EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering (SOU 2020:58)

Fö2020/00954

1 Sammanfattning

Skatteverket ser i huvudsak positivt på det lämnade förslaget.

Vad gäller författningsförslaget föreslår Skatteverket en sanktionsmodell som till sin karaktär liknar sanktionsmodellerna i dataskyddsförordningen (EU) 2016/679. Vidare lyfter Skatteverket några överväganden gällande proportionalitet och sekretess.

Skatteverket ansluter sig också till Myndigheten för samhällsskydd och beredskaps (MSB) bedömning att det är MSB som bör utses till myndighet för cybersäkerhetscertifiering. Det huvudsakliga skälet är behovet av en samhällsövergripande organisation med god inblick i det civila samhället och civila myndigheters behov samt myndighetens potential att uppnå synergieffekter mellan olika säkerhetsområden så som totalförsvar, krisberedskap, NIS-direktivet samt informationssäkerhet.

Det föreslagna FMV/CSEC har en unik certifieringskompetens på hög nivå. Dess erfarenhet bör kunna tillvaratas för att utveckla kompetensen i samhället i stort och fungera som en expertmyndighet inom området.

2 Skatteverkets synpunkter

2.1 Nationell myndighet för cybersäkerhetscertifiering

Utredningens genomgång av potentiella myndigheter som kan utses till myndighet för cybersäkerhetscertifiering visar på svårigheten att skapa en optimal lösning utifrån befintlig myndighetsstruktur och uppdrag.

Cybersäkerhetsakten inrättas med stöd av regelverken för harmonisering av den inre marknaden och omfattar IKT-produkter, processer och tjänster. Akten omfattar såväl den stora civila marknaden med enkla IKT-produkter i vardagen med låga säkerhetskrav som avancerad försvarsmateriel och samhällskritisk infrastruktur med höga säkerhetskrav. Såväl IKT-produkter som molntjänster är dagsaktuella utifrån certifieringsperspektivet och utvecklingen går mycket fort.

Det finns ett behov av att utsedd myndighet har en bred kunskap om, förankring hos, och förmåga att hantera civila och militära myndigheter samt hela civilsamhället. Eftersom dagens regelverk inom informations- och cybersäkerhetsområdet i övrigt är splittrade finns också ett behov av samordning mellan olika regelverk. Lagstiftningen i stort pekar på att informationssäkerhet och cybersäkerhet lyder under kris-, kontinuitet och civilt försvar och

Postadress: 171 94 SOLNA **Telefon**: 0771-567 567
skatteverket@skatteverket.se, www.skatteverket.se

borde därför hamna under MBS:s myndighetsansvar. I detta beaktas även det kommande cybersäkerhetscentrets uppdrag och utveckling under perioden 2021 – 2023.[1]

Skatteverket ansluter sig därför till MBS:s bedömning att MSB bör utses till myndighet för cybersäkerhetscertifiering.

Skatteverket bedömer att den unika kompetens och erfarenhet som finns hos FMV/CSEC bör kunna tillvaratas genom myndighetssamverkan inom ramen för cybersäkerhetscentret.

2.2 Kompletterande nationella bestämmelser

2.2.1 Tillsynsbefogenheter och sanktioner

Betänkandet lämnar förslag till tvångsmedel i form av rätt till tillträde till lokaler med biträde av Kronofogdemyndigheten.[2] Tillsynsobjekten är både tillverkare, leverantörer och organ för bedömning av överensstämmelse.

Tillträde med stöd av tvångsmedel är en särskilt ingripande åtgärd. Skatteverket ställer sig därför frågande till nödvändigheten att ge rätt till tillträde med hjälp av Kronofogdemyndigheten i alla förekommande fall. Skatteverket rekommenderar i första hand mindre ingripande alternativ för tillträde hos tillverkare och leverantörer på den lägsta säkerhetsnivån. Mindre ingripande åtgärder skulle kunna vara de föreslagna åtgärderna för återkallelse av certifikat eller vite, när frivilligt tillträde inte medges av tillsynsobjekten.

Med hänsyn till den storlek på aktörer som kommer att omfattas av regelverket bedömer Skatteverket att sanktionsavgift med ett tak på 15 miljoner kronor är lågt.[3] Denna nivå bedöms inte få avsedd effekt på stora aktörer. Regelverket bör istället tillämpa samma princip som dataskyddsförordningen där sanktionsavgiften baseras på aktörens förutsättningar.

Vad gäller preskriptionstiderna följer utredningen bland annat lagstiftningen som baseras på NIS-direktivet. Då det kan ta tid innan överträdelser de facto upptäcks eller identifieras bör det övervägas om tidpunkten från vilken preskriptionstiden räknas i stället ska utgöra identifikationstillfället.

2.2.2 Sekretess

För att uppnå syftet med en hög nivå i fråga om cybersäkerhet, cyberresiliens och förtroende inom unionen samt att säkerställa en väl fungerande inre marknad krävs det att relevanta nationella organ och myndigheter sinsemellan kan ha ett ändamålsenligt och effektivt informationsutbyte. Utredningens slutsats är att det finns flera sekretessbrytande bestämmelser som kan tillämpas för att uppgifter som omfattas av sekretess ska kunna delas mellan myndigheter i samband med tillsyn och rapportering av sårbarheter. Utredningens slutsats i den här delen vilar bl.a. på en tillämpning av 10 kap. 2 resp. 27 §§ OSL. Tillämpningen av dessa bestämmelser är dock av ad hoc natur och de är inte ägnade att ligga till grund för ett förväntat informationsutbyte.

---

[1] Uppdrag om fördjupad inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter, Fö2019/01330,

[2] Lagförslaget 5 §

[3] Lagförslaget 8 §

Med hänsyn till behovet av ett ändamålsenligt och effektivt informationsutbyte mellan offentliga nationella aktörer, och med beaktande av det lapptäcke av sekretessbestämmelser som enligt utredningen kan bli tillämpliga hos myndigheterna, bör en analys av förutsättningarna för och utformningen av en uppgiftsskyldighet mellan offentliga nationella aktörer genomföras.

3 Konsekvenser för Skatteverket

Om cybersäkerhetscertifiering skulle slå igenom i samhället så medför det, förutom förbättrad cybersäkerhet, även behov av ökade tekniska investeringar och kostnader för tjänster bland andra för Skatteverket. Skatteverkets säkerhetsbehov präglas i första hand av stora kontinuerliga kommunikationsvolymer mot samhällets alla aktörer med höga krav på korrekthet och tillgänglighet.

Den svenska nationella myndigheten för cybersäkerhetscertifiering behöver därför ha förmågan att verka effektivt för civila myndigheters och företags behov såväl inom landet som inom samverkan på europeisk nivå.

Detta remissvar har beslutats av generaldirektören Katrin Westling Palm och föredragits av säkerhetsskyddsexperten Helena Rom. Vid den slutliga handläggningen har också följande deltagit: överdirektören Fredrik Rosengren och avdelningschefen Annette Backlund samt enhetschefen Pär Rylander.

Katrin Westling Palm

Helena Rom