Markedsplassen for skytjenester NIFS

7. mai 2025

Per Jakobsen

Norwegian agency for public and financial management

Kjøper du også sikkerhetsrisiko?

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

Markedsplassen er opprettet på bakgrunn av Nasjonal strategi for bruk av skytjenester

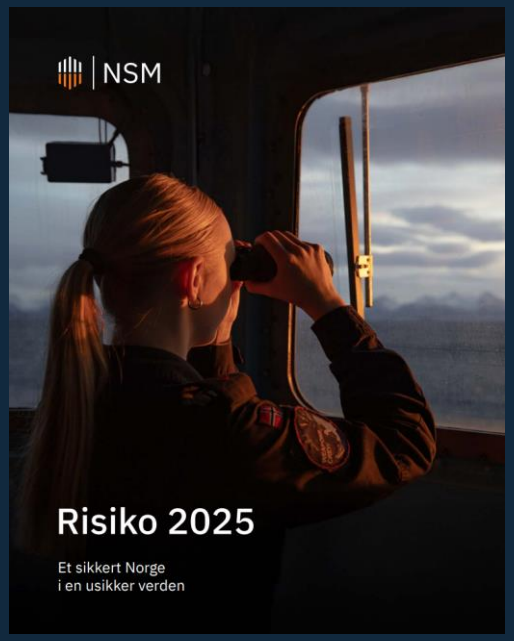
Eies av Finansdepartementet. Styres av DFD

Tildelingsbrev fra Finansdepartementet

Veiledning, anskaffelse, informasjonssikkerhet og oversikt over markedet

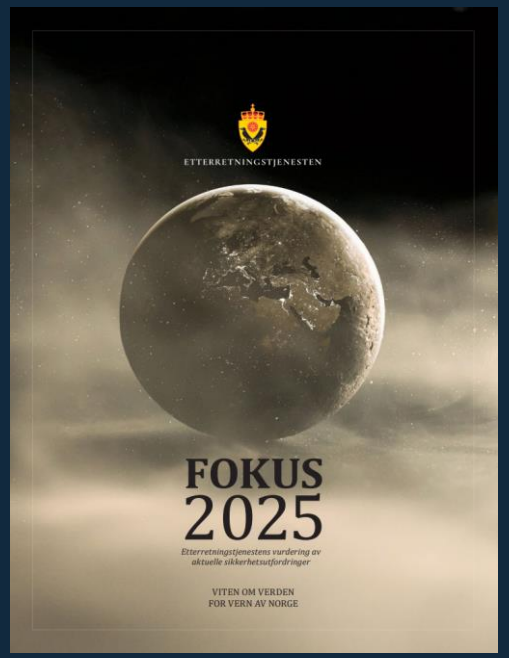
Fullmakt til å inngå statlige fellesavtaler ved kgl. res. av 3. september 2021

Norsk offentlig sektor utsettes for et stadig mer utfordrende trusselbilde og det er behov for en strategisk og risikobasert satsning på cybersikkerhet basert på målbare fakta og informerte beslutninger



| Må redusere konsekvensene av uønskede hendelser, men arbeidet går for sakte | ord må bli til handling | dramatisk endring I trusselvurderingen | endringer i trusselbildet må gi endringer i tiltak | I dag: ikke sammenheng mellom advarsler og virksomhetenes reaksjon

| Statlig etterretningsvirksomhet, påvirkning og sabotasje | Digitale påvirkningskampanjer rettet mot et norsk publikum | Digitale rekrutteringsforsøk | Norsk teknologi er ettertraktet av statlige aktører | Akademiske institusjoner og bedrifter er utsatte mål | Statlige cyberaktører - fordekt, proxy-aktører, uforutsigbart | Kunstig intelligens skaper nye muligheter



| Digitale etterretnings- og påvirkningsoperasjoner | Etterretningsinnsats mot europeisk politikk, næringsliv og forskning | Eierskap i infrastruktur og teknologiselskaper | Strategisk statssubsidiering | Trusler mot undervannsinfrastruktur

Den nasjonale helhetsbildet for sårbarheter innen cybersikkerhet viser økende, bredere og dypere trusselnivå der behovet for at norsk offentlig sektor samarbeider, øker tempo og agerer med konkrete tiltak innen cybersikkerhet, er kritisk!

| OECD analyse: styrke samordning | helhetlig prioritering av investeringer | mer deling av offentlige data | utnytte ny teknologi | digital kompetanse | styrke små og mellomstore virksomheter | utrede pliktig bruk av fellesløsninger | nasjonal arkitektur for felles digitalt økosystem | styrket arbeid med nasjonal sikkerhet og beredskap | stimulere til mer bruk av bransjenormer

Økende kompleksitet krever en høyere grad av tverrsektoriell situasjonsforståelse og bred nasjonal koordinering og samarbeid. Vi må bruke digitalisering til å forbedre den nasjonale situasjonsforståelsen, blant annet gjennom å omsette store mengder data og informasjon til kunnskap

| Cyberkriminalitet, globalt fenomen | rask overføring av trender og metoder på tvers av landegrenser | behov for økt bevissthet | spent sikkerhetspolitisk situasjonen | muliggjørere - teknologisk | tilretteleggere – personer med tilgang og kompetanse | økt digitalisering og teknologiske avhengigheter åpner for nye sårbarheter | verdikjedeangrep og tredjepartsrelasjoner

#MPS | Hvorfor fokus på sikkerhet i anskaffelser?

- ✓ Økt avhengighet av skytjenester og tredjepartsleverandører
- ✓ Potensiell risiko for sensitive data og kritiske tjenester
- ✓ Klare kontraktskrav og risikostyring er avgjørende
- ✓ Krav fra GDPR, NIS2 og nasjonale sikkerhetsmyndigheter (NSM)
- ✓ Markedsplassens krav til informasjonssikkerhet i skyavtaler

KREVER HANDLING: Arne Christian Haugstøyl, direktør i Nasjonal sikkerhetsmyndighet (NSM). Foto: Trond Lepperød (Nettavisen)

– I 2025 er det ikke lov å være så naiv, sier NSM-direktør om norske virksomheters manglende evne til å treffe sikkerhetstiltak mot ting som spionasje og terror.

Kilde: Nettavisen

#MPS | Toolbox - Rammeverk og overordnede styringskrav

- ✓ Virksomhetens egen grunnsikring – ISO/IEC 27001, NSM Grunnprinsipper og NIST Cybersecurity Framework
- ✓ Nasjonalt lovverk (offentlige anskaffelser, sikkerhetslov, GDPR m.m.)
- ✓ Helhetlig virksomhetsstyring (risk management, compliance)

#MPS | Virksomhetens lederforankring og policyer

Toppleder

Lederforankring er essensielt for å forplikte hele organisasjonen. Toppledelsen: ansvar for etablering av sikkerhetspolicy

Risikoeiere

Risikoeiere: typisk på direktør- eller avdelingsledernivå, definerer retningslinjer i tråd med virksomhetens mål og risikobilde.

Alle ansatte

Alle ledd i organisasjonen må forstå hvorfor disse kravene eksisterer, og hvordan de skal praktiseres i hverdagen. Kompetanseheving må prioriteres høyt!

#MPS | Overordnet sikkerhetsvurdering ved valg av leverandører

- ✓ Leverandørens sikkerhetskultur
- ✓ Matcher leverandøren virksomhetens *eget* sikkerhetsnivå
- ✓ Klassifisering av leverandører etter kritikalitet – kreves det redundant leveranse?
- ✓ Dokumentert beslutningsgrunnlag

#mps | Vurdering og valg av sikkerhetsnivå hos leverandører

Kilde: Digi.no

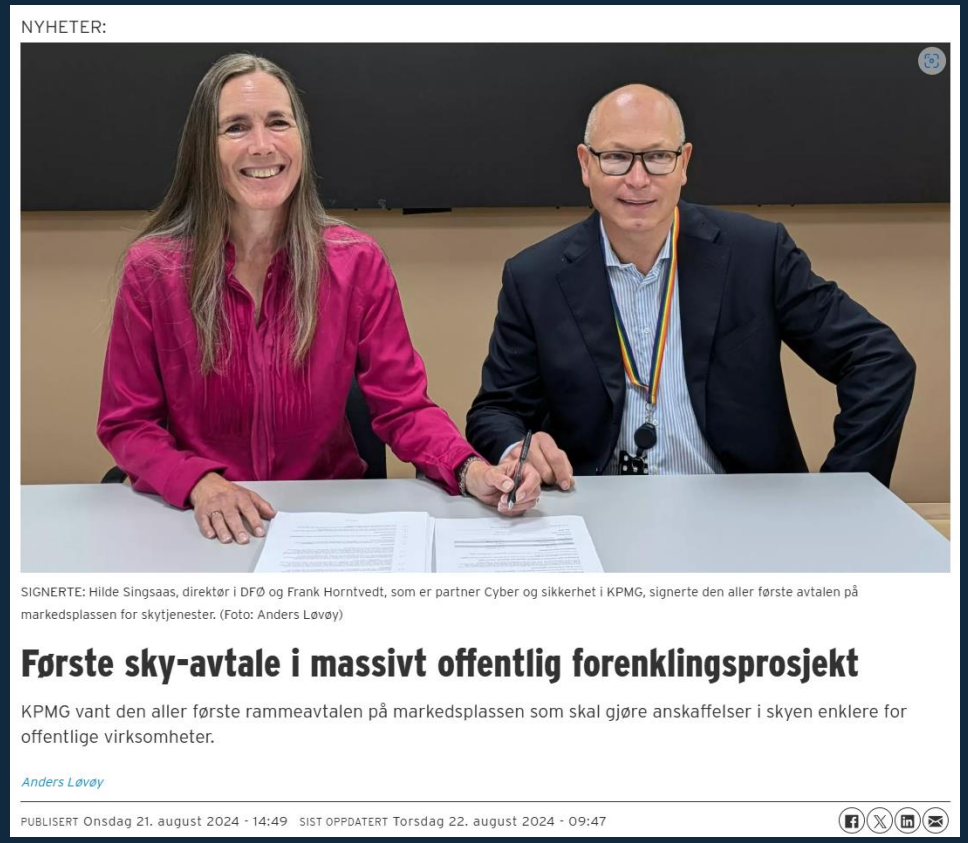
- ✓ Evaluering av leverandørers evne til å møtesikkerhetskrav
- ✓ Dokumentasjon av leverandørers sikkerhetspraksis
- ✓ Bruk av standarder og sertifiseringer (NSM Grunnprinsipper, ISO 27001, CSA CCM, C5)
- ✓ Sikring av en trygg og regelverksetterlevende leverandørkjede

#MPS | Oppfølging av leverandører og kontraktskrav

- ✓ Kontinuerlig monitorering av leverandørens sikkerhetstiltak i tjenesten
- ✓ Leverandørrevisjoner og tilsynsrapporter
- ✓ Avvikshåndtering og eskalering

Cyber Risk Score – avtalen signert onsdag 21. August 2024

- Cyber Risk Score tildelt KPMG/MasterCard med tjenesten RiskRecon
- Rammeavtale med formål å måle og styrke informasjonssikkerhet i offentlig sektor.
- Tjenesten tilrettelegger for:
  - Nasjonal situasjonsforståelse
  - Virksomhetsstyring
  - Operativ bruk
- Ambisjonen er at alle skal med!



NYHETER:

SIGNERTE: Hilde Singsaas, direktør i DFØ og Frank Horntvedt, som er partner Cyber og sikkerhet i KPMG, signerte den aller første avtalen på markedsplassen for skytjenester. (Foto: Anders Løvøy)

Første sky-avtale i massivt offentlig forenklingsprosjekt

KPMG vant den aller første rammeavtalen på markedsplassen som skal gjøre anskaffelser i skyen enklere for offentlige virksomheter.

Anders Løvøy

PUBLISERT Onsdag 21. august 2024 - 14:49 SIST OPPDATERT Torsdag 22. august 2024 - 09:47

Kilde: Computerworld, 21.08.2024

#MPS| Erfaring fra Ringerike kommune om utprøvingen av Cyber Risk Score

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

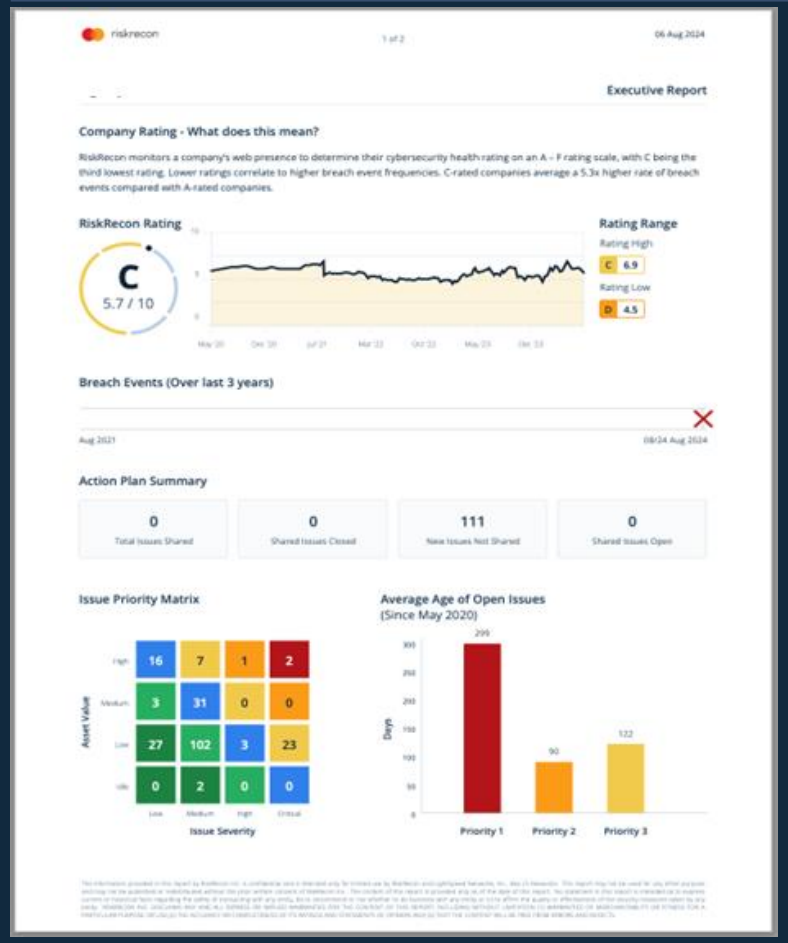
Markedsplassen for skytjenester (MPS) er er i gang med å sjekke interessen for en ny skytjeneste som kartlegger cyberriskofaktorer i offentlig og statlig sektor. Styreleder i offentlig sikkerhetsforening mener programmet er et «must».

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*

Kilde: Digi.no

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.

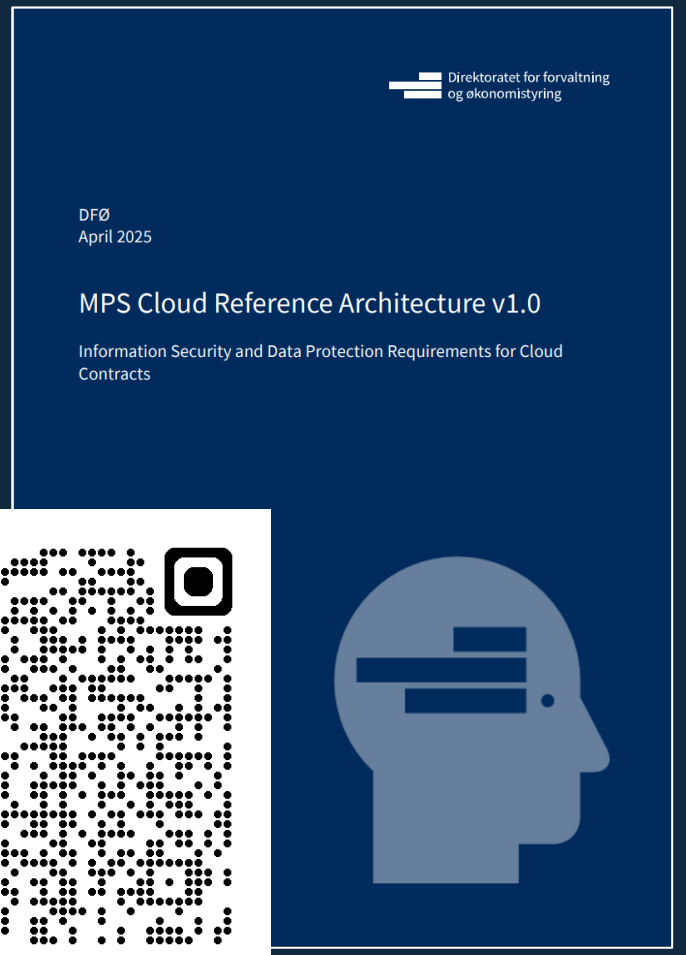
Hva gjør tjenesten for virksomhetene



- Kartlegger virksomhetens/leverandørens systemer, risiko og sårbarhet på Internett
- Beregner en risikoscore som kan følges opp over tid og sammenlignes med andre
- Verktøy for oppfølging av identifiserte risiko og sårbarheter
- Funksjonalitet for dashboards, varsling og rapporter for virksomhetsledelse og operativt bruk hos IT og sikkerhetsansvarlig
- Oppfølging av leverandører og tredjeparter med tilsvarende funksjonalitet som virksomheten selv
- Merk at verktøyet krever en systematisk tilnærming, og det er bare et av flere verktøy i verktøykassa!

#MPS | Referansearkitektur for sikkerhet i anskaffelser for skytjenester v.10

Prinsipielle krav	**Overordnede krav til kontraktsmessige forhold**
Basiskrav	**Obligatoriske krav til cybersikkerhet**
Tilleggskrav	**Leverandørens forslag til cybersikkerhetsarkitektur basert på kundens behov**



#mps

#MPS | Hendelseshåndtering og læring

- ✓ Klare varslingsrutiner og kontaktpunkt
- ✓ Krav til leverandørens planer for håndtering av sikkerhetshendelser
- ✓ Kontinuerlig forbedring gjennom øvelser og erfaringer

#MPS | Etter anskaffelsen: Oppfølging, avvikshåndtering og revisjoner

- ✓ Regelmessig kontroll av leverandørers etterlevelse
- ✓ Etablering av kontaktpunkter og tett dialog med leverandør
- ✓ Revisjonsrettigheter i kontrakter (GDPR, NIS2, etc.)
- ✓ Dokumenterte revisjoner og handlingsplaner for avvikshåndtering

Statistikk over sårbarheter i leverandørkjeder

- Økning i rapporterte leverandørkjedehendelser:
  - 2021: 44 % av organisasjoner rapporterte sikkerhetshendelser knyttet til leverandører
  - 2022: Økning til 56 %
  - 2023: Ytterligere økning til 61 % (ENISA Threat Landscape Report, 2023)

- Kritiske sårbarheter:
  - 40 % av cyberangrep utnytter sårbarheter hos leverandører
  - 2022 hadde rekordhøy økning på 24 % i antall leverandørrelaterte cyberhendelser globalt (IBM Cost of a Data Breach Report, 2023)

- Kostnader og konsekvenser:
  - Gjennomsnittlig kostnad for leverandørrelaterte datainnbrudd økte med 15 % fra 2021 til 2023
  - Gjennomsnittskostnad per hendelse nå på ca. 4,6 millioner USD (IBM Cost of a Data Breach Report, 2023)

ENISA Threat Landscape Report 2023:https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
IBM Cost of a Data Breach Report 2023:https://www.ibm.com/reports/data-breach

#MPS | Oppsummering

- ✓ Ledelsesforankring: den røde tråden
- ✓ Kombinasjon av rammeverk, risikovurdering og jevnlig revisjon
- ✓ Neste steg: Implementere erfaringer og rutineforbedringer