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

Diarienummer: I2022/01758

Gemensamt remissvar Internetstiftelsen & Netnod

Om Internetstiftelsen
Internetstiftelsen är en oberoende, affärsdriven och allmännyttig organisation. Vi verkar för ett internet som bidrar positivt till människan och samhället.

Vi är en stiftelse och vår urkund slår fast att vi ska säkerställa en stark och säker infrastruktur för internet som tillgodoser dagens och framtidens behov i Sverige samt främja forskning, utbildning och undervisning med inriktning på internet. Vi ansvarar för internets svenska toppdomän .se och sköter även drift och administration av toppdomänen .nu. Intäkterna från affärsverksamheten finansierar en rad satsningar i syfte att möjliggöra att människor kan nyttja internet på bästa sätt och att ge kunskap om internetanvändningen i Sverige samt digitaliseringens påverkan på samhället. Vi tillhandahåller evenemang och utbildningsinsatser som gör det enklare att förstå och använda internets tjänster och som bidrar till ökad kompetens och fler möten som främjar internetinnovation. Vi stöttar även olika fristående uppdrags- och forskningsprojekt som på olika sätt gynnar internets utveckling och ger förutsättningar för internetentreprenörer och utvecklare att ta steget från idéstadie till färdig produkt eller tjänst. Med våra identitetsfederationer förenklar vi inloggning och höjer säkerheten i identitets- och kontohantering för både användare och leverantörer av olika tjänster inom skola, hälso- och sjukvård.

Om Netnod
Netnod är organiserat som ett aktiebolag helägt av Stiftelsen för telematikens utveckling. Netnod tillhandahåller tjänster på marknadsmässig grund och verkar för ett robust och öppet Internet.

Netnod driver nationella Internetknutpunkter i Norden, tillhandahåller tjänster för tid och frekvens, och erbjuder sekundära domännamnstjänster på global nivå. Bland annat är Netnod en auktoritär tillhandahållare av den svenska toppdomänen .se på Internet och driver en av världens tretton rotnamnserveridentiteter. Netnod distribuerar även svensk tid på uppdrag av Post- och telestyrelsen.

Nedan benämns Internetstiftelsen och Netnod även som “vi”.

Övergripande synpunkter

Förslaget till förordning om övergripande cybersäkerhetskrav för produkter med digitala element har till syfte att stärka cybersäkerhetsreglerna för att säkerställa säkrare maskin- och programvaruprodukter.

Internetstiftelsen och Netnod arbetar aktivt och förebyggande med cybersäkerhet och har djupa kunskaper inom området. Det är av synnerlig vikt att arbete med cybersäkerhet sker kontinuerligt och genomsyrar alla relevanta verksamheters arbete.

Det finns problematik med föreslagna lagförslag då den enligt Internetstiftelsen och Netnod är vag och bred vilket riskerar att skapa mer skada än nytta. Vi utvecklar vårt resonemang gällande detta nedan.

En lagstiftning på detta område skulle riskera att innebära att alla aktörer är tvungna att leva upp till kraven i regelverket, vilket för organisationer med begränsade resurser riskerar att innebära att man inte väljer metod av levernatören bedömd effektivitet (det vill säga säkerhet per krona enligt aktören själv), utan snarare metod utifrån vad lagstiftningen kräver, för att på så sätt undvika skadeståndsanspråk. Med andra ord, aktörer kommer att börja med certifiering även om de själva tycker att en annan metod hade haft en större effekt på cybersäkerheten.

IT-incidenter i samhället har gjort att cybersäkerhet har hamnat högt upp på listan hos många organisationer, även hos lagstiftaren, vilket i sig är positivt. Men det bör vara upp till respektive aktör att fritt välja metod för att lösa säkerhetsfrågor, och lagstiftningen ska fokusera på att utkräva ansvar om aktören inte lyckats lösa säkerhetsproblematik för produkter, med rimlig proportionalitet.

Certifiering bör vara frivillig och det bör vara upp till beställaren att ange om detta ska krävas, exempelvis i en upphandling.

Skillnaden mellan tekniska beroenden och affärsrelationer
Vi vill även belysa att föreslagen lagstiftning innebär implicit att alla tekniska beroenden åtföljs av en affärsmässig relation, vilket i praktiken inte alltid stämmer.

***Ett konkret exempel*:** Person1 har utvecklat ett programvarubibliotek för att hämta resurser på Internet som hen gör tillgängligt för alla. Det här programvarubiblioteket har blivit mycket populärt och används idag av miljarder av enheter, allt från lastbilar till mobiltelefoner till mikrovågsugnar till ringklockor till radiomaster, men personen har aldrig tagit betalt eller tjänat några pengar på att hen har utvecklat biblioteket. Nu börjar Person2 sälja supporttjänster för biblioteket och är något av en expert på hur man kan använda biblioteket optimalt. Person2 har ingen relation överhuvudtaget till Person1. En oklarhet uppstår här, kan programvarubiblioteket anses vara i en kommersiell kontext för att det finns en kommersiell kontext runt biblioteket, även fast kontexten inte har något att göra med bibliotekets skapare? Om skadestånd blir aktuellt, vem är det som är skadeståndsskyldig, Person1 för att hen utvecklar biblioteket, eller Person2 för att hen säljer tjänster kring biblioteket? Eller biltillverkaren Bil1 som inkluderar biblioteket i programvaran i sin produkt?

Som exemplet ovan illustrerar är det problematiskt med skadeståndsansvar i frågor som rör öppen källkod, och det är även problematiskt i de generella produktfallen då produkter och komponenter idag medvetet levereras med säkerhetsbrister.

***Ett konkret exempel*:** Flertalet processorer, dvs den centrala beräkningsenheten i datorer som är en Klass II produkt enligt Bilaga III, levereras idag med kända sårbarheter[1]. Dessa sårbarheter är kända och är något som operativsystemen, dvs den programvara som körs närmast processorn, får ta höjd för och hantera. Dessa sårbarheter hanteras av operativsystem, exempelvis Windows och Linux, inte av processorn själv eller ens av producenten av processorn. Nuvarande formulering förbjuder en del processortillverkare att sälja processorer, och vi tror inte att det är vad lagstiftaren är ute efter. Det är snarare en norm att man med *security by design* ser till att en produkt slutligen är säker även om dess beståndsdelar inte individuellt har säkrats upp. Detta innebär inte att komponenterna är osäkra, utan att de inte explicit har bedömts var säkra.

Däremot är det rimligt med strängare formuleringar när produkter säljs till konsumenter, men dessa får inte vara krav på affärer mellan juridiska personer.

---

[1]Exempelvis Meltdown (CVE- 2017-5754) och Spectre (CVE-2017-5753 och CVE-2017-5715) är två kända sårbarheter som fanns hos processorer under tiden de fanns tillgängliga marknaden.

Tillämpningsområde

Undantaget för programvara med öppen källkod välkomnas, men det behöver uppmärksammas att undantaget endast gäller programvara med öppen källkod som utvecklas eller tillhandahålls utanför ramen för kommersiell verksamhet. Denna formulering lämnar ett stort utrymme för tolkning av vad som exakt utgör kommersiell verksamhet, särskilt när man tar hänsyn till det faktum att avgifter för tekniska stödtjänster anses vara kommersiell verksamhet, liksom förhållandet att tjäna pengar på andra tjänster som tillhandahålls via en plattform för mjuvarudelning. Se resonemang och exempel ovan.

Riskerar lagstiftning på detta område att försvåra utveckling av nya tjänster, produkter eller lösningar inom cybersäkerhet?
Vi ser en risk med att denna typ av lagstiftning i onödan kan försvåra utveckling av nya tjänster, produkter eller lösningar inom cybersäkerhet.

Vi ser att all teknikutveckling, inklusive öppen källkod, kommer att påverkas av lagförslaget. I sak anser vi att leveransform inte ska påverka lagförslagets tillämplighet. I nuvarande formulering täcks tjänster som i allt väsentligt är mjukvara som levereras, men inte mjukvara som erbjuds som tjänst “remote” (dvs Software as a Service, Saas) eller mjukvara som byggs på plats. Det är problematiskt att mjukvarutillverkare får incitament att paketera mjukvara på andra sätt än som *produkt på en marknad*, då detta förmodligen kommer leda till en överlag sämre granskning och kännedom av mjukvara. Överlag har även SaaS-tjänster högre livscykelkostnader än mjukvaror som produkter, vilket riskerar att negativt påverka konsumenter och slutanvändare.

Fokus på användaren
Internetstiftelsen och Netnod vill även lyfta behovet av att fokus bör ligga på användarna, och inte bara tekniken. Användare ska bli informerade om incidenter och fel som upptäcks i produkter. Detta bör göras på ett sätt som når dem och att informationen därför sprids på ett brett sätt. Det bör också göras inom viss tidsfrist.

Synpunkter på specifika artiklar

Artikel 3 Definitioner

(38) sårbarhet (vulnerability) definitionen är hämtad från direktivet om NIS2:

> *sårbarhet: en svaghet, känslighet eller brist hos IKT-produkter eller IKT-tjänster som kan utnyttjas genom ett cyberhot.*

Här finns en vaghet i innebörden. Alltför vaga och breda definitioner skapar osäkerhet vilket i sin tur kan leda till osäkerhet vid användningen. Notera även att en sårbarhet är något som per definition kan utnyttjas, vilket gör delar av regleringen svårtolkad då regleringen ibland använder begreppet “sårbarheter som kan utnyttjas” (eller liknande) och ibland “sårbarheter” utan en klausul om huruvida de kan utnyttjas.

(24) avsett ändamål*:* En stor del av digitala komponenter används inte som avsett av tillverkaren, utan de byggs med intentionen att tillverkaren inte behöver förstå hur de kan tänkas användas i ett större system. Definitionen riskerar att bli meningslös då den inte kan definieras av tillverkaren i god tro, utan blir en sorts specifikation som specificeras för att lagstiftningen kräver det.

(25) *rimligen förutsebar användning* och *rimligen förutsebar felaktig användning* har

liknande problematik som ovan. Intentionen är med definitionerna är god, men då teknikutveckling inte sker på detta sätt är definitionerna problematiska, speciellt då de även täcker relationen en underleverantör har med en tillverkare i flera led, och inte bara ledet försäljare - privatkonsument.

Artikel 10 paragraf 4:

> *För att fullgöra den skyldighet som fastställs i punkt 1 ska tillverkarna visa tillbörlig aktsamhet när de integrerar komponenter som kommer från tredje part i produkter med digitala element. De ska säkerställa att sådana komponenter inte komprometterar säkerheten för produkten med digitala element.*

Det blir här oklart vad en skapare av mjukvara faktiskt ska göra. I praktiken är det oklart vilken typ av granskning som tillverkaren ska göra av komponenter som används. Det är dessutom oklart varför lagstiftaren väljer att specificera metod snarare än ansvar i frågan, då en tillverkare borde få välja metod för att säkerställa att deras produkt lever upp till förväntade krav.

Kommentarer på bilagor

Angående förslag i bilagorna ser vi flertalet problematiska formuleringar. Vi belyser några av dem här nedan.

Bilaga I Krav på egenskaper hos produkter

De övergripande kraven är skrivna utifrån en situation där produkter med digitala element förlorar tillgänglighet, riktighet, eller konfidentialitet om en av dessa komponenter fallerar. Detta är inte ett korrekt antagande för alla typer av produkter med digitala element. Det går att designa en produkt med digitala element med redundans och diversitet, där flertalet komponenter kan fallera innan produkten får nedsatt funktion.

> *(1) Produkter med digitala element ska utformas, utvecklas och produceras på ett sådant sätt att de säkerställer en lämplig cybersäkerhetsnivå baserat på riskerna.*

Att produkter ska anses vara säkra, i en bred definition för ett någorlunda specificerat syfte, är ett rimligt krav vid överlämning till slutkonsument, men är inte ett lämpligt krav för produkter som andra tillverkare använder som komponenter i sina produkter.

Exempelvis anses det vara god ingenjörskonst att *inte* designa utifrån ett specifikt syfte, utan att designa komponenter så tillåtande det går så att de har bredast möjliga användningsområde. Dvs, det anses god ingenjörskonst att inte begränsa komponentens funktionalitet, vilket går stick i stäv med detta krav.

Det måste finnas möjlighet för handel med komponenter och produkter som man inte rimligtvis kan bestämma en rimlig cybersäkerhetsnivå för, helt enkelt för att man inte vet hur komponenten kan tänkas användas i framtiden.

> *(2) Produkter med digitala element ska levereras utan några kända sårbarheter som kan utnyttjas.*

Krav (2) har två problem, dels att sårbarheter per definition är något som kan utnyttjas (dvs sårbarhet som kan utnyttjas är precis samma sak som sårbarheter), dels att sårbarhet är ett alldeles för vagt begrepp att använda i ett lagrum. Sårbarhet måste preciseras så att tolkningsutrymmet försvinner.

Krav (3) består av flera delkrav, varav några är välformulerade och några är omöjliga att uppnå. Särskilt behöver begrepp som “säker” (för vad?) och “obehörig åtkomst” (enligt vem?) specificeras närmare.

Säker borde rimligen innebära att *användaren* har verktyg för att verifiera en produkt med digitala elements tillgänglighet, riktighet och konfidentialitet.

Obehörig åtkomst borde rimligen vara ur *användarens* perspektiv, dvs om leverantören har access till en produkt med digitala element utan användarens explicita medgivande är detta en obehörig åtkomst.

(3c) är en problematisk punkt, den innebär i praktiken att USB-minnen måste krypteras. Detta innebär att man inte kan använda ett USB-minne mellan två enheter utan att också föra över en nyckel som är tillräckligt lång för att USB-minnet ska anses säkert ur konfidentialitetsynpunkt, vilket är problematiskt.

> *(3c) skydda konfidentialiteten för lagrade, överförda eller på annat sätt behandlade uppgifter, personuppgifter eller andra uppgifter, t.ex. genom kryptering av relevanta data i vila eller i transit med hjälp av de senaste metoderna,*

Nuvarande formulering täcker exempelvis USB-minnen, dock tror vi inte att den är tänkt att göra det eftersom konsekvenserna är problematiska.

Punkterna **(3h)**, **(3i)**, och **(3j)** är väl formulerade.

Bilaga I Krav på tillverkare av produkter

Den andra delen av Bilaga I innehåller krav på tillverkare. Överlag hanterar inte den här delen vad som händer om en tillverkare går i konkurs, eller av andra skäl inte längre agerar på den inre marknaden. En produktlivscykel tar inte slut bara för att tillverkaren inte längre existerar i samma juridiska form längre.

> *(2) när det gäller riskerna för produkter med digitala element, utan dröjsmål åtgärda och avhjälpa sårbarheter, bland annat genom att tillhandahålla säkerhetsuppdateringar,*

Krav som ovan (2), är verkningslösa om tillverkaren inte längre existerar, oavsett skäl. Det borde finnas krav på att tillverkare som lämnar marknaden, oavsett om det är på grund av konkurs eller andra skäl, ska lämna över de specifikationer som krävs, inklusive hemligheter, till exempelvis marknadskontrollmyndigheten eller annan utpekad myndighet, för att tredje part ska kunna åtgärda sårbarheter och erbjuda uppdateringar.

Oavsett formulering måste kraven hantera de fall då en tillverkare inte längre existerar, oavsett skäl, för att säkerställa att produkter med digitala element upprätthåller proportionerlig säkerhet över tid.

Bilaga III beskriver de klasser som regleringen använder sig av. Överlag kan sägas att regleringen består av fyra olika klasser;

1) **Klass 0**, “produkter med digitala element”, innebär de produkter som inte lever upp till några av kraven för Klass II, Klass III eller “mycket kritiska produkter med digitala element”
2) **Klass I**, “kritiska produkter med digitala element”, är de produkter som är uppställda i listan i Bilaga III

3) **Klass II**, “kritiska produkter med digitala element”, är de produkter som är uppställda i listan i Bilaga III
4) **Klass III**, “mycket kritiska produkter med digitala element”, är de produkter som kommissionen ges möjlighet att klassificera efter behov. Dessa tolkar vi som viktiga komponenter av NIS-tjänster.

Vi ser ett par problem med den här uppställningen, och flertalet problem i klassningen av produkter. Det övergripande problemet är dock att regleringen gör en listning snarare än lämnar ett tydligt tolkningsunderlag för var nya tänkbara produktkategorier hamnar.

Lagstiftning som rör implementationer åldras snabbt, den här regleringen måste även hålla för en värld där det finns autonoma robotar som kör själv och kan flyga, där medicinska mikrorobotar flyter runt i blodomlopp, där mjukvara består av tiotusentals komponenter, osv.

Bilaga VI går igenom processerna för kontroll, och vi tycker det är olyckligt att lagstiftaren väljer att sätta metoder istället för att lämna det upp till marknadens aktörer att organisera sig enligt regelverket och att säkerhetsfokus snarast drivs från offentligt håll genom upphandling och direkt marknadspåverkan.

Vi tror, som vi argumenterar ovan, att den här regleringen hade gjort sig bättre på nivån att förtydliga ansvarsutkrävande ex-post snarare än att sätta ett ex-ante-regelverk som behöver uppdateras ofta för att behålla sin relevans.

Resterande bilagor lämnar vi utan specifika kommentarer.

Stockholm den 21 februari 2023

Lars Michael Jogbäck, vd, Netnod AB

Carl Piva, vd, Internetstiftelsen