SVENSKT NÄRINGSLIV

Finansdepartementet

i.remissvar@regeringskansliet.se
i.esd@regeringskansliet.se

Vår referens/dnr:

SN

Er referens/dnr:

I2022/01758

2023-02-21

Remissvar

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

Svenskt Näringslivs anser att:

1. Det är viktigt att förslaget baseras på NLF och att bedömning av överensstämmelse (självvalidering) kan göras för så många produkter som möjligt.

2. Förslagets tillämpningsområde är viktigt för motståndskraften (cyberresliensen) i produkter, men undantaget för Software as a Service (SaaS) och fjärrdatabehandling behöver förtydligas. Undanta maskinvara, programvara och tjänster som används för bearbetning, överföring och lagring av fjärrdata för att undvika överlappning med NIS2 ((EU) 2022/2555).

3. Ett riskbaserat tillvägagångssätt är centralt och måste utgå från avsedd användning av produkten. Detta gäller till exempel sårbarhetskrav, sårbarhetshantering och rapportering av sårbarheter. Det ska krävas att åtminstone två av kriterierna i artikel 6.2 a) uppfylls. Artikel 6.2 b ska strykas. Kraven ska begränsas till svagheter (vunlerabilities) som är kritiska eller signifikanta enligt definitioner etablerade i existerande standarder så som tex CVSS. Den riskbedömning (risk assessment) som redan nu krävs för alla produkter som självvalideras enligt NLF med fördel borde användas.

4. Anmälning av incidenter och sårbarheter behöver förlängas och överensstämma med motsvarande krav i till exempel NIS2 och GDPR på 72 h. Anmälningsplikten bör begränsas till betydande incident eller incident som leder till betydande cybersäkerhetsrisk.

Svenskt Näringsliv Confederation of Swedish Enterprise
Postadress/Address: SE-114 82 Stockholm Besök/Visitors: Storgatan 19 Telefon/Phone: +46 (0)8 553 430 00
svensktnaringsliv.se Org. Nr: 802000-1858

5. Marknadsdrivna internationella standarder och harmoniserade standarder ger förutsägbarhet och konkurrenskraft. Dessutom är de centrala för inte minst SME:s möjlighet till regelefterlevnad och bedömning av överenstämmelse (självvalidering). Självvalidering i sin tur är viktigt för att undvika flaskhalsproblematik vid tredjepartsbedömningar. Gemensamma specifikationer ska inte användas.

6. Tillämpningen av förslaget behöver utökas till 48 månader för att ge tillverkarna skälig tid och möjlighet att uppfylla alla krav från ny övergripande och sektoriell lagstiftning. 48 månader är också en realistisk implementeringsperiod för att både harmoniserade standarder ska komma på plats och sedan användas av företagen i självbedömningen.

INLEDANDE KOMMENTARER

Ett av målen med CRA är att skapa konkurrensfördelar för företag i Europa. För att nå det målet måste onödig byråkrati och onödig börda undvikas. Förslaget behöver kombineras med en stärkt riskhantering för cybersäkerhet, adekvat kompetens och säker och robust infrastruktur. De nya lagar som antagits inom ramen för EU:s strategi för cybersäkerhet kommer ge resultat, men också konsekvenser både för företagens och tillsynsmyndigheternas kapacitet.

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. Svenskt Näringsliv vill därför understryka behovet av en proportionerlig lagstiftning med en riskbaserad metod. Säkerhetsarbetet måste inriktas på att ta itu med kritiska och allvarliga sårbarheter. Fokus bör därför ligga på att minimera cyberincidenter och inte minimera förekomsten av alla former av sårbarhet.

Dessutom bör Europa i största möjliga utsträckning utnyttja internationella standarder och marknadsdrivna initiativ för att stärka konkurrenskraften. Därför bör framtida harmoniserade standarder så långt det är möjligt baseras på befintligt internationellt standardiseringsarbete och avtal om ömsesidigt erkännande bör eftersträvas med tredjeländer. Cybersäkerhet är en global utmaning, en kontinuerlig process och inte ett fast tillstånd i en produkt.

Svenskt Näringsliv instämmer i att cybersäkerheten behöver stärkas i samhället och företagen kommer bidra i stor omfattning. Inte minst med NIS2-direktivet där kraven ökar betydligt på många företag. Myndigheter som arbetar med cybersäkerhet behöver stödja företagens arbete genom informationsdelning och kunskapsöverföring. Det nationella cybersäkerhetscentret bör skyndsamt stärka samverkan med näringslivet med framtagande av rutiner för kommunikation av lägesbild samt information om hantering av cyberangrepp.

BALANSERADE BESTÄMMELSER

På många sätt kommer den övergripande strategi som bygger på NLF att underlätta efterlevnaden. Denna välfungerande regleringsprocess gör det möjligt att täcka olika nivåer av nödvändiga skyddsåtgärder, baserat på produkternas riskprofil och deras avsedda tillämpning.

Vi välkomnar förtydligandet i **artikel 16 om att en väsentlig ändring** (substantial modification) av en produkt som görs av en fysisk eller juridisk person (annan än en tillverkare, importör eller distributör) omfattas av skyldigheter. Detta är en viktig del eftersom det överlåter åt den fysiska eller juridiska personen att välja hur de vill använda och ändra sin produkt, och till och med potentiellt marknadsföra den som en ny produkt.

Av konkurrensskäl är det av avgörande betydelse och välkommet att de anmälda organen tillämpar förfarandena för bedömning av överensstämmelse utan att skapa onödiga bördor för de ekonomiska aktörerna, i linje med avsikten i **artikel 37**.

Den öppna marknadsekonomin gör det möjligt att sälja europeiska produkter utanför EU samt importera produkter från tredje land. Detta ger kunder valmöjligheter och en sund konkurrens. Det är därför mycket viktigt att avtal om ömsesidigt erkännande med tredje land om bedömning av överensstämmelse kan ingås för de produkter som regleras i förslaget. Detta kommer att underlätta handeln och stärka cybersäkerheten på den inre marknaden och globalt. Den inre marknaden bygger också på ett effektivt standardiseringssystem som bör anpassas till internationella standarder för att möjliggöra handel, samarbete och interoperabilitet inom och utanför unionen.

FÖRSLAG PÅ FÖRBÄTTRINGAR

Svenskt Näringsliv anser att lagstiftarna borde fokusera på att ytterligare klargöra definitioner, tillämpningsområde, riskkategorisering och överensstämmelse med andra regler.

TILLÄMPNINGSOMRÅDE OCH DEFINITIONER

Det är mycket viktigt att ha konsekventa definitioner. I artikel 3 måste definitionen av "produkt med digitala delar" förtydligas. Enbart CRA skiljer mellan fyra typer av produkter med digitala element: i) produkter med digitala element, ii) kritiska produkter i klass 1 med digitala element; iii) Kritiska produkter av klass 2 med digitala element. och (iv) mycket kritiska produkter med digitala element. Det är uppenbart att denna differentiering syftar till bättre riskkategorisering och produktidentifiering, men det är otillräckligt för att skapa den klarhet som krävs för att undvika överlappningar eller förväxlingar med NLF-baserade förordningar som ska förhandlas fram eller tillämpas parallellt, såsom AI-akten och maskinförordningen.

I artikel 3.1 definieras dessutom tydligt "produkter med digitala element" som "varje programvaru- eller hårdvaruprodukt och dess lösningar för behandling av fjärrdata, inbegripen programvara eller hårdvarukomponenter, som ska släppas ut på marknaden separat". I skäl 9 anges dock att förslaget inte omfattar programvara som en tjänst (SaaS) utom "för lösningar för databehandling på distans".

Svenskt Näringsliv förespråkar arr utesluta programvara som en tjänst (SaaS), med tanke på att

i) NLF inte har tillämpats på tjänster och det kommer att bli ett nytt område, och

ii) NIS2-direktivet redan föreskriver en skyldighet för molntjänstleverantörer (inklusive SaaS) att genomföra cyber- och riskhanteringsåtgärder, eftersom

de betraktas som leverantörer av samhällsviktiga tjänster.

Uteslutandet av programvara med öppen källkod som inte används i samband med kommersiell verksamhet behöver också förtydligas. I skäl 10 anges vad som ska förstås som kommersiell verksamhet för programvara, men det utvidgas till att omfatta tekniska supporttjänster, som verkar omfatta SaaS. Här behövs ett förtydligande eller vägledning om hur ansvarskraven för programvarukomponenter med öppen källkod kan implementeras i programvara. Programvara med öppen källkod bör hanteras på ett enhetligt sätt oavsett om den är kopplad till en kommersiell verksamhet eller inte.

Definitionen av "väsentlig ändring" bör överenstämma med Blue Guide (2022) och den nyligen reviderade maskinförordningen. I detta syfte ehöver skäl 22 anpassas till artikel 3.31.

Det bör undvikas att varje programvaruversion kräver att produkten genomgår en ny bedömning av överensstämmelse, eftersom detta skulle vara en oproportionerlig börda för utvecklaren och även försena uppdateringarna. Blue Guide klargör att väsentliga ändringar måste bedömas från fall till fall, men för CRAs stora omfattning av produkter kanske detta inte är tekniskt genomförbart?

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. Jämför till exempel skillnaden i miljö för konsumentprodukter eller B2B-systemlösningar.

Alla sårbarheter har samma inverkan och utgör inte någon betydande cybersäkerhetsrisk enligt definitionen i artikel 3 (36). I linje med OECD:s slutsatser finns det inget sätt att eliminera alla sårbarheter. 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. Därför bör syftet vara att minimera cyberincidenter genom att åtgärda de kritiska sårbarheterna (poängsätts av till exempel den globalt erkända CVSS-systemstandarden).

Åtgärder i form av en säkerhetsuppdatering är en rimlig förväntan, men att gratis genomföra en krävande uppdatering för komplexa produkter och system står i strid med nuvarande branschpraxis. I konsumentmiljöer accepterar användarna att en uppdatering resulterar i att enheterna inte är tillgängliga, vilket inte är fallet med många kritiska infrastrukturer. Därför bör förslaget vara proportionerligt och undvika ett generellt införande av kostnadsfri uppdatering. I punkt 8 i bilaga 2, avsnitt 2, bör "kostnadsfritt" kompletteras med "kostnadsfritt eller till en rättvis, transparent och icke-diskriminerande kostnad" som har använts i förordning (EU) 2019/424 om ekodesignkrav för servrar och datalagringsprodukter. Detta skulle vara i linje med befintlig branschpraxis för säkerhetsuppdateringar inom komplexa produkter utan att riskera att splittra marknaden.

Dessutom är det nästan omöjligt att frikoppla säkerhetsuppdateringar från vanliga programvaruuppgraderingar i samband med komplexa system och nätverk i motsats till konsumentprodukter. Jämför bilaga 1, avsnitt 1, punkt 3 k.

RISKKATEGORISERING OCH ÖVERENSSTÄMMELSE

Fokuserar på den avsedda användningen av produkter. Detta är nödvändigt eftersom en produkt kan utföra en mer kritisk eller mindre kritisk funktion beroende på den specifika applikationsmiljön. Till exempel, ur industrins synvinkel, gör det en väsentlig skillnad när det gäller kritiken av samma mikroprocessor om den används i en kaffemaskin eller en router.

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 tredje part. I **artikel 6** regleras närmare vad som ska beaktas för att en **produkt ska anses vara kritisk**. För att artikeln ska vara relevant behövs en riskbaserad bedömning, omfånget begränsas och tydliggöras. Att till exempel alla produkter som användas i industriella miljöer (se paragraf 2 punkten b)) ska anses vara kritiska är orimligt.

Ett stort utbud av produkter omfattas av CRA och kapaciteten för en tredjepartsbedömning av överensstämmelse kan ge upphov till betydande flaskhalsar och arbetsbelastning både hos företagen och bedömningsorganen.

Europeiska och nationella lagstiftare håller för närvarande på att genomföra eller ännu inte införliva ett mycket brett regelverk för cybersäkerhet (NIS2, DORA, sektorsspecifika regler). Inom de förutsebara framtida produktspecifika ordningarna för cybersäkerhetscertifiering, som härrör från cybersäkerhetsakten (till exempel Cloud Scheme (EUCS) och 5G Scheme (EU5G)). Det är därför mycket viktigt att undvika alla former av överlappningar och inkonsekvenser i lagstiftningen. I detta syfte rekommenderar vi starkt att ENISA och kommissionen begränsar utvecklingen av nya system för cybersäkerhetscertifiering enligt cybersäkerhetsakten (CSA) till vad som är absolut nödvändigt.

För att säkerställa rättslig klarhet måste cybersäkerhetskraven i en harmoniserad standard dessutom ha företräde om det finns en konflikt mellan CRA och en annan (befintlig) lagstiftning.

Även om utarbetandet av gemensamma specifikationer i artikel 19 är avsett som en reservåtgärd är det inte uppenbart att det i detta skede är nödvändigt att över huvud taget ha en sådan möjlighet inom den första övergripande lagstiftningen om cybersäkerhetskrav för produkter. Att stryka detta alternativ kommer stärka incitamentet för marknaden att utveckla standarder som är smidiga och resultatinriktade, särskilt när det gäller att uppfylla de övergripande kraven i denna förordning.

ÖVERENSSTÄMMELSE MED ANNAN LAGSTIFTNING

Det är centralt att CRA inte medför överlappning av cyberkraven på en viss produkt. En produkt, som ges en specifik tillämpning, bör omfattas av en uppsättning cybersäkerhetskrav. Detta är kommissionens avsikt att upprätthålla väsentligen likvärdiga krav för produkter i förordningen om allmän produktsäkerhet (GPSR), AI-akten och maskinförordningen (MR) i förhållande till CRA. Vi föreslår att endast CRA ska tillämpas för de produkter som täcks av nämnda regleringar. Dessutom bör ny *lex specialis* alltid bygga på samma principer som CRA.

CRA innehåller rapporteringsmekanismer som kommer att leda till snabbare åtgärder för de berörda produkterna. Det måste dock betonas att rapportering är en betungande uppgift, eftersom det är tidskrävande att samla in information. Incidenthantering och åtgärder måste ha prioritet. Rapporteringskraven bör överensstämma med NIS2-direktivet och GDPR och justeras till 72h.

När det gäller sårbarhetsmeddelanden (vulnerability notifications) bör det observeras att en sårbarhet kan utnyttjas aktivt i flera månader utan att tillverkaren är medveten om det. Eller så kan en sårbarhet identifieras månader efter att en incident hade inträffat. Därför är det nödvändigt med anpassning till NIS2-direktivet, särskilt med tanke på ENISAs kommande sårbarhetsdatabas, det frivilliga offentliggörande av sårbarheter som föreskrivs i det reviderade direktivet och informationen i slutrapporten efter en incident, som också kommer att beskriva vilken sårbarhet som ledde till den. Företagen bör inte vara skyldiga att rapportera samma information flera gånger.

Skyldigheten till sårbarhetsrapportering begränsas till att endast omfatta de sårbarheter som "aktivt utnyttjas av en illvillig aktör", utgör en "betydande cyberrisk" och "en hög risk för den inre marknadens funktion". Förutom ändringarna i artikel 11 behöver skäl 34 ändras, eftersom det står att "varje utnyttjad" sårbarhet bör betraktas som ett hot mot den inre marknaden, vilket är oproportionerligt och inte i linje med den riskbaserade metod som används i hela förordningen om kreditvärderingsinstitut.

Den obligatoriska sårbarhetsrapporteringen ska följa etablerade principer för ansvarsfullt samordnat offentliggörande av sårbarheter. Inrätta ett system för riskvärdering av sårbarhet baserat på objektiva kriterier och i synergi med etablerade poängsättningsmetoder såsom CVSS. För tidiga åtgärder kan ha en negativ effekt och leda till större cyberexponering och mindre motståndskraft.

Det främsta målet för EU:s insatser för cyberresiliens bör vara att stödja marknadsaktörerna och möjliggöra en snabb begränsning av en incident eller en aktivt utnyttjad sårbarhet av en illvillig aktör som utgör en betydande cyberrisk.

För att uppfylla säkerhetsmålen med förslaget behövs rätt balans mellan möjliggöra av nödvändigt informationsutbyte mellan tillverkare och tillsynsmyndigheter, utan att ytterligare utsätta produkter för skadliga angrepp genom att begära att sårbarheten avslöjas när korrigeringar inte finns tillgängliga.

Ett helt digitalt informationsflöde och en säker rapportering måste upprättas både till ENISA och mellan ENISA, behöriga nationella myndigheter och marknadskontrollorgan. Tillverkare av produkter med digitala inslag ska bara behöva rapportera en gång inom EU. Effektiva rapporteringsmekanismer som säkerställer engångsprincipen för uppgiftslämnande är avgörande för företag ska kunna lägga sin tid främst på incident- och sårbarhetshantering och inte på att rapportera samma information till olika nationella institutioner och EU-institutioner.

SVENSKT NÄRINGSLIV
Carolina Brånby