21 februari 2023

# Dataföreningens remissvar avseende diarienummer I2022/01758 dvs Cyberresiliensakten (CRA)

## Dataföreningens inställning är positiv – vi önskar dock vissa klargöranden

Den föreslagna förordningens syfte, säker programvara, information om säkerhetsproblem samt säkerhetsuppdatering av programvara när så behövs är något som i allra högsta grad behövs. Dataföreningen välkomnar och ställer sig positiv till förordningen.

Vi framför också att förordningen kan, och lämpligen bör förbättras på en del punkter. Det är också lämpligt att vissa punkter definieras tydligare. Mer om detta nedan.

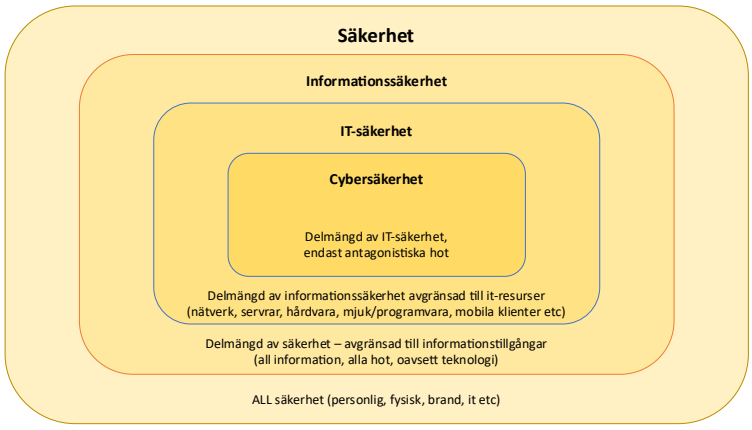
## Behov av entydiga begrepp och innebörder

Ett antal av de begrepp som används i cyberresiliensakten (CRA) torde behöva definieras bättre än vad som framgår av CRA. Dessa begrepp behöver en så entydig definition som möjligt, inte minst för att undvika oklarheter om vad som gäller, särskilt för personer som inte är jurister.

***Säkerhet***
Rekommenderar att **säkerhet, informationssäkerhet, IT-säkerhet** och **cybersäkerhet** definieras så entydigt som möjligt och används/betyder samma sak i alla förordningar och direktiv.

Inte minst noteras att begreppet cybersäkerhet har blivit något av ett modeord. Frågar man till exempel 10 personer så torde man få 10 olika svar beträffande vad cybersäkerhet är. Samma sak torde gälla även för säkerhet, informationssäkerhet och IT-säkerhet.

Det är också lämpligt att klargöra hur dessa begrepp passar ihop, till exempel enligt denna bild. Ref 1.




***Addera definitioner till artikel 3***

I artikel 3 rekommenderas att tydliga och relevanta definitioner av “fri programvara”, “öppen programvara” respektive “fri programvara med öppen källkod” adderas till listan på definitioner.

***Artikel 3.31 - Väsentlig ändring***

I arbetet med detta remissvar har en diskussionspunkt återkommit ett antal gånger från olika håll, nämligen när behövs en ny eller uppdaterad procedur för CE-märkning och/eller en ny alternativt omcertifiering. Likaså när eller under vilka förhållanden startar 5-årsperioden för tillhandahållande av säkerhetsuppdateringar.

Dessa frågor torde bottna i definitionerna av “ny produkt”, när produkten släpps ut på marknaden” respektive vad en “väsentlig ändring” innebär.

En ännu tydligare definition av väsentlig ändring torde vara önskvärd, samt med exempel på vad som menas med väsentlig ändring.

***Dokumentation av cybersäkerhetsrisk***

I artikel 10.2 anges att tillverkaren ska göra en bedömning av cybersäkerhetsriskerna samt i artikel 10.3 att tillverkaren när en produkt släpps ut på marknaden ska inkludera en bedömning av cybersäkerhetsriskerna i den tekniska dokumentationen.

Det är sannolikt lämpligt att tillhandahålla råd och eventuellt en lathund för hur bedömning av risk samt hur denna typ av dokumentation lämpligen tas fram och utformas.

***Förväntad livslängd***

I bland annat artikel 10.6 anges “produktens förväntade livslängd”. Det är sannolikt lämpligt att försöka definiera tydligare vad detta innebär. Vem definierar detta? För en kund kan begreppet vara otydligt.

***Utan dröjsmål***

Artikel 11.4 anger utan dröjsmål. Lämpligt att förtydliga vad som menas med utan dröjsmål. Är det 24 timmar som nämns i andra artiklar eller vad?

***Släppts ut på marknaden***

I artikel 10.6 anges “från utsläppandet på marknaden”, i artikel 13.7 används även begreppet “har släppts ut på marknaden”. Innebörden av dessa begrepp bör

sannolikt tydliggöras. Exakt vad menas med ”när är produkten utsläppt på marknaden”. Hur ska tillverkare och kunder veta från när “klockan börjar ticka”? Hur ska kunden veta vad som gäller efter 5 år?

***Informationskrav***
I artikel 17.1 anges att “Ekonomiska aktörer ska, på begäran och om informationen finns tillgänglig, förse marknadskontrollmyndigheterna med följande information:”

Även i andra artiklar anges att ekonomiska aktörer ska förse marknadskontroll-myndigheterna med information, till exempel avseende programvaruförteckning (i många andra sammanhang oftast benämnd Software Bill of Material, SBOM). Likaså anges det att certifieringsorgan ska förses med information.

Det som inte entydigt går att utläsa ur förordningen är om användare/kunder också ska förses med, eller ha rättighet att kräva programvaruförteckningar/SBOM. Medför till exempel CRA att kunderna vid upphandling har rätt att kräva programvaruförteckning (SBOM)?

Så verkar inte vara fallet utan det är frivilligt för de ekonomiska aktörerna att tillhandahålla programvaruförteckning/SBOM. Stämmer detta?

## Kommentarer

***Fri och öppen programvara/Open Source Software***
Det bör tydliggöras att tillverkare av fri/öppen programvara samt fri programvara med öppen källkod (s.k. open source software) som tjänar pengar på att till exempel tillhandahålla support ej bör hållas ansvariga enligt CRA. Det bör snarare vara den som inkluderar programvaran i sina produkter och erbjudanden som är den som är ansvarig för att tillse säkerheten. Se Ref 2 för mer information.

***Dataskydd som standard och inbyggt dataskydd***
Dessa begrepp bör inkluderas i de väsentliga cybersäkerhetskraven för produkter med digitala element.

***Komplexa system – vad gäller?***
Artikel 5.1 anger “Produkter med digitala element får endast tillhandahållas på marknaden om...”. Den som är mottagare av en leverans, respektive köper, nya enheter och har en installerad bas.

Kan den nya enheten tillåtas konfigureras på ett sätt som inte är CRA-kompatibelt till exempel en osäker kommunikationsförbindelse. Eller medför CRA att allt måste vara säkert dvs “gammal icke CE-märkt” utrustning måste uppdateras till eller bytas ut mot en ny CE-märkt lösning?

***Risk för utslagning av små programvarubolag***
CRA kan innebära risk för utslagning av små programvarubolag och/eller deras konkurrensförmåga. Dataföreningen noterar att det bland annat nämns i CRA att hänsyn ska tas till små och medelstora företags behov. Detta till trots vill vi framföra att behov föreligger att just ta hänsyn till små programvarubolags/små spetsföretags behov och förutsättningar. Dessa torde bland annat på nationell nivå behöva stöd för att klara hela kravbilden.

***Dataföreningen anser***
Dataföreningen anser att införandet av CRA är ett viktigt stöd för samhällets digitalisering. Vår uppfattning är att detta har potentialen att kunna innebära lägre kostnader för både kunder och leverantörer och, inte minst, en tryggare framtid för medborgarna och organisationerna i EU.

I dagsläget ser vi dock att nödvändig kompetens saknas på många nivåer i samhället. Dataföreningen avser att verka för en förstärkning av behövd kompetens.

Dataföreningen

**Per-Erik Eriksson**
Utredare/Talesperson västra kretsen säkerhet och dataskydd

**Christer Berg**
Verksamhetschef, Dataföreningen i Sverige

## Referenser

1. Enligt Kungliga Vetenskapsakademiens definition
2. EU Cyber Resilience Act: Good for Software Supply Chain Security, Bad for Open Source?
   https://blog.sonatype.com/eu-cyber-resilience-act-good-for-software-supply-chain-security-bad-for-open-source