Forundersøgelse af modenheds- og sikkerhedsniveauet inden for cyber- og informationssikkerhed blandt danske el- og naturgasselskaber

Rapport
20. maj 2015

pwc

Revision. Skat. Rådgivning.

Indhold

	Slide
Indledning	3
Om spørgeskemaundersøgelsen	4
Svarprocenter - respondenter	5
Forklaring af resultater og evalueringsmodel	7
Samlet resultat og konklusion	8
A. Ledelsesforankring	9
B. Medarbejdersikkerhed	11
C. Beskyttelse af data	13
D. Beredskab	15
E. Processer	17
F. Fysisk sikkerhed	19
G. Teknologi	21
Delkonklusioner - virksomhedstyper	24
Bilag 1: modenhedsskala	31

Indledning

Som led i den nationale strategi for cyber- og informationssikkerhed har Energistyrelsen (ENS), i samarbejde med Energinet.dk (ENDK), ønsket at skabe et overblik over det nuværende modenhedsniveau og sikkerhedsniveau af informationssikkerhed i energisektoren.

Et sådant overblik skal bidrage med empiri og fakta i den aktuelle debat om, hvorvidt branchen er tilstrækkeligt beskyttet i forhold til de skærpede trusler mod virksomheder, der er en del af Danmarks kritiske infrastruktur.

ENS og ENDK har ønsket at få en indledende vurdering af, om virksomheder i sektoren har implementeret sikkerhedsprocesser, der medvirker til at opnå og vedligeholde et passende sikkerhedsniveau.

Denne vurdering angiver desuden, hvorvidt tilstrækkelige kontroller er implementeret og forankret i de organisationer, der medvirker.

PwC har i foråret 2015 assisteret ENS og ENDK med at gennemføre en spørgeskemaundersøgelse af virksomhederne i el- og naturgassektoren samt med at evaluere de individuelle besvarelser og resultater, der er sammenfattet i denne rapport.

It- og informationssikkerhed er sensitivt, og der er derfor taget særlige forbehold for at beskytte fortroligheden og anonymiteten af de enkelte virksomheders besvarelser. De medvirkende myndigheder har ikke haft adgang til individuelle virksomheders besvarelser i forbindelse med undersøgelsen eller afrapportering, men udelukkende til de aggregerede resultater.

Forbehold

Denne rapport er resultatet af en spørgeskema-undersøgelse og de besvarelser, der danner grundlag for resultaterne, er respondenternes egen vurdering af modenhed og sikkerhedsniveau. Resultaterne afspejler dermed ikke en revision eller anden dybdegående vurdering af sikkerheden foretaget af en uvildig tredjepart.

Ligeledes bør det pointeres, at der i denne rapport ikke er taget udgangspunkt i virksomhedernes kritikalitet i forhold til den samlede forsyningssikkerhed: Besvarelser fra et mindre selskab med få kunder er vægtet på samme måde som svarene fra et større selskab, som dækker en større region.

Om spørgeskemaundersøgelsen

Denne undersøgelse er blevet gennemført i perioden 26. februar 2015 - 20. marts 2015.

Der er blevet udsendt spørgeskemaer til 77 organisationer fordelt på følgende virksomhedstyper:

- El-netselskaber
- El-produktionsselskaber
- Naturgasdistributionsselskaber
- Naturgastransportselskaber
- Produktionsbalanceansvarlige
- Systemansvarlige transmissionsvirksomheder

Undersøgelsen har overordnet set afdækket, hvorvidt de medvirkende virksomheder:

1. Har en tilstrækkelig styring af informationssikkerhed ved at stille spørgsmål til modenheden af de processer, der skal medvirke til at opbygge og vedligeholde et passende sikkerhedsniveau over tid

2. Har implementeret sikkerhedskontroller, der i tilstrækkelig grad beskytter virksomhederne mod relevante it-risici ved at stille spørgsmål til de konkrete tiltag, der er implementeret.

De involverede virksomheder er blevet stillet 29 spørgsmål inden for syv kategorier:

A. Ledelsesforankring af informationssikkerheden

B. Informationssikkerhed i forhold til medarbejdere

C. Beskyttelse af data

D. It-beredskab

E. Processer for styring af informationssikkerhed

F. Fysisk sikring

G. Teknologianvendelse til sikring af it- og informationsaktiver

Spørgsmålene og svarmulighederne er udarbejdet af PwC i samarbejde med Dansk Energi, Energistyrelsen, Energinet.dk såvel som repræsentanter fra branchen.

Kategorierne og de enkelte spørgsmål er beskrevet senere i rapporten.

Svarprocenter - respondenter

Virksomhedstype	Antal virksomheder - udsendelser	Besvarelser antal (%)
El-netselskaber	38	30 (79%)
El-produktionsselskaber	19	15 (79%)
Naturgasdistributionsselskab	4	3 (75%)
Naturgastransportselskab	9	4 (44%)
Produktionsbalanceansvarlige	6	4 (67%)
Systemansvarlig transmissionsvirksomhed	1	1 (100%)
Samlet	77	**57 (74%)**

Resultater for el- og naturgassektorerne

Forklaring af resultater og evalueringsmodel

Som nævnt, så afdækker denne forundersøgelse henholdsvis modenhedsniveauet såvel som det aktuelle sikkerhedsniveau af de medvirkende virksomheder.

Modenhedsniveau

En række af de stillede spørgsmål har fokus på at afdække modenhedsniveauet for de interne processer, der medvirker til, at en virksomhed kan opbygge og vedligeholde et tilstrækkeligt sikkerhedsprogram.

Modenhedsniveauet er angivet på en 5-trins CMMI-modenhedsskala. Niveauerne 1-5 angiver, i hvilken grad virksomheden har formaliseret og optimeret sikkerhedsprocesser og -procedurer, så ensartede resultater kan opnås over tid. Et anbefalet minimums-niveau for styring af sikkerhed på tværs af brancher er på 3, hvilket angiver, at processer er veldokumenterede og kommunikerede i virksomheden. For særligt kritiske processer bør virksomheder have et modenhedsmål på 4, hvilket afspejler, at virksomheden kan måle effekten af de implementerede sikkerhedskontroller og gribe ind, hvis de ikke fungerer effektivt. I en organisation er det naturligvis ikke alle processer, der har samme kritikalitet, og den enkelte virksomhed bør prioritere indsatsen på basis af en risikobetragtning.

Skalaens niveauer er beskrevet i Bilag 1.

Sikkerhedsniveau

Vi har i denne undersøgelse også undersøgt, hvilke konkrete sikkerhedstiltag de medvirkende virksomheder har implementeret for at beskytte deres informationsaktiver.

I modsætning til måling af modenhed, så findes der ikke en entydig vurderingsskala for en virksomheds sikkerhedsniveau.

Vi har i denne undersøgelse anvendt en 5-trins skala, hvor **1** afspejler, at virksomheden ikke har implementeret selv de mest grundlæggende kontroller, og at der dermed er et meget lavt sikkerhedsniveau inden for det pågældende område, og **5** afspejler, at virksomheden har implementeret tiltag, der i høj grad afspejler sikkerhedsmæssig best practice og bør udgøre en meget høj beskyttelse af virksomheden i forhold til det aktuelle trusselsbillede.

Samlet resultat og konklusion

Resultaterne af denne undersøgelse har vist, at branchen samlet set har et sikkerhedsniveau, der ligger på 2,8.

Vores vurdering af energisektorens modenhedsniveau og de implementerede sikkerhedskontroller er et udtryk for et relativt højt sikkerhedsniveau sammenholdt med virksomheder i andre brancher.

Energibranchen har et naturligt fokus på sikkerhed. Det er virksomhedernes primære opgave at opretholde forsyningssikkerheden. Derudover er driftsstabilitet og beredskab såvel som fysisk sikring af faciliteter naturlige opgaver, der varetages.

Dette reflekteres i den måde, hvorpå it- og informationssikkerheden er grebet an. Resultaterne af denne undersøgelse afspejler, at der er implementeret mange gode tiltag, herunder både administrative og tekniske kontroller, der medvirker til at beskytte informationssikkerheden.

Implementering af disse tiltag er dog ikke nødvendigvis foretaget med udgangspunkt i en formaliseret tilgang, hvor alle sikkerhedstiltag er lavet på basis af en aktiv stillingtagen til forretningens risiko. Det er vores vurdering, at i størstedelen af de medvirkende virksomheder er de implementerede tiltag og det høje sikkerhedsniveau et udtryk for en intuitiv tilgang, der er resultat af dygtige medarbejderes erfaring samt traditionelt omfattende beredskabskrav til sektoren.

En sådan tilgang medfører en vis risiko for, at virksomhederne over tid ikke opretholder et sikkerhedsniveau, der i passende grad beskytter virksomheden mod nye komplekse trusler fra organiserede cyberkriminelle og fremmede statslige aktører, der målretter den kritiske infrastruktur.

Resultaterne af undersøgelsen viser, at der er sammenhæng mellem virksomhedernes modenhed og deres størrelse. De større selskaber med regionalt ansvar har etableret formaliserede procedurer for styring af informationssikkerhed.

A. Ledelsesforankring

Kontrolmål

For at sikre, at it- og informationssikkerhed styres og implementeres med udgangspunkt i virksomhedens forretningsrisiko, bør der være implementeret processer, der 1) sikrer, at ledelsen kan forholde sig til risikobilledet, 2) sikrer, at ledelsens forventninger til sikkerhed er dokumenteret og kommunikeret entydigt til organisationen, og 3) sikrer, at roller og ansvar er defineret og forankret i organisationen.

Der er stillet spørgsmål relateret til:

1. It-risikovurdering – Er der foretaget en it-risikovurdering, og har ledelsen accepteret den aktuelle risiko? En it-risikovurdering indebærer en evaluering af sandsynligheden for, at en it-relateret trussel indtræffer, samt af hvilken forretningsmæssig konsekvens den kan have ift. brud på fortrolighed, integritet og tilgængelighed af data, systemer og processer. It-risikovurderingen bør anvendes til at prioritere sikkerhedsmæssige tiltag på både administrative systemer og produktionssystemer.
2. Retningslinjer for informationssikkerhed – Findes der retningslinjer for informationssikkerhed inden for relevante områder? Retningslinjer udtrykker den overordnede politik for informationssikkerhed inden for specifikke områder, evt. struktureret i henhold til en accepteret standard (fx ISO27000).
3. Ledelse af informationssikkerhed – Påser ledelsen styringen af informationssikkerhed i organisationen?

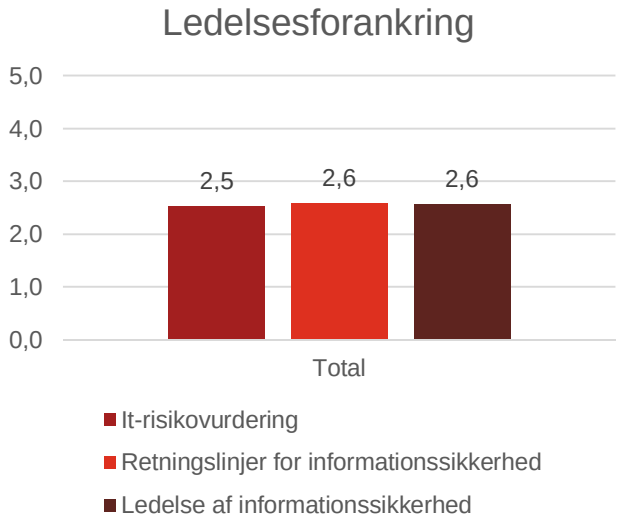
Resultater - ledelsesforankring

Resultaterne af undersøgelsen viser, at ledelsesforankring af informationssikkerhed i energibranchen ligger på et gennemsnitligt niveau på 2,6.

I tre fjerdedele af de adspurgte virksomheder er ledelsen bevidst om, at informationssikkerheden er ledelsens ansvar, og i over halvdelen af de adspurgte virksomheder overvåger ledelsen området i passende omfang.

Der anvendes it-risikovurderinger i over halvdelen af de adspurgte virksomheder, især til vurdering af nye projekter, men det er kun i en tredjedel, at der er etableret en ensartet, formaliseret proces for it-risikovurdering, der muliggør det for den øverste ledelse at vurdere den overordnede it-risiko og godkende risikobilledet såvel som tiltag, der skal medvirke til at bringe it- og informationssikkerhedsrisici til et acceptabelt niveau.

Der er i tre fjerdedele af de adspurgte virksomheder etableret retningslinjer og skriftlige procedurer for, hvordan informationssikkerheden skal styres på de mest kritiske aktiver. Det er dog kun i få virksomheder, at der er etableret kontrolmål (succeskriterier) og processer, der gør det muligt at måle, i hvilken grad de enkelte kontrolmål er opfyldt.



B. Medarbejdere

Etablerede procedurer for personalesikkerhed medvirker til minimering af risici forbundet med medarbejdere, herunder at alle medarbejdere har kendskab til og efterlever deres ansvar i forbindelse med deres arbejde med virksomhedens systemer og data.

Der er stillet spørgsmål relateret til:

4. Efterprøvning af jobkandidaters baggrund – Foretages der en passende efterprøvning af jobkandidaters baggrund med udgangspunkt i kritikaliteten af den jobfunktion, som kandidaten er tiltænkt at bestride? Jobfunktioner, hvor der eksempelvis er adgang til fortrolige data eller til systemer, der er kritiske for forsyningssikkerheden.

5. Information til medarbejderne om informationssikkerhed – Bliver medarbejderne løbende gjort bekendt med deres rolle og ansvar i relation til beskyttelse af informationssikkerhed?

6. Beskyttelse af informationssikkerhed ved afskedigelse/fratrædelse af medarbejdere – Er der etableret en passende procedure til beskyttelse af informationssikkerheden ved afskedigelse/fratrædelse af medarbejdere?

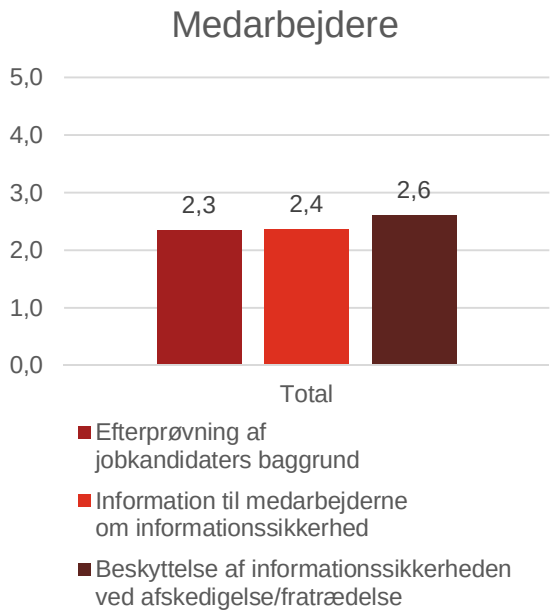
Resultater - medarbejdere

Resultaterne af undersøgelsen viser, at de kontroller, der er relateret til medarbejderens rolle i forhold til informationssikkerhed i energibranchen, ligger på et gennemsnitligt niveau på 2,4.

I ca. halvdelen af de adspurgte virksomheder tages der stilling til, om en jobkandidat skal baggrundstjekkes inden ansættelse, ligesom der i rekrutteringsprocessen er krav til, at referencer og evt. straffeattest skal afgives. Der er i meget få tilfælde krav om, at medarbejdere skal sikkerhedsgodkendes inden ansættelse i kritiske jobfunktioner.

Størsteparten af de adspurgte virksomheder har formelle procedurer såvel som tjeklister, der tager højde for inddragelse af it-aktiver og adgangsrettigheder ved fratrædelse eller afskedigelse af medarbejdere. Ca. en tredjedel af virksomhederne har en procedure for at implementere ekstraordinær overvågning for at påse, om der er forekommet uregelmæssigheder, når en medarbejder fratræder en kritisk jobfunktion.

Størsteparten af de adspurgte virksomheder gør medarbejderne formelt bekendt med deres rolle og ansvar i relation til informationssikkerhed ved ansættelse, og ligeledes kommunikerer størstedelen af virksomhederne de relevante dele af informationssikkerhedspolitikken regelmæssigt til medarbejderne.



C. Beskyttelse af data

Der bør være etableret procedurer, der sikrer beskyttelse af data og informationer i virksomheden såvel som hos tredjepartsleverandører.

Der er stillet spørgsmål relateret til:

7. Kategorisering/klassifikation og beskyttelse af data – Er data kategoriseret/klassificeret, og beskyttes data i henhold til denne kategorisering?
8. Beskyttelse af personhenførbare oplysninger – Hvordan er personhenførbare oplysninger beskyttet? Personhenførbare oplysninger kan henføre til eksempelvis både medarbejderes løn-, ansættelses- og helbredsoplysninger såvel som kunders stamdata, målerdata eller betalingsoplysninger.
9. Krav til databeskyttelse over for eksterne leverandører – Er virksomhedens it-sikkerhedspolitik, herunder krav til databeskyttelse, gjort gældende over for relevante eksterne leverandører?
10. Overblik over vigtige informationsaktiver – Er der et tilstrækkeligt overblik med de vigtigste informationsaktiver (de it-systemer og databærende medier, der er kritiske for at understøtte virksomhedens forretning)?
11. Kryptering – Hvordan anvendes kryptering i virksomheden til at beskytte datas fortrolighed og integritet?

Resultater – beskyttelse af data

Resultaterne af undersøgelsen viser, at niveauet for beskyttelse af data i energibranchen gennemsnitligt ligger på 2,2.

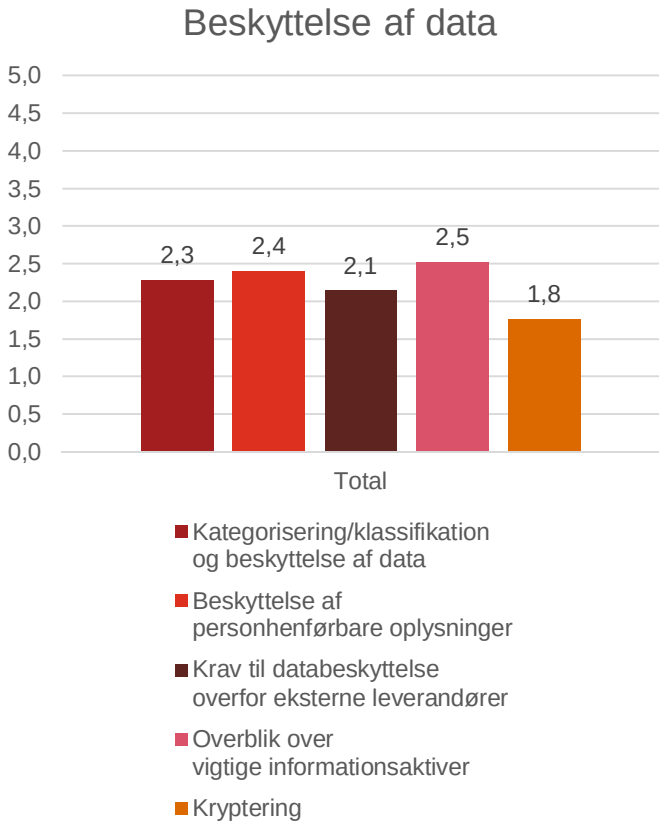
Der er i størsteparten af de adspurgte virksomheder etableret en overordnet politik for, hvordan data skal beskyttes, og hvordan man skal arbejde med beskyttelse af data i henhold til deres kritikalitet.

Næsten alle adspurgte virksomheder har afgrænset adgangen til personhenførbare data til personer med et arbejdsbetinget behov.

Det er under hver tredje virksomhed, der overvåger og logger aktiviteter, der vedrører fortrolige eller personhenførbare data, og kun få virksomheder gennemgår disse logs for uregelmæssigheder.

Over halvdelen af de adspurgte virksomheder har gjort virksomhedens sikkerhedspolitik gældende over for leverandører, men kun en fjerdedel har defineret servicemål for overholdelse af politikken, og kun få har mekanismer etableret, der gør det muligt at vurdere, om leverandøren overholder politikken.

Næsten alle virksomhederne har et overblik med de vigtigste informationsaktiver og har tilknyttet et formelt ejerskab af disse. I en tredjedel af de adspurgte virksomheder er der etableret en procedure for, at aktivejeren etablerer passende sikkerhedsforanstaltninger, herunder kryptering i forhold til aktivets kritikalitet.



D. Beredskab

Beredskabsstyring implementeres som en kontinuerlig proces med det formål at begrænse konsekvenserne ved tab af informationsaktiver forårsaget af katastrofer og sikkerhedsbrister til et acceptabelt niveau samt med det formål at kunne genoprette driften gennem en kombination af forebyggende og udbedrende foranstaltninger.

Der er stillet spørgsmål relateret til:

12. It-beredskabsplan – Er der en godkendt it-beredskabsplan, der beskriver roller, ansvar og operationelle tiltag samt handlinger, der effektivt håndterer it-beredskabssituationer, hvor data eller systemers fortrolighed, integritet eller tilgængelighed er blevet kompromitteret?

13. Håndtering af it-sikkerhedshændelser – Er der en dokumenteret proces for håndtering af it-sikkerhedshændelser?

14. Genetablering af kritisk produktions-it – Har virksomheden implementeret et it-beredskab, der muliggør, at kritiske it-installationer og systemer kan genetableres med minimal konsekvens for driften?

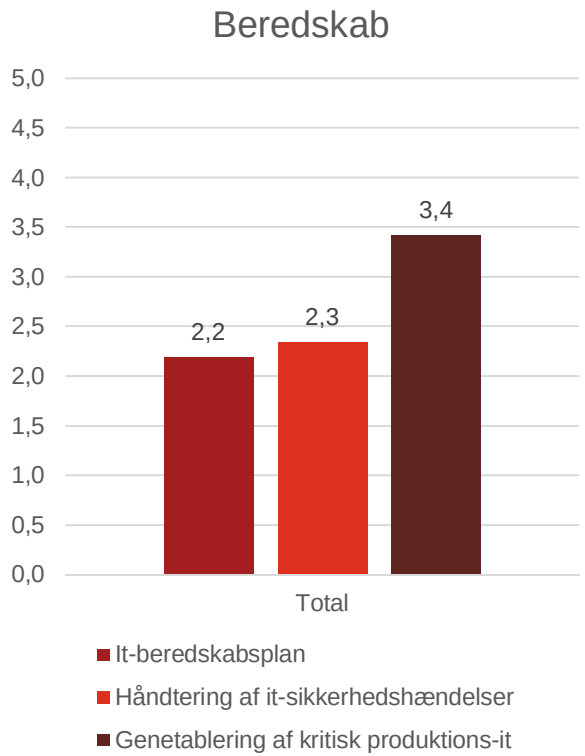
Resultater – it-beredskab

Resultaterne af undersøgelsen viser, at niveauet for it-beredskab i energibranchen gennemsnitligt ligger på 2,6.

I branchen er der et meget højt fokus på, at den kritiske produktions-it, der understøtter forsyningen, kan genetableres effektivt. Tre ud af fire adspurgte har etableret procedurer for manuel genetablering og har de nødvendige værktøjer, reservedele, vagtplaner mv. Disse procedurer testes regelmæssigt.

Det er kendetegnende for branchen, at der er fokus på forsyningssikkerhed og tilgængelighed af systemer. Under halvdelen af de adspurgte har etableret en it-beredskabsplan, der håndterer brud på fortrolighed og integritet af data, ud over tilgængelighed af systemerne.

En tredjedel af de adspurgte har implementeret automatiske værtøjer til at understøtte opdagelsen af hændelser. Størsteparten af de adspurgte rapporterer større it-sikkerhedshændelser til relevante eksterne parter.



E. Processer

Er der implementeret centrale processer, der medvirker til at opbygge og over tid vedligeholde et passende sikkerhedsniveau?

Der er stillet spørgsmål relateret til:

15. Proces for identifikation af og overholdelse af eksterne krav – Er der etableret en proces eller samarbejde, der medvirker til, at alle eksterne krav fra myndigheder og eksterne aftaleparter identificeres og overholdes?

16. Logisk adgang til kritiske it-systemer – Er logisk adgang til kritiske it-systemer og data tildelt efter et arbejdsbetinget behov, og følges der løbende op på, hvorvidt adgangsrettigheder er aktuelle? Adgangsrettigheder bestemmer, hvem der skal have adgang til specifikke data, og hvad de skal kunne med disse data (fx læse- eller skriveadgang)

17. It-driftsprocedurer – Dokumenteres og vedligeholdes it-driftsprocedurer, såsom ændringshåndtering, adgangsstyring, kapacitetsstyring, backup af data, hændelseshåndtering, sårbarhedsstyring mv.?

18. Anskaffelse, udvikling og vedligehold af systemer – Er der implementeret kontroller ved anskaffelse, udvikling og vedligehold af systemer?

Resultater – processer

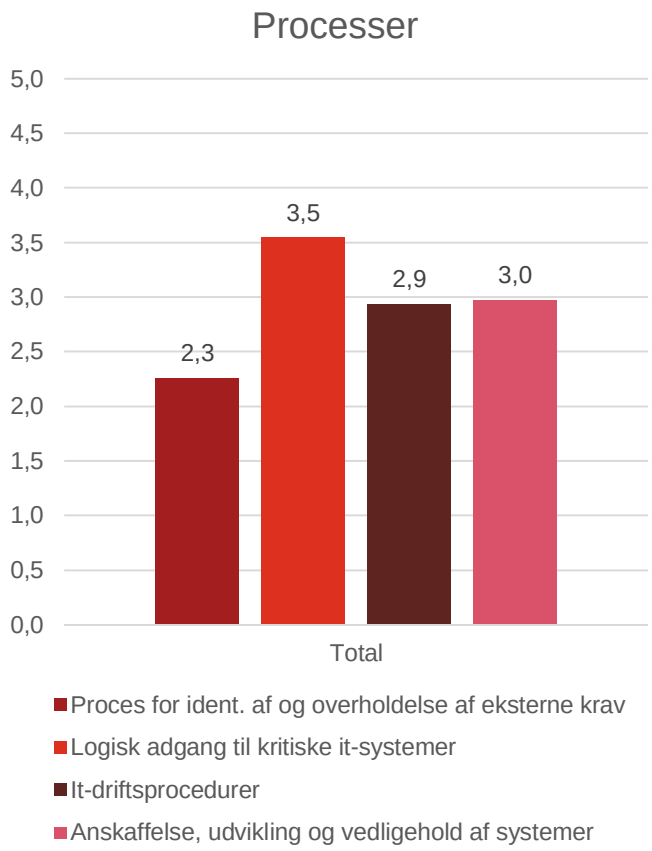
Resultaterne af undersøgelsen viser, at de processer, der medvirker til at opretholde et passende sikkerhedsniveau over tid, gennemsnitligt ligger på 2,9.

Størsteparten af de adspurgte har udpeget en ansvarlig, der skal identificere og indrapportere nye krav til it-sikkerhed, og/eller man har etableret et samarbejde med eksempelvis en brancheforening, der kan holde virksomheden orienteret.

Der er meget højt fokus på at sikre, at kun medarbejdere, der har et arbejdsbetinget behov, tildeles adgang til kritiske it-systemer, og der følges regelmæssigt og proaktivt op på disse adgangsrettigheder.

It-driftsprocedurer er dokumenteret hos mere end tre fjerdedele af de adspurgte virksomheder og vedligeholdes som del af det daglige arbejde. Det er kun i en tredjedel af virksomhederne, at it-driftsprocedurer er dokumenteret i henhold til en standard (fx ITIL), og procedurernes effektivitet vurderes ligeledes årligt i en tredjedel af virksomhederne.

Ca. halvdelen af virksomhederne stiller mindstekrav til sikkerheden i nye systemer, hvorimod mere end tre fjerdedele af virksomhederne stiller specifikt krav til test og godkendelse af it-systemer, der er kritiske for forsyningen inden idriftsættelse.



F. Fysisk sikring

Etablerede procedurer på området sikrer mod uautoriseret fysisk adgang, skader og forstyrrelser mod virksomheden via fysisk adgang både på og uden for virksomhedens lokationer.

Der er stillet spørgsmål relateret til:

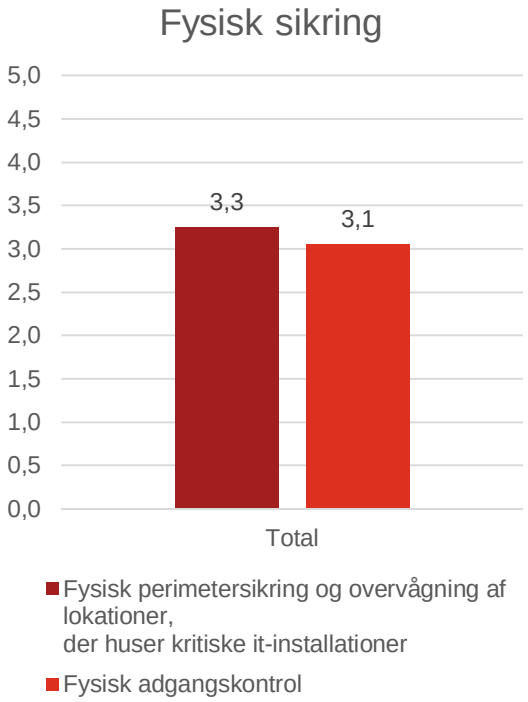
1. Fysisk perimetersikring og overvågning af lokationer, der huser kritiske it-installationer – Har virksomheden etableret passende fysisk sikring og overvågning af kritiske it-installationer, herunder hovedstationer, produktionsenheder, anlæg mv., der er koblet op til det centrale netværk?
2. Fysisk adgangskontrol – Er områder/lokaler i virksomheden, både centralt og decentralt, beskyttet med passende fysisk adgangskontrol for at sikre, at kun autoriseret personale kan få adgang?

Resultater – fysisk sikring

Resultaterne af undersøgelsen viser, at det fysiske sikringsniveau i branchen gennemsnitligt ligger på 3,1.

To ud af tre af de adspurgte virksomheder har implementeret perimetersikring såvel som alarmovervågning af kritiske it-installationer. Ca. en tredjedel af de adspurgte foretager regelmæssig manuel inspektion af alle kontroller med henblik på at opdage fejl, uønsket indtrængen eller manipulation.

Næsten alle de adspurgte virksomheder har en politik for tildeling af adgange til fysiske rum og lokationer, baseret på et arbejdsbetinget behov. To ud af tre overvåger og logger adgangen til fysiske områder, og ca. halvdelen af de adspurgte har ydermere implementeret funktionalitet, hvor uautoriseret adgang eller uregelmæssigheder udløser alarmer.



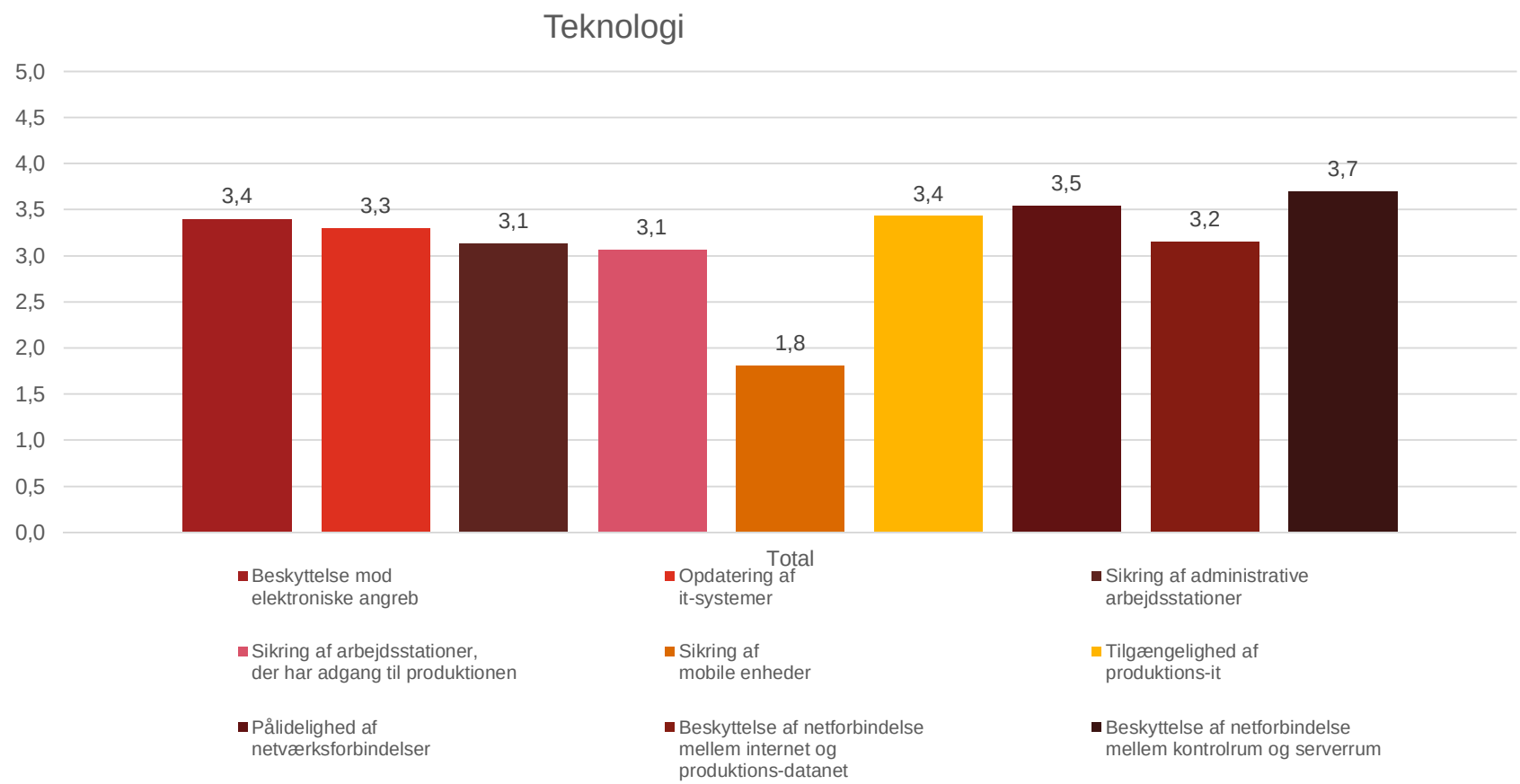
G. Teknologi

Virksomheden bør have implementeret passende tekniske kontroller til at beskytte de mest kritiske dele af forretningen mod de aktuelle trusler.

Der er stillet spørgsmål relateret til:

21. Beskyttelse mod elektroniske angreb – Er der implementeret kontroller til beskyttelse mod elektroniske angreb?
22. Opdatering af it-systemer – Er der implementeret kontroller til at holde it-systemer opdaterede?
23. Sikring af administrative arbejdsstationer – Der skal være implementeret sikkerhedsmekanismer, der beskytter den enkelte arbejdsstation i henhold til den risiko, den udgør ved eksempelvis at have fjernadgang til lukkede netværk eller kritiske data.
24. Sikring af arbejdsstationer, der har adgang til produktionen – Der skal være implementeret sikkerhedsmekanismer, der beskytter den enkelte arbejdsstation i henhold til den risiko, den udgør ved eksempelvis at have fjernadgang til lukkede netværk eller kritiske data.
25. Sikring af mobile enheder – Der skal være implementeret sikkerhedsmekanismer, der beskytter den enkelte mobile enhed i henhold til den risiko, den udgør ved eksempelvis at have fjernadgang til kritiske systemer eller data.
26. Tilgængelighed af produktions-it – Har virksomheden implementeret tekniske kontroller, der afspejler forretningens krav til tilgængelighed for SCADA og styringssystemerne?
27. Pålidelighed af netværksforbindelser – Er der etableret netværksforbindelser, der sikrer en robust tilgængelighed?
28. Beskyttelse af netforbindelse mellem internet og produktionsdatanet – Hvordan er netforbindelsen mellem internet og produktionsdatanet beskyttet?
29. Beskyttelse af netforbindelse mellem kontrolrum og serverrum – Hvordan er netforbindelsen mellem kontrolrum og serverrum beskyttet?

Resultater – teknologi



Se næste side for beskrivelse

Resultater – teknologi

Resultaterne af undersøgelsen viser, at anvendelsen af teknologi til sikring af branchen gennemsnitligt ligger på 3,1.

Alle de adspurgte virksomheder har implementeret de mest grundlæggende tekniske kontroller til beskyttelse mod ondsindet angreb, herunder antivirussoftware og firewalls mod internettet. Størsteparten af de adspurgte har ligeledes procedurer, der medvirker til at holde disse kontroller sikre over tid. Halvdelen har mere avanceret beskyttelse implementeret, i form af fx *intrusion detection*, eller et abonnement på eksterne tjenester, der medvirker til at identificere komplekse trusler eller angreb.

To tredjedele af de adspurgte har procedurer for at holde operativsystemer opdaterede eller implementere kompenserende kontroller i de tilfælde, hvor fx produktions-it ikke kan opdateres uden at påvirke produktionen negativt.

Næsten alle de adspurgte har standardiserede enheder og opsætninger for de administrative arbejdsstationer, og tre fjerdedele har det på arbejdsstationer, der har adgang til produktionen. På disse er der ydermere implementeret kontroller, fx overvågning/scanning med henblik på at sikre, at et passende sikkerhedsniveau opretholdes.

Der er ikke megen fokus på sikring af mobile enheder. Der er primært adgang til mail og kalender via disse typer enheder – ikke til produktionen.

De kritiske it-systemer er enten delvist dublerede eller fuldt redundante, og typiske udfald forventes at have minimal konsekvens for driften.

I næsten alle de adspurgte virksomheder kan produktionssystemer administreres fra mindst to fysisk adskilte kontrolrum eller terminaladgang via fjernarbejdspladser.

I næsten alle de adspurgte virksomheder er kommunikationslinjer til kritiske it-installationer baseret på dedikerede og dublerede forbindelser.

Produktionsnetværk er typisk adskilt fra internettet via firewalls, der er konfigureret restriktivt. Det er dog kun under halvdelen af respondenterne, der har implementeret tekniske begrænsninger i firewallen for at modvirke web-surfing fra produktionsnettet. Sådanne begrænsninger skal modvirke, at medarbejdere fra produktionsnettet tilgår internettet og potentielt er medvirkende til at introducere ondsindet kode.

Delkonklusioner - virksomhedstyper

Delkonklusion – elnetselskaber
Gennemsnitligt niveau: 2,7

Der er 30 besvarelser fra elnetselskaber, hvilket udgør 52 % af det totale antal respondenter, og derfor er besvarelser fra denne virksomhedstype i høj grad afspejlet i de resultater, der er beskrevet i de samlede resultater for branchen.

Der er dog i denne virksomhedstype et noget højere fokus på beskyttelse af data, da elnetselskaberne typisk er tættere på slutbrugeren end de øvrige selskabstyper i branchen. Elnetselskaber opbevarer og behandler i stigende grad personhenførbare informationer om kunderne, herunder deres forbrug. Det antages, at der er et erkendt behov for beskyttelse af disse informationer, hvilket afspejles i et gennemsnitligt højere sikkerhedsniveau.

Dette har også medført, at elnetselskaberne har implementeret bedre processer til at identificere ændringer i lovkrav og sikre overholdelsen af disse.

Elnetselskaberne er ligeledes med til at løfte branchegennemsnittet på beredskabsområdet, hvor der i denne virksomhedstype er højt fokus på genetablering af den kritiske produktions-it.

Det skal herudover nævnes, at resultaterne viser, at selskaber med et regionalt forsyningsansvar har et højere modenhedsniveau end gennemsnittet.

Delkonklusion – elproduktionsselskaber
Gennemsnitligt niveau: 2,6

Der er 15 besvarelser fra elproduktionsselskaber, hvilket udgør 26 % af det totale antal respondenter, og ligesom elnetselskaberne er besvarelser fra denne virksomhedstype også afspejlet i de resultater, der er beskrevet i de samlede resultater for branchen.

Elproduktionsselskaberne har ifølge undersøgelsen et marginalt lavere niveau end de øvrige selskabstyper. Dette skal dog ikke ses som værende kritisk, da det samlet set er 0,2 under det samlede gennemsnit. Desuden skal det nævnes, at de større selskaber med regionalt ansvar har et højere modenhedsniveau.

Elproduktionsselskaberne har ifølge undersøgelsen et lavere niveau af ledelsesforankring for informationssikkerhed end de øvrige selskaber i branchen, især udtrykt i manglende retningslinjer såvel som ansvarsplacering af opgaven.

Resultaterne viser ligeledes et lavere niveau for beskyttelse af personhenførbare oplysninger. Dette er givetvis udtryk for, at denne virksomhedstype typisk ikke behandler personhenførbare kundeoplysninger. Andre personhenførbare oplysninger, som fx medarbejderdata, herunder data relateret til ansættelse, sygefravær mv., bør selvfølgelig sikres tilstrækkeligt.

Delkonklusion – naturgasdistributionsselskaber
Gennemsnitligt niveau: 3,4

Der er tre besvarelser fra naturgasdistributionsselskaberne, hvilket udgør kun 5 % af det totale antal respondenter. De enkelte besvarelser har derfor en høj indflydelse på gennemsnittet for denne virksomhedstype.

Gasdistributionsselskaberne har ifølge undersøgelsen det højeste sikkerhedsniveau i branchen.

Denne virksomhedstype har ifølge undersøgelsen høj fokus på sikkerhed, herunder især kommunikation til medarbejdere om deres rolle og ansvar i forhold til informationssikkerheden; kravstilling til databeskyttelse over for eksterne leverandører; overblik med vigtige informationsaktiver; it-beredskab; styring af logisk adgang til kritiske systemer; og beskyttelse mod ondsindede angreb.

Delkonklusion – naturgastransportselskaber
Gennemsnitligt niveau: 3,0

Der er tre besvarelser fra naturgastransportselskaberne, hvilket udgør kun 7 % af det totale antal respondenter. Ligesom for gasdistributionsselskaberne har de enkelte besvarelser derfor en høj indflydelse på gennemsnittet for denne virksomhedstype.

Gastransportselskaberne har et marginalt højere gennemsnitligt niveau end det samlede branchegennemsnit.

Denne virksomhedstype har ifølge undersøgelsen højt fokus på sikkerhed og har etableret formelle retningslinjer for styring af sikkerheden; har stærke procedurer ved ansættelse såvel som afskedigelse/fratrædelse af medarbejdere; it-driftsprocedurer er veldokumenterede og formaliserede, og der er fokus på fysisk sikkerhed; såvel som sikring af arbejdsstationer, der har adgang til produktionen.

Der, hvor denne virksomhedstype ifølge undersøgelsen har et relativt lavere niveau end branchegennemsnittet, er i forhold til at have en formaliseret it-beredskabsplan.

Delkonklusion – produktionsbalanceansvarlige
Gennemsnitligt niveau: 3,2

Respondenter fra de produktionsbalanceansvarlige virksomheder udgør kun 7 % af det totale antal respondenter, og ligesom de foregående virksomhedstyper inden for naturgas, så har de enkelte besvarelser en høj indflydelse på gennemsnittet for denne virksomhedstype.

De produktionsbalanceansvarlige virksomheder har et marginalt højere gennemsnitligt niveau end det samlede branchegennemsnit.

Denne virksomhedstype har ifølge undersøgelsen højt fokus på sikkerhed og har stærke procedurer ved ansættelse såvel som afskedigelse/fratrædelse af medarbejdere; it-driftsprocedurer er veldokumenterede og formaliserede, og der stilles høje krav til leverandører om overholdelse af procedurer; man har formaliseret it-hændelseshåndtering og har fokus på at beskytte produktionsnetværket.

Delkonklusion – systemansvarlig transmissionsvirksomhed

Gennemsnitligt niveau: 2,8

Der er kun én systemansvarlig transmissionsvirksomhed i Danmark, nemlig Energinet.dk.

Energinet.dk har ifølge undersøgelsen højt fokus på sikkerhed, hvilket afspejles i en høj grad af ledelsesforankring. Der er et højt niveau for risikostyring; krav til eksterne leverandører; beredskab, herunder genetablering af kritisk produktions-it; opdatering af systemer; sikring af arbejdsstationer med adgang til produktionen; tilgængelighed af produktions-it; og sikring af netværksforbindelser.

Bilag 1: Modenhedsniveau

Modenhedsniveauet er vurderet ved anvendelse af Capability Maturity Model (CMMI).

Modenhedsniveau		
X	Ikke relevant	Aktiviteterne er ikke relevante.
0	Ikke-eksisterende	Virksomheden har ikke identificeret og adresseret problemstillingerne.
1	Ad hoc	Virksomheden har identificeret problemstillinger, som bør adresseres. Der findes ingen standardiserede processer, som tager hånd om problemstillingerne – dette sker typisk på en medarbejders eget initiativ.
2	Intuitiv	De samme procedurer følges af forskellige personer, der udfører en opgave. Der er ingen formel træning eller kommunikation omkring standardprocedurer. Udførelse sker på medarbejderens eget initiativ.
3	Defineret	Procedurer er standardiserede, dokumenterede og kommunikerede. Medarbejderne bør følge procedurer. Procedurerne er typisk en simpel formalisering af guidelines.
4	Styret og målbar	Ledelsen overvåger og måler anvendelse af procedurer og griber ind, hvis processer ikke fungerer effektivt. Aktiviteter forbedres konstant og sikrer effektivitet. Automatisering anvendes i begrænset omfang.
5	Optimeret	Aktiviteter er blevet optimeret, baseret på resultater fra integrationen og sammenligning med andre virksomheder. It anvendes som et integreret værktøj til at automatisere processer og støtter op omkring forbedring af kvalitet og effektivitet. Dette gør virksomheden agil.