INTELLIGENT ENERGI

10 anbefalinger om it-sikkerhed i udbudsprocesser

10 anbefalinger om it-sikkerhed i udbudsprocesser

Elsektorens virksomheder har en lang tradition for beredskabsarbejde. Her har it-sikkerhed i de seneste år fået stigende opmærksomhed. En undersøgelse af energisektorens håndtering af it-sikkerhed, foretaget af PwC i sommeren 2015 viser, at sektoren generelt er rustet til at møde nye it-sikkerhedsudfordringer[1]. Udfordringerne ændres løbende, og det er derfor nødvendigt hele tiden at skærpe opmærksomheden over for potentielle sårbarheder.

Med introduktionen af smarte komponenter i el-nettet, er det formålet at sikre en intelligent styring og overvågning af el-nettet. Den intelligente styring af de enkelte komponenter øger dog også sårbarheden ift. data- og it-sikkerhed. Det er derfor vigtigt, at it-sikkerhed tænkes ind, når der indkøbes smartgrid-komponenter og andre komponenter.

Intelligent Energi giver her nogle overordnede anbefalinger til øget fokus på it-sikkerhed i udbudsprocesserne. Vi anbefaler ikke specifikke løsninger eller bestemte sikkerhedsniveauer, men alene, at der tages stilling til it-sikkerhed i udbudsprocesserne. Da it-sikkerhed kan være relativt omkostningsfuldt, vil en manglende præcisering i udbudsmaterialet medføre, at it-sikkerheden ikke indgår som en konkurrenceparameter. Dette kan gøre selve udbuddet billigere i første omgang, men dyrere i sidste ende. Kun ved at tage aktiv stilling til sikkerhedsniveauet kan selskaberne sikre, at de får det niveau, der efterspørges og betales for.

Nedenstående anbefalinger kan bruges som huskeliste, når der planlægges udbud af smart grid-komponenter. Målgruppen er ledelse, udbudsansvarlige og it-sikkerhedsansvarlige i netselskaberne, men anbefalingerne kan også bruges andre steder i energisektoren.

Udbudsprocessen

1. Involver de rigtige personer fra start
Når udbudsmaterialet skal forberedes, er det vigtigt, at de rigtige personer involveres fra starten - herunder også de it-sikkerhedsansvarlige. Dette skal sikre, at de tekniske beskrivelser også tager højde for det ønskede it-sikkerhedsniveau samt potentielle sårbarheder og risici. Det er vigtigt, at de personer, som har ansvar for den efterfølgende drift, også inddrages i udformningen af systemet.

2. Tænk i sammenhæng med eksisterende beredskab
Elsektorens virksomheder opdaterer løbende sit beredskabsarbejde (i forretningen fx driften af el-nettet). Det er vigtigt, at it-sikkerhed i smartgrid-komponenter ses i sammenhæng med dette beredskabsarbejde – herunder de strategiske valg ift. det sikkerhedsniveau, der tilstræbes.

3. Udarbejd behovsanalyse og designmanual
Der bør udarbejdes en behovsanalyse, så alle er enige om de til- og fravalg, der foretages ift. it-sikkerhed. En designmanual skal gøre det klart for leverandørerne, hvilket sikkerhedsniveau, der forventes og skal sikre, at dette bliver et konkurrenceparameter.

[1] http://www.ens.dk/sites/ens.dk/files/energistyrelsen/Nyheder/2015/pwc_rapport_-_it-modenhedsundersoegelse_052015.pdf

4. Vælg serviceniveau – ikke teknologien
Ved at vælge et serviceniveau frem for en bestemt teknologi sikres det, at leverandørerne kan konkurrere på innovation og individuelle løsninger samtidig med, at det ønskede sikkerheds-niveau opnås.

5. Stil krav til kompatibilitet
Det er af stor betydning, at nyindkøbte komponenter er kompatible med de eksisterende komponenter, men også med fremtidige komponenter. Det kan derfor være en god ide med en compliance-manual, der beskriver specifikke standarder, som de indkøbte komponenter bør leve op til.

6. Beskriv krav til datatransport, - håndtering og - opbevaring
Som minimum bør det i udbudsmaterialet beskrives, hvilke ønsker der er til sikringen af data mellem smartgrid-komponenterne: skal kommunikation være krypteret, leve op til specificerede standarder, skal der foretages logning mm.?

7. Beskriv krav til kommunikation med leverandør
Det bør allerede i udbudsmaterialet fremgå, hvilke krav der stilles til kommunikationen med leverandøren. Bør kommunikationen fx være krypteret, og hvem må få adgang til informationer og data?

8. Beskriv krav vedrørende leverandørens adgang til systemet
Leverandørers adgang til smartgrid-komponenter er en potentiel sårbarhed, og bør derfor beskrives i udbudsmaterialet. Bør der fx kræves 2-faktor-login ved fjernadgang, vil der kun kunne gives adgang via tidsbegrænsede servicevinduer, og bør systemadgang begrænses til computere uden internetadgang mv.?

9. Beskriv krav til leverandørens it- og datasikkerhed
Der bør stilles klare krav til leverandørers it- og datasikkerhed – herunder at leverandører har udarbejdet en it-sikkerhedspolitik, som afspejler specificerede krav, og at medarbejderne har fuldt og dokumenteret kendskab til leverandørens sikkerhedspolitik.

10. Beskriv krav til serviceaftale og sikkerhedsopdateringer
Ønsker til det efterfølgende samarbejde med leverandøren bør beskrives i udbudsmaterialet. Det gælder ikke mindst serviceaftale og procedurer for sikkerhedsopdateringer.

INTELLIGENT ENERGI

KONTAKT

DANSK ENERGI
Vodroffsvej 59
1900 Frederiksberg

+45 35 300 400
WWW.DANSKENEI.DK
DE@DANSKENERGI.DK

DANSK ENERGI
Kontakt
Jeppe Røn Hartmann
Tlf. 35 300 442
jrh@danskenergi.dk