krever bedre innsikt, verktøy og tjenester**

White Label Consultancy

Direktoratet for forvaltning og økonomistyring

Om Markedsplassen for skytjenester (MPS)

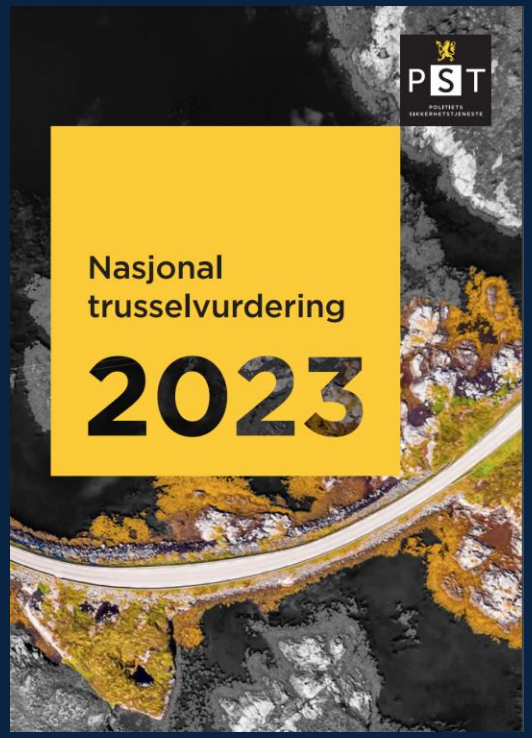
- Markedsplassen er opprettet på bakgrunn av Nasjonal strategi for bruk av skytjenester
- Eies av Finansdepartementet. Styres av KDDs avdeling for IKT-politikk
- Tildelingsbrev fra Finansdepartementet
  - Veiledning, anskaffelse, informasjonssikkerhet og oversikt over markedet
- Fullmakt til å inngå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

Markedsplassen for skytjenester (mps) – 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)	Tilrettelegger nyttig informasjon innen anskaffelser og bruk av skytjenester

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.

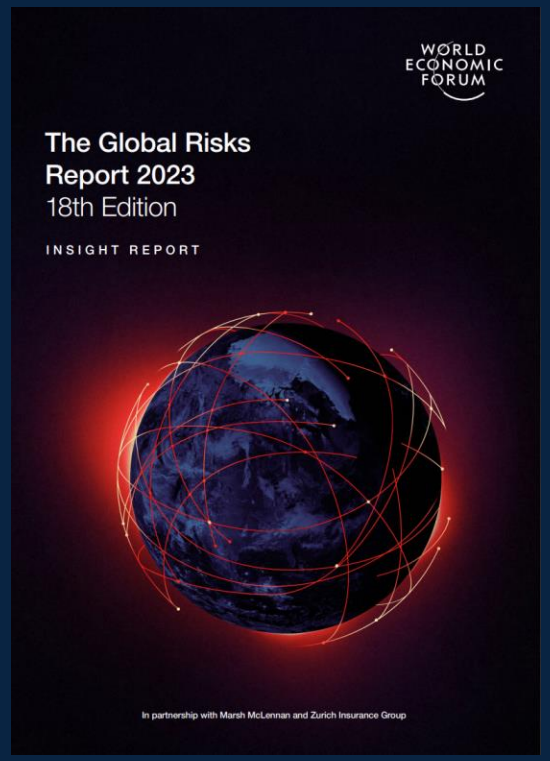
| Digital sårbarhetsflate utvikler seg | Lange og uoversiktlige leverandørkjeder | Tredobling av alvorlige cyberoperasjoner 2019 – 2021 | Kommersielt tilgjengelige brukerdata | Innsidevirksomhet | 5G og skytjenester | Kvantekappløpet | AI | (NSM 2023)



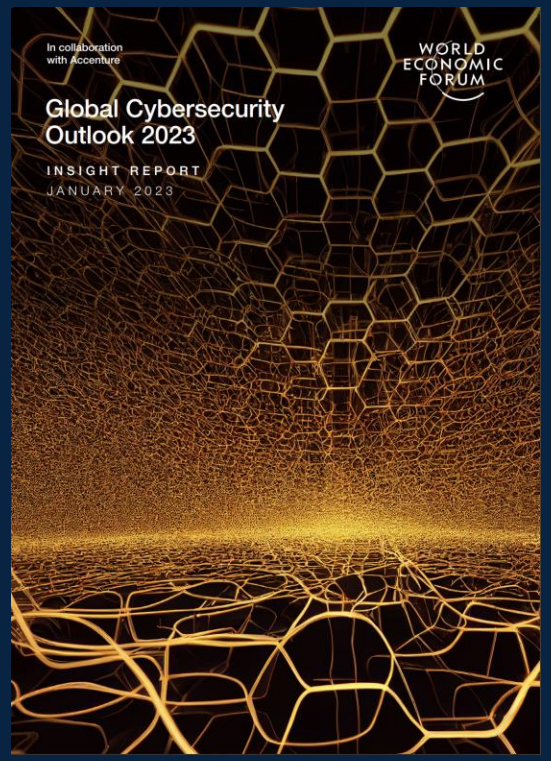
| Nettverksoperasjoner | etterretningsaktivitet | Avanserte digitale trusselaktører | Russland og Kina | Verdikjedeangrep | Operasjoner mot enkeltpersoner | (PST 2023)

| 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)

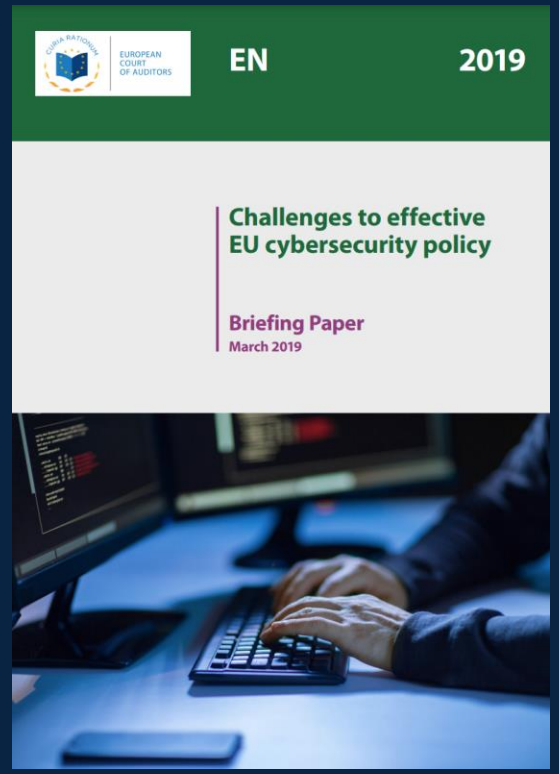


| Gap between business leaders and security leaders | Agreeing on how to best address cyber risk remains a challenge – business disruption and reputational damage | Cyberthreats have changed | Catastrophic cyber event is likely in the next two years | Dependency on supply chain | Balancing digital transformation 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)

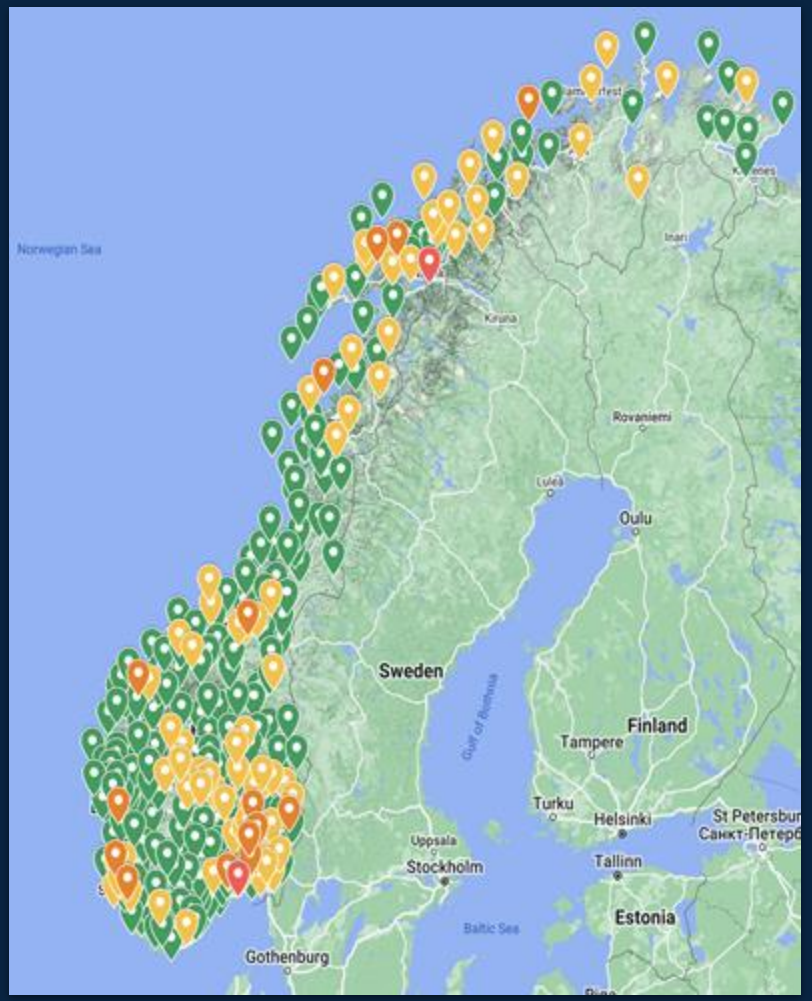
| Mangler i samvirket mellom kommando- og kontrollinformasjonssystemer | Sårbarheter I sikkerheten gir risiko for svekket operativ evne | Ikke greid å realisere effektive og sikre informasjonssystemer | (Riksrevisjonen 3:3 2023)

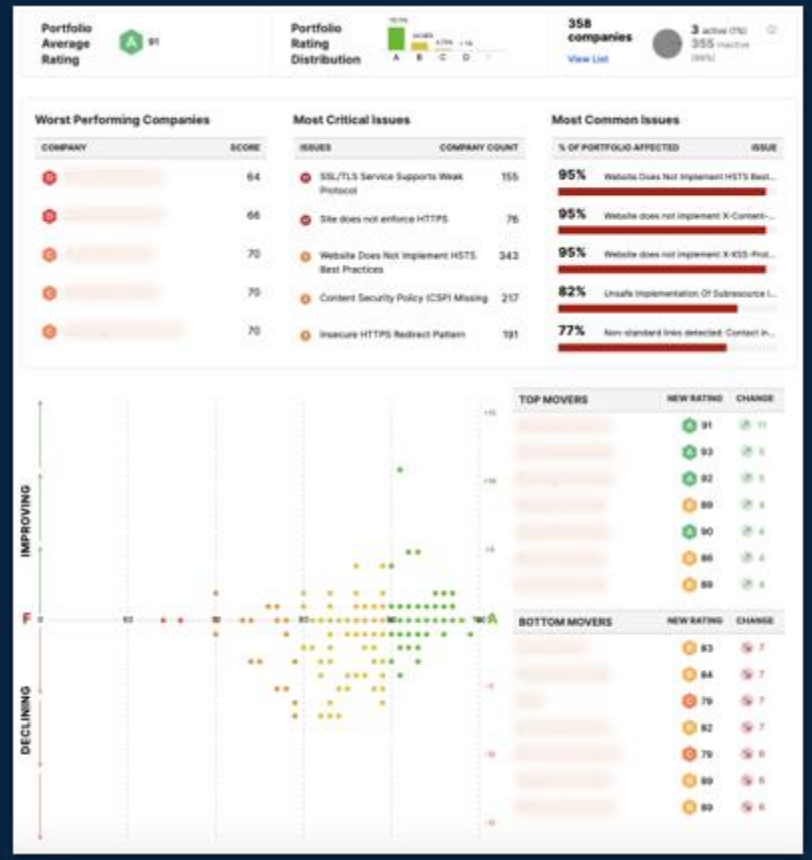


| Aligning investment levels with goals | Constraints in adequate resourcing | Weaknesses in governance | Skills and awareness | Information exchange and coordination | | Rapid detection and response | Protection of critical infrastructure and societal functions | Fragmentation – complex, multilayered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

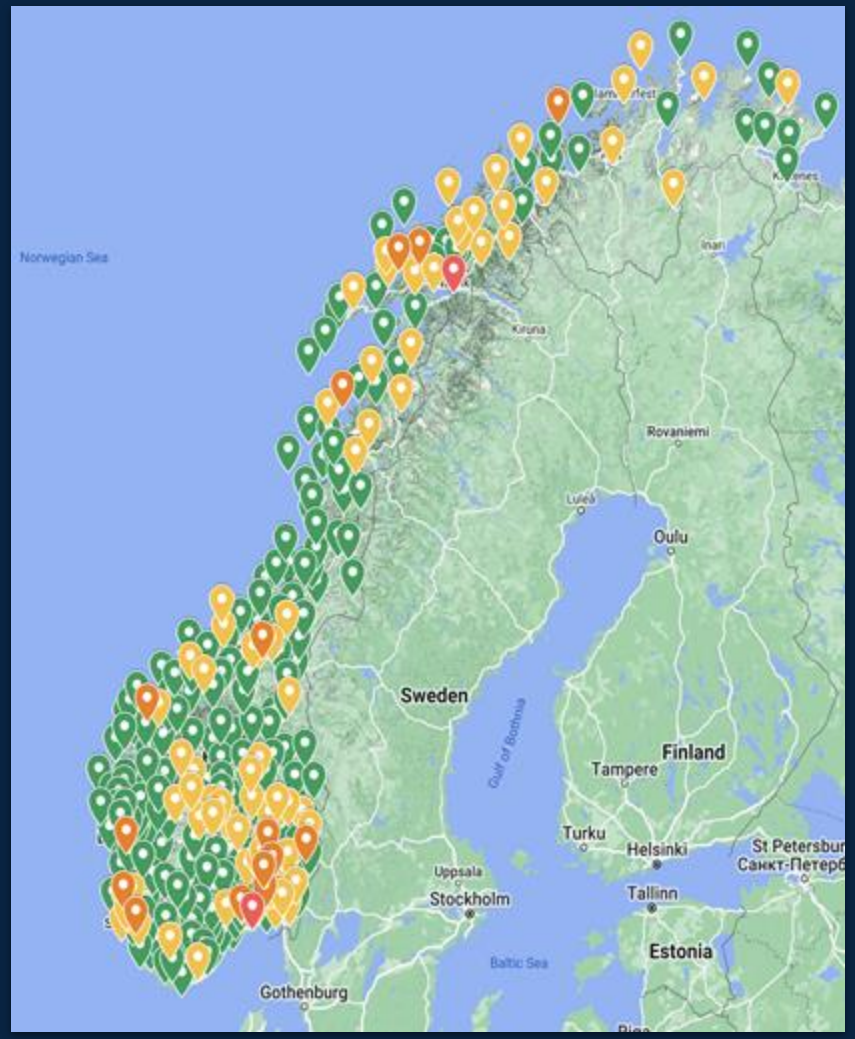
Et situasjonsbilde av sikkerhetsnivået i det offentlige Norge bekrefter et stort potensiale for å måle og forbedre sikkerhetshygienen på nasjonalt nivå.





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 | Cybersecurity | 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

Styrt

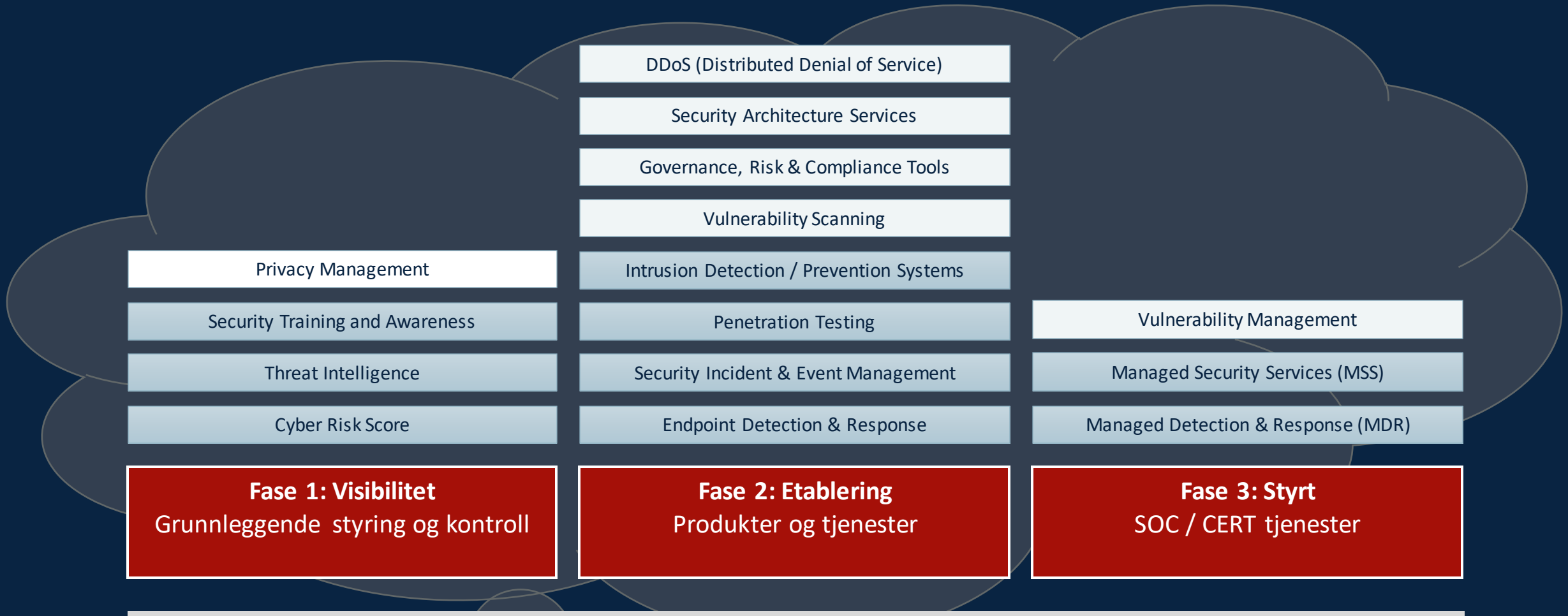
Styrt oppfølging på nasjonalt nivå **1**

Styrt oppfølging på sektor-nivå **2**

Tilrettelagt

Tilrettelegging ved skykontrakter og tilhørende cybersikkerhets-tjenester **3**

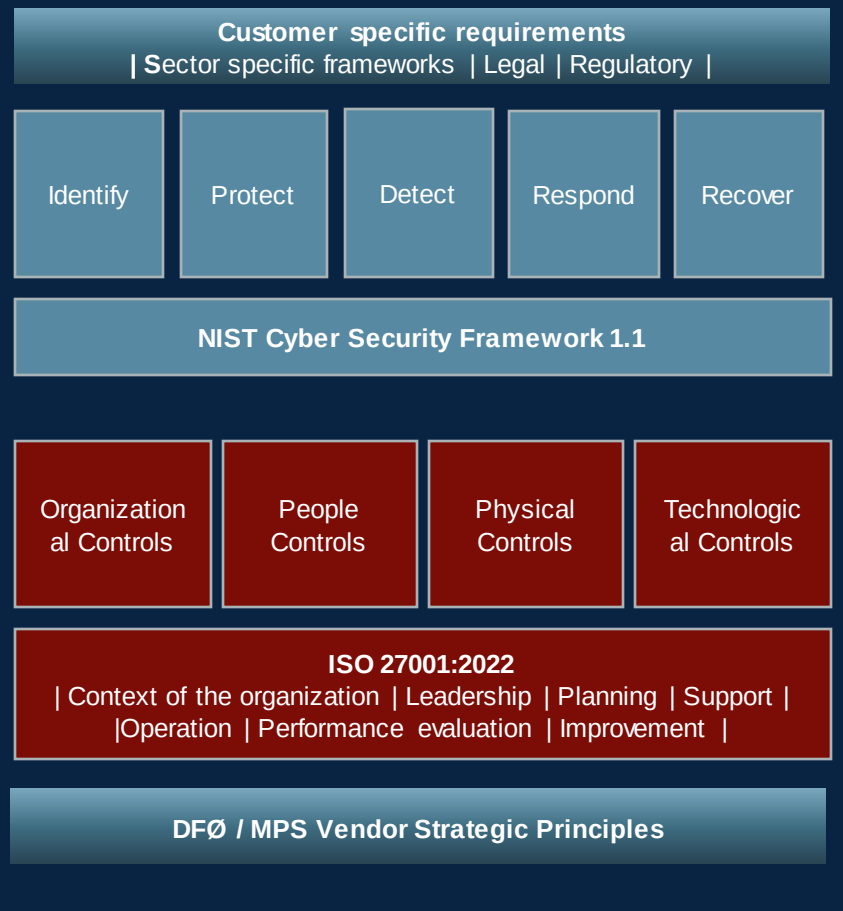
#mps | Portefølje av produkter og tjenester for offentlig sektor



Som førende for alle porteføljeområdene legges til grunn at alle tjenester og produkter skal være:

- 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).
- Multi-vendor. Målbildet er, hvor relevant, å etablere avtaler med flere leverandører innenfor kategoriene og dermed tilrettelegge for fleksibilitet med hensyn på ulike modenhetsnivå.
- Baseline. 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



Secure cloud adoption ("security in the cloud") Vendor cyber security architecture (optional requirements)

Secure cloud platform ("security of the cloud") Basic security requirements – mandatory requirements (mandatory requirements)

- Formålet med MPS Cyber Security-referansearkitekturen er å gi et rammeverk for å administrere cybersikkerhet i MPS-leverandørprosesser og kontrakter.
- Rammeverket etablerer a) et sett av leverandørens strategiske sikkerhetsprinsipper (obligatorisk), b) et sett med grunnleggende sikkerhetskrav (obligatorisk), og c) et rammeverk for leverandørens cybersikkerhetsarkitektur (valgfritt).
- Rammeverket er basert på anerkjente standarder og rammeverk, bransjenormer og referansekontrakter fra norsk offentlig sektor.
- Referansearkitekturen støtter eller viser til relevante standarder/rammeverk/lover:
  - Nasjonale lover: Sikkerhetsloven, Ekomloven, GDPR, Helseregisterloven, Eforvaltningsloven, NIS2
  - Nasjonale krav/retningslinjer: NSM Grunnprinsipper for IKT-sikkerhet, Normen, etc.
  - Standarder: ISO 27001/2:2022, ITIL, etc.
  - Rammeverk: NIST CSF. Cloud Security Alliance CCM, CIS, GSMA Guidelines, etc.

UTPRØVINGER

PROSJEKT CYBERSIKKERHET

Direktoratet
for forvaltning og
økonomistyring

#mps| utprøving av en Cyber Risk Score tjeneste 2022

Formål med utprøvingen

- Kan bedre innsikt i sårbarhet på internett sett utenfra bidra til bedre sikkerhetshygiene?
- Hvilken merverdi kan en slik tjeneste gi ved å benyttes strategisk og operativt

Deltakelse: 26 statlige virksomheter og 4 kommuner

Hva er gjort?

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

Security Scorecard

Direktoratet for forvaltning og økonomistyring

Formålet med prosjektet har vært å prøve ut Cyber Risk Score i statlige og kommunale virksomheter for å se hvilken effekt bedre innsikt i egen sårbarhet på internett vil ha med hensyn på å treffe risikoreduserende tiltak.

Våre konklusjoner basert på innspill og tilbakemeldinger i utprøvingsperioden:

- Indikerer behov for en cyber risk score tjeneste - nyttig verktøy for virksomhetsledelse og for IT- og sikkerhetsledelse.
- Kan benyttes som styringsverktøy og for samhandling i offentlig sektor innen cybersikkerhet

Porteføljen 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. En høy score i verktøyet må ikke være en hvilepute for virksomhetsledelsen, men snarere et mål på minimum sikkerhetshygiene på Internett
- Relevant kompetanse på IT- og sikkerhet. 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| utprøving av en tjeneste for trusseletterretning 2023

Formål med utprøvingen

- Undersøke om kunnskap om dypere innsikt i trusselbildet kan bidra til raskere og mer målrettet problemløsning innen Cybersikkerhet
- Øke utbredelse av tjenester innen trusseletterretning gjennom fellesavtale

Deltakelse

- Mer spesialisert tjeneste som også krever høy kompetanse på brukersiden
- Inviterer utvalgte virksomheter til utprøving
- Inviterer til drøftinger med relevante interessenter innen stat og kommune

Hva skal gjøres?

- Utprøving av en trusseletterretningstjeneste mai – september/oktober
- Deltakende virksomheter vil jobbe sammen med leverandøren i perioden
- Utprøvingsaktiviteter med leverandør er pågående

Recorded Future®

Direktoratet for forvaltning og økonomistyring

#mps| utprøving av en tjeneste for personvern i leverandørkjeden

Formål

- Oversikt over leverandørkjedene er for enhver virksomhet en svært viktig, men krevende oppgave under GDPR
- MPS skal gjennomføre en utprøving av en tjeneste som kan bidra til bedre styring og oversikt over leverandører og deres leveransekjeder.
- GDPR Artikkel 30 Behandlingsansvarlig skal føre protokoll (behandlingsoversikt) over behandling av personopplysninger)

Deltakelse

- MPS vil invitere virksomheter til utprøving – NÅ!
- Virksomhetene vil få støtte fra leverandøren underveis

Hva skal gjøres?

- Virksomhetene som deltar vil få tilgang til tjenesten, teste og evaluere nytteverdien gjennom utprøvingsperioden.

openli

Direktoratet for forvaltning og økonomistyring

#mps| Personvern i leverandørkjeden – hva ønsker vi?

Noen av forholdene som MPS ønsker å få belyst gjennom utprøvingen:

- Mange leverandører og lange leverandørkjeder er komplekse og medfører risiko
- Bidrag til mer effektiv fullmakts basert innhenting av opplysninger fra leverandørene
- Mindre ressursbruk til oppfølging av krav til personvern
- Økt tillit til offentlige virksomheter ved synliggjøring av systematisk personvernarbeid
- Redusert ressursbruk for innsamling av GDPR informasjon fra virksomhetens databehandlere og oppfyllelse av lovmessige krav.
- Ressursbruk ved dokumentering ved tilsyn og revisjon.
- Ressursbruk ved intern kommunikasjon til ledelsen og interessenter
- Øke tillit til offentlig forvaltning sin håndtering av persondata

Direktoratet for forvaltning og økonomistyring

#mps| Søk om deltakelse til utprøving av OpenLi

Offentlige virksomheter kan søke om deltakelse i utprøvingen av **OpenLi**

Virksomhetene som deltar vil bli innkalt til kickoff på DFØ og markedsplassen for skytjenester i Økern Portal 13. oktober

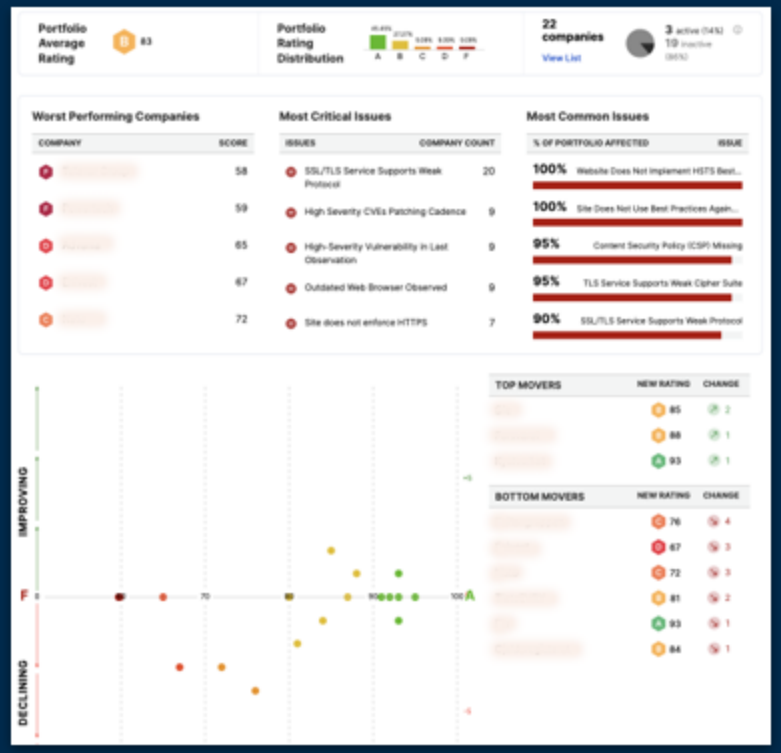
Under utprøvingen vil leverandøren bistå virksomhetene.

Tjenesten vil være tilgjengelig for virksomhetene i 6. måneder

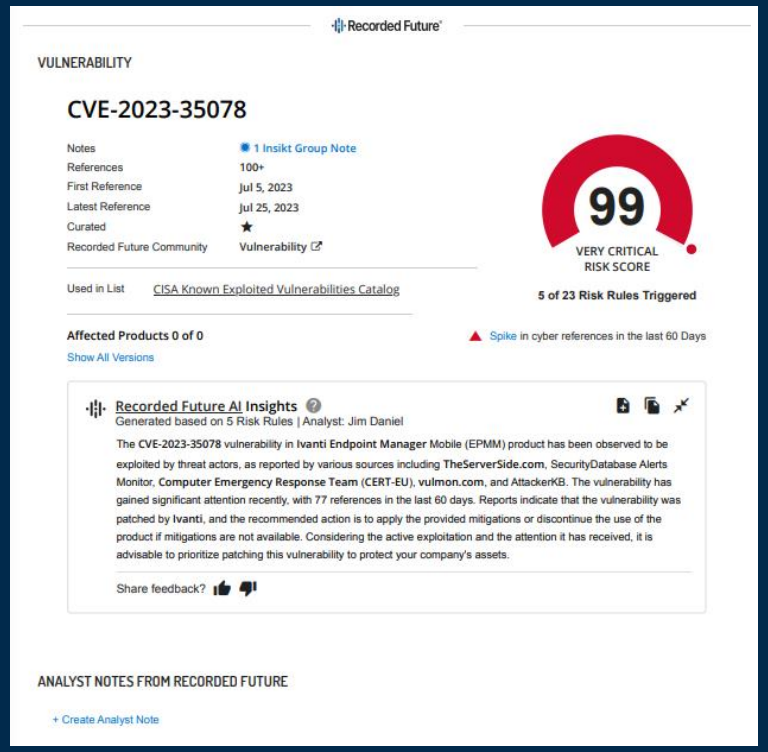
Enkelt søknadsskjema (frist 15.9.2023):
https://response.questback.com/direktoratetforokonomistyring/nbysdyzsi7

Direktoratet
for forvaltning og
økonomistyring

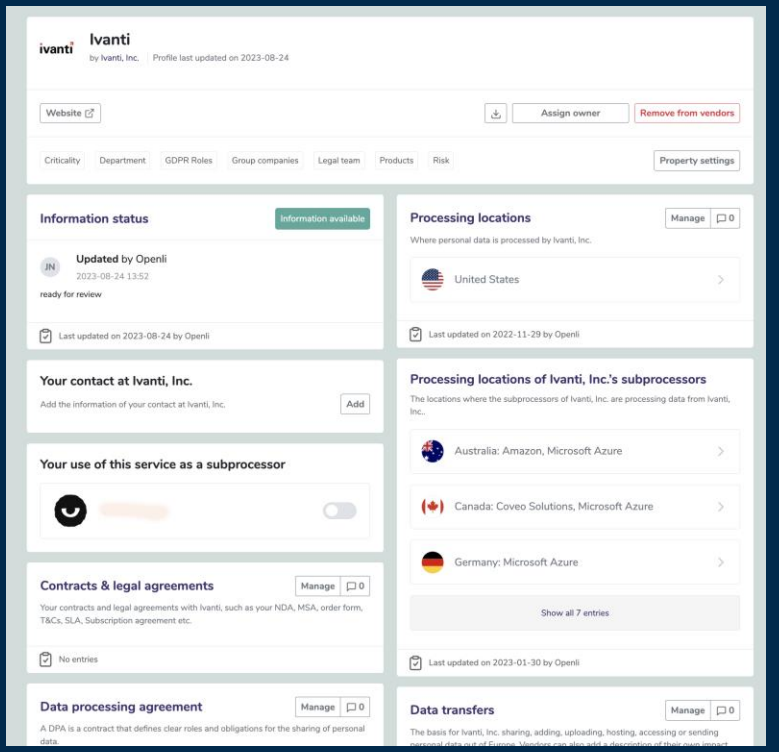
#mps| Use case – Ivanti EPMM/Mobileiron core i Norge



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 13. september
- Anskaffelseskonferansen 31.10 – eget spor med MPS
- Søknad om deltakelse til utprøving – personvern i leverandørkjeden 15. september
- Publisering av konklusjon etter utprøving av tjeneste for trusseletterretning
- Utlyse konkurranse for Cyber Risk Score tjeneste

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

markedsplassen.anskaffelser.no

Mange takk ☺

Direktoratet
for forvaltning og
økonomistyring