Remiss av delbetänkandet Nya regler om cybersäkerhet (SOU2024:18)

Fö2024/00496 Mottagare: Försvarsdepartementet

1 Sammanfattning

Skatteverket tillstyrker att förslagen genomförs. Skatteverket anser dock att man bör pröva huruvida FRA eller MSB borde få ansvaret att vara tillsynsmyndighet för sektorn offentlig förvaltning.

Skatteverket lämnar följande synpunkter på delbetänkandet.

1. Pröva huruvida FRA eller MSB borde få ansvaret att vara tillsynsmyndighet för sektorn offentlig förvaltning
2. Säkerställ hantering av insamlad information
3. Förtydliga begrepp
4. Tydliggörande av lagens tillämpningsområde och gränsdragning
5. Tydliggör övervakning av tillsynsmyndigheterna
6. Tydliggör kraven kring efterlevnad och granskning
7. Tydliggör förhållandet mellan utredningens förslag och säkerhetsskydd
8. Skatteverket tillstyrker att PTS får ansvaret för tillsyn över digitala tjänster

2 Skatteverkets synpunkter

2.1 Tillsynsmyndighet för sektorn offentlig förvaltning

I och med förslaget till förordning (2024:000) om Nationellt cybersäkerhetscenter kommer FRA att få ett större åtagande kring cybersäkerhet och få ansvaret för NCSC. Med den begränsade budget som föreslås till tillsynsmyndigheterna anser Skatteverket att det är svårt för någon myndighet att snabbt komma upp till samma nivå av cybersäkerhet som FRA och MSB.

Skatteverket bedömer därför att starka praktiska, resursekonomiska och säkerhetsrelaterade skäl talar för att verksamheterna inom offentlig förvaltning sammanförs under en tillsynsmyndighet. Skatteverket rekommenderar att man lägger tillsynen på FRA eller MSB istället för föreslagen tillsynsmyndighet.

Postadress: 205 30 MALMÖ **Telefon**: 0771-567 567
skatteverket@skatteverket.se, www.skatteverket.se

2.2 Säkerställa hantering av insamlad information

Utredningen föreslår att varje tillsynsmyndighet ska inom sitt tillsynsområde upprätta ett register över väsentliga och viktiga verksamhetsutövare. [1] Med anledning av att anmälningarna till respektive tillsynsmyndighet ska innehålla en del känsliga uppgifter, behöver den information som samlas in hanteras på ett säkert sätt.

Omfattande befogenheter bör förenas med förpliktelser att på eget initiativ identifiera vilka uppgifter som ska ingå i offentliga beslut. Det finns en stor risk för exponering av teknisk lösning, organisation och driftsförutsättningar och sårbarheter som kan användas av en antagonistisk aktör i kartläggningsfas av svenska myndigheter.

Utredningen har vidare föreslagit i kapitel 1.4 i 29 § att CSIRT-enheten ska samla in och analysera forensiska uppgifter. Det finns ingen information kring hur länge verksamhetsutövare bör spara loggar och forensiska uppgifter, därför anser Skatteverket att bestämmelsen bör förtydligas i förhållande till Riksarkivets ordinarie föreskrifter. Skatteverket föreslår därför att bestämmelsen kompletteras med en minimitid om hur länge verksamhetsutövare ska spara loggar eller forensiska uppgifter.

Skatteverket har även synpunkter på den föreslagna lydelsen av bestämmelsen i 4 kap 9 § Säkerhetsskanning. Skatteverket ser så pass stora risker med genomförande av skanning av it-miljöer att en överprövningsmekanism bör införas om samråd inte leder till en samsyn mellan parterna.

2.3 Förtydliga begrepp

2.3.1 Incident

Skatteverket anser att begreppet *betydande incident* i direktivet och i betänkandet i 3 kap 4 § kan lämna för stort tolkningsutrymme.

Med betydande incident avses
1. En incident som orsakat eller ***kan orsaka*** *allvarlig driftsstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren, eller …*

En incident som ”kan orsaka” allvarlig driftstörning skulle kunna innefatta mycket och innebära otydligheter kring vad som ska rapporteras. För att minska tolkningsutrymmet bör bestämmelsen förtydligas. I NIS2 direktivet används begreppet *tillbud* som beskriver ” *en händelse som kunde ha undergrävt tillgängligheten, autenticiteten, riktigheten”,* Skatteverket föreslår därför att bestämmelsen i 4 § kompletteras med förtydligande av begreppen *incident* och *tillbud.* Det är viktigt att den som får i uppgift att meddela föreskrifter om detta klargör vad som utgör en betydande incident.

Generellt behöver det förtydligas hur olika incidenter ska hanteras när det är både säkerhetshotande händelse och det finns ett allmänt behov av omedelbar rapportering till CISRT.

[1] 6.2 Register över väsentliga och viktiga verksamhetsutövare s.177

2.3.2 Säkerhetsrevision och Säkerhetsskanning

Skatteverket anser även att begreppen ”säkerhetsrevision” och ”säkerhetsskanning” ska definieras. Båda innebär långt gående tillsynsmandat och omfattande exponering av verksamheten och särskilda risker vad avser cybersäkerhet, därför är det viktigt att innebörden är tydlig. Skatteverket förslår därför att begreppen ”säkerhetsrevision” och ”säkerhetsskanning” tydliggörs.

2.4 Tillämpningsområde och gränsdragning

Skatteverket anser att utredningens förslag innebär en gränsdragningsproblematik. Verksamhetsutövare som tillhör fler än en sektor kommer att träffas av direktivet på flera sätt, vilket kan skapa en gråzon kring hur direktivet ska tillämpas. Det kan skapa tolkningssvårigheter och problem med tillämpning av 3 kap, då verksamhetsutövare kommer att träffas av överlappande föreskrifter. För att minska problemen anser Skatteverket att det bör tydliggöras hur gränsdragningen ska ske för verksamhetsutövare som träffas av flera sektorer.

2.5 Övervakning av tillsynsmyndigheterna

Utredningen har vidare föreslagit under kapitel 1.4 i 8-12 § vilka som ska övervaka de Länsstyrelser som är tillsynsmyndigheter. Exempelvis ska Länsstyrelsen i Norrbottens län övervaka Länsstyrelsen i Stockholms län som ska vara tillsynsmyndighet för kommuner och regioner som hör till Stockholms, Uppsala, Södermanlands, Västmanlands, Värmlands, Gotlands, Örebro, Dalarnas eller Gävleborgs län och verksamhetsutövare som har sitt säte i något av dessa län samt.[2] Det är inte tydligt vem/vilka det är som övervakar de andra tillsynsmyndigheterna. Skatteverket föreslår därför att förslaget förtydligas och kompletteras med vem/vilka som ansvarar för att övervaka de övriga tillsynsmyndigheterna.

2.6 Efterlevnad och granskning

Utredningen föreslår att tillsynsmyndigheten får förelägga en verksamhetsutövare att offentliggöra information och att tillsynsmyndigheterna får besluta var ett offentliggörande ska ske och vilka uppgifter offentliggörandet ska innehålla.[3] Skatteverket ser risker med att detta kan medföra offentliggörande av känslig information. Det bör finnas förtydligande vilken typ av uppgifter som offentliggörandet bör innehålla och vilket syfte offentliggörandet har.

Utredningen har vidare föreslagit att tillsynsmyndigheten får anlita oberoende organ för att utföra säkerhetsrevisioner.[4] Skatteverket anser att det kan medföra risker att olämpliga personer får tillgång till våra system och dokument. Det är även otydligt vilka krav som ställs på ett oberoende organ, exempelvis om det krävs en viss certifiering för att genomföra revision.

När det gäller efterlevnad anser Skatteverket att det finns otydligheter kring utredningens förslag, i avsnitt 1.4 29 § punkt 2, att CSIRT-enheten ska erbjuda stöd avseende realtidsövervakning av nätverks- och informationssystem.[5] Det här kan vara svårt att genomföra då det är komplext att bygga upp en sådan förmåga. För att minska problemen

[2] 1.4 Förslag till förordning om cybersäkerhet 11 §

[3] 9.5.3 Offentliggörande av överträdelser av direktivet

[4] 4 kap. Tillsyn 8 §

[5] 1.4 Förslag till förordning om cybersäkerhet 29 § punkt 2

bör bestämmelsen förtydliga vilken hjälp man kan få för att bygga en sådan förmåga och om det avser teknik eller kompetens.

2.7 Utredningens förslag och säkerhetsskydd

Skatteverket anser att förhållandet mellan utredningens förslag och säkerhetsskydd behöver tydliggöras. Skatteverket rekommenderar att nuvarande ordning med kumulativa krav kvarstår.

2.8 Utredningens förslag och LEK

Skatteverket tillstyrker att PTS får ansvaret för tillsyn över digitala tjänster och att det tydligt och i erforderlig omfattning förs in under Lagen om elektronisk kommunikation (2022:482).

3 Konsekvenser för Skatteverket

Förslaget kommer ge ekonomiska konsekvenser för Skatteverket, dels på grund av logg, realtidövervakning, utökad utbildning och risk för oberoende revision som Skatteverket ska bekosta. Skatteverket bedömer därför att det kommer att bli kostnadsökningar men i nuläget är det inte möjligt att estimera exakt kostnadsökning för Skatteverket.