Energistyrelsen
Carsten Niebuhrs Gade 43
1577 København V
Att.: Philip Gunnar Bjerg Mortensen, phlmt@ens.dk

Biogas Danmark
Axeltorv 3
1609 København V

15. november 2024

Ekstern høring af endeligt ROS-scenarie katalog

Energistyrelsen har udsendt endeligt udkast til ROS-scenarie katalog i ekstern høring.

Generelle bemærkninger

Biogas Danmark er enig i, at det er meget vigtigt, at myndigheder, forsyningsselskaber, ejere af gas- og elinfrastrukturen, varme- og vandforsyning m.v. forholder sig til det aktuelle risikobillede – såvel fysisk sikkerhed som cybersikkerhed.

Det samme gælder virksomheder, som leverer via el- og gasinfrastrukturen. Det er imidlertid vigtigt at være opmærksom på, at der er afgørende forskel på om det er Energinets kontrolrum der rammes eller det er et biogasanlæg, som leverer promiller af det årlige gasforbrug.

Det er ikke desto mindre også i virksomhedernes egen interesse at forholde sig til de aktuelle risici med henblik på at sikre virksomhedens drift. Derfor er det vigtigt, at virksomhederne selv forholder sig til de potentielle risici og på baggrund heraf, udarbejder beredskabsplaner på et passende niveau.

I den forbindelse kunne det være hensigtsmæssigt, at tankegangen og sprogbrugen tilpasses, så bliver tydeligt, at det er med henblik på at bistå virksomhederne i at skærpe deres egen årvågenhed, når der er tale om enkeltstående biogasanlæg og ikke Energinet.

I den forbindelse kunne det overvejes i højere grad at fokusere på vejledning af virksomhederne i deres skærpelse af bevågenheden overfor aktuelle og potentielle fremtidige trusler. Der kan for eksempel søges inspiration i det finske system, som blev præsenteret på Nordic Biogas Conference 2024 i Aalborg 22. – 23. oktober 2024.

I den forbindelse kunne det også være hensigtsmæssigt med en kortere og mere overskuelig præsentation af helt basale anbefalinger til skærpelse af agtpågivenheden – såvel i forhold til fysiske trusler som til cybertrusler. Sådanne værktøjer kan bruges af ledelsen til at formidle i hele virksomheden / organisationen.

De kan også bruges i forhold til virksomhedernes dialog med leverandører af IT-systemer. Her er det vigtigt at være opmærksom på, at det jo i høj grad er leverandøren af IT-systemerne til de enkelte biogasanlæg, som kan sikre grundlaget for, at sikkerheden er i orden, hvorimod virksomhedens egen ledelse skal sikre adfærden.

Specifikke bemærkninger

En lang række af scenarierne er slet ikke eller kun i begrænset omfang relevante for biogasanlæg. Det er i høj grad leverandører af IT-systemer, som skal sikre systemerne er hensigtsmæssigt opbygget. Samtidig adskiller biogasanlæg sig fra andre i energisektoren i forhold til råvaregrundlag. I det følgende nævnes en række eksempler:

- Biogasanlæg har høj grad af mulighed for at fjernbetjene anlægget, hvorfor manglende adgang til kontrolrum er af mindre betydning (scenarie 1 og 2).
- Alle biogasanlæg har et vist oplag af biomasse og er i forvejen gearet til ikke at tilføre biomasse i weekender, og gasproduktionen vil køre videre i ugevis efter stop af tilførsel, hvorfor en kort periode med vintervejr ikke vil være kritisk (scenarie 2 og 3).
- Ekstremvejr er næppe en særlig udfordring for velplacerede biogasanlæg (scenarie3, 4, 5 og 6)
- Solstorm er et generelt IT-issue – ikke specielt i forhold til biogasanlæg (Scenarie 7)
- Biogasanlæg er ikke et kraftværk og bruger derfor ikke kølevand (scenarie 8).
- Pandemier fik alle virksomheder en fuldscala øvelse på med corona (scenarie 9)
- Adgang til anlægget er individuelt for anlæggene, herunder i fx besøgende, skoleklasser m.v. (scenarie 10)
- I forhold til aktivisme og lignende, så er biogasanlæg ikke kritiske på time/dagsbasis (scenarie 11)
- Det er altid godt at lave awareness kampagner (scenarie 14)
- Biogasanlæg har ikke et hovedbrændsel – alle biogasanlæg bruger mange forskellige råvarer (scenarier 16)
- Regionale udfald i elsystemet er ikke relevante for biogasanlæg (scenarie 17-18)
- Fjernaflæste målere er relevante for forsyningsselskaber, ikke biogasanlæg (scenarie 20)
- IT-scenarierne er vigtige for leverandørerne af IT-systemer mere end biogasanlægget selv (scenarie 21 ff)
- Biogasanlæg har i sig selv ikke forsyningskritisk IT – er kun en lille bidragsyder til forsyningen (scenarie 32 mfl)
- Kompromittering igennem mobile enheder er et klart observationspunkt (scenarie 36)
- Utilstrækkelig cyberhygiejne er et klart fokuspunkt i forhold til virksomheders drift (scenarie 41 og 43)
- Strømsvigt kan være en udfordring – men vil ofte være håndteret med nødstrømsanlæg (scenarie 44)

Afsluttende bemærkninger

Biogas Danmark står naturligvis til rådighed for en uddybning og for videre dialog.

Med venlig hilsen

Bruno Sander Nielsen
2724 5967
bsn@biogas.dk