

REFERAT Informationssikkerhedsudvalget d. 23-01-2019

Mødedato Onsdag d. 23. januar 2019 kl. 13:00

Mødested Bogense Rådhus, Mødelokale IT

Indholdsfortegnelse

Living document.....	3
Udkast til ledelsesbrev, IT revision.....	4
IT-beredskabsplan.....	6

Punkt 1: Living document

Sagsfremstilling

1. Living document

Åbent

Sagsnr. 480-2018-17097 Dok.nr. 480-2019-8955

Sagens kerne

Informationssikkerhedsudvalgets "Living document" viser, hvad der har været arbejdet med siden sidst.

Indstilling

Til orientering.

Sagens baggrund

Informationssikkerhedsudvalgets "Living document" viser, hvad der har været arbejdet med siden sidst.

Økonomiske oplysninger

-

Lovgrundlag

-

Bilag

480-2019-12167 Kopi af Living document 2018 - rev. januar 2019

Beslutning

Informationssikkerhedsudvalg den 23. januar 2019

Fraværende: Gitte Clemmensen

Orientering foretaget.

Bilag

Kopi af Living document 2018 - rev. januar 2019

Punkt 2: Udkast til ledelsesbrev, IT revision

Sagsfremstilling

2. Udkast til ledelsesbrev, IT revision

Åbent

Sagsnr. 480-2019-1558 Dok.nr. 480-2019-12061

Sagens kerne

BDO har udarbejdet udkast til ledelsesbrev i forhold til IT-revision. BDO kommer i udkastet med en række anbefalinger.

Anbefalingerne drøftes i Informationssikkerhedsudvalget med henblik på at sikre, at der arbejdes videre med anbefalingerne hos de respektive data- og systemejere jf. organiseringen af kommunens informationssikkerhedsarbejde.

Indstilling

Det indstilles, at:

- Kravet til password til logon på Windows skærpes jf. anbefalingerne.
- Der igangsættes en proces omkring udarbejdelsen af en samlet IT-beredskabsplan.
- På nuværende tidspunkt vurderes det ikke relevant at gennemføre regelmæssige sårbarheds- og penetrationstests.
- Mulige løsninger på at lukke for administratorrettigheder på egne enheder undersøges fortsat, men det er vigtigt at den valgte løsning fortsat tillader, at kommunens kerneopgave kan løses effektivt.
- De øvrige anbefalinger arbejdes der videre med af Økonomi og Løn, som er system- og dataansvarlig for OPUS mv.

Sagens baggrund

BDO har udarbejdet udkast til ledelsesbrev i forhold til IT-revision.

BDO kommer i udkastet med en række anbefalinger.

Anbefalingerne drøftes i Informationssikkerhedsudvalget med henblik på at sikre, at der arbejdes videre med anbefalingerne hos de respektive data- og systemejere jf. organiseringen af kommunens informationssikkerhedsarbejde.

Ansaret for følgende anbefalinger vurderes at ligge i Informationssikkerhedsudvalget:

1. Skærpelse af password politik.
2. IT-beredskabsplan.
3. Løbende sårbarheds- og penetrationstests.
4. Sikre at brugere ikke er lokaladministrator på egne enheder.

Ad 1.

Kravet til password til logon på Windows (første logon) kan skærpes jf. anbefalingerne. Krav til password fra KMDs systemer kan ikke umiddelbart skærpes, da sikkerheden styres af KMD. Sikkerheden ved KMD vurderes at være god, og ved de løbende udbud af IT-systemer forventes det, at KOMBIT sikrer at kravene til password løbende tilpasses arbejdet med Informationssikkerhed.

I forbindelse med Aula (erstatning for Skole-intra) bliver der samtidig opsat 2-faktor login ved ekstern login. Brugen af 2-faktor login er således i proces for hele organisationen.

Ad 2.

Der igangsættes en proces omkring udarbejdelsen af en samlet IT-beredskabsplan, se andet punkt på dagsordenen. Det bemærkes, at der allerede er indarbejdet beredskabsmæssige tiltag, som nu samles i en beredskabsplan. Det er vigtigt, at organiseringen i IT-beredskabsplanen følger den øvrige organisering af informationssikkerhedsarbejdet, så der ikke oparbejdes en parallel organisation.

Ad 3.

Nordfyns Kommune kører med både antivirus beskyttelse og firewall, som overvåges af KMD. Nordfyns Kommune har tidligere fået udarbejdet en sårbarheds- og penetrationstest. På nuværende tidspunkt vurderes en sådan test ikke at kunne bidrage væsentligt til at øge sikkerheden, når der ses på det sikkerhedsniveau, som Nordfyns Kommune allerede nu kører.

Ad 4.

IT-afdelingen har arbejdet på at lukke for administratorrettigheder på egne enheder. Imidlertid er der ikke på nuværende tidspunkt fundet en løsning som samtidigt sikrer, at organisationens kerneopgave kan løses tilstrækkeligt effektivt, hvis adgangen lukkes eller indskrænkes meget. Systemer/software og hardware har ofte brug for at skrive til lokale enheder for at fungere. Mulige løsninger undersøges fortsat.

Økonomiske oplysninger

-

Lovgrundlag

-

Bilag

480-2019-12046 Udkast_Ledelsesbrev_it-revision_2018_Nordfyns Kommune

Beslutning

Informationssikkerhedsudvalg den 23. januar 2019

Fraværende: Gitte Clemmensen

Indstillingen godkendt med følgende tilføjelser:

Vedrørende penetrationstest modtager Nordfyns Kommune kvartalsvis en rapport over status på vores firewall fra KMD, hvor KMD også analyserer resultaterne. Rapporterne vil fra februar 2019 komme hver måned. Iøvrigt reagerer KMD, jf. servicekontrakt, hvis der er særlig og kritisk kommunikation mod firewall.

Vedrørende brugeradgangen til egne enheder (administratorrettigheder) så er en softwareløsning til sikring af enhederne i test pt. Løsningen betyder, at brugeradgangen til den enkelte enhed ikke lukkes, men sikres. Denne løsning vurderes at give god sikkerhed uden at de enkelte enheder sløves unødigt.

Bilag

Udkast_Ledelsesbrev_it-revision_2018_Nordfyns Kommune

Punkt 3: IT-beredskabsplan

Sagsfremstilling

3. IT-beredskabsplan

Åbent

Sagsnr. 480-2019-1623 Dok.nr. 480-2019-12357

Sagens kerne

Ved seneste gennemgang af Nordfyns Kommunes It-sikkerhed af firmaet BDO, som blev afsluttet i indeværende måned, er der nogle anbefalinger.

Nogle af anbefalingerne er der taget aktion på i den mellemliggende periode. Andre bør tages op til en drøftelse i forhold til de tiltag, der i øvrigt er sat i værk.

Men et af de punkter hvor BDO har givet anbefalinger, er på det It-beredskabsmæssige område, hvor anbefalingen er, at Nordfyns Kommune udarbejder en It-beredskabsplan – eller i hvert fald dele af den.

Indstilling

Det er anbefalingen, at kommunen beskriver og indfører en It-beredskabsplan, der gør nøglemedarbejdere i stand til at varsle og kommunikere en kritisk situation. En It-beredskabsplan skal endvidere løbende afprøves og evalueres.

Sagens baggrund

Det er BDO's vurdering, at det er en mangel i den interne kontrol, idet der ikke er udarbejdet en It-beredskabsplan til brug i forbindelse med en kritisk situation, hvorved der er en risiko for, at medarbejderne med ansvar inden for kritisk It-drift ikke har et fornødent værktøj til etablering og kommunikation i forbindelse med væsentlige nedbrud.

I forhold til kommunens nuværende status, er der i 2016 gennemført en drøftelse med de enkelte direktørområder i forhold til kritiske systemer. Denne risikovurdering mundede ud i, at der reelt var et system, der var virkeligt risikobetonet, nemlig det system der anvendes til hjemmeplejen, KMD Nexus.

Men i forhold til at holde de enkelte systemer i drift i en krisesituation, er der mange aspekter, der skal vurderes på. Det kan være beredskab uden for normal arbejdstid, som senest har været drøftet i Direktionen i efteråret 2018, nødberedskaber i forhold til tilkald af eksterne leverandører med flere.

Uanset hvilken løsning der måtte vælges, er det ikke muligt at sikre alt altid.

En ting er dog sikkert – det vil kræve yderligere ressourcer at opbygge en It-beredskabsplan.

Der er vedlagt 2 beredskabsplaner fra henholdsvis Horsens og Assens Kommuner til inspiration.

Økonomiske oplysninger

-

Lovgrundlag

-

Bilag

480-2019-12337 Kommunalt eksempel_It-beredskabsstrategi for Horsens Kommune (1)

480-2019-12336 BEREDSKAB 2018

Beslutning

Informationssikkerhedsudvalg den 23. januar 2019

Fraværende: Gitte Clemmensen

Godkendt.

Bilag

Kommunalt eksempel_It-beredskabsstrategi for Horsens Kommune (1)

BEREDSKAB 2018