Datum
2023-02-21

Er referens
I2022/01758
Vår referens
FS

TechSverige

Finansdepartementet

i.remissvar@regeringskansliet.se

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

Remissvar avseende Europeiska kommissionens förslag till förordning om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020

TechSverige har beretts tillfälle att lämna ett remissyttrande över rubricerat förslag (dnr I2022/01758).

TechSverige är en bransch- och arbetsgivarorganisation för företag inom techsektorn med drygt 1 400 medlemsföretag – som sammantaget har närmare 100 000 medarbetare i Sverige. TechSverige ingår i förbundsgruppen Almega och därmed i Svenskt Näringsliv.

Synpunkter på förslaget

TechSverige välkomnar att förslaget baseras på New Legislative Framework (NLF) och att tillverkare kan göra självvalidering, i stället för att behöva använda tredjepartsbedömningar, för majoriteten av produkterna. Det finns dock behov av att förtydliga hur de föreslagna reglerna förhåller sig till annan lagstiftning för att undvika överlappning eller konflikter mellan regelverken. Reglerna för tidsfrister för rapportering bör överensstämma med till exempel motsvarande regler i NIS2. Ett riskbaserat tillvägagångssätt är centralt och måste utgå från avsedd användning av produkten. Detta gäller till exempel sårbarhetskrav, sårbarhetshantering och rapportering av sårbarheter.

Enligt förslaget ska produkter, men inte tjänster, omfattas. Det nu föreslagna regelverket är dock inte helt tydligt och det finns skäl att undantaget för Software as a Service (SaaS) och fjärrdatabehandling behöver förtydligas. Sådant har tidigare inte reglerats under NLF. Undanta maskinvara, programvara och tjänster som används för bearbetning, överföring och lagring av fjärrdata för att undvika överlappning med NIS2 ((EU) 2022/2555).

Säkerhetskrav

Konceptet att släppa ut en produkt på marknaden "utan någon känd sårbarhet som kan utnyttjas" är inte riskproportionerligt, eftersom upprätthållandet av en tillräcklig cybersäkerhetsnivå är en process som måste vara riskbaserad. Dessutom kan en produkts cyberresiliens och därmed förekomsten av en sårbarhet påverkas av många faktorer, inklusive produktens distributionsmiljö.

För att nå lagstiftning som minskar cybersäkerhetsincidenter med påverkan på en produkts säkerhet måste den vara tillämpbar i olika sammanhang. Till exempel skiljer sig sårbarheter avsevärt åt beroende på om det gäller telekomnät, företag, eller konsumenters hantering av IoT-produkter. Även om det är viktigt att ta itu med sårbarheter skulle det inte vara ett realistiskt mål att åtgärda alla sårbarheter på grund av kostnad och teknisk genomförbarhet. Fokus bör därför ligga på att minimera cyberincidenter och inte minimera förekomsten av alla former av sårbarhet. Därför är det viktigt att de essentiella kraven begränsas till svagheter (vulnerabilities) som är kritiska eller signifikanta enligt

definitioner etablerade i existerande standarder så som till exempel CVSS. Vidare ska det fortsatt vara möjligt för leverantörerna att leverera uppdateringar (som felkorrigeringar) separat eller som en del av en funktionell uppdatering av program. För komplexa system skall det fortsatt vara möjligt att integrera korrigeringar enligt gällande industripraxis mot ersättning.

Tidsfrister

Tidsfristen för anmälningar av incidenter och sårbarheter behöver förlängas utöver 24 timmar. Kravet på anmälningar bör begränsas till betydande incidenter eller incidenter som leder till en betydande cybersäkerhetsrisk.

Standarder

Det finns redan ett antal marknadsdrivna internationella standarder på området. De harmoniserade standarder som tas fram med hänvisning till det föreslagna regelverket måste, i så hög utsträckning som möjligt, vara förenliga med dessa för att ge näringslivet i EU förutsägbarhet och konkurrenskraft. Det är av stor betydelse för företagens möjlighet till att följa regler och att använda självvalidering. Tydliga standarder möjliggör att tillverkare kan undvika kapacitetsbegränsningar som kan uppkomma för tredjeparts-bedömningar. Gemensamma specifikationer ska inte användas annat än i undantagsfall. Goda möjligheter till marknadstillträde i tredjeland bör också vara en faktor när standarder och validering regleras.

Kompetensförsörjning

Ett stort utbud av produkter omfattas av CRA och kapaciteten för en tredjepartsbedöm-ning av överensstämmelse kan ge upphov till betydande flaskhalsar och arbetsbelastning både hos företagen och bedömningsorganen. Både i Sverige och inom övriga EU råder det kompetensbrist inom digitalisering, inte minst inom informations- och cybersäkerhet. Detta förslag, tillsammans med flera andra, kommer att öka behovet av kompetens och riskerar att öka kompetensbristen om inte åtgärder vidtas. Kompetensbristen kommer att drabba tillverkare, men också andra aktörer som till exempel marknadskontrollmyndig-heter och organ som ska genomföra tredjepartsbedömningar. Utöver att kompetens-försörjningen måste lösas, så måste de regler som beslutas vara proportionerliga och väl avvägda för att inte gå utöver vad som krävs för att uppnå målen.

Tid för genomförande

Tiden för genomförande bör utökas till 48 månader för att underlätta standardiserings-arbetet och undvika flaskhalsar vid tredjepartsbedömning.

För TechSverige

Fredrik Sand
näringspolitisk expert