Johanna Parikka Altenstedt
Enhet för Digital Säkerhet
Datavetenskap
+46-(0)10-2284660
johanna.parikka.altenstedt@ri.se

Försvarsdepartementet
Remissvar Fö2026/00576
fo.remissvar@regeringskansliet.se
fo.ech.remissvar@regeringskansliet.se.

Remissvar från RISE avseende Europeiska kommissionens cybersäkerhetspaket med förslag om ändringar i cybersäkerhetsakten (EU 2019/881) samt riktade ändringar i NIS 2-direktivet (EU 2022/2555) KOM (2026)

Härmed framförs synpunkterna från Research Institutes of Sweden, RISE, på Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 samt om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

Syftet med de riktade ändringarna i NIS2

RISE välkomnar syftet att underlätta efterlevnaden av cybersäkerhetskrav och frigöra resurser för att stärka den operativa cybersäkerhetsberedskapen hos väsentliga och viktiga aktörer inom unionens kritiska sektorer. Detta sker genom föreslagna riktade ändringar i NIS 2-direktivet för att förenkla vissa delar av cybersäkerhetsramverket, öka den rättsliga förutsebarheten och harmonisera genomförandet. Generellt är ändringsförslagen för att minska krångel samt de små och medelstora företagens börda relevanta och proportionerliga, och RISE finner det särskilt tillfredställande att EU har tagit fram dessa skyndsamt baserade på medlemsstaternas synpunkter.

RISE vill dock påpeka att ändringarna i NIS2 presenteras bara drygt tre månader efter den svenska implementeringen av cybersäkerhetslagen och cybersäkerhetsförordningen av det ursprungliga NIS2 förslaget, som skulle ha funnits på plats i den 18 oktober 2024. Den svenska transponeringen av NIS2 innefattar även föreskrifter från ansvariga sektorsmyndigheter, varav några har inte kommit särskilt långt i sitt arbete. Det är oerhört viktigt för regleringens trovärdighet, samt för näringslivets förutsättningar att få en rättssäkerhet oc förutsebarhet kring NIS2 -skyldigheterna. Därmed bör medlemsstaten

Sverige säkerställa att det inte uppstår en situation där det ursprungliga nationella genomförandet av NIS2 och dessa uppdateringar av NIS2 hamnar i ofas i den svenska rättsordningen.

RISE lyfter även i detta svar det faktum att några av förslagen innebär även en risk för normkonflikter med den nationella rättsordningen om de skulle genomföras som föreslagits. Naturligtvis bör sådana konflikter eliminieras.

Cybersäkerhetscertifieringssystemet

För att göra det enklare för verksamheter och leverantörer att visa att de uppfyller kraven i NIS 2-direktivet ska verksamheter som omfattas av NIS 2-direktivet kunna erhålla certifikat inom orgasatoriska cybersäkerhetscertifieringssystem som utvecklas inom ramen för ECCF. Grundtanken med en sådan cyberposture-certifiering som efterlevnadsverktyg är god, dvs. att företag ska kunna visa sin efterlevnad av NIS2 genom ett certifikat och slippa parallella tillsynsprocesser. Det underlättar också agerandet på den gemensamma marknaden.

Men artikel 24(5) i ändringsdirektivet innebär att ett giltigt certifikat i praktiken begränsar tillsynsmyndigheternas möjlighet att kräva ytterligare åtgärder avseende de krav som certifikatet täcker. RISE menar att det krävs en juridisk analys av en mer principiell fråga om var ansvaret för att bedöma säkerhetsnivån egentligen ska ligga; hos offentliga tillsynsmyndigheter eller hos privata certifieringsorgan, särskilt när hotbilden ändras så snabbt och nya angreppssätt utvecklas ideligen mot organisationer och företag.

RISE påpekar också att ett parallellt certifieringsarbete pågår med CRA (EU NNNN) och det är av stor vikt att koordinera certifieringarna på ett sätt som gör det enkelt för verksamheter att förstå syftet och kraven i samband med dem.

Riktlinjer för leverantörsskedjan

Kommissionen ska anta riktlinjer för tillämpningen av krav på säkerhet i leveranskedjan som verksamheter inom NIS 2-direktivets tillämpningsområde för vidare till sina leverantörer, i syfte att säkerställa rättslig klarhet och förhindra att skyldigheter i onödan förs vidare till aktörer som inte omfattas av NIS 2-direktivet.

RISE välkomnar att kommissionen förtydligar vad som krävs av väsentliga och viktiga verksamheter i samband med att hantera leveranskedjan enligt NIS2, samt att minska den administrativa bördan för dessa leverantörer. RISE ser framemot att en konsekvent, proportionerlig och effektiv metod för bedömningar av leveranskedjesäkerhet tas fram med riktlinjer om lämplig detaljeringsnivå, struktur och form för sådana informationsförfrågningar, så att t ex samma information ej efterfrågas flera gånger.

Maximumharmonisering

RISE förstår att syftet med maximumharmonisering (specificering av cybersäkerhetsåtgärder för riskhantering) är att underlätta för företag och tillsynsmyndigheter som agerar på flera av EU:s marknader. Men RISE uppmuntrar lagstiftaren och EU att nogrant analysera effekterna

av ett sådant tak. I det nuvarande NIS2-direktivet är medlemsstater fria att gå längre än direktivets minimikrav, något som ändras enligt den föreslagna ändringen av artikel 21(5) som konstaterar att medlemsstaterna inte längre ska kunna ställa ytterligare tekniska eller metodologiska krav på entiteter som omfattas av kommissionens genomförandeakter.

RISE vill påminna att om detta i praktiken innebär att Sverige inte längre kan ställa strängare krav på svenska energibolag än kommissionens de som kommer att finnas i kommissionens genomförandeakt för energisektorn, kan besvärliga normkonflikter uppstå. I och med energisektorn är av avgörande vikt även för nationell säkerhet, kan det uppstå en normkonflikt i fall vår nationella hotbild eller totalförsvarsplanering motiverar högre säkerhetsnivå enligt säkerhetsskyddslagen, som trumfar NIS2. RISE anser att det är önskvärt att inte bygga in denna typ av normkonflikter mellan nationella och EU-rättsliga regler i uppdateringen av NIS2.

Undantaget till definitionen av elproducent

RISE välkomnar justeringen av definitionen av elproducent genom undantaget för elproducenter under 1 MW i Annex I till ändringsdirektivet. Det har visat sig att stora anläggningar som annars ej träffas av NIS2 gjorde det t ex pga några solceller på taket vilket var orimligt.

RISE påpekar dock att regleringen borde formuleras så att den även kan ta hänsyn till aggregeringseffekten. Det finns idag tusentals uppkopplade anläggningar under 1 MW som delar samma tillverkares styrsystem, växelriktare eller molnplattform. En angripare skulle kunna slå ut en sådan plattform och därigenom många anläggningar samtidigt.

Nationella strategier för migration till post-kvantkryptografi

RISE stödjer initiativet till att ta fram nationella strategier för post-kvantkryptografi.
RISE vill dock understryka att det krävs mycket tydlig styrning för att kunna genomföra allt som krävs inom mindre än fyra år eftersom kritiska system ska vara migrerade till 2030; inventera alla system som använder kryptering, prioritera dem, testa nya lösningar och rulla ut dem – även för dual-use -system samt för avancerade AI-system. För att denna styrning kommer på plats anser RISE att den nationella strategin ska innehålla tydliga mål och krav på finansieringen.

Harmoniserad insamling av data om ransomware-attacker

RISE finner det som en god tanke att insamla information om ransomware -attacker och på detta sätt förstärka säkerheten på hela den gemensamma marknaden. Det är också fullt

begripligt att en sorts amnesti föreslås dvs efterlevnad av skyldigheterna att rapportera relevant information om ransomwareincidenter bör inte leda till att ytterligare skyldigheter åläggs enligt direktivet, som annars skulle ha krävts, om rapporteringen inte hade skett.

Grundtanken är naturligtvis att det är mer värdefullt att samla information och öka kunskapsnivån inom EU, för att kunna förebygga och varna andra. RISE vill dock påpeka att det finns en risk för normkonflikt genom att NIS2 trumfar inte säkerhetsskyddslagen, GDPR eller bråttsbalken. Det kan uppstå en situation där aktören som lämnar information om ransomeware-attacken blir skyldig för brott i alla fall. Denna aspekt bör analyseras noga.

Europeiska digitala identitetsplånböcker och Affärsplånböcker

RISE välkomnar kraven på digitala ID-tjänster att bli klassificerade som väsentliga eftersom dessa är en så kritisk del av den digitala infrastrukturen i samhället med igenkännings-, validerings- och signeringstjänster. RISE välkomnar särskilt en oberoende nationell ID-tjänst med hög säkerhetsnivå.

ENISA:s nya roll

RISE välkomnar förslaget om att ytterligare underlätta efterlevnaden av åtgärder för cybersäkerhetsriskhantering för verksamheter som är verksamma i flera länder och står under tillsyn av behöriga myndigheter i flera medlemsstater, genom att ge ENISA en ny roll i att stödja medlemsstaterna underlätta ömsesidigt bistånd och skapa en bättre överblick över vilka verksamheter som omfattas av NIS 2-direktivet.

RISE vill samtidigt påminna om att ett sådant uppdrag kräver att ENISA får en proper finansiering och tillräckliga personresurser för att kunna bli detta stöd.