DIGITALISERINGSSTYRELSEN

CENTER FOR CYBERSIKKERHED

Anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift

2014

August 2014

Anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift
August 2014

Denne publikation er udarbejdet af

Digitaliseringsstyrelsen
Landgreven 4
Postboks 2193
1017 København K
Telefon 33 92 80 00
digst@digst.dk

og

Center for Cybersikkerhed
Kastellet 30
2100 København Ø
Telefon: +45 3332 5580
E-mail: cfcs@cfcs.dk

Elektronisk publikation:
ISBN: 978-87-93073-07-4

Publikationen kan hentes på:

Digitaliseringsstyrelsens hjemmeside
www.digst.dk

og

Center for Cybersikkerheds hjemmeside
www.cfcs.dk

Indledning

Denne rapport er den tredje rapport om CSC-sagen. Rapporten indeholder fremadrettede anbefalinger til statslige myndigheder vedrørende sikring af outsourcet it-drift.

I 2013 kom det frem, at it-leverandøren CSC var blevet ramt af et omfattende hackerangreb, hvor en række statslige myndigheders følsomme data potentielt var blevet kompromitteret.

Denne rapport er den tredje rapport om CSC-sagen. Rapporten oversendes til Folketinget og offentliggøres. Rapporten indeholder de fremadrettede anbefalinger på grundlag af konklusionerne på de undersøgelser i forbindelse med CSC-sagen, som beskrives i de to øvrige rapporter om sagen.

En stor del af den statslige it-drift er outsourcet til eksterne leverandører. Outsourcing er en model, som har givet staten en række fordele gennem årene, både i forhold til økonomi, kvalitet og organisering. Den omfattende brug af outsourcing stiller dog en række krav til, hvordan den sikkerhedsmæssige styring af leverandørerne sker på tilfredsstillende vis. I de seneste år er der set flere konkrete eksempler på alvorlige sikkerhedshændelser hos statens eksterne it-leverandører, og undersøgelserne i forbindelse med CSC-sagen har vist, at myndighederne skal være mere opmærksomme på at stille passende sikkerhedsmæssige krav til leverandørerne, og følge løbende op på, at leverandørerne efterlever kravene.

Denne rapport indeholder en række anbefalinger til styrkelse af sikkerhed i statens outsourcede it-drift med det formål at understøtte en styrkelse af såvel sikkerheden i de outsourcede statslige løsninger som myndighedernes kontrol hermed. Rapporten og dens anbefalinger skal danne baggrund for, at statslige myndigheder i højere grad kan agere kompetent, rettidigt – og i passende omfang koordineret – i forhold til it-sikkerheden i nye og eksisterende outsourcede løsninger.

Forsvarets Efterretningstjenestes Center for Cybersikkerhed og Digitaliseringsstyrelsen vurderer i dag, at myndighederne – generelt set – kun i mindre grad tager hensyn til det aktuelle trusselsbillede, dvs. hvilke trusler, it-løsningerne kan blive udsat for.

I rapporten gennemgås på den baggrund det aktuelle trusselsbillede som baggrund for de konkrete anbefalinger til myndighederne om relevante sikkerhedstiltag i forbindelse med løsninger, som drives af eksterne leverandører samt om samarbejde med Center for Cybersikkerhed.

Rapportens anbefalinger, som er rettet til den øverste ledelse i statslige myndigheder, er fremhævet i tekstbokse og mærket ”Anbefalinger til ledelsen”. En samlet oversigt over anbefalingerne til ledelsen fremgår af bilaget i kapitel 7.

Teksten indeholder i øvrigt anbefalinger, der er rettet mod myndighedernes systemansvarlige og informationssikkerhedsmedarbejdere med henblik på at understøtte det konkrete arbejde med at øge sikkerheden. Disse anbefalinger kan dog samtidig tjene som en tjekliste for den øverste ledelse i dennes dialog med organisationen om it-sikkerhed. Myndighederne kan endvidere med fordel videregive rapporten til deres eksterne leverandører, hvorefter den kan tjene som udgangspunkt for et tættere samarbejde om at sikre, at sikkerheden er på et tilstrækkeligt niveau og i øvrigt svarer til det aftalte.

Det understreges, at sikkerheden i forbindelse med outsourcet it-drift skal ses som en del af den samlede indsats i forhold til cyber- og informationssikkerhed. Rapporten indeholder derfor også mere generelle betragtninger og anbefalinger til myndighedernes styring af informationssikkerhed.

Anbefalingerne i rapporten ligger inden for rammerne af sikkerhedsstandarden ISO27001, som tager udgangspunkt i ledelsesforankret risikovurdering, og som statens institutioner er forpligtede til at efterleve.

Anbefalingerne er et bidrag til myndighedernes arbejde med at etablere et passende sikkerhedsniveau og deres efterlevelse af standarden i forbindelse med brugen af eksterne leverandører.

I kapitel 2 og 3 opsummeres konklusioner efter CSC-sagen, og der gives som baggrund for sikkerhedsarbejdet en oversigt over trusselbilledet og risici ved sårbarheder – samt muligheden for bistand fra Center for Cybersikkerhed, som er national it-sikkerhedsmyndighed.

I kapitel 5 beskrives, hvorledes ISO27001-standarden anvendes som rammeværk for sikkerhedsarbejdet.

Indhold

1. Konklusioner efter CSC-sagen

Nedenfor gennemgås de overordnede konklusioner efter CSC-sagen.

CSC-sagen viser først og fremmest, at der findes en reel trussel om cyberangreb imod danske myndigheders digitale systemer. Sagen viser også, at de angrebne systemer på angrebstidspunktet var sårbare i en sådan grad, at det lykkedes angriberne at kompromittere fortroligheden af følsomme oplysninger, og at angriberne havde etableret et fodfæste i systemerne, så de potentielt kunne have forårsaget tab eller forvanskning af uerstattelige data.

På baggrund af sagen må det konkluderes, at det er af afgørende betydning for cyber- og informations-sikkerheden, at en myndighed internt udvikler en moden it-sikkerhedsorganisation, som kan forestå en tilstrækkelig leverandørstyring for så vidt angår it-sikkerheden. Herunder er det væsentligt, at der hos myndigheden er kompetencer, som (bl.a. i dialog med leverandøren) kan vurdere behov for tilkøb af sikkerhedsrelaterede ydelser (såsom opdeling af netværk, vedligehold af forbindelse til internettet, opdatering af systemer mv.).

Det er i den forbindelse af betydning, at myndigheden løbende forebygger "tilsanding" af systemer, dvs. at myndigheden løbende opdaterer sin it-anvendelse og sine leverandørkontrakter i lyset af det aktuelle trusselbillede. Det er samtidig vigtigt, at tjenester og funktionalitet, som ikke anvendes, løbende tages ud af drift, ligesom etableringen af ny funktionalitet bør ledsages af konkrete og dokumenterede risikovurderinger.

Erfaringerne fra CSC-sagen viser blandt andet, at et aktivt og kontinuerligt samarbejde mellem leverandøren og kunderne – i tråd med den gældende sikkerhedsstandard ISO27001 – kan danne grundlag for en væsentlig forbedring af sikkerheden i løsningerne. I den pågældende sag har leverandøren således på den baggrund gennemført en række tiltag for at øge sikkerheden i de leverede ydelser. Der er redegjort nærmere herfor i rapporten til regeringen om sikkerhedsbrud hos CSC.

1.1 Hovedanbefalinger til ledelsen

1. Ledelsen bør sikre, at myndighederne – med udgangspunkt i de opnåede erfaringer fra CSC-sagen – aktivt vurderer cyber- og informationssikkerheden, specielt i de løsninger, som drives af eksterne leverandører, og går i dialog med leverandøren herom med henblik på at sikre, at alle leverandører gennemfører relevante tiltag for at opnå den ønskede sikkerhed i de leverede ydelser.

2. Ledelsen bør sikre, at myndighedernes risikovurdering og risikoledelse tager udgangspunkt i et opdateret trusselbillede, jf. kapitel 2.1 og 5 nedenfor. Dette bør sikres både ved nyudvikling, drift og videreudvikling af it-løsninger.

3. Ledelsen bør indlede og løbende indgå i en aktiv dialog internt i myndigheden om efterlevelse af de øvrige anbefalinger i denne rapport.

2. Trusler mod myndighedernes outsourcede it-drift

Danske virksomheder, privatpersoner og offentlige myndigheder blev i 2013 dagligt udsat for forstyrrende eller skadelige aktiviteter via internettet. Der var i 2013 cyberangreb, som i en kortere periode forstyrrede eller hindrede anvendelsen af dansk digital infrastruktur, og der er i de seneste år konstateret cyberangreb mod væsentlige mål i Danmark, hvor informationssikkerheden er blevet kompromitteret. Center for Cybersikkerheds seneste trusselsvurdering viser, at denne tendens meget sandsynligt vil fortsætte.

2.1 Generelle trusler

Forsvarets Efterretningstjenestes "Efterretningsmæssig risikovurdering 2013" beskriver truslen imod danske myndigheder og virksomheder:

Det fremgår af risikovurderingen, at de alvorligste cybertrusler mod Danmark kommer fra statslige aktører, der udnytter internettet til at spionere og stjæle dansk intellektuel ejendom og forretningshemmeligheder såsom forretningsplaner, forskningsresultater, teknisk knowhow, budgetter og aftaler. Denne trussel kommer i særdeleshed fra stater, der bruger informationerne til at understøtte deres egen økonomiske, militære og samfundsmæssige udvikling. Flere stater har midlerne til at gennemføre særdeles omfattende spionage mod danske myndigheder og virksomheder.

Sårbarheder i systemer kan ved et angreb medføre, at driften af danske myndigheders digitale tjenester påvirkes på flere måder:

- Sårbarheder kan ved angreb medføre nedbrud, således at tjenester helt eller delvist ophører med at virke i et kortere eller længere tidsrum. Der er f.eks. set eksempler på såkaldte 'Denial of Service'-angreb mod offentlige løsninger gennem de seneste år.

- Sårbarheder kan medføre, at offentlige data ved et angreb blotlægges og kan tilgås af uvedkommende. Der har været en række tilfælde, hvor personfølsomme data, f.eks. sundhedsoplysninger, er blevet blotlagt. Angrebet mod CSC, hvor der skete en kompromittering af visse data fra politiet, er et eksempel herpå.

- Sårbarheder kan medføre, at offentlige data ændres eller slettes af uvedkommende. Der kendes dog ikke til eksempler på, at dette har fundet sted i Danmark, men Center for Cybersikkerhed har set eksempler på, at sårbarheder har muliggjort så omfattende kompromitteringer af systemer, at angriberne havde reel mulighed for at ændre eller slette data.

Data kan være vanskelige at erstatte i tilfælde, hvor det er meget svært eller umuligt at genskabe data elektronisk efter tab. Det gælder særligt store databaser med mange transaktioner, hvor det i dag ofte vil være umuligt at 'rulle tilbage', såfremt det konstateres, at data på et tidligere tidspunkt er ændret i betydelig grad. Hyppig sikkerhedskopiering af databasen, separat logning af transaktioner og løbende test af databasens integritet øger chancen for, at databasen kan rekonstrueres.

ANBEFALING TIL LEDELSEN

Ledelsen bør sikre, at myndighedens risikovurderinger og risikoledelse, jf. kapitel 5, tager udgangspunkt i et opdateret trusselbillede. Ledelsen bør endvidere sikre, at organisationen vurderer risici ud fra karakteren og værdien af data og systemer, som myndigheden er ansvarlig for, herunder hvor kritiske de er for myndigheden.

Center for Cybersikkerhed er national it-sikkerhedsmyndighed og udarbejder som led heri trusselvurderinger. Centeret kan bistå myndigheder med at udforme sektorspecifikke og – i relevante tilfælde – myndighedsspecifikke trusselvurderinger. Center for Cybersikkerhed leverer en række øvrige sikkerhedsydelser til statslige myndigheder, herunder mulighed for tilslutning til centerets netsikkerhedstjeneste, der har til opgave at opdage, analysere og bidrage til at imødegå cyberangreb.

ANBEFALING TIL LEDELSEN

Ledelsen bør tage initiativ til, at myndigheden indleder en dialog med Center for Cybersikkerhed vedrørende mulighederne for at gøre brug af centerets it-sikkerhedsydelser.

2.2 Specifikke trusler ved brug af eksterne leverandører

Alt efter, hvilken driftsform en myndighed måtte vælge at anvende til sine systemer og datalagring, optræder der forskellige typer risici.

Outsourcet drift er forbundet med en række særlige risici. Disse er ikke nødvendigvis mere problematiske end de risici, der eksisterer ved intern drift, men myndighederne skal være opmærksomme herpå for at kunne leve op til deres ansvar for it-sikkerheden. Som led heri skal myndighederne stille relevante krav til leverandørernes styring af informationssikkerheden, herunder styring af underleverandører.

- *Trusler i forbindelse med ejerskab, strategi og investering*

  Ved ejerskifte vil en ny ejer som udgangspunkt være forpligtet til at videreføre gældende kontrakter. Det er imidlertid en trussel mod myndigheden, såfremt en leverandør, f.eks. ved ejerskifte eller andet strategisk skift i fokus, ikke lægger vægt på investeringer og tiltag, som imødekommer myndighedens behov for sikkerhed, robust drift, support, udvikling mv. Dette gælder også ved skift af leverandørens underleverandører.

- *Trusler i forbindelse med andre landes lovgivning*

  Det er en trussel mod myndigheden, såfremt en leverandørs (eller dennes underleverandørs) infrastruktur ejes eller i øvrigt kontrolleres af virksomheder, som falder under jurisdiktion eller anden indflydelse fra lande, som den danske stat ikke har (fuld) tillid til. Det kan være, at krav i dansk lovgivning ikke finder anvendelse eller ikke kan håndhæves i praksis. Herunder er det muligt, at databehandling og revision ikke sker i henhold til danske regler, eller parter, som ikke nyder dansk tillid (både virksomheder og stater), får indsigt i systemer eller transaktioner på en måde, som potentielt kompromitterer driftssikkerhed eller fortrolighed. Det bemærkes, at det i en række lande er i overensstemmelse med den nationale lovgivning, at den pågældende stat eller andre parter kan tilgå data, som tilhører en infrastrukturleverandørs kunder.

- *Trusler i forbindelse med integrationen af en leverance i myndighedens øvrige it-miljø*

  Selve integrationen af leverancen i myndighedens øvrige it-miljø kan rumme sårbarheder i og med, at myndighedens it-miljø skal åbnes i relevant omfang imod leverandørens systemer, f.eks. ved åbning for særlig netværkstrafik og aktivering af bestemte tjenester i myndighedens udadvendte it-miljø. Denne åbning udgør en øget angrebsflade for cyberangreb.

Ovenstående trusler bør ses i lyset af, at en leverandør uanset ejerforhold eller strategi skal leve op til de forpligtelser, denne juridisk er bundet af via kontrakten. På trods af dette er det vigtigt, at myndigheden løbende vurderer, om truslerne er eller bør føre til, at leverandørstyringen eller kontrakten skærpes.

3. Eksisterende anbefalinger vedrørende outsourcet it-drift

Nedenfor gennemgås internationale og nationale anbefalinger og vejledninger vedrørende outsourcet it-drift.

Der er få udenlandske eksempler på strategier på informationssikkerhedsområdet, som berører emnet outsourcet drift. Storbritannien har udarbejdet og opdaterer løbende en ramme for informationssikkerhed[1]. De krav, som indgår heri, omhandler myndighedernes informationssikkerhed i bred forstand. De steder, hvor det er relevant, betoner strategien myndighedernes ansvar for at sikre, at myndighedernes styring af leverandører er tilstrækkelig til, at myndighedernes samlede it-drift, inklusive den outsourcede drift, lever op til målsætningerne for sikker it-drift.

Det Europæiske Net- og Informationssikkerhedsagentur, ENISA, har udgivet en sikkerhedsstrategi for outsourcet drift specifikt på cloud-området[2], som imidlertid indeholder en række elementer, der også er relevante for andre former for outsourcet it-drift.

Der fokuseres således på håndtering af risici i forbindelse med f.eks.:

- Tekniske forhold, så som manglende sikkerhed og robusthed overfor angreb, datahåndteringen, tab af kontrol med krypteringsnøgler og manglende dokumentation eller styring af medarbejderes adgangsrettigheder mv.

- Juridiske og andre forhold hos leverandøren, så som risikoen for at blive afhængig af leverandøren (lock-in), leverancestop ved konkurs, opkøb af leverandøren, andre landes lovgivning mv.

I Danmark har Dansk It udgivet en vejledning om sikkerhed ved it-outsourcing[3]. Vejledningen giver detaljerede anbefalinger til en organisations interne forberedelse af outsourcing (krav til modenheden i myndighedens organisation, risikovurdering, sikring af revision, exit-strategi mv.), den løbende styring af leverancen i hele aftalens løbetid (kontrol af sikkerhedsniveauet, hændelseshåndtering, beredskab mv.) og eksekvering af en forud fastlagt og sikker exit-strategi i tilfælde af kontraktophør.

Endvidere har Digitaliseringsstyrelsen udgivet en vejledning om "Cloud computing og de juridiske rammer"[4]. Vejledningen beskriver, hvilke lovkrav offentlige myndigheder skal iagttage, når de benytter cloud- og/eller outsourcing-leverandører. Vejledningen beskriver også konkrete forhold, som myndighederne bør overveje ved kontraktindgåelse med en cloud- og/eller outsourcing-leverandør.

Anbefalinger og opmærksomhedspunkter i de ovennævnte rapporter finder generelt anvendelse, også for statens outsourcede it-drift, hvilket er afspejlet i denne rapports øvrige afsnit.

[1] *HMG Security Policy Framework (2014)*, findes på *www.gov.uk*
[2] *Cloud Computing – Benefits, risks and recommendations for information security* (2009), findes på *enisa.europa.eu*
[3] *Sikkerhed ved it-outsourcing – quickguide* (2012), findes på *dit.dk*.
[4] *Cloud computing og de juridiske rammer* (2011) findes på digst.dk

4. Sikkerhedsstyring ved brug af eksterne leverandører

Der er mange fordele forbundet ved at få en ekstern leverandør til at drive hele eller dele af løsninger for offentlige myndigheder. Men outsourcing kræver, at den offentlige myndighed har kompetencerne til at styre processen.

I udgangspunktet er leverandørstyring et element i den generelle sikkerhedsstyring, der for statens institutioner er reguleret af den internationale sikkerhedsstandard ISO27001. I kapitel 5 fremgår mere generelle beskrivelser og anbefalinger til efterlevelse af ISO27001, men erfaringen fra CSC-sagen viser, at det er nødvendigt med særlig fokus på netop leverandørstyring og de nødvendige kompetencer til varetagelse af hele outsourcing-opgaven, som herunder beskrives mere detaljeret.

Myndigheden skal have kompetencerne til:

- At gennemføre en fyldestgørende risikovurdering inden kontraktindgåelse.
- At indgå en kontrakt, der sikrer, at leverandøren træffer de fornødne tekniske og organisatoriske sikkerheds-foranstaltninger, og med mulighed for at justere aftalen i takt med at risikobilledet ændrer sig.
- At foretage en løbende styring af, om leverandøren lever op til kontrakten og styrer sikkerheden forsvarligt.

Det er vigtigt, at der i forbindelse med udfærdigelse af outsourcing-kontrakter indgår krav om, hvordan sikkerhedshændelser håndteres. Det skal være aftalt mellem myndigheden og leverandøren, hvilken part der har ansvaret for de enkelte aspekter af håndteringen af en sikkerhedshændelse, herunder kriterier for, hvornår hændelser rapporteres til kunden, og for eskalering af tiltag til håndtering af hændelser.

Aftaler om håndtering af hændelser skal revideres med jævne mellemrum i takt med den generelle udvikling i risikobilledet.

Myndigheden bør sikre sig, at leverandører i relevant omfang er underlagt uafhængig ekstern it-sikkerheds-revision, og at revisionsrapporter løbende gøres tilgængelige for myndigheden.

Det er endvidere væsentligt at understrege, at det altid er myndigheden, der er ansvarlig for sikkerhedsniveauet. Selvom myndighederne outsourcer driften, er myndigheden ansvarlig for, at leverandøren leverer et tilfredsstillende sikkerhedsniveau.

ANBEFALING TIL LEDELSEN

Ledelsen bør sikre, at der er en tydelig ansvarsfordeling mellem kunde og leverandør om, hvem der er ansvarlig for specifikke sikkerhedstiltag, herunder leverandørens ansvar for underleverandører. Der skal sikres en klar ansvarsfordeling mellem kunde og leverandør i forhold til sikkerhedsaktiviteter.

Derudover belyser erfaringerne fra CSC-sagen behovet for, at myndighederne:

- Indgår i en aktiv dialog med leverandøren om sikkerhedsløsninger og sikrer, at myndigheden i kontrakten har mulighed for løbende at fastholde et passende sikkerhedsniveau.
- Koordinerer og samordner deres krav til it-sikkerhed og deler viden om hændelser, såfremt flere myndigheder deler leverandører.
- Arbejder aktivt med kontrakterne om it-leverancer og ejerskab og løbende opdaterer krav.
- Løbende har godt overblik over de indkøbte leverancer, herunder fjerner services, som ikke (længere) er nødvendige.
- Løbende vurderer sikkerheden i løsningen og sikrer, at den er tidssvarende, især fordi mange ældre systemer er udviklet med en sikkerhedsmodel, som ikke inkluderede at systemerne kunne tilgås udefra. Sammenkoblingen med internettjenester udgør en særlig sikkerhedsmæssig udfordring for disse systemer.
- Løbende følger op på kontrakter med henblik på at sikre, at it-sikkerhedsarkitekturen stadig opdateres efter behov og afspejler det nuværende trusselbillede, herunder sikrer sig, at der i leverandørens systemer er den relevante logiske adskillelse mellem sikkerhedslag

og systemkomponenter, og at der er etableret teknisk sikring mellem disse.

- Lader sikkerhed indgå i it-projekter med passende vægt.

- Undersøger muligheden for at anvende eksempelvis pseudonymisering[5] af personoplysninger eller andre tekniske foranstaltninger til at mindske risici.

Derudover belyser erfaringerne fra SE og HØR-sagen behovet for, at myndighederne:

- Stiller krav til adgangskontroller og sikkerheds-godkendelser, herunder til, at leverandøren vurderer behovet for betroede personers adgang til systemer og data samt sikrer, at adgangen ikke er videre, end behovet tilsiger.

Overordnet bør myndigheden nøje gennemgå kapitel 15 i sikkerhedsstandarden ISO27002 om leverandørforhold med henblik på at dokumentere og indarbejde alle relevante kontroller i aftalerne med leverandøren.

4.1 Sikkerhedsmæssige krav til leverandøren (i kontrakten)

Angrebet mod CSC viste, at der er en række konkrete trusler mod myndighedernes outsourcede drift på mainframe-området. Sagen viste en række generelle forhold ved outsourcet drift, hvor myndighederne skal være opmærksomme på at sikre sig, at leverandørens systemer på passende vis er sikret imod trusler. Dette gælder især sikring af, at en angriber, som udnytter en sårbarhed til at kompromittere sikkerheden i én del af systemet, ikke har mulighed for ad den vej at skaffe sig adgang til andre dele af systemet.

I den forbindelse er det særligt af betydning, at internetvendte services er tilstrækkeligt isoleret fra det bagvedliggende system til at forhindre, at en angriber via internettet kan komme til at udnytte sårbarheder i de bagvedliggende systemer.

[5] Pseudonomisering afkobler følsomme data fra personhenførbare data. I stedet tildeles de følsomme data en nøgle, som følger dem igennem databehandlingen. De personhenførbare data opbevares sammen med nøglen i en separat sikret database; eventuelt kontrolleres nøglen af personen selv. I tilfælde, hvor databehandlingen fordrer kendskab til den konkrete person (f.eks. til fremsendelse af en afgørelse), kan personhenførbare data sættes på sagen ved brug af nøglen - alternativt kan sagens data tilgås af rette vedkommende med brug af nøglen.

ANBEFALING TIL LEDELSEN

Ledelsen bør sikre, at der stilles relevante krav til sikkerhedsforanstaltninger hos eksterne leverandører.

Myndighederne skal sikre, at leverandører:

- Har passende processer for bruger-/rettighedsstyring og fører den nødvendige løbende kontrol.

- Begrænser medarbejderes adgang til data og systemer til, hvad der er behov for, og i øvrigt vurderer behovet for sikkerhedsgodkendelse af medarbejdere.

- Har passende logisk og fysisk opdeling af systemer, og regler for hvilke typer datatrafik som tillades mellem delene.

- Har effektive sikkerhedsprocesser, som sikrer, at kunden har overblik og løbende kan vurdere sikkerhedsniveauet.

- Løbende gennemfører test af det etablerede sikkerhedsniveau.

Ved indgåelse af nye kontrakter bør myndigheder, på baggrund af en vurdering af blandt andet sikkerhedskrav og økonomi, stille relevante krav til løbende udvikling og modernisering af systemerne med henblik på at forebygge at der med tiden drives systemer på legacy-platforme, som kun vanskeligt og med store omkostninger kan vedlige-holdes sikkerhedsmæssigt.

Nedenfor er yderligere eksempler på forhold, som myndigheder bør overveje ved indgåelse af kontrakter med eksterne leverandører (listen er ikke udtømmende):

- Regulerer aftalen, hvorledes det håndteres, hvis leverandøren udsættes for pludselige og udefrakommende uforudsete omstændigheder, der fører til tab af data?

- Stiller kontrakten krav til leverandørens sikkerhedsmæssige styring og forankring i ledelsen, f.eks. gennem ISO27001-certificering?

- Indeholder kontrakten bestemmelser om, hvorledes leverandøren skal sikre kundens data i forhold til tilgængelighed, fortrolighed og integritet?

- Indeholder kontrakten bestemmelser om, hvorledes kunden er sikret adgang til de data, der lagres hos leverandøren?

- Indeholder kontrakten bestemmelser om, hvorledes kundens adgang til egne data sikres - både under normal drift, men også i forhold til driftsstop, misligholdelse, opsigelse, konkurs mv?

- Indeholder kontrakten bestemmelser om leverandørens forpligtigelse til at dokumentere og rapportere på

væsentlige sikkerhedsbrud og krav om relevant opfølgning på disse?

- Præciserer kontrakten, hvorledes leverandøren skal agere i tilfælde af uvedkommendes adgang til data (eksempelvis i form af en pligt til straks at orientere kunden)?

- Er der i kontrakten indsat bestemmelse om, at kunden straks skal orienteres, såfremt myndigheder, herunder regeringer og domstole, ønsker adgang til data hos leverandøren?

- Er det i kontrakten anført, at kunden (oftest via en uafhængig revisor) skal have adgang til eksempelvis en gang årligt at foretage en passende inspektion "on site" i forhold til leverandørens håndtering af data? Eller alternativt at leverandøren via en uafhængig revisor redegør for, hvorledes leverandørens infrastruktur, herunder sikkerhedsspecifikationer, håndteres?

- Stiller kontrakten krav til løbende opdatering af systemer og til passende logning af datatrafik?

- Skal der gennemføres øvelser og etableres beredskab?

Ovenstående overvejelser om sikkerhedsmæssige forhold i kontrakten giver anledning til at overveje, om myndigheden skal kræve specifikke sikkerhedskrav indarbejdet i 'Service Level Agreements' (SLA-aftaler).

Det er nødvendigt for kunden at afklare alle krav i kontrakten vedr. sikkerhedsleverancer, således at der er klarhed over, hvilke leverancer leverandøren forventes at levere til kunden. Dette kan eksempelvis angå (SLA-)krav til håndtering og rapportering på sikkerhedshændelser, hyppighed for sikkerhedstest, afprøvning og rapportering, hyppighed for beredskabstest, afprøvning og rapportering.

Kunden/myndigheden kan med fordel ligeledes formidle egne krav til egen organisation vedr. sikkerhedsleverancer ift. den outsourcede driftskontrakt.

4.2 Sikkerhedstest og kontrol

Sikkerhedstest kan anvendes til at kontrollere sikkerhedsniveauet i en outsourcet infrastruktur. Eksterne sikkerhedstest tester kvaliteten af det "sikkerhedsskjold", leverandøren har til at imødegå eksterne angreb, f.eks. fra internettet. Interne sikkerhedstest anvendes til at vurdere, hvor god leverandørens baseline for opsætning af sikkerhedsparametre er generelt. Sikkerhedstest af de aftalte ydelser i den outsourcede drift anvendes til at vurdere, om leverandøren lever op til de krav, som er aftalt i kontrakten, eller som må anses at være best practice / good practice på området.

Disse typer af sikkerhedstest giver en idé om, hvor der er risiko ved, at de nuværende kontroller kan omgås, og dermed hvilke kompenserende kontroller, der bør opstilles. Såfremt sikkerhedstest ønskes anvendt til enten at afdække svagheder i applikationer eller infrastruktur, er det essentielt, at de overordnede spilleregler for dette aftales i forbindelse med indgåelse af kontrakten - hvor, hvordan og hvornår der skal gennemføres sikkerhedstest.

Tilsvarende bør myndigheden være meget omhyggelig med at få aftalt og formuleret en ret til at foretage kontrol af efterlevelsen af aftalte sikkerhedskrav samt økonomisk ansvar i den forbindelse.

4.3 Salg eller ophør af leverandørens virksomhed

Myndighederne bør vurdere salg eller ophør af leverandørens virksomhed ud fra risikobeskrivelser såsom:

- Risikoen for lock-in (til systemer eller dataformater).
- Risikoen for mangelfuld sikkerhedsmæssig håndtering af data i forbindelse med kontraktophør, konkurs eller andet pludseligt ophør.
- Risikoen for datalækage, overdragelse til kreditor, mangelfuld sletning etc.
- Risikoen for, at data håndteres under anden jurisdiktion end forudsat i kontrakten, jf. kapitel 2.2..
- Risikoen for manglende adgang til systemer/data, herunder tab af krypteringsnøgle.

Yderligere eksempler på forhold, som kan indgå i kontrakten vedrørende ophør og salg af leverandørens virksomhed (listen er ikke udtømmende):

- Myndigheden bør i kontrakten præcisere, hvorledes kunden får adgang til egne data, f.eks. i tilfælde af leverandørskift eller i tilfælde af, at kontrakten ophæves. Overdragelse af sådanne data kan f.eks. ske ved, at der gives en fuldstændig backup af kundens data, der er placeret på leverandørens servere.
- Myndigheden bør orienteres, såfremt leverandøren bliver opkøbt eller underlagt andre selskabsretlige konstruktioner end de på aftaleindgåelsestidspunktet gældende, og den nye ejer bør være forpligtet til at fortsætte aftalen.

ANBEFALING TIL LEDELSEN

Ledelsen skal inden kontraktindgåelse nøje vurdere risikoen for og konsekvenserne af, at det fornødne sikkerhedsniveau ikke videreføres ved et evt. salg eller ophør af leverandørens virksomhed.

ANBEFALING TIL LEDELSEN

Ledelsen skal sikre, at kontrakten om outsourcet it-drift indeholder konkrete bestemmelser, der tager højde for evt. salg eller ophør af leverandørens virksomheder samt ved skift af leverandørens teknologi/underleverandører etc.

5. Styring af informationssikkerhed efter ISO27001-standarden

Regeringen har truffet beslutning om, at statens institutioner skal følge sikkerhedsstandarden ISO27001. Beslutningen er en følge af Finansministeriets plan for enkel administration i staten (2010).

5.1 Efterlevelse af sikkerhedsstandarden ISO27000-serien

I ISO27001-standarden stilles krav til styringen af sikkerhedsarbejdet – herunder en governancestruktur eller et ledelsessystem for organiseringen af sikkerheds-arbejdet. Dette sker gennem etablering af et Information Security Management System (ISMS) i organisationen. Et ISMS er et samlet udtryk for de politikker, procedurer, beslutningsgange og aktiviteter, som udgør komponenterne i organisationens arbejde med informationssikkerhedsstyring. Et ISMS er en metode til at styre sikkerhed, som gør det nemmere at efterleve standarden.

Organisationens efterlevelse af standarden skal dokumenteres i et såkaldt SoA-dokument (Statement of Applicability). Dette er et af de mest centrale dokumenter i sikkerhedsarbejdet efter ISO27001-standarden. Af dette dokument fremgår ledelsens prioritering af sikkerheden, herunder beslutninger om valg af sikkerheds-foranstaltninger i forhold til forretningens mål og risikoprofil. Uden et godkendt SoA-dokument kender informations-sikkerhedskoordinatoren ikke formelt ledelsens prioriteringer af sikkerheden.

Digitaliseringsstyrelsen har udarbejdet en guide til SoA-dokumentet og et skema, som indeholder alle sikkerhedsområderne i standarden. Når skemaet er udfyldt, har man sin SoA-dokumentation, som viser ledelsens prioriteringer for informationssikkerheden, der også løbende kan bruges til at rapportere fremskridt for etablering af de valgte sikkerhedsforanstaltninger. Guide og skema kan findes og downloades fra Digitaliseringsstyrelsens hjemmeside, www.digst.dk

ANBEFALING TIL LEDELSEN

Myndigheden bør inddrage eventuelle outsourcing-leverandører i arbejdet med at implementere sikkerhedsstandarden ISO27001.

5.2 Risikovurdering

Myndighederne bør lade de generelle og specifikke trusselvurderinger udarbejdet af Center for Cybersikkerhed indgå i deres risikovurdering. Myndighedernes styring af informationssikkerheden og af risici ved egne systemer og procedurer skal tage udgangspunkt i opdaterede trusselbilleder og viden om sårbarheder.

En myndighed skal i sin risikovurdering specifikt besvare spørgsmålene:

- Hvad er konsekvensen og omkostningerne, såfremt et cyberangreb forårsager et nedbrud i et betydeligt omfang af en tjeneste?
- Hvad er konsekvensen og omkostningerne, såfremt et cyberangreb forårsager en kompromittering af fortroligheden af data (persondata eller andre typer data)?
- Hvad er konsekvensen og omkostningerne, såfremt et cyberangreb forårsager tab eller forvanskning af data (er der data, som i praksis er uerstattelige, og som derfor kræver særlig beskyttelse)?

Myndigheden skal i sin risikovurdering vurdere truslerne i forhold til karakteren og værdien af de data og systemer, som myndigheden ejer, samt tage stilling til sikring heraf i relation til de relevante trusler.

Myndigheden skal desuden med henvisning til ISO27001 sikre et robust og afprøvet beredskab (politikker, procedurer og planer for ledelsesmæssige tiltag) ved sikkerhedshændelser, som potentielt kan kompromittere eller på anden vis påvirke vigtige tjenester eller sikkerheden omkring data, som myndigheden er ansvarlig for.

Myndigheden skal endvidere vurdere sit beredskab med henblik på at sikre, at den har passende forudsætninger for at opdage, kortlægge og imødegå angreb, herunder i størst mulig grad opretholde sikkerheden af øvrige data og systemer i tilfælde af en kompromittering.

ANBEFALING TIL LEDELSEN

Ledelsen bør sikre, at myndigheden etablerer et dokumenteret kendskab til trusselbilledet. Trusselsvurderinger af sektor- og myndighedsspecifikke områder kan med fordel i relevante tilfælde udarbejdes i samarbejde med Center for Cybersikkerhed og myndighederne.

Digitaliseringsstyrelsen har udarbejdet en vejledning for risikovurdering i relation til fortrolighed, integritet og tilgængelighed af data og systemer, og hvorledes dette benyttes i sammenhæng med ISO27001-standarden. Vejledningen kan findes og downloades fra Digitaliseringsstyrelsens hjemmeside, www.digst.dk.

Myndigheden bør endvidere vurdere risikobilledet ved outsourcing af it-drift sammenholdt med risikobilledet ved egen drift/insourcing. Risikobilledet sammenholdes med de forretningsmæssige mål og myndighedens risikovillighed på områder, hvor der ikke er risiko for personfølsomme eller nationale data.

Myndighederne skal herunder ved udbud eller indkøb af it-leverancer vurdere it-sikkerhedsrisici ved den påtænkte it-leverance og it-sikkerhedsrisici ved integrationen af leverancen i myndighedens øvrige it-miljø og beslutte passende sikringstiltag.

Det er afgørende for myndighedens it-sikkerhed, at den løbende identificerer de sårbarheder, der måtte være ved at vælge en outsourcet løsning, således at it-sikkerheds-foranstaltningerne kan justeres eller nye indføres.

Ydermere bør den enkelte myndighed i forbindelse med risikovurderingen løbende sikre et samlet overblik over sin anvendelse af eksterne leverandører (i forhold til outsourcet drift, software og hardware).

Center for Cybersikkerheds bidrag til koordinering og videndeling i staten vedrørende sikkerhedshændelser i forbindelse med outsourcet drift styrkes, såfremt der i myndighederne i staten er et dokumenteret overblik over egen anvendelse af it-leverandører (outsourcet drift, software, hardware) og myndighederne deler oplysninger herom med Center for Cybersikkerhed.

ANBEFALING TIL LEDELSEN

Ledelsen skal sikre, at myndighedens risikovurdering udarbejdes med udgangspunkt i sikkerhedsstandarden ISO27001, således at der tages stilling til, om det påtænkte sikkerhedsniveau matcher risikobilledet af de pågældende systemer, der påtænkes outsourcet.

ANBEFALING TIL LEDELSEN

Ledelsen skal sikre, at myndigheden på baggrund af risikovurderingen udfærdiger relevante sikkerhedspolitikker og implementerer og dokumenterer relevante procedurer. Endvidere skal ledelsen sikre, at disse politikker og procedurer er kendte og forståede i organisationen.

5.3 Behandling af personoplysninger

Hvis der er tale om behandling af persondata, skal reglerne i persondataloven og den tilhørende sikkerhedsvejledning iagttages, inden behandlingen starter.

Efter persondataloven må personoplysninger kun behandles, hvis den dataansvarlige har hjemmel (lovgrundlag) til at behandle de pågældende persondata. Overlader den dataansvarlige behandlingen til en databehandler, er det et krav, at der indgås en databehandleraftale mellem parterne, som blandt andet entydigt sikrer, at databehandleren kun behandler data efter den dataansvarliges instruks.

Datatilsynets krav til databehandleraftaler findes her:
http://www.datatilsynet.dk/offentlig/databehandler/

Når der behandles persondata, er det desuden nødvendigt at overholde de overordnede sikkerhedskrav, som er beskrevet i persondataloven. Offentlige myndigheder er endvidere forpligtede til at iagttage de specifikke sikkerhedskrav i sikkerhedsbekendtgørelsen.

Behandling af persondata skal i mange tilfælde anmeldes til Datatilsynet, både når behandlingen sker for private og for offentlige myndigheder. I visse tilfælde og særligt, når der behandles særligt følsomme data, skal Datatilsynets tilladelse også indhentes inden behandling igangsættes.

Digitaliseringsstyrelsen har udarbejdet en vejledning om de juridiske rammer for brug af cloud computing. Vejledningens anden del omhandler kontraktuelle forhold der bør iagttages, ved indgåelse af kontrakt med en sourcingleverandør. En række af kravene er relevante ud fra en sikkerhedsmæssig betragtning. Vejledningen kan findes her:
http://www.digst.dk/Arkitektur-og-standarder/Cloud-computing/De-juridiske-rammer

http://www.digst.dk/Arkitektur-og-standarder/Cloud-computing/De-juridiske-rammer

5.5 Evaluering af sikkerheden

Det er en god ide for myndigheden at evaluere sit sikkerhedsniveau, så der skabes et overblik over den aktuelle status på området. En sådan evaluering kan samtidig bruges til overfor ledelsen at synliggøre behov for ændringer i prioriteringerne i indsatsen.

Digitaliseringsstyrelsen har udviklet to evalueringsværktøjer, der kan bruges i organisationens arbejde med ISO27001:

> "**Værktøj til selvevaluering**" - kan bruges til selvevaluering af, hvor langt en organisation er nået i implementeringsarbejdet. Formålet er at bidrage med konkrete krav til at etablere, implementere, vedligeholde og forbedre et informations-sikkerhedssystem i organisationer. Værktøjet er designet som en hjælp til at holde styr på de forskellige krav fra standarden og organisationens implementeringsgrad.
>
> "**ISO27001-benchmark**" - kan bruges som et benchmark i forhold til Anneks A i ISO27001. Værktøjet gennemgår alle områder i Anneks A og stiller spørgsmål til, hvordan organisationen placerer sig på det aktuelle niveau i forhold til de enkelte områder, og hvilket niveau organisationen ønsker.

Når alle spørgsmål er udfyldt, kan der trækkes en rapport, der viser områderesultater og det overordnede resultat. Værktøjet lægger op til, at man skal vurdere sig på en skala fra 0-5.

Begge værktøj kan findes og downloades fra Digitaliseringsstyrelsens hjemmeside sammen med yderligere materiale om informationssikkerhed og ISO27001: www.digst.dk

6. Koordinering og videndeling mellem statslige myndigheder

Koordinering og videndeling styrker sikkerheden.

Center for Cybersikkerhed har etableret en tværministeriel kontaktgruppe, som skal have fokus på styrkelse af cybersikkerheden for de centrale statslige myndigheder. Kontaktgruppens formål er at videndele, udvikle og koordinere de ministerielle indsatser på cybersikkerhedsområdet. Målet er at styrke cybersikkerheden i Danmark ved at fremme løbende koordination og informationsudveksling mellem relevante offentlige myndigheder på tværs af sektorerne.

Center for Cybersikkerhed arbejder endvidere med at etablere flere offentlig-private arbejdsgrupper med sigte på videndeling og udbredelse af kendskabet til trusler fra internettet. Der arbejdes på at etablere et forum vedrørende ICS/SCADA (industrielle kontrolsystemer) og et forum vedrørende mainframe-systemer.

Digitaliseringsstyrelsen driver et forum for statens myndigheder, Statens Informationssikkerhedsforum (SISF), som samarbejder om it-sikkerhedsområdet på et praktisk niveau. SISF fungerer i dag primært som videndelingsforum, men forummet er sammensat, så det fremover kan udgøre et velegnet forum til koordination af den praktiske håndtering af konkrete sager, som måtte blive identificeret i den tværministerielle kontaktgruppe.

Det styrker det offentliges position overfor it-leverandører, såfremt myndighederne som kunder fremstår homogene og konsistente over for leverandører. Det er i den forbindelse af betydning, at myndigheder, som deler samme infrastrukturkomponenter hos en leverandør, samordner deres krav til leverandøren. Herunder er det f.eks. af betydning, at de pågældende myndigheder alle er modne indkøbere af sikkerhedsydelser, således at leverandøren understøttes i at indføre en passende sikkerhed på hele sin platform, og at der ikke er svage led i sikkerhedskæden, ved at en myndighed har væsentligt ringere sikkerhed end de andre myndigheder på samme platform.

Det er ligeledes af betydning, at myndighederne samarbejder væsentligt mere aktivt om kontrakter vedr. it-leverancer.

Endelig er det af betydning, at myndighederne sikrer, at services og anden funktionalitet, som ikke anvendes, deaktiveres med henblik på at forebygge unødige sårbarheder.

Myndighederne bør sammen med leverandørerne gennemgå og i relevant omfang justere kontrakter med henblik på at sikre, at it-sikkerheden er tidssvarende og afspejler det nuværende trusselbillede.

Der gælder en særlig udfordring for en række systemer i staten, hvor it-arkitekturen, herunder sikkerhedsarkitekturen, i en række tilfælde er mere end 15 år gammel, og formodes kun i begrænset omfang at være udviklet med en sikkerhedsmodel, som inkluderer, at systemerne nu kan tilgås udefra og ofte er sammenkoblet med internettjenester.

ANBEFALING TIL LEDELSEN

Ledelsen skal sikre, at myndigheden i tilstrækkelig grad deltager i den statslige koordination og videndeling på området, herunder er repræsenteret i relevante fora.

7. Bilag – Oversigt over anbefalinger til ledelsen

Rapportens 11 anbefalinger til ledelsen er herunder samlet i en oversigt, der afspejler de direkte og indirekte erfaringer, som er indhentet gennem analysen af CSC-sagen. Oversigten kan anvendes som tjekliste for ledelsen i informationssikkerhedsdialogen med organisationen. Alle anbefalinger er i tråd med den gældende sikkerhedssandard ISO27001.

Kapitel- og sideangivelse refererer til rapporten Anbefalinger til styring af sikkerheden i statens outsourcede it-drift, juni 2014.

Kapitel 2, side 7, trusler
Ledelsen bør sikre, at myndighedens risikovurderinger og risikoledelse, jf. kapitel 5, tager udgangspunkt i et opdateret trusselbillede. Ledelsen bør endvidere sikre, at organisationen vurderer risici ud fra karakteren og værdien af data og systemer, som myndigheden er ansvarlig for, herunder hvor kritiske de er for myndigheden.
Ledelsen bør tage initiativ til, at myndigheden indleder en dialog med Center for Cybersikkerhed vedrørende mulighederne for at gøre brug af centerets it-sikkerhedsydelser.

Kapitel 4, side 10-13, sikkerhedsstyring – eksterne leverandører
Ledelsen bør sikre, at der er en tydelig ansvarsfordeling mellem kunde og leverandør om, hvem der er ansvarlig for specifikke sikkerhedstiltag, herunder leverandørens ansvar for underleverandører. Der skal sikres en klar ansvarsfordeling mellem kunde og leverandør i forhold til sikkerhedsaktiviteter.
Ledelsen bør sikre, at der stilles relevante krav til sikkerhedsforanstaltninger hos eksterne leverandører.
Ledelsen skal inden kontraktindgåelse nøje vurdere risikoen for og konsekvenserne af, at det fornødne sikkerhedsniveau ikke videreføres ved et evt. salg eller ophør af leverandørens virksomhed.
Ledelsen skal sikre, at kontrakten om outsourcet it-drift indeholder konkrete bestemmelser, der tager højde for evt. salg eller ophør af leverandørens virksomheder samt ved skift af leverandørens teknologi/underleverandører etc.

Kapitel 5, side 14-15, sikkerhedsstyring – organisationen
Myndigheden bør inddrage eventuelle outsourcing-leverandører i arbejdet med at implementere sikkerhedsstandarden ISO27001.
Ledelsen bør sikre, at myndigheden etablerer et dokumenteret kendskab til trusselbilledet. Trusselsvurderinger af sektor- og myndighedsspecifikke områder kan med fordel i relevante tilfælde udarbejdes i samarbejde med Center for Cybersikkerhed og myndighederne.
Ledelsen skal sikre, at myndighedens risikovurdering udarbejdes med udgangspunkt i sikkerhedsstandarden ISO27001, således at der tages stilling til, om det påtænkte sikkerhedsniveau matcher risikobilledet af de pågældende systemer, der påtænkes outsourcet.
Ledelsen skal sikre, at myndigheden på baggrund af risikovurderingen udfærdiger relevante sikkerhedspolitikker og implementerer og dokumenterer relevante procedurer. Endvidere skal ledelsen sikre, at disse politikker og procedurer er kendte og forståede i organisationen.

Kapitel 6, side 17, koordinering og videndeling
Ledelsen skal sikre, at myndigheden i tilstrækkelig grad deltager i den statslige koordination og videndeling på området, herunder er repræsenteret i relevante fora.