FOLKETINGET
RIGSREVISIONEN

Læringspunkter fra beretninger om it-sikkerhed

Danmark er et af de mest digitaliserede lande i verden. Det gælder også den offentlige sektor. Med den omfattende digitalisering er det en forudsætning for stabil drift og beskyttelse af data, at vi kan forsvare os mod hackerangreb og andre it-hændelser som fx nedbrud på grund af manglende vedligeholdelse af it-systemer.

Informationssikkerhed har til formål at beskytte hardware, software, netværk mv. mod uautoriseret adgang, ødelæggelse eller lækage af data.

Den offentlig sektor har bl.a. ansvaret for store og komplekse samfundskritiske systemer på områder som forsvar, retsvæsen, sundhed og skat, hvor det er af afgørende betydning, at myndighederne har et højt sikkerhedsniveau.

Finansministeriet har siden 2016 stillet krav om, at statslige myndigheder skal følge den internationale standard for informationssikkerhed ISO 27001. Standarden består af en række kontroller, som myndighederne skal indføre for at opnå et passende sikkerhedsniveau. Myndighederne skal desuden som led i den nationale cyber- og informationssikkerhedsstrategi efterleve de tekniske minimumskrav. Kravene skal beskytte mod ondsindede angreb på cyber- og informationssikkerheden.

Rigsrevisionen udfører hvert år revisioner af it-sikkerheden i staten og regionerne. Vi har siden 2013 afgivet 14 beretninger om it-sikkerhed. Derudover har vi løbende rapporteret om mangler i it-sikkerheden i beretningerne om revisionen af statsregnskabet og revisionen af statens forvaltning. Vi har på baggrund af beretningerne samlet den mest væsentlige og brugbare viden inden for 5 temaer. Målet er at bidrage til at styrke it-sikkerheden i det offentlige. Temaerne er:

- it-beredskab
- sikkerhedsopdateringer
- leverandørstyring
- it-risikovurdering
- rettighedsstyring.

Under hvert tema har vi grafisk fremhævet de største udfordringer med at sikre et tilfredsstillende it-sikkerhedsniveau. Vi giver også et eksempel, der er med i én af vores beretninger. Til sidst henviser vi til de beretninger, hvor temaet er omtalt, og til, hvor du kan finde inspiration til at løse udfordringerne.

It-beredskab

Større it-nedbrud kan have store konsekvenser for både myndigheden, borgere og virksomheder. Hvis it-beredskabet ikke er tilstrækkeligt, er der risiko for, at et nedbrud medfører, at driften ikke kan fortsætte. Det er særligt alvorligt, hvis der er tale om samfundskritiske opgaver.

Boks 1

Baggrund

Myndighederne skal ifølge ISO 27001 planlægge it-beredskabet ved at vurdere sårbarhed, trusler, konsekvenser og sandsynlighed for it-nedbrud. Det skal munde ud i en risikovurdering, der er udgangspunktet for en målrettet reetableringsplan.

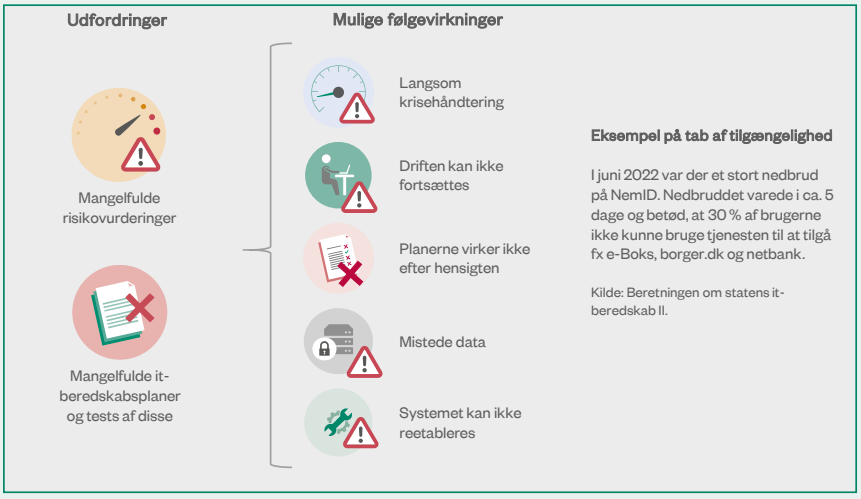
Boks 2

Hvad ved vi

Vores beretninger om it-beredskab har bl.a. vist:

- At myndighederne enten ikke har udarbejdet risikovurderinger, eller at risikovurderingerne er mangelfulde. Fx at myndigheder ikke har overblik over, hvilke andre systemer der er afgørende for, at et samfundskritisk it-system fungerer. Det kan betyde, at it-beredskabet planlægges på et forkert grundlag, og at sikkerhedsniveauet dermed ikke er tilstrækkeligt.
- At myndighederne ikke har udarbejdet brugbare beredskabsplaner. Det gælder særligt i forhold til reetableringsplaner, som er planer for, hvordan systemerne kan komme til at fungere igen efter et nedbrud. Det kan derfor betyde, at myndighederne ikke kan videreføre driften efter et it-nedbrud.
- At myndighederne ikke har testet beredskabsplanerne. Det kan betyde, at medarbejderne ikke har trænet beredskabet og dermed ikke ved, om fx reetableringsplanerne virker efter hensigten.

Myndighedernes udfordringer med at sikre et tilfredsstillende it-beredskab



Boks 3

Hvad skal du være opmærksom på

Myndighedernes it-beredskabsplaner kan være struktureret på forskellige måder og have forskellige navne, men overordnet er der ifølge Digitaliseringsstyrelsens "Vejledning i it-beredskab" 3 typer af planer, der skal være på plads:

- **Krisestyringsplaner** beskriver myndighedernes interne krisestyring ved et større it-nedbrud, fx kontaktoplysninger og rollefordeling i en beredskabssituation.
- **Forretningsnødplaner** beskriver, hvilke nødprocedurer myndighederne kan tage i brug i tilfælde af et nedbrud på de it-systemer, der normalt varetager myndighedens opgaver, fx manuelle procedurer til at løse myndighedens opgaver.
- **Reetableringsplaner** beskriver, hvordan it-systemer teknisk genskabes efter et nedbrud. Hvis it-systemet driftes af en ekstern leverandør, er det typisk leverandøren, der står for at genskabe systemet og udarbejde en plan for reetablering. Uanset driftsforhold er det dog myndighedens ansvar, at systemet kan reetableres.

Myndighederne skal desuden teste it-beredskabsplanerne for at vurdere, om procedurerne for beredskabet virker, og for at træne relevante medarbejdere i beredskabshåndteringen.

Boks 4

Her kan du læse mere

Vores beretninger om mangler i it-beredskabet:

- Beretning om statens it-beredskab II (nr. 5/2023)
- Beretning om statens it-beredskab (nr. 3/2022)
- Beretning om Skatteministeriets it-beredskab (nr. 20/2020)
- Beretning om beskyttelse mod ransomwareangreb (nr. 11/2017).

It-beredskab er også omtalt i beretninger om revisionen af statsregnskabet for regnskabsårene 2014, 2016 og 2017 og i beretninger om revisionen af statens forvaltning for regnskabsårene 2018 og 2019.

Du kan læse mere om, hvilke krav der er til it-beredskabet for it-systemer i staten, og hvordan myndighederne og institutionerne sikrer opdaterede og relevante it-beredskabsplaner, i bl.a. ISO 27001-/27002-standarderne, Digitaliseringsstyrelsens vejledning og skabeloner til it-beredskab og "Vejledning til kommunikation i en beredskabssituation", Center for Cybersikkerheds vejledning "Cyberforsvar, der virker" samt på sikkerdigital.dk.

Sikkerhedsopdateringer

Når hardware, software, netværk mv. ikke sikkerhedsopdateres regelmæssigt, øges risikoen for alvorlige sårbarheder. Konsekvensen kan være, at hackere får adgang til fx følsomme oplysninger og vigtige forretningsdata, der kan misbruges eller ødelægges.

Boks 5

Baggrund

It-systemer og udstyr har begrænset levetid. Levetiden er den periode, hvor leverandøren forpligter sig til at udvikle sikkerhedsopdateringer, i takt med at sårbarheder opdages. I løbet af levetiden udgiver leverandøren jævnligt og ofte flere gange om måneden opdateringer, der forbedrer og sikrer it-sikkerheden ved at inddæmme sikkerhedsbrister og beskytte mod nye, kendte trusler. Når levetiden udløber, kan systemet og udstyret ikke længere sikkerhedsopdateres. Det vil nu udgøre en sikkerhedsrisiko.

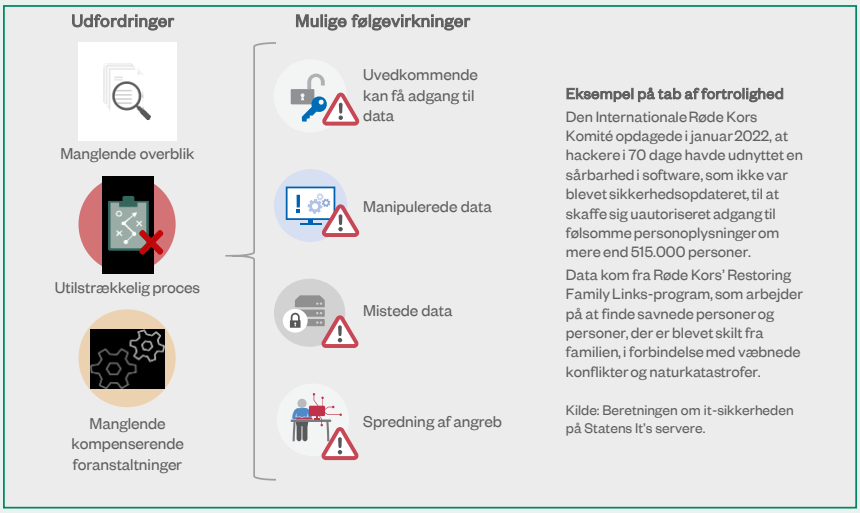
Boks 6

Hvad ved vi

Vores beretninger om sikkerhedsopdateringer har bl.a. vist:

- At myndighederne kan mangle overblik over omfanget af sikkerhedsopdateringer. Det kan betyde, at myndighederne ikke får opdateret relevante enheder og derfor bliver mere sårbare over for potentielle hackerangreb.
- At myndighederne ikke har en fast procedure for, at især kritiske sikkerhedsopdateringer bliver gennemført. Det kan betyde, at hackere får adgang, inden opdateringerne sker.
- At myndighederne ikke har etableret kompenserende foranstaltninger for it-systemer, som ikke længere kan sikkerhedsopdateres, men som myndighederne fortsat bruger. Det kan betyde, at risikoen for hackerangreb øges. Kompenserende handlinger skal reducere sårbarheden eller risikoen for succesfulde angreb.

Myndighedernes udfordringer med at sikkerhedsopdatere



Boks 7

Hvad skal du være opmærksom på

Myndigheder skal prioritere implementeringen af tekniske tiltag højt, når de arbejder med cyber- og informationssikkerhed. Det anbefaler Center for Cybersikkerhed i vejledningen "Cyberforsvar, der virker".

Center for Cybersikkerhed understreger også vigtigheden af, at myndighederne sikrer systematiske sikkerhedsopdateringer af deres programmer. Center for Cybersikkerhed tilslutter sig i Rigsrevisionens beretning om forebyggelse af hackerangreb følgende 2 tiltag, der forebygger hackerangreb:

- teknisk begrænsning af download af programmer og nyt udstyr
- begrænsning af brugen af lokaladministratorer og medarbejdere med udvidede rettigheder, der kan downloade nye og ukendte programmer.

Myndighederne bør i god tid håndtere it-systemer og udstyr, hvor det er varslet, at leverandøren ikke længere vil sikkerhedsopdatere systemerne og udstyret. Hvis en myndighed allerede har it-systemer og udstyr, der ikke kan sikkerhedsopdateres eller udskiftes, bør myndigheden have kompenserende foranstaltninger klar. De kompenserende foranstaltninger vil fx kunne opdage et angreb eller mindske, at angrebet kan sprede sig.

Boks 8

Her kan du læse mere

Vores beretninger om manglende sikkerhedsopdateringer:

- Beretning om it-sikkerheden på Statens It's servere (nr. 6/2023)
- Beretning om universiteternes beskyttelse af forskningsdata (nr. 8/2018)
- Beretning om beskyttelse mod ransomwareangreb (nr. 11/2017)
- Beretning om 3 regioners beskyttelse af adgangen til it-systemer og sundhedsdata (nr. 4/2017)
- Beretning om forebyggelse af hackerangreb (nr. 3/2013).

It-sikkerhedsopdateringer er også undersøgt i beretningen om revisionen af statsregnskabet for 2013 (nr. 28/2013).

Du kan læse mere om it-sikkerhedsopdateringer i bl.a. ISO 27001-/27002-standarderne, de tekniske minimumskrav, Center for Cybersikkerhed, som bl.a. offentliggør varsler om kritiske sårbarheder, Center for Cybersikkerheds vejledning "Cyberforsvar, der virker" samt på sikkerdigital.dk.

Leverandørstyring

Myndighederne kan outsource deres it-drift, men ikke ansvaret for it-sikkerheden. Uden aktiv risikobaseret styring og opfølgning på sikkerheden har myndighederne ingen garanti for, at leverandøren i tilstrækkelige grad beskytter systemer og data.

Boks 9

Baggrund

Myndighederne anvender i stigende grad eksterne leverandører til hele eller dele af it-driften. Når driften er outsourcet, har myndigheden ikke længere direkte kontrol over it-sikkerheden. Myndigheden indgår i et kundeforhold med leverandøren. Men det er fortsat myndighedens ansvar at definere kravene til it-sikkerhed og sikre, at kontrakten er dækkende og bliver efterlevet.

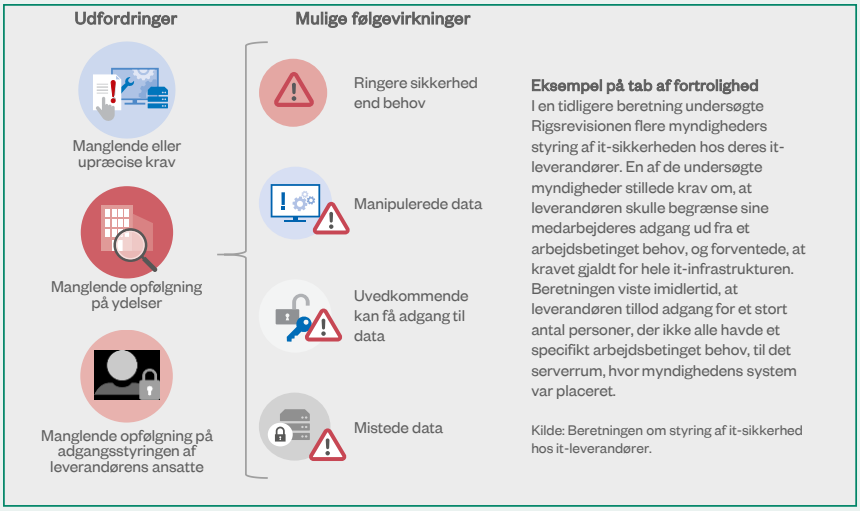
Boks 10

Hvad ved vi

Vores beretninger om leverandørstyring har bl.a. vist:

- At myndighederne ikke altid stiller krav eller stiller upræcise krav i kontrakten med leverandøren. Det kan betyde, at leverandøren fortolker kravene og deres forpligtelser. Det giver en risiko for, at leverandøren ikke lever op til det niveau af sikkerhed, myndigheden forventer.
- At myndighederne ikke følger op på, om leverandøren overholder kontrakten og leverer det aftalte. Det kan betyde, at leverandøren ikke lever op til den sikkerhed, der følger af kontrakten.
- At myndighederne ikke holder sig opdateret om adgangsstyring og logning hos leverandøren. Det kan betyde en øget risiko for uautoriseret adgang til it-systemer og data, fx at ansatte ved leverandøren tilgår it-systemer og data uden at have et arbejdsbetinget behov eller mangler sikkerhedsgodkendelse.

Myndighedernes udfordringer med leverandørstyring



Boks 11

Hvad skal du være opmærksom på

ISO 27001 understreger vigtigheden af at evaluere og styre risici i forbindelse med leverandører. Det gælder især dem, der har adgang til – eller behandler – især følsomme data og oplysninger på vegne af myndigheden. Ud over klare kontraktlige krav til leverandørens it-sikkerhed, herunder behandling af data og rapportering af sikkerhedsbrud, indebærer leverandørstyringen ifølge ISO 27001/27002:

- overvågning og gennemgang af, om leverandøren overholder sikkerhedskravene
- retningslinjer og kontrolforanstaltninger for håndtering af ændringer i leverandørsamarbejdet, herunder opdatering af kontrakter og sikkerhedsforanstaltninger
- fortsatte forbedringer af samarbejdet baseret på resultater af evalueringer af samarbejdet.

Det er bl.a. nævnt i Digitaliseringsstyrelsens katalog over kontraktbestemmelser over samfundskritiske it-systemer, at myndigheden bør kræve en revisorerklæring i kontrakten. Revisorerklæringen fungerer som dokumentation for leverandørens overholdelse af lovkrav og god it-skik. En erklæring omfatter typisk en gennemgang og vurdering af den overordnede styring af informationssikkerheden, herunder organisering, politik om informationssikkerhed, risikovurderinger og beredskabsplaner.

Boks 12

Her kan du læse mere

Vores beretninger om leverandørstyring:

- Beretning om Energinets outsourcing af driften af forsyningskritisk it-infrastruktur (nr. 14/2021)
- Beretning om outsourcede persondata (nr. 15/2019)
- Beretning om styring af it-sikkerhed hos it-leverandører (nr. 5/2016).

Leverandørstyring er også undersøgt i beretninger om revisionen af statens forvaltning for regnskabsårene 2019 og 2020.

Du kan læse mere om krav til leverandørstyring i staten, og hvordan myndighederne sikrer tilfredsstillende leverandørkontrakter, i ISO 27001-/27002-standarderne, Digitaliseringsstyrelsens "Krav til kontrakt- og leverandørstyring for samfundskritiske it-systemer", "Katalog over kontraktbestemmelser for samfundskritiske it-systemer" og "Vejledning i anvendelse af cloudservices" samt Center for Cybersikkerheds vejledning "Cybersikkerhed i leverandørforhold".

It-risikovurdering

Manglende eller utilstrækkelig risikovurdering af it-systemer kan føre til en for lav it-sikkerhed. Uden en aktiv styring ved myndighederne ikke, om it-systemerne lever op til den nødvendige it-sikkerhed.

Boks 13

Baggrund

Ifølge ISO 27001 skal myndighederne udarbejde en risikovurdering, som inddrager risici, der kan påvirke evnen til at udføre den pågældendes myndigheds opgave. Risikovurderingen skal beskrive potentielle trusler mod it-systemerne, fx cyberangreb eller nedbrud, og myndigheden skal fastsætte et mål for sikkerhed. Resultaterne af vurderingen skal derefter omsættes til konkrete handlinger, for at målet kan nås. Risikovurderingen skal desuden være godkendt af ledelsen i den enkelte myndighed for at sikre opmærksomhed på de identificerede risici og på, hvordan de bliver nedbragt.

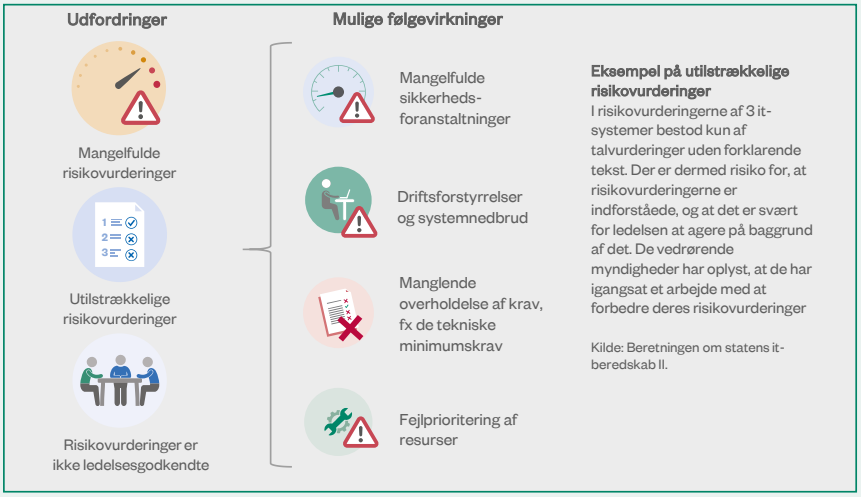
Boks 14

Hvad ved vi

Vores beretninger om it-risikovurdering har bl.a. vist:

- At myndighederne ikke har foretaget tilstrækkelige risikovurderinger af deres it-systemer. Risikovurderingerne er meget overordnede og omfatter ikke alle relevante dele som fx afhængigheder til andre it-systemer. Det kan betyde, at myndighederne ikke handler på uønskede risici.
- At myndighedernes risikovurderinger ikke er godkendt af den øverste ledelse. Det betyder, at ledelsen ikke er klar over – eller har taget stilling til – den risiko, der er ved systemerne. Ledelsen har derved heller ikke taget stilling til, om de ønsker at fjerne eller reducere risiciene, så den ønskede it-sikkerhed opnås.
- At myndighederne ikke har vurderet risici for it-sikkerheden, før udvikling og driften overlades til en ekstern leverandør. Det kan betyde, at myndigheden ikke har et grundlag for at fastsætte passende krav om sikkerhed i aftalen med leverandøren.

Myndighedernes udfordringer med risikovurdering



Boks 15

Hvad skal du være opmærksom på

Formålet med it-risikovurderingen er, at den skal være en hjælp til at vise vej til og fastlægge relevante prioriteringer, der øger sikkerheden. Myndigheden skal ikke udsætte sig for større risiko, end hvad ledelsen finder acceptabelt, jf. ISO 27001. Digitaliseringsstyrelsen kommer i sin "Vejledning til risikostyring inden for informationssikkerhed" med 5 aktiviteter, som kan anvendes i risikostyringsprocessen:

- **Etablering af kontekst.** Myndigheden skal definere den situation og de rammer, den samfundsmæssigt arbejder inden for. Derudover skal myndigheden definere, hvad formålet med risikovurderingen er, hvad den skal dække, hvilke trusler og sårbarheder der er relevante, og hvilke regler, krav og mål myndigheden har. Det sikrer, at risikovurderingen er fokuseret og tilpasset myndighedens specifikke behov og omgivelser.
- **Risikovurdering.** Myndigheden skal identificere, analysere og vurdere de potentielle risici, der er for myndighedens it-systemer. Myndigheden skal vurdere sandsynligheden for, at en trussel udnytter en sårbarhed, og hvilken skade det kan forårsage. Det giver et billede af, hvilke risici der er mest alvorlige.
- **Risikohåndtering.** På baggrund af risikovurderingen skal myndigheden udarbejde en plan for, hvordan myndigheden vil håndtere de identificerede risici. I planen skal myndigheden beskrive, hvilke tiltag myndigheden vurderer som de bedste og mest effektive.
- **Risikoaccept.** Myndighedens risici skal rapporteres til den øverste ledelse. Ledelsen skal vurdere, om ledelsen vil acceptere den eventuelle risiko, der er tilbage efter håndteringen af den.
- **Opfølgning på risici.** Myndigheden skal løbende følge op på de identificerede risici. Derved sikrer myndigheden, at risikohåndteringen virker efter hensigten.

Risikovurderinger er et øjebliksbillede af situationen på det tidspunkt, hvor vurderingen udarbejdes. Derfor skal myndigheden løbende indarbejde nye sårbarheder og trusler i risikovurderingen.

Boks 16

Her kan du læse mere

Vores beretninger om mangler i it-risikovurdering:

- Beretning om statens it-beredskab II (nr. 5/2023)
- Beretning om outsourcede persondata (nr. 15/2019)
- Beretning om styring af it-sikkerhed hos it-leverandører (nr. 5/2016)
- Beretning om forebyggelse af hackerangreb (nr. 3/2013).

It-risikovurdering er også omtalt i beretninger om revisionen af statsregnskabet for regnskabsårene 2014, 2016, 2017, 2019 og 2023.

Du kan læse mere om, hvilke krav der er til risikovurdering for it-systemer i staten, og hvordan myndighederne og institutionerne sikrer opdaterede og relevante it-risikovurderinger, i bl.a. ISO 27001-/27002-standarderne, på sikkerdigital.dk's "Vejledning om risikostyring" samt i Digitaliseringsstyrelsens publikationer "Vejledning til risikostyring" og "It-projekter: Vejledning til risikovurdering og rådgivning ved Statens It-råd".

Rettighedsstyring

Manglende styring af brugernes rettigheder i it-systemer øger risikoen for, at medarbejdere kan få adgang til oplysninger og data, som de ikke har et arbejdsbetinget behov for. Når myndighederne ikke aktivt styrer brugerrettighederne, øges risikoen også for manglende funktionsadskillelse, fx mellem oprettelse af en udbetaling og selve udbetalingen.

Boks 17

Baggrund

Rettighedsstyring skal sikre, at brugerrettigheder afgrænses og tildeles i overensstemmelse med medarbejderens behov for at kunne løse den enkeltes arbejdsopgaver, dvs. brugerne har et arbejdsbetinget behov. Tildeling, ændring og afvikling af brugerrettigheder skal ske i overensstemmelse med myndighedens politik og retningslinje og skal dokumenteres, jf. ISO 27001. Hvis medarbejdere har flere brugerrettigheder til myndighedens it-systemer end nødvendigt – eller har rettigheder i forskellige it-systemer, der tilsammen giver unødvendige rettigheder – er der en risiko for, at medarbejderen fx kan at oprette og godkende en udbetaling til sig selv.

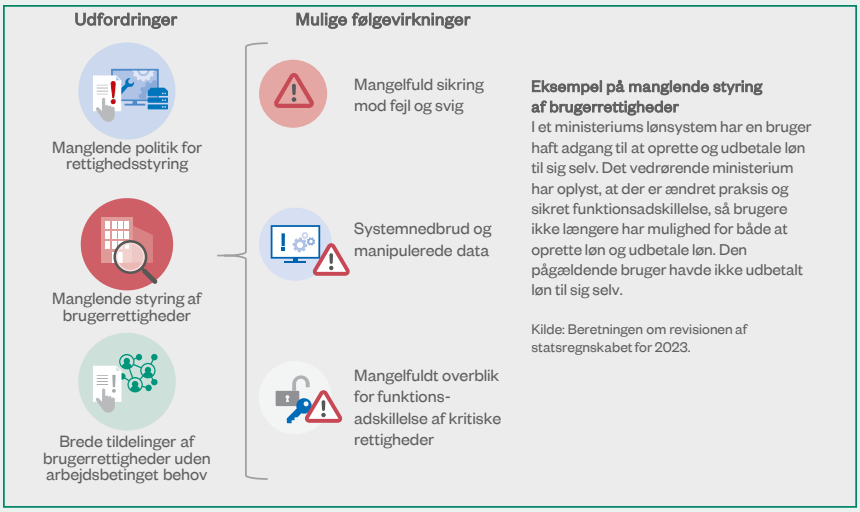
Boks 18

Hvad ved vi

Vores beretninger om rettighedsstyring har bl.a. vist:

- At myndighederne mangler styring af brugerrettigheder til deres it-systemer, herunder manglende politikker og retningslinjer, fx en politik for, hvor ofte gennemgangen af brugernes rettigheder skal ske. Det betyder, at myndighederne ikke i tilstrækkelig grad kontrollerer, om en bruger fx både kan bestille og betale en vare, eller om en bruger kan udbetale løn til sig selv.
- At myndighederne ikke er opmærksomme på, at en kontrol i et it-system kan omgås. En kontrol skal bl.a. forhindre medarbejderne i at foretage handlinger, som de ikke er godkendt til, eller som kræver funktionsadskillelse.
- At myndighederne har et stort antal brugere med flere rettigheder, uden at brugerne har et behov for at have rettighederne. Det kan betyde, at medarbejdere tilsigtet eller utilsigtet kan ændre på eller misbruge informationer.

Myndighedernes udfordringer med risikovurdering



Boks 19

Hvad skal du være opmærksom på

Styring, dvs. oprettelse, ændring og nedlæggelse, af brugernes rettigheder til data og it-systemer skal ske i overensstemmelse med myndighedens politikker og regler, jf. ISO 27001. Det gælder også for brugere, der har flere rettigheder end en almindelig bruger. Det kan fx være rettigheder til at oprette og nedlægge andre brugere eller ændre i data. Styring af rettighederne skal også sikre, at konfliktende opgaver og ansvarsområder adskilles. Det fremgår af regnskabsbekendtgørelsen:

- At udbetalingsforretninger skal tilrettelægges, så der etableres en personmæssig adskillelse mellem den regnskabsmæssige registrering og betalingen. Hvis dette ikke er muligt, skal der optages særskilte bestemmelser herom i regnskabsinstruksen med henblik på at sikre kontrollen med betalingerne på anden måde.
- At medarbejdere, der er beskæftiget med systemudvikling, programmering, driftsafvikling og kontrol hermed, ikke må varetage funktioner i forbindelse med den regnskabsmæssige registrering og betalingsforretninger.

Nogle myndigheder kan have behov for at tildele rettigheder, der betyder, at den personmæssige adskillelse ikke kan håndhæves. I givet fald er det vigtigt, at myndigheden laver kompenserede foranstaltninger, der kan opdage en eventuel uregelmæssighed. En kompenserede foranstaltning kan fx være løbende at gennemgå brugernes handlinger for at bekræfte, at de alle er godkendte.

Boks 20

Her kan du læse mere

Vores beretninger om manglede rettighedsstyring:

- Beretning om indsatsen for undgå statsansattes besvigelser (nr. 7/2020)
- Beretning om Skatteministeriets it-beredskab (nr. 20/2020).

Rettighedsstyring er også omtalt i beretninger om revisionen af statsregnskabet for regnskabsårene 2019, 2020, 2021 og 2023 og i beretningen om revisionen af statens forvaltning for regnskabsåret 2019.

Du kan læse mere om rettighedsstyring i bl.a. ISO 27001-/27002-standarderne, i Datatilsynet.dk's vejledning "Styr på rettighedsstyring", i sikkerdigital.dk's vejledninger "Adgangsstyring" og "Privilegerede rettigheder" samt i databeskyttelsesforordningen.

Kontakt: Vicky la Cour.