Notat

Dato: 09. september 2024

Beredskab Cybersikkerhed

Dette Notat er lavet på baggrund af at Regeringen juni 2024 har hævet trusselsniveauet for destruktive cyberangreb mod Danmark fra LAV til MIDDEL, på baggrund af, at FE og PET har informeret om en skærpet hybrid trussel mod Danmark.

Natur og Miljø har bedt forsyningsselskaberne i Norddjurs, om at beskrive hvad de enkelte selskaber gør med henblik på at sikre sig mod cyberangreb. - Herunder om det øgede trusselsniveau konkret har givet anledning til ændringer, overvejelser.

Varmeværker

Grenaa Varmeværk har fremsendt følgende:

Grenaa Varmeværk har tilsluttet sig SektorCERT, som er de kritiske sektorers cybersikkerhedscenter.

SektorCERT er en væsentlig del af sektorernes forsvar mod cybertrusler. Vi er med til at opdage og håndtere, når den kritiske infrastruktur udsættes for cyberangreb, og det er hos os, den afgørende viden som kan forebygge det næste angreb, opbygges og deles.

Vi varetager blandt andet monitoreringen af de virksomheder i sektorerne, som er tilsluttet vores omfattende sensornetværk. Via sensornetværket monitorerer vi internettrafikken med henblik på at opdage cyberangreb mod dansk, kritisk infrastruktur.

SektorCERT er en nonprofit forening ejet og finansieret af danske selskaber inden for kritisk infrastruktur. Vi samarbejder med Europas andre CERT'er og er med i en række cybersikkerhedsorganisationer som gør, at vi har stor viden om truslerne mod kritisk infrastruktur.

Se eventuelt mere på www.sektorcert.dk her er der en lang række beskrivelser af hændelser der har fundet sted m.m.

TLV Forsyning har fremsendt følgende:

Vores beredskab i forhold til de stigende usikkerheder i verden og det generelle hævede trusselsniveau er det samme som beskrevet af Søren og Grenaa Varmeværk A.m.b.a.

Vi er ligeledes tilsluttet SektorCERT, og har derigennem tilsluttet både software- og hardwaremæssige installationer som hjælper dels sektoren med konstant at overvåge, og ligeledes lokalt imødegå mulige cyberangreb.

Derudover har vi vores egne lokale og generelle beredskabsplaner for både vand- og varmeværker, samt opbygget et redundant serversystem, hvor vi i givet fald vil kunne udskille det/de ramte servere og lægge IT-driften over på andre fysiske maskiner.
Dette omfatter både produktions- og administrative systemer.

De har efterfølgende uddybet det yderligere:

TLV Forsyning har anskuet cybersikkerhed som en essentiel del af vores forsyning og daglig drift.

Derfor er der taget de nødvendige skridt for at forsøge at være på forkant med udviklingen indenfor cybersikkerhed.

Det omfatter uden at gå for meget i detaljer følgende:

- *Multi faktor godkendelse på så meget vi kan (Systemer kan blive valgt fra hvis dette ikke tilbydes)*
- *Lokalt styret data fremfor at være afhængig af ''skyen''. Skyen bruges stadig, bare i en anden funktion.*
- *Backup strategi 3-2-1 (3 kopier af data, på 2 forskellige medietyper og 1 off-site). Hvor vi her udvider det løbende så vores ombygget værker spiller en essentiel del i denne plan på deres lokationer.*
- *Multi redundante SRO styringer i forbindelse med ombygninger og moderniseringer af vores varme- og vandværker. Som sikre at vi kan forsætte driften lokalt og på tværs af vores MPLS netværk.*
- *Sikring af brugers arbejdsstationer/Pc'er, hvor der bliver skabt daglige backups/snapshots som vi gøre os i stand til hurtigt at få en medarbejder op at køre igen ved nedbrud eller sågar hvis hele TLV Forsyning blev ramt.*
- *Tilslutning af SektorCERT og løbende dialog i deres fora om hvad kan gøres bedre osv.*

Spildevand
AquaDjurs har fremsendt følgende:

AquaDjurs havde cybersikkerhed på bestyrelsens dagsorden her i foråret, hvor vi fik bevilget 1. mill. til at gøre AquaDjurs compient på IT-sikkerhed, NIS2 og GDPR.

Der blev stillet spørgsmål til IT-sikkerhed på selskabets generalforsamling – den skriftlige orientering til ejerkommunerne er vedhæftet (afsnit 1 i redegørelsen.)

Jeg vedhæfter hele sagsfremstillingen og beslutningen fra bestyrelsesmødet, som jeg tror dokumenterer at vi har taget truslen alvorligt.

Til yderligere orientering har vi netop indgået aftale med GAP-solution om at implementere manglende IT, NIS2 og GDPR løsninger her i efteråret.

Vandværker

For at forenkle overblikket, fremgår vandværkerne af vedhæftede skema.