Sikt
Kunnskapssektorens tjenesteleverandør

Saksdokument

Porteføljestyret for data og infrastruktur

Til	Porteføljestyret for data og infrastruktur
Dato	18.09.2025
Saksnummer	19/25
Sakstype	D-Sak
Saksansvarlig	Bjørn Helge Kopperud
Saksbehandler	Emil Henry Flakk

Satsingsforslag cybersikkerhet 2027 - 2030

Forslag til vedtak

Porteføljestyret stiller seg bak hovedelementene i satsingsforslaget innen cybersikkerhet:

1. lettvekts sikkerhetsoperasjonssenter (miniSOC)
2. vern mot tjenestenektangrep (DDoS)
3. gjennomføring av sektorøvelser

Porteføljestyret ber om at satsingsforslaget forankres digitalt i produktrådet før innsending til KD.

Bakgrunn

Cybersikkerhet er et av flere høyt prioriterte tjenesteområder for sektoren, som over flere år har hatt for lav finansiering. Sikt jobber nå med en utredning og tydeliggjøring av Sikts rolle og prioriterte tjenester og utbredelse av tjenestene. Sikkerhet er et område hvor Sikt har et særskilt ansvar for, og satsingsforslaget vil derfor sees i sammenheng med sak 18/25 i dette møtet.

Porteføljestyret ble orientert 27. mai 2025 om planlagt innsending av nytt satsingsforslag for 2027–2030. Produktrådet for cybersikkerhet har tilrådd å sende satsingsforslag, med totalforsvar som gjennomgående tema.

I produktrådsmøte 10. september 2025 var det enighet om at satsingsforslaget bør videreføre tiltakene fra i fjor: et lettvekts sikkerhetsoperasjonssenter, DDoS-vern og sektorøvelser. Enkelte i produktrådet uttrykte også ønske om å inkludere informasjonssikkerhet/GRC.

Produktområdeleder anbefaler å bygge på fjorårets satsingforslag (vedlagt) og oppdatert trusselbilde når nytt satsingsforslag skal utarbeides. Satsingsforslaget må sendes til Kunnskapsdepartementet før fristen 1. november, etter digital forankring i produktrådet.

Begrunnelse og forventede gevinster:

Et lettvekts sikkerhetsoperasjonssenter (miniSOC) er et tiltak som skal sikre god og kostnadseffektiv deteksjon, med særlig vekt på små og mellomstore virksomheter. Tiltaket bygger på sektorens eksisterende arbeid med Microsoft Sentinel/Lighthouse. Gjennom dette forventes det en betydelig

reduksjon i tid til deteksjon og håndtering av hendelser, samt en forbedret situasjonsforståelse på tvers av sektoren. Det kan også bli enklere og kjappere å ta i bruk spesialister utenfor sektoren ved alvorlige hendelser, for eksempel gjennom den pågående anskaffelsen av sikkerhetspartner.

Vern mot tjenestenektangrep (DDoS) er et annet sentralt tiltak som skal sikre tilgjengeligheten av kritiske sektortjenester ved både volum- og applikasjonsangrep. Dette tiltaket organiseres og forvaltes av Sikt som internettleverandør (ISP), i tett samarbeid med Cybersikkerhetssenteret. Forventede gevinster inkluderer redusert nedetid og færre hendelser som påvirker brukerne.

Gjennomføring av sektorøvelser er et tiltak som skal styrke beredskap, krisehåndtering og informasjonsdeling gjennom systematisk trening og samhandling på tvers av virksomheter. Dette vil bidra til økt modenhet i sektoren, tydeligere rolle- og ansvarsfordeling, samt identifisering og oppfølging av nødvendige forbedringstiltak.

Vedlegg:

1. Satsingsforslag 2026 – 2029
2. Foreløpig protokoll fra produktrådsmøte 10. september 2025