SVENSKA KRAFTNÄT

Informationsklass
K1

Generaldirektören

Regeringskansliet
Försvarsdepartementet

2024-05-22 2024/1093 REMISSVAR

Remissvar till delbetänkandet SOU 2024:18 - Nya regler om cybersäkerhet

Affärsverket svenska kraftnät (Svk) har mottagit delbetänkandet ”Nya regler om cybersäkerhet” (SOU 2024:18) från Utredningen om genomförande av NIS2- och CER-direktiven. Myndigheten ställer sig i grunden positiv till lagförslaget och de bakomliggande resonemang som förs av utredningen.

Allmänna kommentarer

En gemensam och hög basnivå för informations- och cybersäkerheten hos samhällsviktig verksamhet i hela Europa, tydligt reglerad och utformad på ett sätt som även säkerställer regelefterlevnad, är enligt Svenska kraftnäts uppfattning grundläggande för att säkerställa samhällets funktionalitet, såväl inom Sverige och andra medlemsstater som mellan den inre marknadens medlemsstater.

Samtidigt har NIS tillfört, och NIS2 kommer att tillföra, en grundberedskap och handlingsförmåga som i många fall behöver kompletteras. Det kan ske på flera sätt, inte enbart genom allmän lagstiftning eller sektorföreskrifter, utan även genom helt andra regelverk. Svenska kraftnät ser positivt på att förslaget innebär en anpassning till internationell standard för informationssäkerhet (främst ISO 27000) som bland andra MSB och dess föregångare Krisberedskapsmyndigheten förespråkat sedan drygt 15 år tillbaka.

Svenska kraftnät stödjer sedan länge kraven på systematiskt och riskbaserat cybersäkerhetsarbete, baserat på ett allriskperspektiv. Detta bör genomsyra arbetet hos alla samhällsviktiga verksamheter. Här ser Svenska kraftnät en svaghet hos lagförslaget i det att vissa offentliga verksamhetsutövare undantas från lagens tillämpningsområde, och därmed från dess krav på systematiskt cybersäkerhetsarbete. Verksamhetsutövarna i fråga är visserligen undantagna från NIS2-direktivets tillämpningsområde, men då NIS2 är ett *de minimis*-direktiv vore det lämpligt att låta Cybersäkerhetslagen omfatta även dessa verksamhetsutövare för att på så sätt skapa en gemensam lägstanivå för cybersäkerhet.

BOX 1200
172 24 SUNDBYBERG

STUREGATAN 1,
SUNDBYBERG

TEL: 010-475 80 00

REGISTRATOR@SVK.SE
WWW.SVK.SE

Svenska kraftnät tillstyrker förslagets krav på att redovisa riskhanteringsåtgärder. Flera av de angivna åtgärderna och rutinerna kan betraktas som grundläggande i en samhällsviktig verksamhet. De bör vara proportionerliga i förhållande till föreliggande riskexponering. Det är emellertid viktigt att hålla isär kraven på lämplighet och proportionalitet (mer om detta nedan).

Hanteringen av större cybersäkerhetskriser i samhället har avhandlats i ett särskilt regeringsuppdrag till MSB och kommenteras därför inte inom ramen för detta yttrande. Svenska kraftnät vill dock understryka att behovet av specialiserat stöd till organisationer som förvaltar verksamhetskritiska industriella styrsystem är fortsatt högt.

Inom sektorn energi har även verksamheterna aggregering och batterilager inkluderats i betänkandet som berörda av NIS2. Sådana tjänster kan redan inom några år nå sådana samlade volymer att påverkan på frekvens- och systemstabilitet i det svenska elnätet, åtminstone på regional nivå, inte kan uteslutas. Detta oavsett de tekniska begränsningskrav som redan ställs av Svenska kraftnät i samband med förkvalificering till leverans av stödtjänster. Tekniska fel eller it-angrepp mot ett stort antal likadana, uppkopplade system kan på sikt medföra stora konsekvenser för såväl samhällskritisk som säkerhetskänslig verksamhet. Av den anledningen anser Svenska kraftnät att det är viktigt att myndigheten ges tillfälle till samråd vid utformningen av tekniska föreskrifter med utgångspunkt från NIS2 för alla tjänster med potential att väsentligt påverka elnätsdriften.

Författningskommentarer

Kap 1 – Inledande bestämmelser

1 kap. 2 § 33 (definitionen av ”verksamhetsutövare”)
Enligt 1 kap. 2 § 33 definieras en *verksamhetsutövare* som en ”juridisk eller fysisk person som bedriver verksamhet”. Det anges också att det är en samlingsterm för ”bland annat leverantör, producent, vårdgivare, leverantör och tillhandahållare”.

Svenska kraftnät uppfattar definitionen som oprecis. Definitionen använder begreppet ”[bedriva] verksamhet” för att definiera ”verksamhetsutövare”, vilket är cirkulärt. Det anges inte i definitionen vilket slags aktivitet ”bedriva verksamhet” är, och den exemplifiering som lämnas i definitionen är inte tillräckligt tydlig för att precisera och avgränsa det definierade begreppet. Detta kan leda till tillämpningsproblem och rättsosäkerhet, i synnerhet då ”verksamhetsutövare” är ett så centralt begrepp i lagen.

1 kap. 3 och 4 §§ (offentliga/enskilda verksamhetsutövare)
I lagförslaget har utredningen gjort en huvudsaklig indelning av verksamhetsutövarna i två kategorier: offentliga och enskilda. Det saknas motsvarighet till denna indelning i artikel 2.1 i direktivet, där det inte görs någon

principiell åtskillnad mellan offentliga och privata rättssubjekt. Istället bestäms direktivets tillämplighet för såväl offentliga som privata entiteter utifrån typ enligt de angivna bilagorna och deras storlek.

I och med lagförslagets uppdelning av verksamhetsutövarna i offentliga respektive enskilda verksamhetsutövare, framstår det som att statliga myndigheter, regioner och kommuner endast kan omfattas i egenskap av just myndighet, region eller kommun (*offentliga förvaltningsentiteter*), vilket inte är fallet enligt direktivet. Det görs inte tydligt i lagförslaget att t.ex. en kommun som bedriver verksamhet inom hemsjukvård eller avfallshantering, eller en myndighet som bedriver verksamhet inom energisektorn, enligt direktivet också ska omfattas på de grunder som anges i artikel 2.1 (1 kap. 4 §).

Uppdelningen medför också en otydlighet med avseende på tillämpningen av 1 kap. 7 och 8 §§, som genomför artiklarna 2.2a-e och 2.4 i direktivet. Eftersom 7 och 8 §§ hänvisar till 1 kap. 4 § verkar dessa bestämmelser endast omfatta enskilda verksamhetsutövare, vilket avviker från direktivets utformning, då artiklarna 2.2a-e och 2.4 avser både offentliga och privata entiteter.

1 kap. 3 § - offentliga verksamhetsutövare
Enligt 1 kap. 3 § tredje punkten ska kommuner omfattas av lagens tillämpningsområde. Direktivet uppställer inget krav på detta. Som framgår av utredningen kommer de flesta kommuner att omfattas redan genom att de bedriver hemsjukvård, och med hänsyn till detta anges i utredningen att det ”i huvudsak [saknas] skäl att ta ställning till artikel 2.5 a om att medlemsstaterna får föreskriva att direktivet även ska tillämpas på offentliga verksamhetsutövare på lokal nivå” (s. 136 i utredningen). Den enda motivering som lämnas i utredningen för förslaget att låta samtliga kommuner omfattas av lagens tillämpningsområde är att det sker ”i fullständighetens namn” (s. 136 och s. 159).

1 kap. 4 § - enskilda verksamhetsutövare
Direktivets skrivning ”eller överstiger de trösklar för medelstora företag som avses i punkt 1 i den artikeln” har fallit bort i 1 kap. 4 § tredje punkten. Detta får till följd att inga företag med fler anställda, mer i årsomsättning eller mer i balansomslutning än vad som framgår av trösklarna för medelstora företag kommer att omfattas av lagens tillämpningsområde.

1 kap. 7 och 8 §§
Som framgår av kommentaren till 1 kap. 3 och 4 §§, så hänvisar 7 och 8 §§ endast till enskilda verksamhetsutövare. Någon motsvarande avgränsning finns inte enligt artiklarna 2.2a-e och 2.4 i direktivet. Hänvisningen till enbart enskilda verksamhetsutövare, som är en följd av lagförslagets struktur (där verksamhetsutövare delas in i offentliga resp. enskilda, och där merparten av direktivets krav endast tycks gälla för enskilda verksamhetsutövare), innebär en

otydlighet i fråga om de grunder på vilka olika verksamhetsutövare omfattas enligt direktivet.

Kap 2 – Klassificering och registrering

2 kap. 1 §
I 1 § anges vilka verksamhetsutövare som är väsentliga. Enligt andra punkten är ”verksamhetsutövare som bedriver verksamhet enligt bilaga 1 till NIS2-direktivet, är en kommun eller ett lärosäte med examenstillstånd och vars verksamhet överstiger trösklarna för medelstora företag enligt artikel 2 och 3.1–3 i bilagan till kommissionens rekommendation 2003/361/EG” väsentliga verksamhetsutövare.

Men skrivningen är otydlig, då den ger intrycket av att endast kommuner eller lärosäten omfattas. Otydligheten bör kunna läkas om det framgår att verksamhetsutövare som ”bedriver verksamhet enligt bilaga 1 till NIS2-direktivet *eller* är en kommun eller ett lärosäte med examenstillstånd *och* vars verksamhet överstiger trösklarna” omfattas av bestämmelsen. Med denna ändring skulle klassningen av verksamhetsutövare ske i enlighet med vad direktivet anger.

Kap 3 – Riskhanteringsåtgärder och incidentrapportering

3 kap. 1 §
I 3 kap. 1 § har man angett att ”*åtgärderna ska* utgå från ett allriskperspektiv och en riskanalys och *vara proportionella i förhållande till risken*.” Istället för att säkerhetsnivån ska vara proportionell i förhållande till risken, anges att *själva åtgärden* ska vara proportionell i förhållande till risken. Detta innebär att man förlorar den reglering av åtgärdernas ändamålsenlighet/lämplighet, som alla tidigare regelverk, inklusive NIS2-direktivet, åstadkommit. Valet av åtgärd kan emellertid inte enbart reduceras till en fråga om nivåer.

För att motverka betydelseförluster och bibehålla direktivets tydlighet bör därför en tydligare distinktion göras mellan de krav som avser åtgärderna själva och de krav som avser de säkerhetsnivåer som ska uppnås; som en del av detta bör rekvisitet ”lämpliga” (utöver ”proportionerliga”) föras in i lagtexten för att beskriva de riskhanteringsåtgärder som ska vidtas.

3 kap. 6 §
I 3 kap. 6 § används begreppet ”kunder”. Det definieras inte i lagen, men enligt utredningens uppfattning (s. 202) har uttrycket samma innebörd som formuleringen ”mottagarna av deras tjänster” i artikel 23.1 i direktivet.

Ordvalet är otydligt och innebär en betydelseförlust jämfört med direktivets formulering. Direktivets formulering ”mottagare av tjänster” bör ersätta lagförslagets ”kund”. Med hänsyn till det breda spektrum av mottagare som kan förekomma i t.ex. leverantörskedjor inom olika sektorer bör direktivets

formulering ”mottagare av tjänster” också definieras för att undvika tolknings- och tillämpningssvårigheter.

Kap 4 – *tillsyn*

4 kap. 1 §
Av 4 kap. 1 § ska ”den myndighet regeringen bestämmer” vara tillsynsmyndighet. Detta ger intrycket att regeringens bemyndigande begränsar sig till att utse en enda tillsynsmyndighet. Såväl kommittédirektivet som utredningen (avsnitt 8.4.1 och 8.4.2 samt s. 376) gör tydligt att det ska finnas en eller flera tillsynsmyndigheter för varje sektor. Om förslaget att dela upp tillsynsansvaret genomförs, bör ordalydelsen återspegla detta förhållande, så att regeringens bemyndigande blir tydligt.

Kap. 4 och 5 Cybersäkerhetslagen samt 8 och 13 §§ Cybersäkerhetsförordningen – *tillsyn och ingripanden*

Sektorstillhörigheten i centrum
Användningen av sektorer i NIS2 har ett huvudsyfte: att ringa in de mest samhällsviktiga aktörerna, de som ska omfattas av direktivet, så att cybersäkerheten höjs där detta behövs som mest. Men sedan de samhällsviktiga aktörerna väl har pekats ut, blir sektorstillhörigheten relativt oviktig. Det är det riskbaserade förhållningssättet, allriskperspektivet, riskanalyserna, riskhanteringsåtgärderna, incidentrapporterna etc. som tillsammans bygger upp den högre gemensamma nivån av cybersäkerhet. Mot denna bakgrund är det förvånande att tillsynsansvaret, så som det fördelas enligt 8 § i förslaget till Cybersäkerhetsförordning, helt utgår från sektorstillhörighet.

Svenska kraftnät vill inte förespråka någon centralisering av tillsynsverksamheten på cybersäkerhetsområdet till en enda myndighet, även om det skulle kunna ge vissa effektivitetsvinster. Informations- och cybersäkerhet har visserligen sedan länge utpekats som ett särskilt sektorsansvar med hemvist hos beredskapsmyndigheten MSB. Men cybersäkerhet finns hos i princip all samhällsverksamhet och får snarast betraktas som en metod eller ett verktyg, svår att separera från respektive organisations kärnverksamhet. Därför finns också en naturlig koppling till sektorsspecifika förmågor, vilket understryker vikten av att behålla nuvarande ordning. Emellertid finns det vissa oklarheter i lagförslaget gällande tillsynsmyndigheternas ansvar och ingripanden. Det gäller till exempel de mekanismer som föreslås hantera det s.k. dubbelprövningsförbudet. I 13 § i förslaget till Cybersäkerhetsförordningen anges att ”om tillsyn över en verksamhetsutövare utövas av fler än en tillsynsmyndighet ska respektive tillsynsmyndighet inte utöva tillsyn gällande den del av verksamheten som anges som en annan tillsynsmyndighets tillsynsområde i 8 §”. Bestämmelsen ger inte vägledning vad som gäller tillsynen av de intersektoriella verksamhetsutövarna eftersom dessa omfattas av flera sektorer och därmed tillsynsområden.

Ytterligare ett problem uppkommer i och med att tillsynsmyndigheterna *ska* ingripa enligt 5 kap. 1 § om en verksamhetsutövare har åsidosatt sina skyldigheter enligt lagen, men *får* avstå från att ingripa om någon annan tillsynsmyndighet har vidtagit åtgärder med anledning av överträdelsen. Eftersom det snarare kommer att vara regel än undantag att de intersektoriella verksamhetsutövarnas överträdelser berör samtliga dess sektorer blir frågan vilken av de olika sektorsmyndigheterna som ska ingripa mot överträdelsen (5 kap. 1 § i lagen), vem som inte ska utöva tillsyn mot överträdelsen (13 § i förordningen), och vem som får avstå från att ingripa (5 kap. 2 § i lagen). Det tycks inte finnas någon angiven turordning, och saken kan bli svår att avgöra. Det finns en risk att detta leder till en ineffektivitet och rättsosäkerhet samt medför ett stort behov av avstämningar och kontakter mellan tillsynsmyndigheterna.

MSB:s roll

Svenska kraftnät ser i sammanhanget positivt på den roll MSB hittills har haft som insamlande part i befintlig NIS-incidentrapportering. Svenska kraftnät ställer sig också bakom de förslag utredaren lagt fram vad gäller MSB:s sammanhållande och koordinerande roll.

En utökad roll för MSB skulle kunna diskuteras, till exempel vid framtagandet av gemensamma metoder för tillsyn, eller som koordinerande part då bilateral samverkan mellan sektorsmyndigheter inte räcker till. Det gäller även sådana multilaterala diskussioner som kan komma ifråga då flera sektorsmyndigheter berörs och det dessutom krävs samverkan kring säkerhetsskyddsfrågor. Detta kan dock kräva ytterligare reglering för utbyte av information som kan omfattas av sekretess.

Beslut i detta ärende har fattats av generaldirektör Lotta Medelius-Bredhe efter föredragning av informationssäkerhetschef Cem Göcgören och informationssäkerhetsspecialist Svante Nygren. I ärendets handläggning har även deltagit verksjurist Per Ekare och avdelningschef, tillika säkerhetschef och säkerhetsskyddschef, Erik Nordman

Sundbyberg, dag som ovan

Lotta Medelius-Bredhe

Cem Göcgören

DOKUMENT SIGNATURER

Innehållet i detta dokument är digitalt signerat.
Namn och tidpunkter visas på denna sida.

Signerad av:
Cem Göcgören
Tidpunkt:
2024-05-22 14:22:02

Signerad av:
Lotta Ebba Kristina Medelius Bredhe
Tidpunkt:
2024-05-22 15:19:27