KraftCERT AS, org. Nr. 914881722
Vollsveien 19
1366 Lysaker
Tlf. 99436166

Lysaker 28.2.2018

Svar fra KraftCERT AS på høringsbrev om endringer i beredskapsforskriften, 201709983-1

Generelt anser vi det som svært positivt med de foreslåtte forenklinger, dette gjør forskriften klarere og lettere å forstå. Dette i ny §1-3, hvem forskriften gjelder for, §1-4 om ansvar, §1-5 om beredskapsplaner og §2-10 om internkontroll.

Vi vil gjerne fremheve en problemstilling, og det er leverandørenes kritikalitet. Dersom en leverandør leverer til et klasse2 eller 3 driftskontrollsystem, må de forholde seg til de aktuelle krav til disse, men dersom man har en leverandør som leverer til alle klasse1-anlegg så blir ikke dennes betydning eller krav til denne leverandør skjerpet. Samfunnsmessig er det problematisk om en leverandør står for levering av f.eks. AMS til 2 millioner innbyggere, og dette ikke fører til skjerpede krav overfor leverandøren.

§2-6d: «Sensitiv informasjon» kan fortsatt spisses til å bli mer presist.

§3-6: Ad sektorvist responsmiljø:
Vi tror at det vil være mest hensiktsmessig å pålegge tilknytning til sektorvist responsmiljø.

- Dette vil styrke beredskapen på tvers i sektoren, da det vil gi en bedre forutsetning for å å håndtere hendelser i selskap i hele landet.
- Både det enkelt selskap og beredskapsmyndigheter vil få et mer helhetlig bilde av faktiske angrepstall og situasjonsbilde.
- Det vil også bygge opp en fellesskapsfølelse der alle selskap er med på å sikre den felles infrastrukturen i landet, ikke bare de selskapene som velger å satse.

Det er naturlig responsmiljøet pålegges å levere trusselbilde, statistikker og annen relevant informasjon til NVE, slik at beslutninger kan tas på et korrekt og oppdatert grunnlag.

§3-7: Sektor-CERT/sektorvis responsmiljø bør også involveres dersom arbeidet med sikkerhetsmyndigheten er innenfor sektorCERTs virkeområde

§6-5, §6-9e-f: Anskaffelser.

- Det bør presiseres at alle selskaper som gjør anskaffelser eller outsourcer må sjekke at underleverandører til deres underleverandør også har tilsvarende sikkerhetskrav.
- Det bør inkluderes at myndighetene har mulighet til å være med på revisjon/gjennomgang av underleverandør.
- Dersom selskap outsourcer bør det kunne stilles krav til underliggende hardware. I den siste tiden har vi sett sårbarheter som har muliggjort lesing av andres data på tvers av virtuelle maskiner dersom man var på samme hardware. Man kan lett se for seg at det kommer sårbarheter som åpner for skriving. Man kan enten kreve noe om at det er isolert hardware, eller kanskje at de som er på samme hardware er på samme sikkerhetsnivå.

KraftCERT AS, org. Nr. 914881722
Vollsveien 19
1366 Lysaker
Tlf. 99436166

§6-10:
a) “Fjernstyring av brytefunksjonaliteten skal utføres fra en adgangskontrollert sone”. Den fysiske sonen betyr lite i forhold til adgangskontroll og -audit digitalt. Dessuten er det ikke oppgitt hva adgangsreguleringen skal gå ut på.
b) (gjelder også §7-14) Bør det i stedet for bare å henvises til EU/EØS, heller fokuseres på sikkerhetssjekk av de person hos underleverandør som skal jobbe med løsningene, jfr. Transportstyrelsen?
I tillegg: “tidsavgrenset” I tilgangsbeskrivelse bør spesifiseres så man unngår “1 år”. Det bør også inkludere fortløpende aksesslogg på personbasis.
c) Det er i praksis ikke mulig å sperre for at en person kobler ut flere målepunkter samtidig dersom dette er en som i utgangspunktet har tilegnet seg urettmessig tilgang. Kan man koble ut en, kan man koble ut flere. Man kan forhindre at noen med legitim adgang gjør en glipp, men ikke en villet handling, det er alltids mulig å automatisere enkeltutkoblinger.
x) Det bør inn at det skal finnes en recoverymetode. Dersom uvedkommende utløser brytefunksjonen og deretter krasjer enheten bør det finnes mekanismer for recovery av enheten.

§7-4, §7-14: Det er beskrevet hvorfor man går fra “person” til “bruker”. Vi mener derimot at dette kan tolkes til “rolle” slik det står nå, og at det åpnes for deling av “bruker” mellom flere personer. Det bør spesifiseres at dette ikke er tillatt.

§7-7: Om det er cyberrelatert så bør det sektorCERT/sektorvise responsmiljøet også involveres.