Regeringskansliet, Finansdepartementet
samt sändlista

Ert tjänsteställe, handläggare
Regeringskansliet, Finansdepartementet

Ert datum
2022-11-21

Er beteckning
I2022/01758

Vårt tjänsteställe, handläggare
HKV FST JUR Ofr, Sara Westerlund,
sara.westerlund@mil.se

Vårt föregående datum

Vår föregående beteckning

Försvarsmaktens remissyttrande

Försvarsmakten 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.

Försvarsmaktens yttrande sker med utgångspunkt från myndighetens huvuduppgift att försvara Sverige mot ett väpnat angrepp, samt Försvarsmaktens verksamhet rörande säkerhets- och underrättelsetjänst. Cyberförsvar ingår som en integrerad del av det militära försvaret. Försvarsmakten är också en av de myndigheter som utövar tillsyn och utfärdar föreskrifter enligt säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen (2021:955), bl.a. vad gäller informationssäkerhet. Försvarsmakten inhämtar information om cyberhot inom ramen för sin underrättelse- och säkerhetstjänst. Vidare samverkar Försvarsmakten genom Nationellt cybersäkerhetscenter med andra myndigheter för att förebygga, upptäcka och hantera cyberhot.

Att stärka samhällets motståndskraft blir allt viktigare för en stark totalförsvarsförmåga. Försvarsmakten konstaterar att det finns ett behov av att höja den allmänna cybersäkerhetsnivån. Det är dock viktigt att de åtgärder som vidtas är ändamålsenliga. Enligt Försvarsmaktens mening är det tveksamt om förslaget kommer att uppnå avsedd effekt.

Försvarsmakten vill i detta sammanhang erinra om att det inte är tillräckligt att höja kvaliteteten enbart i produkterna, eftersom det med nuvarande utvecklingsmetoder är omöjligt att producera helt säkra produkter. I många fall uppstår eller förvärras it-incidenter till följd av handhavandefel. En av de cyberattacker som nämns i motiven till förslaget, WannaCry, berodde t.ex. på att många

Postadress
Högkvarteret
107 85 Stockholm

Besöksadress
Lidingövägen 24

Telefon
08-788 75 00

Telefax
08-788 77 78

E-post, Internet
exp-hkv@mil.se
www.forsvarsmakten.se/hkv

organisationer inte hade installerat den säkerhetsuppdatering som publicerats ett par månader innan den skadliga koden spreds, trots att information om denna gjorts tillgänglig för användarna. Det råder också för närvarande en stor brist på kompetens inom cybersäkerhetsområdet, varför tillgängliga resurser behöver nyttjas så effektivt som möjligt. Försvarsmakten ifrågasätter därför om obligatorisk tredjepartsbedömning av kritiska produkter är den åtgärd som ger mest effekt.

Försvarsmakten lämnar utifrån detta följande synpunkter på förslaget.

Tillämpningsområdet för den föreslagna förordningen

Som framgår av art. 4.2 fördraget om Europeiska unionen ska medlemsstaternas suveräna rättigheter avseende nationell säkerhet respekteras. Enligt kommissionens förslag ska den nu remitterade förordningen inte tillämpas på sådana produkter med digitala element som utvecklats uteslutande för ändamål som rör nationell säkerhet eller militära ändamål eller på produkter som utformats specifikt för att behandla säkerhetsskyddsklassificerade uppgifter. Enligt Försvarsmaktens mening kan det uppstå tolkningssvårigheter gällande samhällsviktiga funktioner som är en del av totalförsvaret och därmed av betydelse för Sveriges säkerhet. Undantaget för nationell säkerhet behöver därför förtydligas i förordningen.

Vidare innebär kommissionens förslag att produkter med dubbla användningsområden kommer att omfattas av förordningens tillämpningsområde. Vissa produkter som används av Försvarsmakten, eller i annan verksamhet som rör nationell säkerhet, skulle alltså omfattas av förordningen. Det innebär bl.a. att en incident som ska rapporteras in till ENISA (The European Union Agency for Cybersecurity) enligt förslaget samtidigt kan utgöra en incident som rör Sveriges säkerhet och därmed bör tillkännages Försvarsmakten inom ramen för dess uppgifter inom säkerhetsskyddslagstiftningen. Därutöver har Försvarsmaktens cyberförsvar ett behov av att skyndsamt få rapporter om sårbarheter i produkter som används inom det militära försvaret, i syfte att snabbt kunna vidta nödvändiga skyddsåtgärder. Försvarsmakten anser att incidenter som rör nationell säkerhet i första hand ska hanteras nationellt i stället för genom ENISA.

Försvarsmakten ser också en risk med att de krav som ställs på tillverkarna under produktens livscykel medför att tillverkarna behöver utöva en större kontroll över hur produkterna används. Tillverkarna kan även ändra förutsättningarna för att undgå den föreslagna förordningens krav. Exempelvis kan trenden att erbjuda produkter och annan innovation som olika typer ”as-a-service” eller molntjänster accelereras. Det kan minska Försvarsmaktens samt andra organisationer inom totalförsvarets handlingsutrymme att anpassa produkterna till den egna verksamheten och vidta egna säkerhetsåtgärder. Samlat inom Europa skulle den totala affärsvolymen för specifika produkter, vilka används inom skyddsvärd verksamhet, kunna vara för liten för att tillverkaren ska välja att utvärdera produkterna för att göra dem tillgängliga på EU:s inre marknad. Det kan skapa en brist på vissa

specifika lösningar, alternativt bara göra dem tillgängliga genom molntjänster, vilket kan minska den digitala suveräniteten och därmed påverka Sveriges säkerhet.

Försvarsmakten förutsätter att myndigheten under alla omständigheter inte kan anses som en sådan ekonomisk aktör som ikläds skyldigheter enligt förordningen, när Försvarsmakten själv utvecklar eller importerar produkter för eget bruk. Om det råder några tveksamheter kring detta bör det förtydligas i förordningstexten.

Försvarsmaktens bedömning av förslagets konsekvenser i övrigt

Förslaget innebär att en svåröverskådlig mängd produkter, mjukvara och firmware ska gå från dagens oreglerade status till att behöva uppfylla långtgående och detaljerade krav. De föreslagna sanktionsavgifterna kan medföra stora kostnader för företagen för produkter som betingar ett lågt pris i konsumentledet. Det är viktigt att förslaget inte får oavsedda konsekvenser som inverkar negativt på cybersäkerheten, vare sig vad gäller produktsäkerhet eller på övergripande nivå. Om kraven blir för betungande för små och medelstora aktörer kan urvalet av aktörer minska och beroendet öka av ett fåtal stora aktörer och aktörer i tredjeland, vilket riskerar att öka sårbarheten och minska den digitala suveräniteten. Ett stort antal produkter på den inre marknaden riskerar att inte längre finnas tillgängliga eller att drabbas av prisökningar. Detta kan medföra skada för samhällsviktig verksamhet.

Det kan också inverka negativt på cybersäkerheten om förordningens krav leder till att lanseringen av nya och uppdaterade produkter drar ut på tiden och en snabb uppdatering av produkter med säkerhetshål därigenom försvåras.

Vidare finns risker med att användare invaggas i en falsk trygghet om de köper produkter med någon form av säkerhetsutvärdering. Det är därför viktigt med transparens kring vad tillverkaren respektive användaren ansvarar för, då även säkra produkter kan användas på ett osäkert sätt.

Slutligen finns det stora risker förknippade med att samla information om användare av produkter, sårbarheter och incidenter. Det är viktigt att denna information omgärdas av ett tillräckligt skydd.

Sammantaget är Försvarsmaktens bedömning att en så omfattande reglering av en så stor mängd hård- och mjukvara på så kort tid kan förväntas få konsekvenser som direkt motverkar syftet med förordningen.

Sammanfattning av Försvarsmaktens ståndpunkter

Sammantaget anser Försvarsmakten

- att förslaget är alltför långtgående och inte bör genomföras i nuvarande utformning utan att konsekvenserna av förslaget har fått en bättre belysning,
- att undantaget rörande nationell säkerhet, militära ändamål och säkerhetsskyddsklassificerade uppgifter är för snävt och behöver göras vidare,
- att förslaget ska utformas så att den nationella suveräniteten avseende nationell säkerhet värnas så långt möjligt,
- att hänsyn ska tas till att behoven hos myndigheter och andra större aktörer skiljer sig åt från behoven hos konsumenter samt mindre företag och organisationer,
- att det är viktigt att kraven enligt förordningen inte utformas eller tillämpas så att de i praktiken får negativa effekter på cybersäkerheten.

I beredningen av detta ärende har kommendörkapten Rickard Almlöf, informationssäkerhetsspecialist Pekka Andelin och IT-säkerhetsstrateg Fredrik Börjesson deltagit.

Detta yttrande har beslutats av ställföreträdande chefsjurist Helene Arango Magnusson**.** I den slutliga handläggningen har sektionschef Annika Grahn Sulusi, kryptostrateg Pia Gruvö, handläggare Annika Avén och, som föredragande, försvarsjurist Sara Westerlund deltagit.

Helene Arango Magnusson

Ställföreträdande chefsjurist

Sara Westerlund

Sändlista
Regeringskansliet, Finansdepartementet — i.remissvar@regeringskansliet.se, med kopia till i.esd.remisser@regeringskansliet.se

Försvarsdepartementet (för kännedom e-post)

Inom myndigheten för kännedom
MUST SÄKK