Remiss

Datum	Diarienummer	Ärendetyp
2023-02-21	23FMV803-2	1.3
	Dokumentnummer	Sida
	-	1(8)

Regeringskansliet
Finansdepartementet

Er referens	Ert datum	Er beteckning
	2022-11-21	I2022/01758

FMV:s yttrande avseende Europeiska kommissionens förslag till förordning om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020 (cyberresiliensakten)

Försvarets materielverk (FMV) har beretts tillfälle att yttra sig över Europeiska kommissionens förslag till förordning om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020.

FMV:s yttrande sker med utgångspunkt från dels myndighetens uppgift att upphandla och utveckla materiel och tjänster till det svenska försvaret, dels myndighetens uppgift att verka som nationell myndighet för cybersäkerhetscertifiering inom ramen för cybersäkerhetsakten.
FMV yttrande

Sammanfattning av FMV:s ståndpunkter

FMV välkomnar på många sätt ambitionen och visionen med förslaget till förordning.

En ändamålsenlig kravställning av kommersiella produkter kan, under förutsättning att den är kostnadseffektiv och ändamålsenlig, bidra till en höjning av cybersäkerheten och vara till gagn för samhället i stort, så väl för kritisk infrastruktur som för nationell säkerhet.

FMV delar förslagets målsättningar.

FMV delar synen att det är riktigt och viktigt att klargöra tillverkares ansvar, samt att kraven ska fokusera på tillverkaren och dess arbetsprocesser.

FMV stöder principen om att någon form av reglering av hur sårbarheter ska hanteras kan vara ändamålsenlig.

FMV bedömer att principen från New Legislative Framework kan vara en bra utgångspunkt. Dock förutsätter detta att standarder utvecklas som främjar den sökta förbättringen av cybersäkerheten på ett kostnadseffektivt sätt.

FMV
Försvarets materielverk
115 88 Stockholm
Besöksadress: Banérgatan 62
Tel: 08-782 40 00
Fax: 08-667 57 99
registrator@fmv.se
www.fmv.se
Org.nr: 202100-0340
VAT nr: SE202100-0340-01

Sådana standarder måste utvecklas transparent, inkluderande och konsensusbaserat för att undvika att vissa aktörer gynnas på bekostnad av andra.

FMV menar att det finns en uppenbar risk att EU:s säkerhet och konkurrenskraft försämras om inte adekvata standarder finns att tillgå. Det är nödvändigt att regleringen inte genomförs innan effektiva standarder, etablerats. I annat fall riskerar förordningen att skapa en situation med ojämn rättstillämpning mellan olika medlemsstater och därmed få en motsatt effekt till vad som är förordningens syfte.

FMV:s menar därutöver att:

- Förslaget till undantag för nationell säkerhet är alltför snävt formulerat och innebär tolkningssvårigheter avseende vilka produkter som kan tänkas omfattas av undantaget.

- Det föreslagna förfarandet för rapportering av sårbarheter som genererar stora mängder känslig information riskerar utgöra ett hot mot nationell säkerhet, både vad avser rapporteringsförfarandet i sig och det senare omfattande hanteringen och lagringen av känslig information vid ENISA.

- Förslagets omfattande reglering av en stor mängd hård- och mjukvara i kombination med ett genomförande inom relativt kort tid, kan få konsekvenser som motverkar syftet med förordningen.

- Kombinationen av förordningens omfattning, den i sammanhanget korta tiden för ikraftträdande och bristen på cybersäkerhetskompetens gör att förslaget i sin nuvarande utformning förefaller orealistiskt.

- Det är förenat med betydande svårigheter att göra denna typ av förordning tekniskt, och därmed juridiskt, förutsebar och innebär därmed en svårbedömd juridisk och ekonomisk risk för ekonomiska operatörer på den inre marknaden.

- Konsekvensen och rimligheten av kraven för produkter baserade på öppen källkod måste analyseras vidare, samt att förordningen anpassas så att den inte får en negativ eller disruptiv effekt på den inre marknaden.

FMV vill även framföra att myndigheten har begränsade möjligheter att ta sig an nya uppgifter inom befintliga ramar för kommande budgetperiod mot bakgrund av bl.a. den tillväxt som sker inom totalförsvaret. Eventuellt nya uppgifter behöver dessutom finansieras utanför nuvarande ram.

FMV kan delta i utredning om aktens genomförande i Sverige. FMV vill framhålla att det är viktigt att det inte sker en ökad splittring av ansvar mellan de svenska myndigheter som har olika cybersäkerhetsuppdrag.

FMV:s ståndpunkter på förslagets olika områden

Relation med regler för nationell säkerhet

Av art 4.2 i Fördraget om Europeiska Unionen framgår att den nationella säkerheten är varje medlemsstats eget ansvar och faller utanför EU-rättens område. Medlemsstaterna ska, när det gäller nationella säkerhetsintressen, kunna köpa och utveckla produkter som inte ska omfattas av förordningens krav. Medlemsstaterna ska, med hänvisning till nationell säkerhet, fritt kunna tillföra ytterligare krav på produkter som omfattas av förordningen.

FMV menar att det inte återspeglas i förslaget till undantag i art. 2.5 i förordningen. Förslaget till undantag är alltför snävt formulerat och innebär tolkningssvårigheter avseende vilka produkter, med användningsområde inom nationell säkerhet, som kan tänkas omfattas av undantaget. Formuleringar som ”utvecklats uteslutande för ändamål som rör nationell säkerhet” och ”produkter som utformats specifikt för att behandla säkerhetsskyddsklassificerade uppgifter” lämnar få produkter utanför den föreslagna förordningens tillämpningsområde.

FMV förordar därför att artikel 2.5 får en skrivning som är samma eller liknande som finns i cybersäkerhetsakten artikel 1.2: ”Denna förordning påverkar inte medlemsstaternas befogenheter i fråga om verksamhet som berör allmän säkerhet, försvar, nationell säkerhet och statens verksamhet på straffrättens område.”

Rapportering av incidenter till ENISA

I art. 11 förordningen föreslås ett mycket omfattande och detaljerat rapporteringskrav för tillverkare.

FMV ser en risk med att det föreslagna förfarandet genererar stora mängder känslig information och att rapportera och samla all denna känsliga information i sig kan utgöra en risk. En insamling av kunskap om sårbarheter i samtliga produkter som omfattas av förordningen, dvs. kommersiell mjuk- och hårdvara med digitala element, skulle göra ENISA till ett mål för många olika hotaktörer. och skulle kunna utgöra ett hot mot enskilda medlemsstaters nationella säkerhet.

FMV anser att en sådan inrapportering till ENISA inte bör genomföras på det sätt som föreslås. Istället bör t.ex. nationella CERT:arnas roll utvärderas.

Förslagets omfattning

I förslaget föreslås att en mängd produkter, inklusive produkter som importeras från tredje land, ska gå från, inom detta område idag oreglerade status, till att behöva uppfylla förordningens krav: de väsentliga säkerhetskrav som anges i bilaga I samt krav på hantering av sårbarheter enligt bilaga II. Därutöver ska samtliga producenter, importörer, handlare osv. producera krav på information till användaren enligt bilaga III, upprätta och underhålla en teknisk dokumentation enligt bilaga V, samt genomföra en självbedömning, eller (för kritiska produkter) godkänd bedömning av överensstämmelse genom oberoende tredjepartsgranskning.

FMV bedömer att förslagets omfattande reglering, av en stor mängd hård- och mjukvara i kombination med ett genomförande inom relativt kort tid, kan få konsekvenser som motverkar syftet med förordningen genom att produkter som i dag är tillgängliga framför allt från små och medelstora företag, riskerar att inte kunna motsvara kraven med resultatet att de därmed inte får göras tillgängliga inre marknaden. De produkter som kan möta kraven kan förväntas öka i pris p.g.a. ökade kostnader och minskad konkurrens. Stora internationella bolag, många gånger lokaliserade utanför EU, kan gynnas på bekostnad av mindre europeiska bolag.

FMV bedömer även att det finns betydande risker för att den digitala innovationskraften inom EU hämmas om förordningen genomförs i dess nuvarande utformning.

Tiden för ikraftträdande otillräcklig

Förordningen föreslås tillämpas i sin helhet 24 månader efter dess ikraftträdande. Inom två år ska därmed alla tillverkare på inre marknaden, inklusive tillverkare i tredje land, anpassa sina rutiner och utbilda personal för att möta aktens krav. Till detta kommer kraven på all nödvändig teknisk dokumentation ska utvecklas. Ackrediteringsorganen ska anställa personal och etablera nödvändig kapacitet för att kunna ackreditera anmälda organ. Anmälda organ ska anställa personal och, i tid, bli ackrediterade i enligt förordningen. Slutligen ska därefter tillverkare av kritiska produkter hinna genomgå granskning och godkännande av ett anmält organ. Alla andra tillverkare ska hinna genomföra sina självkontroller.

FMV bedömer att tillverkare, ackrediteringsorgan, anmälda organ och myndigheter för marknadstillsyn inom EU kommer ha ökat behov av experter med it- och cybersäkerhetskompetens för att kunna möta förordningens krav. Det råder dock mycket stor efterfrågan och brist på sådan kompetens. Om förslaget genomförs enligt nuvarande utformning och omfattning, riskerar detta läge förvärras.

FMV bedömer att kombinationen av förordningens omfattning, den i sammanhanget korta tiden för ikraftträdande och bristen på cybersäkerhetskompetens gör att förslaget i sin nuvarande utformning förefaller orealistiskt.

Kommissionens mandat

Kommissionens möjligheter enligt förslaget att lägga fram genomförandeakter och delegerade akter är stora. Det ger kommissionen omfattande inflytande i styrningen av cybersäkerhetsområdet. Det förutsätter att kommissionen har teknisk expertis som möjliggör ändamålsenlig reglering.

FMV bedömer att det kan ifrågasättas om omfattningen av delegerade befogenheter till kommissionen är ändamålsenligt.

Gränsdragningsproblem avseende vad som utgör en produkt som omfattas av förordningen

FMV anser att förslaget inte tillräckligt tydligt anger en tydlig gräns mellan kommersiella produkter och dynamiskt distribuerade programvaror. Det är t.ex. vanligt att (kommersiella) webbsidor innehåller hypertextlänkar som refererar nerladdningsbar, exekverbar kod. När sådana sidor öppnas, laddas koden (s.k. javascript mm.) ner via hypertextlänkar och exekveras sedan lokalt. Som förordningen är utformad förefaller även sådan kod ingå i omfattningen.
FMV bedömer att det är behäftat med stora svårigheter om sådan kod ska omfattas av förordningen. Det behöver därför klargöras om sådan kod omfattas av förslaget och hur sådan kod i så fall ska CE-märkas, samt hur användaren ska kunna kontrollera detta. Vidare behöver det klargöras vem som ska ses som ansvarig tillverkare då kod distribueras via t ex webbsidor från servrar som är lokaliserade utanför EU.

Väsentliga krav är otydliga och inte alltid tillämpliga

De väsentliga kraven i förordningen förefaller syftar till ett tillstånd där sårbarheter i stort sett saknas i kommersiella produkter som sätts på marknaden. Detta är enligt FMV:s bedömning ett

orealistiskt mål. Dagens it-produkter består av så stor mängd kod och många funktioner att det i praktiken alltid kommer finnas sårbarheter. Moderna it-system som innehåller kommersiella produkter omsluter därför ofta principen ”*defence-in-depth*”, där enskilda produkter organiseras i flera olika ”lager” som tillsammans med andra åtgärder skapar nödvändig säkerhet, trots risken för sårbarheter i enskilda komponenter.

En strikt tolkning av kravet på frihet från kända sårbarheter för att en produkt få göras tillgänglig på marknaden skulle därmed innebära att många, både befintliga och framtida, produkter helt enkelt inte längre får göras tillgängliga. Detta skulle även gälla produkter som kan betraktas som väsentliga för inre marknadens konsumenter och systemägare.

Det är ett väsentligt krav är att produkter ska ”levereras med en säker standardkonfiguration, inbegripet möjlighet att återställa produkten till dess ursprungliga skick”. FMV konstaterar att en och samma it-produkt kan användas för många olika ändamål i många olika riskmiljöer. Vad som är ”säkra konfigurationer” för olika användningsfall kan vara ömsesidigt uteslutande. Därmed är det otydligt vad kravet innebär.

Det är ett väsentligt krav är att produkter ska ”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”.
Det är oklart om t ex USB-minnen måste levereras med kryptering påslagen eller om de får levereras utan kryptering aktiverad. Det även oklart om därmed okrypterad kommunikation via t.ex. Wifi är tillåten eller inte.

Juridisk förutsebarhet och risk för sanktioner

FMV bedömer att förordningens ansats att föreskriva en serie generella säkerhetsåtgärder som å ena sidan ska gälla samtliga produkter, men samtidigt, å andra sidan, ska bedömas baserat på en subjektiv riskbedömning, skapar juridisk osäkerhet. I kombination med de potentiellt höga sanktionsavgifterna riskerar detta att hämma den inre marknaden och nya innovationer inom området.

Bristande efterlevnad av de väsentliga cybersäkerhetskraven för de produkter som hör till kategorin ”kritiska produkter” listade bilaga I kan medföra sanktionsavgifter på upp till 15 000 000 EUR eller, om överträdelsen begås av ett företag, upp till 2,5 procent av dess totala globala årsomsättning, beroende på vilket som är högst. Produkter kan komma från företag där om globala omsättningen uppgår till flera 1 000 miljarder kronor. Straffavgifter kan därmed uppgå till mycket höga belopp för produkter som kostar någon hundralapp i konsumentledet.

FMV ser en risk med att förekomsten av de höga sanktionsavgifterna, i kombination med svårigheterna att göra förordningen juridiskt och tekniskt förutsebar, kan hämma utvecklingen och innovationskraften inom EU, samt minska antalet aktörer och tillgängliga produkter inom EU. Förordningen innebär således en svårbedömd juridisk och ekonomisk risk för alla ekonomiska operatörer på den inre marknaden.

FMV kan samtidigt notera att det är behäftat med betydande svårigheter att göra denna typ av förordning tekniskt, och därmed juridiskt, förutsebar.

FMV förordar därför att listan av de väsentliga kraven omarbetas och reduceras, samt att de enbart gäller för mer specifikt definierade funktioner för mer specifikt definierade användningsfall.

Kommersiella produkter baserade på öppen källkod

Förordningen omfattar produkter med digitala element för distribution eller användning på unionsmarknaden i samband med kommersiell verksamhet, antingen mot betalning eller kostnadsfritt. Det anges att en kommersiell verksamhet inte bara kännetecknas av att det tas ut en avgift för produkten utan också av att en avgift tas ut för tekniska stödtjänster, att en programvaruplattform tillhandahålls som tillverkaren använder för att monetarisera andra tjänster eller av att personuppgifter används för andra syften än uteslutande att förbättra programvarans säkerhet, kompatibilitet eller interoperabilitet.

Öppen källkod utvecklas av en mycket stor mängd frivilliga programmerare i hela världen. Eftersom en stor mängd kommersiella produkter på inre marknaden idag baseras på öppen källkod, innebär därmed detta att alla dessa produkter och den tillhörande koden omfattas av förordningen, inklusive kraven på teknisk dokumentation och rapportering av sårbarheter.

FMV bedömer att ett stort antal sådana källkoder inte uppfyller kraven på den tekniska dokumentation som krävs enligt förordningen. Det är därför mycket tveksamt om det finns förutsättningar för att på frivillig väg etablera sådan dokumentation. Det finns även risk för att tillverkare som baserar sina produkter på öppen källkod inte heller har tillräckliga resurser.

Därmed är det FMV:s bedömning att ett stort antal produkter, flera av dem väsentliga för näringsliv och samhälle, i realiteten inte har förutsättningar att kunna motsvara kraven. En strikt tillämpning av förordningen, som den när utformad, riskerar därmed att en stor mängd produkter inte längre får göras tillgängliga på inre marknaden. Detta riskerar att minska innovation och konkurrens den inre marknaden.

Det är FMV:s uppfattning väsentligt att konsekvensen och rimligheten av kraven för produkter baserade på öppen källkod analyseras, samt att förordningen anpassas så att den inte får en negativ eller t.o.m. störande effekt på den inre marknaden.

Utveckling av effektiva standarder tar tid

FMV anser att det är av avgörande betydelse att de tekniska krav som ska tillämpas ska vara i form av standarder framtagna enligt vedertagna internationella regler för sådan standardutveckling. Det gäller bl.a. särskilt för de olika krav som uttrycks i bilagorna till förslaget till förordning. Sådana standarder behöver utvecklas öppet och transparens för att minska risken för snedvridning av konkurrensen på inre marknaden.

Att utveckla standarder och som sedan efter praktisk användning förbättras är en lång process som kan ta flera år.

FMV anser att förordningens intentioner är goda, men att mer tid och resurser behövs för att utveckla nödvändiga standarder. Om förordningen träder i kraft innan nödvändiga standarder utvecklats är risken stor att bedömningen av förordningens krav blir ojämn mellan medlemsstaterna, eftersom den då måste baseras på enbart de väsentliga kraven, eller tekniska specifikationer som inte genomgått en standardiseringsprocess. Kostnaderna kan bli höga för tillverkarna samtidigt som förbättringen av cybersäkerheten kan utebli.

FMV anser därför att förordningen enbart bör träda ikraft för sådana produkter och områden där det finns etablerad och beprövad standard, utvecklad av EU erkända standardsorgan och i enlighet med principerna för New Legislative Framework .

Rollen som tillsynsmyndighet

Förordningens omfattning kopplat till krav på marknadskontroll får budgetära konsekvenser för medlemsstaterna. Storleken på detta bör klargöras och omfattning av förordningen anpassas till medlemsstaternas förmåga och villighet att bära dessa kostnader.

Förordningen kommer att beröra den verksamhet som bedrivs vid FMV genom myndighetens uppdrag att vara Nationell myndighet för cybersäkerhetscertifiering enligt cybersäkerhetsakten. FMV kommer därmed att behöva förhålla sig till och samverka med övriga myndigheter i Sverige som på olika sätt har ansvar enligt akten. FMV får genom den föreslagna förordningen ett utökat tillsynsansvar över aktörer som kommer utge eller använda sig av certifieringsordningar utvecklade för förordningens tillämpningsområde. Till detta kommer frågan om vilken myndighet som ska ges uppdraget att vara tillsynsmyndighet och marknadskontrollmyndighet enligt förordningen.

FMV vill framhålla att myndigheten har begränsade möjligheter att inom befintliga ramar ta sig an nya uppgifter för kommande budgetperiod mot bakgrund av bl.a. den tillväxt som sker inom totalförsvaret. Eventuellt nya uppgifter behöver därför finansieras utanför nuvarande ram.

FMV vill i detta sammanhang framhålla att det är viktigt att det inte sker en ökad splittring av ansvar mellan de svenska myndigheter som har olika cybersäkerhetsuppdrag. FMV ser det därför som angeläget att kunna få möjlighet att delta i en eventuell utredning om förordningens genomförande i Sverige.

Föredragande har varit Rådgivare cybersäkerhet Dag Ströman. Vid den slutliga handläggningen har bl a Chef Juridiska avdelningen Maria Gutensparr och Chef Inspektionen för cybersäkerhetscertifiering John Billow deltagit.

Försvarets materielverk

Anders Sjöborg
Chefsjurist

Sändlista

Finansdepartementet i.remissvar@regeringskansliet.se med kopia till i.esd.remisser@regeringskansliet.se

Kopia till

Försvarsdepartementet forsvarsdepartementet.registrator@regeringskansliet.se med kopia till myndighetshandläggare FMV

Inom FMV:

Ledningsstaben

Juridik- och säkerhetsstaben

Arkiv (original)