Finansdepartementet

i.remissvar@regeringskansliet.se
kopia till: i.esd@regeringskansliet.se

2023-02-21

MB
my.bergdahl@teknikforetagen.se
08-782 08 61

Teknikföretagens remissyttrande avseende Europeiska kommissionens förslag till förordning om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020 - I2022/01758

Teknikföretagen är en bransch- och arbetsgivarorganisation som företräder svensk industri. Tillsammans står våra 4 300 medlemsföretag för en tredjedel av Sveriges export. Gemensamt för våra medlemsföretag är att de utvecklar varor och tjänster i världsklass och att nästan all försäljning sker i global konkurrens.

Teknikföretagen tackar för möjligheten att få inkomma med synpunkter på rubricerat förslag. Vi noterar dock att förslaget publicerades redan i september i fjol och att förhandlingarna kring innehållet pågår och kompromissförslag således har tagits fram och diskuterats. Nedan kommentarer från Teknikföretagen baseras emellertid, i enlighet med förfrågan, på det förslag som EU-kommissionen presenterat. Skulle regeringen vilja få Teknikföretagens kommentarer på senare kompromissförslag bidrar vi gärna med sådana.

Kommentarer till förslaget

Teknikföretagen **välkomnar EU-kommissionens förslag till horisontell lagstiftning** avseende cybersäkerhetskrav för produkter med digitala element. Vi är särskilt till freds med det faktum att förslaget baseras på NLF[1] och att tillverkare för majoriteten av produkterna kan göra en egen bedömning av överensstämmelse (självvalidering) i stället för att behöva genomföra en tredjepartsbedömning. Det finns emellertid **behov att förtydliga** hur detta föreslagna regelverk samverkar med andra regler på området och säkerställa att det inte uppstår överlapp eller i värsta fall motstående regler. I detta avseende är det väsentligt att det blir klarhet kring hur förslaget förhåller sig till den delegerade akt om cybersäkerhet som utarbetas på basis av radioutrustningsdirektivet, RED[2]. Vidare bör det

[1] New Legislative Framework, se: New legislative framework (europa.eu)

[2] 2014/53/EU

Teknikföretagen
Box 5510, 114 85 Stockholm
Storgatan 5, Stockholm
Telefon 08-782 08 00
www.teknikforetagen.se

säkerställas att tidsfrister för rapportering överensstämmer med bl.a. reglerna i NIS2[3].

Enligt förslaget ska produkter (och inte tjänster) omfattas. Det nu föreslagna regelverket är dock inte helt tydligt i detta avseende och det finns t.ex. skäl att se över definitionen av fjärrbehandling av data.

Teknikföretagen noterar också att det i art 2 p 5 anges att regelverket inte ska vara tillämpligt på produkter som utvecklats *uteslutande* för ändamål som rör nationell säkerhet etc. Många produkter utvecklas emellertid för att kunna användas av såväl civila som militära ändamål (***dual use***) varför ett sådant undantag skulle kunna påverka konkurrensförhållanden mellan producenter till produkter som till sin natur är likartade men har utvecklats mot olika kundsegment. I detta sammanhang bör det också säkerställas att definitionen av begreppet *nationell säkerhet* är tydlig och överensstämmer med andra relevanta lagstiftningar.

Enligt förslaget kan produkter med digitala element enkelt uttryckt delas upp i två kategorier. En större grupp där tillverkarna kan göra en självvalidering om produkterna uppfyller cybersäkerhetskraven. Den andra guppen består av *kritiska produkter med digitala element*, vilkas överensstämmelse med kraven ska bedömas av en utomstående part. I artikel 6 regleras närmare vad som ska beaktas för att en produkt ska anses vara kritisk. Enligt Teknikföretagens bedömning är formuleringen här alltför vid. Det kan till exempel inte rimligen vara så att alla produkter som är avsedda att användas i *industriella miljöer* (se paragraf 2 punkten b)) ska anses vara kritiska. Här **behövs ett riskbaserat förhållningssätt** och omfånget behöver begränsas och tydliggöras.

Teknikföretagen anser därför att

i) det ska krävas att åtminstone två av kriterierna i 6.2 a) uppfylls, samt
ii) ii) 6.2 b) stryks. Generellt sett behövs ett riskbaserat förhållningssätt utifrån hur produkterna används. Här ser Teknikföretagen att den riskbedömning (*risk assessment*) som redan nu krävs för alla produkter som självdeklareras enligt NLF med fördel borde användas.

När det gäller anmälningar av incidenter och sårbarheter behöver **tidsfristen** förlängas utöver 24 timmar. Vidare måste kravet på anmälningar begränsas till betydande incidenter eller incidenter som leder till en betydande cybersäkerhetsrisk. I linje med detta behöver det också justeras i bilaga 1 avsnitt 1 punkt 2 så att det framgår att kravet på att produkter är att de ska levereras utan kända *kritiska eller allvarliga* sårbarheter.

Vidare är det viktigt att förtydliga att kraven i art 10.4 vad gäller integrering av **komponenter från tredje part** ska förstås i kontext med NIS2 och blåboken om genomförande av EU:s produktbestämmelser (*Blue Guide*[4]).

För att säkerställa att standardiseringsorganisationerna ges rimligt förutsättningar att utarbeta **standarder** är det viktigt att de ges tillräckligt med tid men också att

[3] 2022/2555

[4] 2022/C 247/01

de får tydliga beställningar. Det finns redan ett antal internationella standarder på området att beakta för standardiseringsorganisationerna och det är viktigt att de harmoniserade standarder som utarbetas inom ramen för detta regelverk i så hög utsträckning som möjligt är förenliga med dessa för att ge europeiskt näringsliv förutsägbarhet och konkurrenskraft. De är centrala för företagens möjlighet till regelefterlevnad och självvalidering och tydliga standarder möjliggör att vi tillverkare kan undvika flaskhalsproblematik vid tredjepartsbedömningar. Enligt Teknikföretagen bör *gemensamma specifikationer* inte användas annat än i yttersta undantagsfall och då i linje med standardiseringsförordningen[5] och särskilt de grundprinciper som denna hänvisar till.[6]

Vad gäller **genomförandetiden** anser Teknikföretagen att denna måste utökas till 48 månader för att ge marknadsaktörerna realistisk tid och möjlighet att uppfylla alla krav från en ny och övergripande lagstiftning. Med en sådan tidshorisont ges också bättre möjlighet för att standarder ska komma på plats och kunna användas av tillverkarna vid självvalidering.

I tillägg till ovan kommentarer om förslaget vill Teknikföretagen också understryka vikten av att på såväl nationell som EU-nivå arbeta vidare med **kompetensfrågan**. Det finns redan ett underskott på kompetens inte minst inom cybersäkerhetsområdet. Det nu aktuella förslaget kommer, i kombination med annan lagstiftning med samma fokus, att öka behovet av kompetens. Inte bara hos tillverkarna utan också hos många fler aktörer som t.ex. de marknadskontrollmyndigheter som ska tillsyna efterlevnaden, hos standardiseringsorganisationer som ska ta fram standarder och hos organ som ska genomföra tredjepartsbedömningar m.fl. Det är därför angeläget såväl att kompetensfrågan uppmärksammas som att de regler som beslutas är proportionerliga med rimliga åtgärder och inte går utöver vad som krävs för att uppnå målen.

--

För Teknikföretagen,

Maria Rosendahl
Näringspolitisk chef

My Bergdahl
Näringspolitisk expert

[5] 1025/2012

[6] Skältext 2; ”de principer som erkänts av Världshandelsorganisationen (WTO) i fråga om standardisering, nämligen enhetlighet, insyn, öppenhet, samförstånd, frivillig tillämpning, oberoende i förhållande till särintressen samt effektivitet (nedan kallade grundprinciperna)”