Energimyndigheten

Box 310

Gredbyvägen 10

631 04 Eskilstuna

Er ref; Dnr 2019-003457

Vår ref; Dnr 2019-003457

Stockholm den 31 augusti 2020

SPBI Remissvar gällande Energimyndighetens föreskrifter och allmänna råd om riskanalys och säkerhetsåtgärder för energisektorn

SPBI har fått rubricerade remiss och har följande att anföra:

BAKGRUND

Statens Energimyndighet (STEM) har tagit fram förslag på föreskrifter om riskanalys och säkerhetsåtgärder för energisektorn i enlighet med lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (”NIS-lagen”). Förslaget är framtaget med stöd av 8 § i förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster (”NIS-förordningen”).

HUVUDSYNPUNKTER

SPBI anser att föreskriftsförslaget är väl utformat men behöver i vissa detaljformuleringar förtydligas för föreskriftstexten lättare kan förstås korrekt av verksamhetsutövaren.

- **Föreskriften 2 kap. 2;**

  Under 2 kapitlet ”Riskanalys”, § 2 första stycket sista meningen, pkt. 2, står följande formulering:

  ”Vid utförandet av omvärldsbevakningen ska leverantören särskilt analysera

2) tekniska trender och etablerad praxis avseende hotaktörer och sårbarheter i den hårdvara och mjukvara som används inom energisektorn”,

SPBI menar denna formulering ”etablerad praxis” har en alltför otydlig syftning på vad som avses med ”etablerad praxis avseende hotaktörer…”.

Hur kan verksamhetsutövaren veta vad "etablerad praxis avseende hotaktörer" egentligen är? Sådan ”etablerad praxis” kan f.ö. variera inom mycket stora spann i skilda typer av verksamheter. Skrivningen bör därför förtydligas.

Förslag till förtydligad formulering är t.ex.:

2) ”tekniska trender och kända modus operandi hos hotaktörer för intrångsförsök, cyberattack eller annan avsiktlig skadlig påverkan”.

- **Allmänna råden Kap. 2 § 4**

” I 2 kap 4 § tredje och sista stycket står*:*

” Incidenter som bör ingår i en riskanalys kan exempelvis vara antagonistiska angrepp, tekniska fel, fel orsakade av människan eller naturpåverkan”

Som det nu är skrivet kan texten förstås som att Energimyndigheten vill öppna upp för en mycket bred tolkning av vilka risker som behöver hanteras.

Ordvalen ger troligen även en felaktig hänsyftning. Det står under denna paragraf ”tekniska, fel orsakade av människan eller naturpåverkan” faller normalt under ”driftsäkerhet” och inte nödvändigtvis under ”cybersäkerhet”.

Enligt konsekvensutredningens definitioner på sida 6 menar Energimyndigheten att NIS-direktivet ämnar till en generell tolkning av säkerhet. SPBI menar att detta inte är tydligt utsagt eller ens att det behöver vara den korrekta tolkningen.

I Lag (2018:1174) 2§ pkt 2 beskrivs just att säkerhet med att motstå åtgärder.

”Säkerhet i nätverk och informationssystem: nätverks och informationssystems förmåga att vid en viss tillförlitlighetsnivå ***motstå åtgärder*** *som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de besläktade tjänster som erbjuds genom eller är tillgängliga via dessa nätverk och informationssystem”*

SPBI menar att det i Allmänna råden borde stå precis samma formulering om ”motstå åtgärder” som det redan står inskrivet i Lagen (2018:1174), snarare än den bredare tolkning som finns i nuvarande formulering som Energimyndigheten lagt in. Det saknas även råd och vidare beskrivning i hur ”tekniska, fel orsakade av människan eller naturpåverkan” ska motverkas och vad de innefattar.

Föreskriften 3 kap. § 5, punkten 1:

I 3 kap. §5, punkten 1 står det:

5 § ” Leverantören ska arbeta för att förebygga och minimera incidenter genom att

1. härda IT och OT hårdvara innan de börjar användas”, *när det är möjligt.*

Alternativt tillägg i pkt.1 kan även vara ….*”när de börjar användas” alt. ”när det är lämpligt i förhållande till identifierad risk”.*

SPBI menar att det bör läggas till ”när det är möjligt” i samma mening. Syftet med denna punkt är att ha en risk-baserad ansats till ett sådant krav. I vissa fall kan ett sådant krav på ”härdning” av OT system även skapa ökade risker i ”äldre” OT nätverk genom att det uppstår oväntade funktionsproblem (d.v.s. inter-operabiliteten mellan systemen försämras).

Generellt bedöms det som lämpligt att Energimyndighetens föreskrift korrelerar med Säkerhetsskyddslagens krav på riskvärdering d.v.s. samma krav borde speglas i båda lagstiftningarna.

- **Forts. Föreskriften Kap. 3, §5**

I §5 står följande: ”Leverantören ska arbeta för att förebygga och minimera incidenter genom att

Pkt. 1: "härda IT och OT hårdvara innan de börjar användas, ".

Är ordet "härda" det korrekta ordvalet i informationssäkerhetsnomenklatur? Läsaren kan givetvis intuitivt förstå innebörden, men nuvarande ordval associeras närmast till en annan metafor som relaterar till härdning av metallegering.

SPBIs förslag till ny formulering pkt. 1 är istället:

…/leverantören ska/ 1) ”säkerställa att IT och OT är skyddat genom t.ex. avstängning av icke nödvändiga funktioner i mjuk- och hårdvara eller funktion i nätverk som inte behövs för det avsedda syftet med installationen. Det kan t.ex. handla om att stänga av ej nödvändiga USB-portar, ej nödvändiga mjukvarufunktioner o.s.v. (s.k. "härdning").

3 kap. 3 § Allmänna råden

I 3 Kap 3§ i de föreslagna Allmänna råden beskrivs sätt att skydda IT och OT.

Dessa beskriver inte tydligt sätt att skydda sig mot tex naturpåverkan utan ser ut att huvudsakligen skydda mot antagonistiska angrepp.

I MSBFS 2018:8 2§ ska även externa aktörer kontrolleras om hantering av nätverk och informationssystem är utkontrakterade.

SPBI menar att denna breda tolkning kan innebära extremt stor arbetsmängd för berört företag, och SPBI menar det är ytterst olyckligt eftersom det inte är klargjort att tolkningen ens är korrekt.

Johan G Andersson

VD SPBI

Per Brännström

Ansvarig handläggare
HMS-Logistikansvarig