09 DES 2024

POLITIETS
SIKKERHETSTJENESTE

Postboks 4773 Nydalen
0421 OSLO
post@pst.politiet.no
Tlf.nr. 23 30 50 00
Besøksadresse:
Nydalen allé 35

Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 OSLO

Deres ref.: 24/3567 - ODTV
Vår ref.: 24/04583-4
Dato: 2. desember 2024

Høring - Forslag til forskrift til digitalsikkerhetsloven - Høringssvar fra Politiets sikkerhetstjeneste

Det vises til høringsbrev av 11. september 2024 med forslag til digitalsikkerhetsforskrift. Vi har i oppgave å forebygge og etterforske handlinger som rammes av straffeloven §§ 121 – 126. Handlinger som etter sin art kan rammes av disse bestemmelsene er blant annet trusselaktørers informasjonsinnhenting ved dataangrep mot nettverk og informasjonssystemer som forvalter opplysninger av grunnleggende nasjonale interesser. Det vises her til Nasjonal trusselvurdering for 2024 på s. 6, hvor PST vurderer at fremmed etterretning vil innhente informasjon ved å bruke cyberoperasjon mot mål i Norge.

Vi anser forebyggende sikkerhet som et viktig tiltak i arbeidet med bekjempelse av slike trusler. Vi støtter derfor departementets forslag til nye krav til digital sikkerhet hos tilbyder av digitale eller samfunnsviktige tjenester. PST er i det vesentlige enig i forslaget.

Vi vurderer at forskriften sammen med digitalsikkerhetsloven er et godt rammeverk for å øke motstandsdyktigheten i nettverk og informasjonssystemer og gir eiere av slike nettverk og informasjonssystemer økt bevissthet rundt de samfunnsverdier de forvalter. Økt motstandsdyktighet er et viktig forebyggende tiltak mot dataangrep fra trusselaktører. Særlig reglene om styringssystemer og regler for varsling er viktige i det forebyggende sikkerhetsarbeid.

Vi gjør likevel oppmerksom på en mulig feil i forslagets § 17. Det følger av høringsnotat på s. 6, 1.ledd avsnitt under punkt 3 at *«Der det er hensiktsmessig har imidlertid departementet allerede forsøkt å tilnærme seg kravene i NIS2-direktivet, se blant annet forslag til § 15 om varslingsplikt og omtalen i punkt 7.».* Det siktes her til at departementet i forskriften forsøker å implementere deler av NI2-direktivet. Direktivet er ikke vedtatt, og departementet foregriper dermed vedtakelsen. Det er videre gjengitt fra varslingsreglene i direktivet i punkt 8.4 i høringsnotatet. Her fremkommer det at NIS2 inneholder bestemmelser om at det innen 72 timer skal gis en oppdatering til det tidligere varselet. Oppdateringen skal blant annet gi en innledende vurdering av «indikatorer for kompromittering». Dette kravet er imidlertid ikke inntatt i forslaget til § 17 om varslinger. De fleste andre kravene til varsel og oppdatering etter NIS2 er samtidig inntatt i § 17. Det

kan derfor fremstå som at kravet om «indikatorer for kompromittering» i oppdateringen etter 72 timer er utelatt utilsiktet.

Indikatorer for kompromittering er viktig i arbeidet med å forebygge dataangrep og andre uønskede hendelser i nettverk og informasjonssystemer. Indikatorene kan formidles videre av Nasjonale sikkerhetsmyndighet til andre virksomheter i samme sektor. Disse virksomhetene kan deretter søke i sine egne nettverk og informasjonssystemer. Ved funn av indikatorer kan de iverksette tiltak for å forebygge eller redusere skadeomfang. Vi ber derfor om at departementet vurderer å innta kravet om «indikatorer på kompromittering» i § 17 i forskriften.

Inga Bejer Engh
assisterende sjef PST