RIGSREVISIONEN

Beretning til Statsrevisorerne om adgangen til it-systemer, der understøtter samfundsvigtige opgaver

Oktober 2015

Indholdsfortegnelse

Rigsrevisionen har selv taget initiativ til denne undersøgelse og afgiver derfor beretningen til Statsrevisorerne i henhold til § 17, stk. 2, i rigsrevisorloven, jf. lovbekendtgørelse nr. 101 af 19. januar 2012.

Beretningen vedrører finanslovens § 7. Finansministeriet, § 11. Justitsministeriet, § 16. Ministeriet for Sundhed og Forebyggelse (nu Sundheds- og Ældreministeriet), § 28. Transportministeriet (nu Transport- og Bygningsministeriet) og § 29. Klima-, Energi- og Bygningsministeriet (nu Energi-, Forsynings- og Klimaministeriet).

I undersøgelsesperioden har der været følgende ministre:

Finansministeriet:
Bjarne Corydon: oktober 2011 - juni 2015
Claus Hjort Frederiksen: juni 2015 -

Justitsministeriet:
Mette Frederiksen: oktober 2014 - juni 2015
Søren Pind: juni 2015 -

Sundheds- og Ældreministeriet:
Nick Hækkerup: februar 2014 - juni 2015
Sophie Løhde: juni 2015 -

Transport- og Bygningsministeriet:
Magnus Johannes Heunicke: februar 2014 - juni 2015
Hans Christian Schmidt: juni 2015 -

Energi-, Forsynings- og Klimaministeriet:
Rasmus Helveg Petersen: februar 2014 - juni 2015
Lars Christian Lilleholt: juni 2015 -

Beretningen har i udkast været forelagt Finansministeriet, Justitsministeriet, Sundheds- og Ældreministeriet, Transport- og Bygningsministeriet og Energi-, Forsynings- og Klimaministeriet, hvis bemærkninger er afspejlet i beretningen.

1. Introduktion og konklusion

1.1. Formål og konklusion

1. Denne beretning handler om, hvad en række statslige institutioner gør for at beskytte adgangen til it-systemer og data, som understøtter samfundsvigtige opgaver, via de såkaldte udvidede administratorrettigheder. Rigsrevisionen har selv taget initiativ til undersøgelsen.

2. It-systemer, der understøtter samfundsvigtige opgaver, kan – ligesom andre it-systemer – tilgås med udvidede administratorrettigheder. Disse rettigheder giver det højeste niveau af rettigheder, adgang og kontrol over institutionernes it-systemer og data, som styres i brugeradministrationssystemet Active Directory (AD). Desuden kan rettighederne give mulighed for at omgå institutionernes sikkerhedsforanstaltninger. I nogle tilfælde kan de udvidede administratorrettigheder – afhængigt af institutionens systemopbygning – også give adgang til andre væsentlige it-systemer og data, der ikke styres i AD.

Active Directory (AD) *er et brugeradministrationssystem, hvori institutionen styrer og kontrollerer adgang og rettigheder til it-systemer og data.*

Sikkerhedsforanstaltninger *skal bidrage til at forhindre eller opdage misbrug og kompromittering af it-systemer og data. Det er fx tekniske regler i it-systemerne, der kan forhindre uønskede handlinger.*

3. Beretningen vedrører følgende 6 institutioner: Energinet.dk (under Energi-, Forsynings- og Klimaministeriet), Banedanmark (under Transport- og Bygningsministeriet), National Sundheds-it (under Sundheds- og Ældreministeriet), der varetager it-drift for Sundheds- og Ældreministeriet, Statens It (under Finansministeriet), der varetager it-drift for en række ministerområder, samt Direktoratet for Kriminalforsorgen og Rigspolitiets Koncern IT (under Justitsministeriet). De 6 institutioner dækker tilsammen en bred vifte af forskellige samfundsvigtige opgaver.

4. Institutionernes opgaveløsning er afhængig af en velfungerende og sikker it-understøttelse. Det er derfor afgørende, at institutionerne styrer og kontrollerer de udvidede administratorrettigheder, dels mod internt misbrug, hvor betroede it-medarbejdere misbruger deres udvidede administratorrettigheder eller håndterer rettighederne uforsigtigt, dels mod eksternt misbrug, hvor fx en hacker, der har haft held til at komme ind i institutionens it-systemer, overtager og misbruger de udvidede administratorrettigheder. En hacker kan fx få adgang til institutionens it-systemer og data, der styres i AD. Det er også vigtigt, at institutionerne sikrer en tilstrækkelig logning af anvendelsen af de udvidede administratorrettigheder med henblik på at opdage og opklare misbrug og kompromittering af it-systemer og data.

Misbrug og kompromittering af it-systemer og data *indebærer, at en person uretmæssigt kan få adgang til en række af institutionens it-systemer og data. Der kan fx være tale om, at personen uretmæssigt afbryder eller ændrer datakørsler, eller at personen uretmæssigt ændrer, sletter eller læser/stjæler data.*

5. Det fremgår af "Efterretningsmæssig Risikovurdering 2014" fra Forsvarets Efterretningstjeneste, at den teknologiske udvikling gør, at risikoen for at blive hacket øges, og at risikobilledet ændrer sig løbende. Det stiller ifølge risikovurderingen store krav til sikkerhedsforanstaltningerne. Desuden fremgår det af risikovurderingen fra 2013, at truslen fra ansatte, der ubevidst eller bevidst bryder sikkerheden på deres arbejdsplads, vokser.

6. Misbrug og kompromittering af institutionernes it-systemer og data vil kunne påvirke og forstyrre institutionernes opgaveløsning. Derudover kan misbrug og kompromittering af it-systemer og data for nogle institutioner true en sikker opbevaring af fortrolige personoplysninger og øvrige fortrolige data. Konsekvenserne af misbrug og kompromittering af institutionernes it-systemer og data varierer på tværs af institutionerne afhængigt af deres opgaveportefølje.

Institutionerne har oplyst, at de har forskellige kompenserende foranstaltninger, der bidrager til at begrænse risikoen for og konsekvensen af uretmæssig adgang via de udvidede administratorrettigheder og misbrug og kompromittering af it-systemer og data. Ifølge institutionerne betyder det fx, at misbrug af de udvidede administratorrettigheder i de undersøgte AD ikke kan påvirke forsyningssikkerhed af el og gas og sikkerheden af togdriften. Desuden er det ifølge institutionerne fx heller ikke muligt via de udvidede administratorrettigheder i de undersøgte AD at skaffe sig adgang til it-systemer og data, der bruges i den direkte patientbehandling, og heller ikke til flere af Rigspolitiets kritiske it-systemer og data.

7. Beretningen sætter fokus på den væsentlige risiko, der er ved en mangelfuld styring og kontrol af de udvidede administratorrettigheder, hvilket indebærer, at personer uretmæssigt kan få adgang til institutionernes it-systemer og data. Rigsrevisionen har ikke undersøgt, hvad den uberettigede adgang specifikt kan udnyttes til i institutionernes konkrete it-systemer og data.

8. Undersøgelsen, som beretningen bygger på, er baseret på it-revisioner, som Rigsrevisionen har udført i første halvdel af 2015.

9. Rigsrevisionen har undtagelsesvist besluttet at anonymisere resultaterne ud fra et it-sikkerhedshensyn, da revisionen har påvist en række alvorlige mangler, der udgør en it-sikkerhedsrisiko, indtil institutionerne har rettet op på manglerne.

Rigsrevisionen finder det vigtigt at offentliggøre de resultater, som beretningen indeholder, for at bidrage til at forbedre it-sikkerheden i staten generelt, idet resultaterne kan gøre sig gældende for en større kreds af statslige institutioner end de 6 institutioner, som beretningen omhandler.

10. Formålet med undersøgelsen er at vurdere, om de statslige institutioner følger anbefalinger om god it-sikkerhedspraksis for at beskytte adgangen til it-systemer og data, som understøtter samfundsvigtige opgaver. Vi har derfor undersøgt, hvordan institutionerne styrer og kontrollerer de udvidede administratorrettigheder, herunder hvordan institutionerne sikrer logning af anvendelsen af udvidede administratorrettigheder.

KONKLUSION

Rigsrevisionen vurderer samlet, at de 6 institutioner på undersøgelsestidspunktet ikke har efterlevet en række anerkendte anbefalinger om god it-sikkerhedspraksis for at beskytte adgangen til it-systemer og data, som understøtter samfundsvigtige opgaver. Særligt 2 institutioner har ikke efterlevet anbefalingerne.

De 6 institutioners manglende efterlevelse af anbefalingerne kan øge risikoen for, at personer uberettiget kan få adgang til institutionernes it-systemer og data, der styres i AD. Det kan påvirke og forstyrre løsningen af de samfundsvigtige opgaver og kan true en sikker opbevaring af fortrolige data, som institutionerne har ansvaret for.

Undersøgelsen viser, at der i alle institutionerne er en række mangler i styringen og kontrollen af de udvidede administratorrettigheder. Rigsrevisionen vil særligt fremhæve, at institutionerne ikke i tilstrækkelig grad har begrænset tildelingen af disse rettigheder. Desuden har ingen af institutionerne skiftet ikke-personlige passwords årligt, og størstedelen af de pågældende passwords er op til 7 år gamle. Enkelte passwords er ikke blevet skiftet siden slutningen af 1990'erne.

Undersøgelsen viser også, at der er en række væsentlige mangler i institutionernes logning af anvendelsen af de udvidede administratorrettigheder. Fx har 4 institutioner ikke sikret funktionsadskillelse i adgangen til logfilerne, hvilket gør det muligt at slette sine spor i loggen. Desuden gennemgår 5 institutioner ikke logfilerne regelmæssigt. Det hæmmer muligheden for at opdage og opklare misbrug af de udvidede administratorrettigheder og it-sikkerhedsbrud.

Rigsrevisionen finder i lyset af risikobilledet vedrørende it-sikkerhed i staten, at institutionerne bør forbedre deres styring, kontrol og logning af de udvidede administratorrettigheder for at modvirke misbrug og kompromittering af it-systemer og data, der styres i AD. Institutionerne bør desuden jævnligt tage aktivt stilling til tilstrækkeligheden af deres styring, kontrol og logning af de udvidede administratorrettigheder, da risikobilledet ændrer sig løbende.

Rigsrevisionen vurderer, at flere af de konstaterede mangler i styringen, kontrollen og logningen af de udvidede administratorrettigheder er forholdsvist lette at rette op på, mens andre er mere omfattende og omkostningsfulde. Det er derfor Rigsrevisionens vurdering, at der er behov for ledelsesmæssig fokus og prioritering for at rette op på de konstaterede forhold.

Institutionerne har oplyst, at de har forskellige kompenserende foranstaltninger, og at de, siden undersøgelsen blev gennemført, har planlagt, igangsat og gennemført tiltag, der retter op på en række af de konstaterede mangler.

1.2. Baggrund

11. Rigsrevisionen har tidligere udarbejdet en beretning om forebyggelse af hackerangreb og en beretning om statens behandling af fortrolige oplysninger.

Denne beretning handler om beskyttelse af adgangen til it-systemer og data via de udvidede administratorrettigheder med henblik på at undgå internt og eksternt misbrug af rettighederne og uberettiget adgang til it-systemer og data.

12. De udvidede administratorrettigheder knytter sig i denne undersøgelse dels til betroede it-medarbejdere, der skal anvende deres eget personlige password for at anvende rettighederne og tilgå it-systemer og data, dels til såkaldte system- og servicekonti, der er brugeruafhængige og derfor ikke er personhenførbare, jf. boks 1.

BOKS 1. SYSTEM- OG SERVICEKONTI

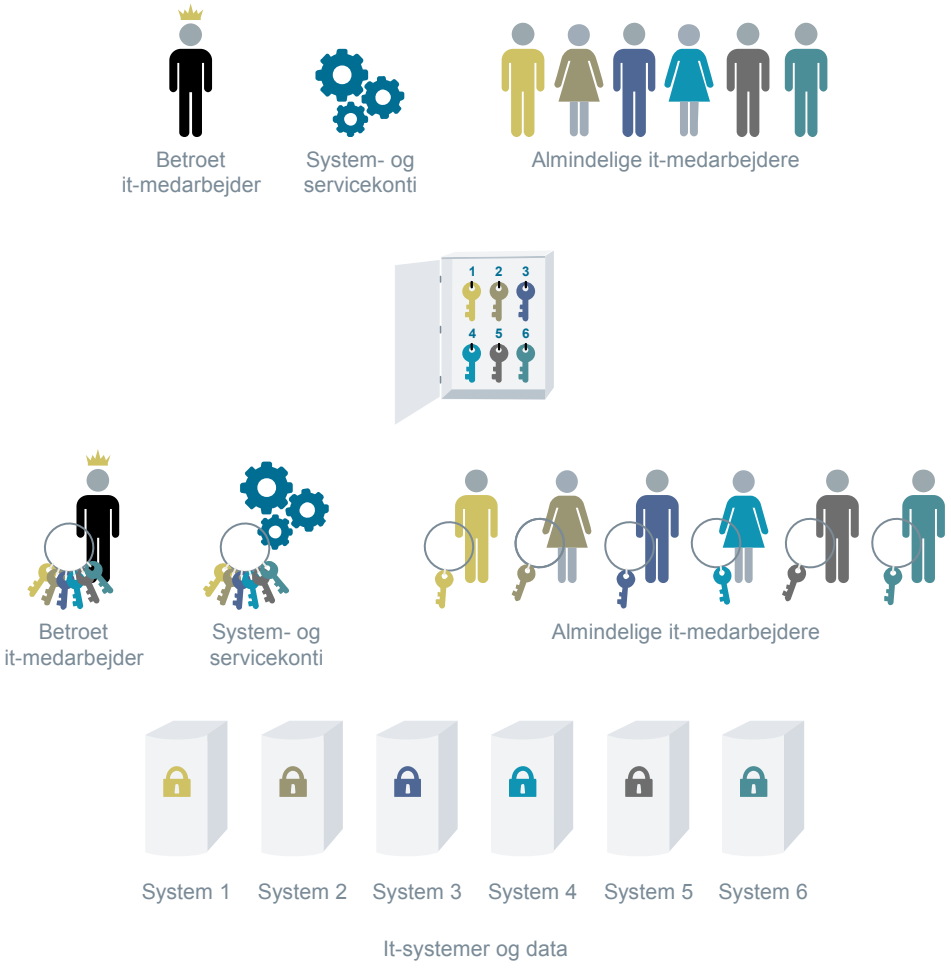
System- og servicekonti anvendes bl.a. til automatiserede kørsler i it-driften. Det kan fx være periodiske overførsler af store mængder data, backupkørsler og overvågning af it-driften.

System- og servicekonti har tilknyttet nogle rettigheder, som bestemmer, hvad de kan bruges til. De system- og servicekonti, der er omfattet af undersøgelsen, har udvidede administratorrettigheder.

System- og servicekonti er brugeruafhængige. Hver system- og servicekonto har ét password, som betroede it-medarbejdere har kendskab til. System- og servicekonti anvendes dermed ikke med personlige passwords. Al anvendelse af system- og servicekonti, herunder misbrug, er derfor ikke personhenførbar.

13. AD er en helt central og kritisk del af institutionernes it-infrastruktur. Her styres adgang og rettigheder til en række af institutionernes it-systemer og data, jf. figur 1.

Figur 1. Styring og kontrol af adgang og rettigheder til it-systemerne og data i AD



Kilde: Rigsrevisionen.

Det fremgår af figur 1, at AD helt forenklet kan ses som et nøgleskab med nøgler, der giver adgang og rettigheder til institutionens it-systemer og data, som styres i AD. Almindelige it-medarbejdere får kun adgang (nøgle) til specifikke it-systemer og data. Betroede it-medarbejdere og system- og servicekonti, der får tildelt udvidede administratorrettigheder i AD, har i kraft af disse rettigheder adgang (nøgler) til alle institutionens it-systemer og data, som styres i AD.

14. Kompromittering af AD kan også føre til kompromittering af it-systemer og data i institutionens øvrige it-miljø, da AD kan udgøre grundlaget for autentificering (login), autorisation (rettighedstildeling) og sikkerhedspolitikker for tilkoblede systemer. Med uhindret adgang til AD kan en hacker tage kontrol over den del af it-miljøet, der styres i AD, og udgive sig for at være en hvilken som helst bruger (dvs. overtage vedkommendes brugeridentitet). Desuden vil hackeren i nogle tilfælde – afhængigt af institutionens systemopsætning – kunne skaffe sig adgang til andre af institutionens it-systemer og data. Det er derfor Rigsrevisionens opfattelse, at det må forventes, at statslige institutioner prioriterer sikkerhedsindsatsen meget højt i forhold til udvidede administratorrettigheder og AD.

15. Problemstillingen om styring, kontrol og logning af udvidede administratorrettigheder er aktuel, da det fremgår af "Efterretningsmæssig Risikovurdering 2014" fra Forsvarets Efterretningstjeneste, at danske myndigheder er truet af en omfattende og voksende spionage via internettet fra statsstøttede aktører. Kriminelle og politisk motiverede hackere udgør også en trussel, om end denne trussel er mindre. Den teknologiske udvikling gør, at risikoen for at blive hacket øges, og at risikobilledet ændrer sig løbende. Det stiller ifølge risikovurderingen store krav til sikkerhedsforanstaltningerne. Det fremgår samtidig af risikovurderingen fra 2013, at truslen fra ansatte, der ubevidst eller bevidst bryder sikkerheden på deres arbejdsplads, vokser. Sådanne sikkerhedsbrud kan fx betyde tyveri af data eller infektion med skadelig software (malware), som hackere kan udnytte. Det kan fx ske på grund af et svagt fokus på it-sikkerhed i institutionen eller som følge af en bevidst handling med det formål at stjæle eller lække data.

Malware *er en sammentrækning af de engelske ord malicious software. Malware er en fællesbetegnelse for ondsindede computerprogrammer, der gør skadelige eller uønskede handlinger på brugerens computer.*

16. Ifølge Center for Cybersikkerhed og it-sikkerhedsfirmaet FortConsult skal virksomheder og myndigheder i dag arbejde ud fra den antagelse, at de allerede – uden at der er synlige tegn på det – er blevet angrebet af en hacker og dermed kan have fået en hacker eller malware inden for murene, der i ubemærkethed forsøger at tiltvinge sig adgang til kritiske it-systemer og data, fx ved at overtage en medarbejders udvidede administratorrettigheder. Institutionerne bør derfor indrette deres it-sikkerhed derefter, så de kan imødegå disse trusler.

Center for Cybersikkerhed *er en del af Forsvarets Efterretningstjeneste under Forsvarsministeriet.*

1.3. Revisionskriterier, metode og afgrænsning

Revisionskriterier

17. Informationssikkerhedsstandarden ISO 27001 er udarbejdet som et værktøj til ledelse af informationssikkerhed, som de statslige institutioner har skullet følge fra januar 2014, og som de skal have færdigimplementeret primo 2016. Standarden er overordnet og giver ikke konkrete it-sikkerhedsmæssige anvisninger, fx til et minimum for antallet af karakterer for administratorpasswords eller et maksimalt antal it-medarbejdere med udvidede administratorrettigheder. Der er således ikke centralt udmeldte konkrete standarder og krav.

Microsoft *er producenten af AD, som beretningen fokuserer på. Microsoft har udarbejdet en række anbefalinger, der medvirker til en sikker anvendelse af AD.*

SANS Institute *er et amerikansk privat forsknings- og uddannelsesinstitut, som arbejder med en lang række offentlige og private aktører. SANS Institute har udarbejdet en liste med vigtige fokusområder til brug for it-sikkerhedskontroller (SANS CSC – Critical Security Controls).*

Derfor har vi til brug for undersøgelsen opstillet mere konkrete revisionskriterier. Vi har taget udgangspunkt i de anbefalinger, som producenten af AD (dvs. Microsoft) har formuleret, og øvrige anerkendte internationale anbefalinger formuleret af branchen (fx SANS Institute). Nogle af revisionskriterierne er desuden baseret på logvejledningen fra Center for Cybersikkerhed.

Anbefalingerne, som revisionskriterierne har afsæt i, beskriver, hvad en institution bør gøre for at styre, kontrollere og logge de udvidede administratorrettigheder (god it-sikkerhedspraksis). Anbefalingerne er anerkendte og offentligt tilgængelige. Efter Rigsrevisionens opfattelse bør de ansvarlige i institutionerne for styring, kontrol og logning af udvidede administratorrettigheder derfor kende disse anbefalinger og anvende dem i overvejelserne om, hvordan institutionen i praksis styrer, kontrollerer og logger de udvidede administratorrettigheder på en tilstrækkelig måde.

Vi har desuden defineret, hvad der skal til, for at et revisionskriterium er opfyldt, delvist opfyldt eller ikke opfyldt (målepunkter). Vi har fx fastsat et minimum for antallet af karakterer for administratorpasswords og en maksimal grænse for antal it-medarbejdere med udvidede administratorrettigheder. Vi har baseret definitionen af målepunkter på de samme anerkendte anbefalinger og på vores erfaringer fra it-revisionen generelt. Målepunkterne er således efter Rigsrevisionens opfattelse et udtryk for god praksis på området.

18. Vi har drøftet revisionskriterier og målepunkter med Center for Cybersikkerhed og it-sikkerhedsfirmaet FortConsult for at kvalificere dem yderligere. Revisionskriterierne og målepunkterne fremgår af bilag 1.

19. Rigsrevisionen understreger, at revisionskriterierne/målepunkterne og de anbefalinger, de har afsæt i, ikke er statiske. Da risikobilledet ændrer sig løbende, vil anbefalinger til god praksis også ændre sig. Opfyldelse af revisionskriterierne er dermed ikke nødvendigvis ensbetydende med et tilstrækkeligt it-sikkerhedsniveau fremover.

20. De udvalgte institutioner har forskellige risikobilleder og forskellige opsætninger af AD. Institutionernes konkrete tekniske løsninger vil derfor alt andet lige afspejle disse forskellige rammevilkår. Det er dog Rigsrevisionens opfattelse, at de opstillede revisionskriterier og målepunkter kan anvendes på tværs af de 6 institutioner.

Metode

21. Undersøgelsen er baseret på 6 it-revisioner, som Rigsrevisionen har udført i perioden januar-juni 2015. Undersøgelsen har bestået af revisionsbesøg hos hver institution og opfølgende møder. For at sikre sammenlignelighed på tværs af institutionerne har vi ved de 6 it-revisioner undersøgt, om institutionerne opfylder de samme revisionskriterier, jf. bilag 1. Vores dokumentation bygger primært på kopier af skærmbilleder fra systemgennemgangen og dataudtræk fra AD. Vi har også indhentet og gennemgået relevant skriftligt materiale fra institutionerne.

Herudover har vi været i dialog med Center for Cybersikkerhed og gjort brug af konsulentbistand fra it-sikkerhedsfirmaet FortConsult for at kvalificere undersøgelsen yderligere.

Da resultaterne som nævnt er anonymiseret, benævnes institutionerne med numre i tabellerne i kap. 2. Desuden varierer institutionernes numre på tværs af tabellerne. Beretningen kæder derfor ikke de enkelte institutioner og deres konkrete resultater sammen og viser hverken de enkelte resultater eller det samlede billede for hver institution.

22. Revisionen er udført i overensstemmelse med god offentlig revisionsskik, jf. boks 2.

BOKS 2. GOD OFFENTLIG REVISIONSSKIK

God offentlig revisionsskik er baseret på de grundlæggende revisionsprincipper i rigsrevisionernes internationale standarder (ISSAI 100-999).

Afgrænsning

23. Beretningen tegner et øjebliksbillede af, hvordan de 6 institutioner på dagen for it-revisionsbesøget styrede, kontrollerede og loggede de udvidede administratorrettigheder, der giver adgang til it-systemer og data, som understøtter samfundsvigtige opgaver.

Institutionerne har efterfølgende gjort opmærksom på, at de har planlagt, igangsat og gennemført flere initiativer, der forbedrer en række af de forhold, som Rigsrevisionen konstaterede i forbindelse med it-revisionen, og som fremgår af beretningen.

24. De undersøgte institutioner varetager selv driften af en del af deres egne væsentlige it-systemer. Undersøgelsen omfatter det it-miljø, som institutionerne selv varetager driften af.

Beretningen handler om institutionernes styring, kontrol og logning af de udvidede administratorrettigheder i AD og ikke om institutionernes konkrete it-systemer.

25. Beretningen omfatter 16 revisionskriterier, som er en del af en større it-revision. Rigsrevisionen anser de 16 kriterier som væsentlige ud fra en it-sikkerhedsmæssig vurdering.

26. Bilag 2 indeholder en ordliste, der forklarer udvalgte ord og begreber.

2. Styring, kontrol og logning af udvidede administratorrettigheder

2.1. Styring og kontrol af betroede it-medarbejderes udvidede administratorrettigheder

27. Vi har undersøgt, hvordan de statslige institutioner har styret og kontrolleret de udvidede administratorrettigheder, der knytter sig til konkrete betroede it-medarbejdere, jf. tabel 1.

Tabel 1. Styring og kontrol af betroede it-medarbejderes udvidede administratorrettigheder

	Institution 1	Institution 2	Institution 3	Institution 4	Institution 5	Institution 6
Institutionen har et begrænset antal medarbejdere, der permanent har udvidede administratorrettigheder.	🟡	🔴	🔴	🔴	🔴	🔴
Institutionen har implementeret en regelmæssig kontrol af udvidede administratorrettigheder.	🟢	🟡	🔴	🟢	🔴	🟢
Institutionen har implementeret en procedure, der sikrer, at udvidede administratorrettigheder inddrages ved fratrædelse.	🟢	🟢	🟢	🟢	🟢	🟢
Institutionen har sikret, at personlige administratorpasswords følger god praksis (har en længde på mindst 9 karakterer, er komplekse, fx små og store bogstaver og tal, og skiftes inden 90 dage).	🟡	🟡	🟡	🟡	🔴	🟡
Institutionen har sikret, at medarbejdere med udvidede administratorrettigheder ikke kan tilgå internettet, når de er logget på med udvidede administratorrettigheder.	🟡	🟡	🔴	🟡	🟡	🟢

🔴 Ikke opfyldt.
🟡 Delvist opfyldt.
🟢 Opfyldt.

Kilde: Rigsrevisionen.

Nedenfor følger en uddybning af resultaterne, som fremgår af tabel 1.

Begrænsning af antal betroede it-medarbejdere med udvidede administratorrettigheder
28. Da de udvidede administratorrettigheder giver omfattende adgang og beføjelser til it-systemer og data, bør institutionerne ud fra et it-sikkerhedshensyn begrænse antallet af it-medarbejdere med udvidede administratorrettigheder, så kun ganske få betroede it-medarbejdere har disse rettigheder permanent og/eller kun får dem tildelt, når det er nødvendigt. Jo flere it-medarbejdere, der har permanent udvidede administratorrettigheder, desto større er risikoen for misbrug af rettighederne alt andet lige.

Derfor har Rigsrevisionen ud fra et it-sikkerhedshensyn undersøgt, om institutionerne har et meget begrænset antal (under 5) betroede it-medarbejdere med permanent udvidede administratorrettigheder. Institutionerne kan dog i deres risikovurderinger have taget ledelsesmæssigt stilling til antallet af it-medarbejdere med udvidede administratorrettigheder og accepteret et højere antal ud fra en afvejning af driftshensyn og risikovillighed. Rigsrevisionen har ikke undersøgt dette, men har alene set på antallet af betroede it-medarbejdere med udvidede administratorrettigheder ud fra et it-sikkerhedshensyn.

29. Det fremgår af tabel 1, at ingen af de 6 institutioner har opfyldt kriteriet om at have et begrænset antal betroede it-medarbejdere, der permanent har udvidede administratorrettigheder. Der er dog stor variation i antallet heraf på tværs af de 6 institutioner, da de har mellem 8 og 151 it-medarbejdere, som permanent har fået tildelt disse rettigheder.

Det er på baggrund af undersøgelsen Rigsrevisionens opfattelse, at institutionernes størrelse ikke har betydning for antallet af it-medarbejdere, som permanent har udvidede administratorrettigheder.

Regelmæssig kontrol med udvidede administratorrettigheder
30. Institutionerne bør sikre, at betroede it-medarbejdere ikke har rettigheder og adgang til flere it-systemer og data, end de har et arbejdsbetinget behov for. Når de udvidede administratorrettigheder ikke bruges mere, bør de inddrages. Institutionerne bør derfor foretage regelmæssig dokumenteret brugerrettighedskontrol af de tildelte udvidede administratorrettigheder mindst én gang om året.

31. Det fremgår af tabel 1, at 3 ud af de 6 institutioner foretager en regelmæssig og dokumenteret brugerrettighedskontrol mindst én gang om året. 2 af disse institutioner har automatiserede kontroller, hvilket letter processen.

Én af de øvrige 3 institutioner kan sandsynliggøre, men ikke dokumentere, at institutionen har foretaget brugerrettighedskontrol mindst én gang om året. 2 ud af de 3 institutioner har ikke foretaget brugerrettighedskontrol mindst én gang om året. De 2 institutioner har henholdsvis 39 og 59 betroede it-medarbejdere med udvidede administratorrettigheder. Det høje antal øger vigtigheden af at føre kontrol med, om der er it-medarbejdere med udvidede administratorrettigheder, der ikke har et arbejdsbetinget behov for de tildelte rettigheder.

Inddragelse af udvidede administratorrettigheder ved fratrædelse
32. Institutionerne bør have implementeret en procedure, der sikrer, at de udvidede administratorrettigheder altid inddrages/deaktiveres, umiddelbart efter at betroede it-medarbejdere fratræder deres stilling i institutionen, så forhenværende it-medarbejdere ikke kan få adgang til institutionens it-systemer og data.

33. Det fremgår af tabel 1, at alle 6 institutioner har implementeret en procedure, der sikrer, at udvidede administratorrettigheder inddrages ved fratrædelse.

Systemunderstøttelse af krav til god praksis for passwords

Systemunderstøttelse *er en regel i AD, der ikke kan afviges. Hvis institutionen fx har implementeret systemunderstøttelse af en passwordlængde på mindst 8 karakterer, er det ikke muligt at formulere passwords på færre karakterer.*

34. Da de udvidede administratorrettigheder giver omfattende adgang og beføjelser til it-systemer og data, bør institutionerne ved hjælp af systemunderstøttelse sikre, at passwords til anvendelse af disse rettigheder følger god praksis for antal karakterer, kompleksitet og regelmæssige skift. På den måde kan institutionerne mindske risikoen for, at passwords brydes, og uvedkommende personer derved kan tildele sig rettigheder og tiltvinge sig adgang til it-systemer og data. Administratorpasswords bør derfor have en længde på mindst 9 karakterer, være komplekse (fx små og store bogstaver og tal) og skiftes inden 90 dage.

Komplekse passwords *indeholder fx både små og store bogstaver og tal.*

Der findes i dag en række værktøjer på internettet til at bryde passwords. Antallet af karakterer i passwords har stor betydning for, hvor lang tid det tager at bryde et password. Derudover er det sværere at bryde komplekse passwords. Endelig reducerer hyppige skift af passwords risikoen for, at de bliver brudt, da der er kortere tid til rådighed til at bryde dem.

35. Det fremgår af tabel 1, at 5 ud af de 6 institutioner delvist systemunderstøtter god praksis for administratorpasswords. Disse 5 institutioner har komplekse passwords og skifter dem inden 90 dage, men deres systemunderstøttelse tillader administratorpasswords på ned til 8 karakterer, som er anbefalingen for passwords til almindelige brugere. De har således ikke stillet skærpede krav til antallet af karakterer for passwords til de udvidede administratorrettigheder, dvs. krav om mindst 9 karakterer.

Den sidste institution systemunderstøtter ikke god praksis for administratorpasswords. Institutionen skifter dem inden 90 dage, men institutionens systemunderstøttelse tillader administratorpasswords på ned til kun 6 karakterer og passwords, der ikke er komplekse. Institutionen tillader dermed svage passwords, som er lette at bryde.

Adgang til internettet med udvidede administratorrettigheder

36. I dag sker mange hackerangreb via hjemmesider, der er inficeret med malware, som spreder sig til de besøgende på hjemmesiden. Hvis en betroet it-medarbejder er logget på med sine udvidede administratorrettigheder og tilgår en inficeret hjemmeside, kan malware eller hackere overtage rettighederne og få adgang til institutionens it-systemer og data.

Derfor bør institutionerne sikre, at betroede it-medarbejdere ikke kan tilgå internettet, når de er logget på med de udvidede administratorrettigheder. Som hovedregel er der ingen grund til, at de kan tilgå internettet med disse rettigheder.

37. Det fremgår af tabel 1, at én af de 6 institutioner har sikret, at betroede it-medarbejdere ikke kan tilgå internettet med udvidede administratorrettigheder. De øvrige 5 institutioner har begrænset adgangen til internettet for it-medarbejdere, der er logget på med udvidede administratorrettigheder.

Segmentering af netværk *betyder, at institutionen har opdelt netværket i afgrænsede områder. Det medvirker fx til at sikre, at hackerangreb og malware ikke kan sprede sig til alle it-systemer og data, men kun rammer en begrænset del af netværket.*

Én af de 5 institutioner, der har begrænset adgangen til internettet, har dog ikke segmenteret sit netværk. Derfor er risikoen større, hvis der fx kommer malware ind i institutionens it-miljø i forbindelse med, at betroede it-medarbejdere tilgår internettet, når de er logget på med udvidede administratorrettigheder. Rigsrevisionen anser dette som en væsentlig mangel, og institutionen opfylder derfor ikke kriteriet.

Resultater

38. Undersøgelsen viser, at der generelt er flere væsentlige mangler i institutionernes styring og kontrol af betroede it-medarbejderes udvidede administratorrettigheder, som giver adgang til og kontrol over institutionernes it-systemer og data, der styres i AD.

Rigsrevisionen vurderer, at manglerne øger risikoen for misbrug og uretmæssig adgang til institutionernes it-systemer og data, der styres i AD.

39. Rigsrevisionen vurderer, at alle de konstaterede mangler som udgangspunkt er forholdsvist lette at rette op på. Dog kan det i nogle tilfælde være mere tidskrævende og omkostningsfuldt at rette op på de pågældende forhold på grund af ældre teknologi.

2.2. Styring og kontrol af udvidede administratorrettigheder for system- og servicekonti

40. Vi har undersøgt, hvordan de statslige institutioner har styret og kontrolleret de udvidede administratorrettigheder, der knytter sig til system- og servicekonti, som er brugeruafhængige og derfor ikke er personhenførbare, jf. tabel 2.

Tabel 2. Styring og kontrol med udvidede administratorrettigheder for system- og servicekonti

	Institution 1	Institution 2	Institution 3	Institution 4	Institution 5	Institution 6
Institutionen har begrænset antallet af system- og servicekonti med udvidede administratorrettigheder.	🔴	🔴	🔴	🔴	🟢	🟡
Institutionen har sikret, at system- og servicekonti med udvidede administratorrettigheder ikke kan anvendes til at logge på lokalt, dvs. at de ikke kan tilgå netværket fra en hvilken som helst arbejdsstation eller server i institutionen.	🔴	🟢	🔴	🔴	🟢	🔴
Institutionen har sikret, at passwords til system- og servicekonti bliver skiftet mindst én gang om året.	🔴	🔴	🔴	🔴	🔴	🔴
Institutionen har sikret, at passwords til system- og servicekonti altid skiftes, når betroede it-medarbejdere fratræder.	🔴	🔴	🔴	🔴	🔴	🔴
Institutionen har sikret, at passwords til system- og servicekonti er komplekse (fx små og store bogstaver og tal) og på mindst 15 karakterer.	🟡	🟡	🔴	🔴	🟡	🟡

🔴 Ikke opfyldt.
🟡 Delvist opfyldt.
🟢 Opfyldt.

Kilde: Rigsrevisionen.

Nedenfor følger en uddybning af resultaterne, som fremgår af tabel 2.

Begrænsning af antallet af udvidede administratorrettigheder

41. System- og servicekonti med udvidede administratorrettigheder giver samme omfattende adgang og beføjelser til it-systemer og data, som de udvidede administratorrettigheder, der knytter sig til betroede it-medarbejdere. Derfor bør institutionerne ud fra et it-sikkerhedshensyn begrænse antallet af system- og servicekonti med disse rettigheder til højst 5, og som udgangspunkt bør de ikke have udvidede administratorrettigheder.

42. Det fremgår af tabel 2, at kun én af de 6 institutioner har begrænset antallet af system- og servicekonti med udvidede administratorrettigheder, da denne institution kun har 4. De øvrige 5 institutioner har mellem 8 og 44 system- og servicekonti med udvidede administratorrettigheder og opfylder derfor ikke kriteriet.

Nogle af institutionerne har oplyst, at de har system- og servicekonti med udvidede administratorrettigheder på grund af ældre teknologi, som kræver disse rettigheder for at fungere korrekt.

Rigsrevisionen finder, at institutionerne i stedet for at acceptere et reduceret sikkerhedsniveau bør overveje at udskifte eller opgradere teknologien.

Sikring af, at system- og servicekonti med udvidede administratorrettigheder ikke kan logge på lokalt

43. I de tilfælde, hvor det er nødvendigt, at system- og servicekonti har udvidede administratorrettigheder (fx på grund af ældre teknologi), bør institutionerne sikre, at disse konti kun kan anvendes til deres specifikke formål, dvs. kun kan logge på de relevante servere i it-miljøet. Institutionerne bør derfor via "regler" i AD have sikret, at system- og servicekonti med udvidede administratorrettigheder ikke kan anvendes til at logge på lokalt, fx på andre computere og andre servere i it-miljøet.

44. Det fremgår af tabel 2, at 2 ud af de 6 institutioner har sikret, at system- og servicekonti med udvidede administratorrettigheder ikke kan anvendes til at logge på lokalt, fx på andre computere og andre servere i it-miljøet.

De øvrige 4 institutioner har ingen "regler", som forhindrer dette. Det øger risikoen for, at de udvidede administratorrettigheder kan blive misbrugt, uden at det efterfølgende kan opklares, hvem der har gjort det, da rettighederne ikke er personhenførbare.

Skift af passwords til system- og servicekonti mindst én gang om året

45. Institutionerne bør sikre, at passwords til system- og servicekonti skiftes mindst én gang om året. Det reducerer risikoen for, at passwords bliver brudt, da den, der forsøger at bryde passwordet, dermed har kortere tid til rådighed.

46. Det fremgår af tabel 2, at ingen af de 6 institutioner årligt har skiftet de passwords, der giver adgang til system- og servicekonti med udvidede administratorrettigheder. Størstedelen af disse passwords er mellem 2 og 7 år gamle. 3 af institutionerne har enkelte passwords, der ikke er skiftet siden slutningen af 1990'erne.

Flere af institutionerne har oplyst, at de ikke har skiftet passwords til system- og servicekonti, da de forventer, at det kan indebære en risiko for alvorlige driftsforstyrrelser i it-systemer, der understøtter samfundsvigtige opgaver, dvs. at it-systemerne i større eller mindre grad ikke virker.

47. Det er Rigsrevisionens opfattelse, at manglende skift af passwords til system- og servicekonti med udvidede administratorrettigheder er forbundet med væsentlige it-sikkerhedsmæssige risici. Rigsrevisionen finder derfor, at institutionerne bør analysere og vurdere risikoen ved henholdsvis at skifte og ikke skifte passwords.

Skift af passwords til system- og servicekonti, når betroede it-medarbejdere fratræder

Andre personer kan fx få fat i passwords, som tidligere it-medarbejdere er i besiddelse af, ved hjælp af afpresning, bedrag (social engineering) eller hacking af en tidligere medarbejders private mailkonto, som ved en fejl eller af uforsigtighed kan indeholde oplysninger om passwords.

48. Institutionerne bør sikre, at passwords til system- og servicekonti med udvidede administratorrettigheder altid skiftes, når betroede it-medarbejdere med kendskab til disse passwords fratræder deres stilling. Hvis forhenværende it-medarbejdere er i besiddelse af disse passwords, er der risiko for, at personer uden for institutionen kan få adgang til institutionens it-systemer og data. Det kan være de tidligere it-medarbejdere selv eller andre personer, der får fat i de pågældende passwords via en tidligere medarbejder.

49. Det fremgår af tabel 2, at ingen af de 6 institutioner har skiftet passwords til system- og servicekonti, når betroede it-medarbejdere med kendskab til passwordet er fratrådt.

Sikring af, at passwords til system- og servicekonti er komplekse og lange
50. Institutionerne bør sikre, at passwords til system- og servicekonti er komplekse (fx små og store bogstaver og tal) og på mindst 15 karakterer for at reducere risikoen for, at de bliver brudt. Passwords for system- og servicekonti bør have flere karakterer end de personlige administratorpasswords, da de skiftes sjældnere end personlige administratorpasswords.

Det fremgår af tabel 2, at ingen af de 6 institutioner fuldt ud opfylder kriteriet om tilstrækkeligt lange og komplekse passwords. Det gør det lettere at bryde dem og kan dermed give mulighed for at få adgang til institutionernes it-systemer og data.

Resultater
51. Undersøgelsen viser, at der generelt er en række væsentlige mangler i styringen og kontrollen med system- og servicekonti med udvidede administratorrettigheder.

52. Rigsrevisionen vurderer, at manglerne i styringen og kontrollen med system- og servicekonti med udvidede administratorrettigheder øger risikoen for misbrug og uretmæssig adgang til institutionernes it-systemer og data, der styres i AD. Da system- og servicekonti ikke er personhenførbare, er det vanskeligt for institutionerne at opdage og/eller opklare et eventuelt misbrug af it-systemer og data, hvilket efter Rigsrevisionens opfattelse er en skærpende omstændighed i forhold til de konstaterede mangler.

53. Rigsrevisionen vurderer, at én af de konstaterede mangler er forholdsvist let at rette op på. Det gælder opsætning af regler i AD, der hindrer, at system- og servicekonti med udvidede administratorrettigheder kan logge på lokalt.

2.3. Sikring af logning af udvidede administratorrettigheder

54. Vi har undersøgt, hvordan de statslige institutioner har sikret logningen af anvendelsen af de udvidede administratorrettigheder med henblik på at opdage og opklare misbrug, jf. tabel 3.

Med det nuværende risikobillede kan statslige institutioner ikke forvente at kunne forhindre alle angreb. Derfor er det vigtigt, at institutionerne er i stand til at opdage sikkerhedshændelser hurtigst muligt, hvilket logning bidrager til.

*En **sikkerhedshændelse** er en uventet hændelse i it-miljøet, der indikerer, at der er eller kan være noget galt.*

Da de udvidede administratorrettigheder som nævnt giver det højeste niveau af rettigheder og adgang til institutionens it-systemer og data, der styres i AD, er det særligt vigtigt, at institutionerne sikrer en tilstrækkelig logning af anvendelsen af disse rettigheder med henblik på at kunne opdage og opklare misbrug af disse rettigheder og sikkerhedshændelser.

Tabel 3. Logning af udvidede administratorrettigheder

	Institution 1	Institution 2	Institution 3	Institution 4	Institution 5	Institution 6
Institutionen har sikret, at logning i AD følger god praksis (logning af validering af brugere, administration af brugerkonti, sikkerhedsgruppernes tildeling af rettigheder, ændring af regler i AD, låsning af konti ved mislykkede adgangsforsøg mv.).	🟢	🟢	🟡	🟡	🟡	🟡
Institutionen har sikret, at alle computere, der får tildelt en IP-adresse, logges.	🔴	🟢	🟢	🟢	🟢	🟢
Institutionen har sikret, at administratorer, der logges, ikke har adgang til AD-loggen (funktionsadskillelse).	🔴	🟢	🔴	🔴	🔴	🟢
Institutionen har sikret, at AD-logfiler opbevares i en tilstrækkelig lang periode med henblik på opklaring af sikkerhedshændelser mv.	🟡	🟡	🟢	🟡	🟢	🟢
Institutionen har sikret, at AD-logfiler gennemgås regelmæssigt med henblik på at opdage uautoriserede ændringer eller uhensigtsmæssigheder i it-miljøet.	🔴	🟡	🔴	🔴	🟢	🔴
Institutionen har etableret en overvågning af anomalier i it-miljøet, dvs. en hændelsesovervågning, der kan koble informationer fra forskellige systemer sammen, så institutionen kan handle proaktivt på hændelser.	🔴	🔴	🔴	🔴	🔴	🔴

🔴 Ikke opfyldt.
🟡 Delvist opfyldt.
🟢 Opfyldt.

Kilde: Rigsrevisionen.

Nedenfor følger en uddybning af resultaterne, som fremgår af tabel 3.

Logningen i AD bør leve op til "Stronger Recommendation" i god praksis i henhold til Microsofts "Audit Policy Recommendations" og Center For Cybersikkerheds logvejledning.

Efterlevelse af god praksis for logning i AD

55. Logning i AD har primært 2 anvendelsesformål – dels alarmering om en given uventet hændelse, så institutionerne bliver klar over, at der er noget galt og kan gribe ind, dels efterfølgende opklaring af, hvad der er sket, og hvem der har gjort det.

Institutionerne bør sikre, at logningen i AD lever op til god praksis, så loggen er så anvendelig som muligt. Loggen bør give information om, at en person har logget sig på institutionens AD eller har forsøgt på det uden held. Loggen bør også give information om, hvad personen har foretaget sig i AD, fx om personen har anvendt de udvidede administratorrettigheder i AD til at ændre i sikkerhedsgrupper eller ændre i rettigheder og regler.

56. Det fremgår af tabel 3, at 2 ud af de 6 institutioner har sikret, at logning i AD følger god praksis. De øvrige 4 institutioner har mangler i deres logning, som kan begrænse muligheden for at opklare sikkerhedshændelser.

3 ud af de 4 institutioner foretager fx ikke logning af mislykkede adgangsforsøg, hvor de pågældende konti efterfølgende låses. Det gør det vanskeligt at opdage, hvis fx en hacker forsøger at overtage konti med udvidede administratorrettigheder.

3 ud af de 4 institutioner logger desuden ikke ændringer foretaget for sikkerhedsgrupper i AD. Det gør det vanskeligt at opdage og opklare, om nogen – og i så fald hvem – har tildelt sig selv eller andre udvidede administratorrettigheder i AD.

__Sikkerhedsgrupper__ er grupper i AD, hvorigennem institutionen tildeler og administrerer rettigheder til it-systemer og data.

Herudover foretager én af de 4 institutioner ikke logning af ændringer i regler i AD. Dermed kan regler i AD ændres, uden at institutionen opdager det. Fx kan en intern betroet it-medarbejder med udvidede administratorrettigheder eller en hacker ændre i logningsreglerne med det formål at sløre sine spor.

Logning af computere med IP-adresse

57. Institutionerne bør logge alle computere, der har fået tildelt en IP-adresse, så de til enhver tid kan se, hvilken IP-adresse en given computer har haft på et givent tidspunkt. Den information er vigtig i forbindelse med opklaring af sikkerhedshændelser.

En __IP-adresse__ er computerens "identitet" eller "afsenderadresse" på netværket. Ved hjælp af IP-adressen kan man identificere, hvilken computer der har udført en given handling på et givent tidspunkt.

58. Det fremgår af tabel 3, at 5 ud af de 6 institutioner logger computere, der får tildelt en IP-adresse. Den sidste institution logger også dette, men gemmer ikke logfilerne i mere end 7 dage. Det svækker muligheden for at anvende logfilerne til opklaring betydeligt. Derfor opfylder institutionen ikke kriteriet.

Funktionsadskillelse i adgang til AD-logfiler

59. Logfilerne er et vigtigt redskab til at opklare eventuelle sikkerhedshændelser. Hvis en person (enten en betroet it-medarbejder med udvidede administratorrettigheder eller en hacker, der har overtaget disse rettigheder) har misbrugt it-systemer eller data, vil vedkommende typisk forsøge at sløre sine spor i logfilerne. Institutionerne bør derfor sikre, at der er funktionsadskillelse i loggen af de udvidede administratorrettigheder, dvs. at udvidede administratorrettigheder ikke giver adgang til logfiler. Logfilerne bør hurtigst muligt overføres til et skrivebeskyttet program, som hverken tillader ændring eller sletning i logfilerne. Herved kan institutionen undgå, at der enten tilsigtet eller utilsigtet slettes eller ændres i logfilerne, hvilket kan forhindre eller forsinke opklaringen.

60. Det fremgår af tabel 3, at 2 ud af de 6 institutioner har sikret funktionsadskillelse i forhold til adgang til logfilerne. De 2 institutioner har valgt en løsning, hvor de gemmer en kopi af logfilerne og gemmer den uden for AD, så de betroede it-medarbejdere med udvidede administratorrettigheder ikke har adgang til loggen.

De øvrige 4 institutioner har ikke sikret funktionsadskillelse i adgangen til logfilerne. Dermed har betroede it-medarbejdere mulighed for at slette i loggen og derved slette deres spor – enten ved at anvende deres egne eller en system- og servicekontos udvidede administratorrettigheder. Ligeledes kan en hacker, som har overtaget disse rettigheder, slette i logfiler, hvilket vanskeliggør opklaring af sikkerhedshændelser.

Én af de 4 institutioner har en logningsløsning, hvor de betroede it-medarbejdere med udvidede administratorrettigheder eller en hacker, som har overtaget disse rettigheder, ikke blot kan slette i loggen, men også kan ændre i loggen og dermed plante falske spor.

Opbevaring af AD-logfiler

61. Institutionerne bør opbevare AD-logfilerne længe nok til, at de kan anvendes til at opklare eventuelle sikkerhedshændelser. Center for Cybersikkerhed har oplyst, at der for visse angrebstyper, fx APT-angreb, typisk går op til 18 måneder, fra sikkerhedshændelsen sker, til institutionen opdager det. Rigsrevisionen finder derfor, at institutionerne bør gemme AD-logfilerne i mere end 18 måneder.

__APT-angreb__ (Advanced Persistent Threat) betegner trusslen fra hackere, der forsøger at opnå uautoriseret adgang til en udvalgt myndighed eller et virksomhedsnetværk. Angrebet gennemføres som regel med spionage for øje og forberedes normalt grundigt. Hackerne bruger en bred vifte af angrebsmetoder til at forsøge at skaffe sig adgang, og når de først er inde, kan de operere skjult gennem længere tid, fx flere år.

Nogle af institutionerne har oplyst, at de er usikre på, om dette er i overensstemmelse med bestemmelsen i sikkerhedsbekendtgørelsen om logning. Rigsrevisionen har drøftet dette med Datatilsynet, jf. boks 3.

BOKS 3. OPBEVARING AF LOGFILER

Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger (persondataloven).

Logning, jf. persondatalovens § 41, stk. 3
Ifølge persondatalovens § 41, stk. 3, skal den dataansvarlige træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, og mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere.

Datatilsynet har oplyst, at det er den dataansvarlige myndighed, der i første omgang må vurdere og beslutte, om der som led i myndighedens tilvejebringelse af de fornødne sikkerhedsforanstaltninger er behov for AD-logning, og hvor længe det i givet fald er nødvendigt at opbevare AD-logfilerne.

Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsbekendtgørelsen).

Logning, jf. sikkerhedsbekendtgørelsens § 19, stk. 1
For visse behandlinger (behandlinger omfattet af anmeldelsespligten til Datatilsynet) kræves der imidlertid en særlig logning efter bestemmelsen i sikkerhedsbekendtgørelsens § 19, stk. 1. Det fremgår af bestemmelsen, at der skal foretages maskinel registrering (logning) af alle anvendelser af personoplysninger. Registreringen skal mindst indeholde oplysning om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium. Loggen skal opbevares i 6 måneder, hvorefter den skal slettes. Myndigheder med et særligt behov kan opbevare loggen i op til 5 år.

Datatilsynet har oplyst, at det er de enkelte myndigheder, der vurderer, om der er et særligt behov for at opbevare en sådan log, der dannes efter sikkerhedsbekendtgørelsens § 19, stk. 1, i længere tid end 6 måneder. Opbevaring af en sådan log i op til 5 år kræver således ikke forelæggelse for Datatilsynet.

På baggrund af oplysningerne fra Datatilsynet er det Rigsrevisionens opfattelse, at der ikke er noget til hinder for i den nævnte lovgivning, at institutionerne gemmer de nødvendige logfiler i mere end 18 måneder for at kunne opklare eventuelle sikkerhedshændelser.

62. Det fremgår af tabel 3, at 3 ud af de 6 institutioner gemmer deres logfiler i mere end 18 måneder. De øvrige 3 institutioner gemmer kun deres logfiler i 6-18 måneder. Herved er der en risiko for, at institutionerne ikke kan opklare sikkerhedshændelser, fordi de gemmer logfilerne i for kort tid.

Regelmæssig gennemgang af AD-logfiler

63. I lyset af det øgede risikobillede og i lyset af, at de udvidede administratorrettigheder giver omfattende adgang og beføjelser til it-systemer og data, bør institutionerne gennemgå AD-logfilerne regelmæssigt – enten via medarbejdere, der er uddannet i at gennemgå logfiler, eller via automatiserede overvågningssystemer. På den måde kan institutionerne opdage adfærd og hændelser i it-miljøet, der ikke er, som de bør eller plejer at være.

64. Det fremgår af tabel 3, at kun én af de 6 institutioner gennemgår logfilerne regelmæssigt. De øvrige 5 institutioner foretager ingen regelmæssig gennemgang af logfilerne. Det medfører en risiko for, at der kan ske misbrug af institutionernes it-systemer eller data, uden at institutionerne opdager det.

Én af disse 5 institutioner har dog opsat en række alarmkriterier, der automatisk udløser en alarm i it-sikkerhedsafdelingen. Det sker fx, hvis en betroet it-medarbejder med udvidede administratorrettigheder – eller en hacker, der har overtaget disse rettigheder – sletter i loggen eller tildeler sig selv større rettigheder i AD.

Overvågning af anomalier i it-miljøet

65. Anomalier er adfærd eller hændelser i it-miljøet, der ikke er, som de bør eller plejer at være. Anomalier kan derfor være tegn på hackerangreb eller andre sikkerhedsbrud. Institutionerne bør derfor overvåge anomalier i it-miljøet og fx opsætte alarmkriterier, så anomalier automatisk udløser en alarm i it-sikkerhedsafdelingen. Herved kan institutionerne tidligt opdage og begrænse hackerangreb eller andre sikkerhedsbrud. Boks 4 viser eksempler på anomalier i it-miljøet, som institutionerne kan overvåge.

BOKS 4. EKSEMPLER PÅ ANOMALIER I IT-MILJØET, SOM KAN INDGÅ I OVERVÅGNINGEN

Anomalier er atypiske hændelser eller atypisk adfærd i it-miljøet. Eksempler herpå kan være:

- at der logges på netværket med udvidede administratorrettigheder fra en IP-adresse i et andet land, samtidig med at den pågældende it-medarbejder er logget på netværket fra en IP-adresse i Danmark
- at en betroet it-medarbejder med udvidede administratorrettigheder logger på en server, som vedkommende aldrig har været logget på før, og/eller logger på i et tidsrum, hvor vedkommende normalt ikke er aktiv, fx om natten
- at en betroet it-medarbejder med udvidede administratorrettigheder logger på 8 forskellige computere inden for 10 sekunder
- at unormalt store mængder data uploades til en ekstern server, fx Dropbox eller Google Drive, søndag eftermiddag.

66. Det fremgår af tabel 3, at ingen af de 6 institutioner overvåger anomalier i it-miljøet. Manglende overvågning af anomalier kan betyde, at der fx kan ske ikke-godkendte ændringer i it-systemerne eller hos brugerne, som ikke bliver opdaget og standset i tide.

67. Nogle af institutionerne har gjort opmærksom på, at de ikke finder kriteriet om overvågning af anomalier rimeligt, fordi det ikke er almindelig praksis i dag, og fordi der ikke er udviklet systemer, der muliggør dette.

68. Rigsrevisionen noterer sig, at en række institutioner har oplyst, at de allerede har påbegyndt arbejdet med at anskaffe og implementere logningssystemer, der kan håndtere og analysere store mængder af logfiler, så de på sigt kan udføre automatiske kontroller, herunder overvåge anomalier. Rigsrevisionen anerkender, at det kræver en vis indsats at blive i stand til at overvåge anomalier, da det bl.a. forudsætter, at institutionerne definerer, hvad der er atypiske hændelser.

Det er Rigsrevisionens opfattelse, at det er et ambitiøst, men ikke urealistisk revisionskriterium. Rigsrevisionen anerkender, at overvågning af anomalier ikke er almindeligt udbredt i dag. I lyset af at institutionerne varetager samfundsvigtige opgaver, må det dog med rimelighed forventes, at institutionernes sikkerhedsmæssige foranstaltninger modsvarer det øgede risikobillede, som statslige institutioner ifølge risikovurderinger fra Forsvarets Efterretningstjeneste står over for. Ifølge en trusselsvurdering fra Center for Cybersikkerhed fra 2013 bør it-systemer og netværk kontinuerligt overvåges for at fastholde en acceptabel sikkerhed.

Resultater

69. Undersøgelsen viser, at der er variation på tværs af institutionerne, men at der generelt er flere mangler i de undersøgte institutioners logning af udvidede administratorrettigheder.

70. Rigsrevisionen vurderer, at manglerne i logningen hæmmer institutionernes mulighed for at opdage og opklare sikkerhedsbrud og misbrug af de udvidede administratorrettigheder. Rigsrevisionen vurderer, at flere af de konstaterede mangler er forholdsvist lette at rette op på. Det gælder fx sikring af, at logning i AD følger god praksis, og at logfilerne opbevares i en tilstrækkelig lang periode.

Rigsrevisionen, den 30. september 2015

Lone Strøm

/Mads Nyholm Jacobsen

Bilag 1. Metode

Undersøgelsens forløb og aktiviteter
Undersøgelsen, som beretningen bygger på, er baseret på it-revisioner hos 6 institutioner, som Rigsrevisionen har udført i perioden januar-juni 2015.

Som led i it-revisionerne har vi foretaget revisionsbesøg hos hver institution. Via gennemgangen af en række revisionskriterier har vi foretaget en systematisk gennemgang, primært af brugeradministrationssystemet Active Directory (AD), hos hver institution. Vi har dokumenteret resultaterne af gennemgangen i form af kopier af skærmbilleder og dataudtræk fra AD.

Ved at undersøge, om institutionerne har opfyldt de samme revisionskriterier, har vi sikret sammenlignelighed på tværs af institutionerne. Beretningen omfatter 16 revisionskriterier, som er en del af en større it-revision. Rigsrevisionen anser de 16 revisionskriterier som væsentlige ud fra en it-sikkerhedsmæssig vurdering.

Ud over revisionsbesøgene har vi afholdt supplerende møder med institutionerne i forbindelse med it-revisionen og i forbindelse med udarbejdelsen af beretningen.

Derudover har vi indhentet og gennemgået relevant skriftligt materiale fra institutionerne, fx risikovurderinger, systemoversigter og netværkstegninger.

Revisionskriterier og målepunkter
Der findes flere centralt udmeldte vejledninger og standarder, som handler om it-sikkerhed generelt, men ikke om opsætningen af AD og styring og kontrol af udvidede administratorrettigheder specifikt.

Det gælder fx den internationale informationssikkerhedsstandarden ISO 27001, som de statslige institutioner skulle følge fra januar 2014, og som de skal have færdigimplementeret primo 2016. ISO 27001 afløser den tidligere sikkerhedsstandard DS484. ISO 27001 skal ifølge Digitaliseringsstyrelsen bidrage til en enklere sikkerhedsstyring og stiller færre bindende krav til institutionerne.

Kontrolmålene og kontrollerne i ISO 27001 er ikke konkrete, men udgør en overordnet ramme. Fx fremgår det, at "tildeling og anvendelse af privilegerede adgangsrettigheder[1)] skal begrænses og styres", og at "systemer til administration af adgangskoder skal sikre adgangskoder med god kvalitet", uden at det er uddybet, hvad det indebærer.

Da der ikke er centralt udmeldte standarder og krav, har Rigsrevisionen opstillet mere konkrete revisionskriterier til brug for revisionen. Vi har taget udgangspunkt i de anbefalinger, som leverandøren af AD (dvs. Microsoft) har formuleret, og øvrige anerkendte internationale anbefalinger formuleret af branchen (fx SANS Institute). Nogle af revisionskriterierne er desuden baseret på logvejledningen fra Center for Cybersikkerhed.

Anbefalingerne, som revisionskriterierne har afsæt i, beskriver, hvad en institution bør gøre for at styre, kontrollere og logge de udvidede administratorrettigheder (god it-sikkerhedspraksis). Anbefalingerne er anerkendte og offentligt tilgængelige. Efter Rigsrevisionens opfattelse bør de ansvarlige i institutionerne for styring, kontrol og logning af udvidede administratorrettigheder derfor kende disse anbefalinger og anvende dem i overvejelserne om, hvordan institutionen i praksis styrer, kontrollerer og logger de udvidede administratorrettigheder på en tilstrækkelig måde.

[1)] Svarende til det, vi i beretningen betegner som udvidede administratorrettigheder.

Vi har desuden defineret, hvad der skal til, for at et revisionskriterium er opfyldt, delvist opfyldt eller ikke opfyldt (målepunkter). Vi har fx fastsat et minimum for antallet af karakterer for administratorpasswords og en maksimal grænse for antal it-medarbejdere med udvidede administratorrettigheder. Vi har baseret definitionen af målepunkter på de samme anerkendte anbefalinger og på vores erfaringer fra it-revisionen generelt. Målepunkterne er således efter Rigsrevisionens opfattelse et udtryk for god praksis på området.

Vi har drøftet revisionskriterier og målepunkter med Center for Cybersikkerhed og it-sikkerhedsfirmaet FortConsult for at kvalificere dem yderligere.

Med de opstillede revisionskriterier har vi undersøgt, hvordan institutionerne styrer, kontrollerer og logger de udvidede administratorrettigheder, da der efter Rigsrevisionens opfattelse er en væsentlig risiko forbundet med mangler heri.

Vi har således ikke undersøgt, om institutionerne opfylder ISO 27001, og om institutionerne har taget stilling til risici forbundet med den måde, de styrer, kontrollerer og logger de udvidede administratorrettigheder.

Oversigten nedenfor viser de revisionskriterier, som indgår i beretningen, og de tilhørende målepunkter.

Revisionskriterier	Målepunkter
Institutionen har et begrænset antal medarbejdere, der permanent har udvidede administratorrettigheder.	● Over 9 medarbejdere har permanent udvidede administratorrettigheder. ● 5-9 medarbejdere har permanent udvidede administratorrettigheder. ● Under 5 medarbejdere har permanent udvidede administratorrettigheder.
Institutionen har implementeret en regelmæssig kontrol af udvidede administratorrettigheder.	● Institutionen har ikke udført brugerrettighedskontrol mindst én gang om året. ● Institutionen kan sandsynliggøre, at de har foretaget brugerrettighedskontrol mindst én gang om året, men kan ikke dokumentere det. ● Institutionen har foretaget regelmæssig dokumenteret brugerrettighedskontrol mindst én gang om året.
Institutionen har implementeret en procedure, der sikrer, at udvidede administratorrettigheder inddrages ved fratrædelse.	● Udvidede administratorrettigheder inddrages/deaktiveres ikke ved fratrædelse. ● Udvidede administratorrettigheder inddrages/deaktiveres i forbindelse med brugerrettighedskontrol. ● Udvidede administratorrettigheder inddrages/deaktiveres altid umiddelbart efter fratrædelse.
Institutionen har sikret, at personlige administratorpasswords følger god praksis (har en længde på mindst 9 karakterer, er komplekse, fx små og store bogstaver og tal, og skiftes inden 90 dage).	● Passwords er på under 8 karakterer og komplekse eller er på mindst 8 karakterer og ikke komplekse eller skiftes sjældnere end 90 dage (skal være systemunderstøttet). ● Passwords er på 8 karakterer, er komplekse og skiftes inden 90 dage (skal være systemunderstøttet). ● Passwords er på mindst 9 karakterer, er komplekse og skiftes inden 90 dage (skal være systemunderstøttet).
Institutionen har sikret, at medarbejdere med udvidede administratorrettigheder ikke kan tilgå internettet, når de er logget på med udvidede administratorrettigheder.	● Medarbejdere med udvidede administratorrettigheder kan godt tilgå internettet, når de er logget på med disse rettigheder. ● Medarbejdere med udvidede administratorrettigheder kan i meget begrænset omfang tilgå internettet, når de er logget på med disse rettigheder. ● Medarbejdere med udvidede administratorrettigheder kan ikke tilgå internettet, når de er logget på med disse rettigheder.
Institutionen har begrænset antallet af system- og servicekonti med udvidede administratorrettigheder.	● Over 9 system- og servicekonti med udvidede administratorrettigheder. ● 6-9 system- og servicekonti med udvidede administratorrettigheder. ● 0-5 system- og servicekonti med udvidede administratorrettigheder.
Institutionen har sikret, at system- og servicekonti med udvidede administratorrettigheder ikke kan anvendes til at logge på lokalt, dvs. at de ikke kan tilgå netværket fra en hvilken som helst arbejdsstation eller server i institutionen.	● System- og servicekonti med udvidede administratorrettigheder kan logge på lokalt. ● Ingen system- og servicekonti med udvidede administratorrettigheder kan logge på lokalt.
Institutionen har sikret, at passwords til system- og servicekonti bliver skiftet mindst én gang om året.	● Passwords skiftes ikke mindst én gang om året. ● Passwords skiftes mindst én gang om året.
Institutionen har sikret, at passwords til system- og servicekonti altid skiftes, når betroede it-medarbejdere fratræder.	● Passwords skiftes ikke, når betroede it-medarbejdere med kendskab til passwords fratræder. ● Passwords skiftes nogle gange, når betroede it-medarbejdere med kendskab til passwords fratræder. ● Passwords skiftes altid, når betroede it-medarbejdere med kendskab til passwords fratræder.

Revisionskriterier	Målepunkter
Institutionen har sikret, at passwords til system- og servicekonti er komplekse (fx små og store bogstaver og tal) og på mindst 15 karakterer.	● Der er passwords på under 8 karakterer eller simple passwords. ● Alle passwords er på 8-14 karakterer og komplekse (fx små og store bogstaver og tal). ● Alle passwords er på mindst 15 karakterer og komplekse (fx små og store bogstaver og tal).
Institutionen har sikret, at logning i AD følger god praksis (logning af validering af brugere, administration af brugerkonti, sikkerhedsgruppernes tildeling af rettigheder, ændring af regler i AD, låsning af konti ved mislykkede adgangsforsøg mv.).	● Ingen logning i AD eller logning, der ikke lever op til "Windows Default" i god praksis, jf. Microsofts "Audit Policy Recommendations" og Center for Cybersikkerheds logvejledning. ● Logning i AD, der lever op til "Baseline Recommendation" i god praksis, jf. Microsofts "Audit Policy Recommendations" og Center for Cybersikkerheds logvejledning. ● Logning i AD, der lever op til "Stronger Recommendation" i god praksis, jf. Microsofts "Audit Policy Recommendations" og Center for Cybersikkerheds logvejledning.
Institutionen har sikret, at alle computere, der får tildelt en IP-adresse, logges.	● DHCP (Dynamic Host Configuration Protocol) logdata genereres ikke eller overskrives efter få dage. ● DHCP (Dynamic Host Configuration Protocol) logdata genereres, og der tages en daglig backup.
Institutionen har sikret, at administratorer, der logges, ikke har adgang til AD-loggen (funktionsadskillelse).	● Ingen funktionsadskillelse på loggen for administratorkonti. ● Funktionsadskillelse på loggen for administratorkonti.
Institutionen har sikret, at AD-logfiler opbevares i en tilstrækkelig lang periode med henblik på opklaring af sikkerhedshændelser mv.	● Backup af logfiler opbevares og kan genskabes i op til 6 måneder. ● Backup af logfiler opbevares og kan genskabes i 6-18 måneder. ● Backup af logfiler opbevares og kan genskabes i mere end 18 måneder.
Institutionen har sikret, at AD-logfiler gennemgås regelmæssigt med henblik på at opdage uautoriserede ændringer eller uhensigtsmæssigheder i it-miljøet.	● Ingen regelmæssig gennemgang eller overvågning af AD-logfiler. ● Delvis gennemgang eller overvågning af AD-logfiler. ● Regelmæssig og systematisk gennemgang og overvågning af AD-logfiler.
Institutionen har etableret en overvågning af anomalier i it-miljøet, dvs. en hændelsesovervågning, der kan koble informationer fra forskellige systemer sammen, så institutionen kan handle proaktivt på hændelser.	● Ingen overvågning af anomalier i it-miljøet. ● Delvis overvågning af anomalier i it-miljøet. ● Hele it-miljøet overvåges for anomalier.

Bilag 2. Ordliste

Active Directory (AD)	Et brugeradministrationssystem, hvori institutionen styrer og kontrollerer adgang og rettigheder til it-systemer og data.
Administratorpassword	Password, som en betroet it-medarbejder skal benytte, når vedkommende skal anvende sine udvidede administratorrettigheder.
APT-angreb (Advanced Persistent Threat)	Betegner truslen fra hackere, der forsøger at opnå uautoriseret adgang til en udvalgt myndighed eller et virksomhedsnetværk. Angrebet gennemføres som regel med spionage for øje og forberedes normalt grundigt. Hackerne bruger en bred vifte af angrebsmetoder til at forsøge at skaffe sig adgang, og når de først er inde, kan de operere skjult gennem længere tid, fx flere år.
Betroet it-medarbejder	It-medarbejder, der har udvidede administratorrettigheder.
God it-sikkerhedspraksis	Hvad en institution bør gøre for at styre, kontrollere og logge de udvidede administratorrettigheder med udgangspunkt i de anbefalinger, leverandøren af AD (dvs. Microsoft) har formuleret, øvrige anerkendte internationale anbefalinger formuleret af branchen (fx SANS Institute) og logvejledningen fra Center for Cybersikkerhed.
Hacker	Betegner i denne beretning en ukendt og uautoriseret person, der foretager en ulovlig handling ved i det skjulte at skaffe sig adgang til og/eller anvende andres it-systemer eller data. Formålet med hacking og de anvendte metoder afhænger af de personer eller organisationer, der står bag, dvs. om det er fremmede stater, kriminelle organisationer eller individer, som på egen hånd misbruger institutionens svagheder.
IP-adresse	Computerens "identitet" eller "afsenderadresse" på netværket. Ved hjælp af IP-adressen kan man identificere, hvilken computer der har udført en given handling på et givent tidspunkt.
ISO 27001	Den internationale informationssikkerhedsstandard, som de statslige institutioner skulle følge fra januar 2014, og som de skal have færdigimplementeret primo 2016. ISO 27001 afløser den tidligere sikkerhedsstandard DS484.
Logfiler/log	De filer, hvori institutionen gemmer registreringerne af oplysninger om anvendelse af og hændelser i institutionens it-systemer og data.
Logning	Registrering af oplysninger om anvendelse af og hændelser i institutionens it-systemer og data i en fil. Logning i AD af anvendelsen af de udvidede administratorrettigheder bør fx give information om, at en person har logget sig på institutionens it-systemer eller har forsøgt det uden held og om, hvad personen har anvendt de udvidede administratorrettigheder til.
Malware	En sammentrækning af de engelske ord malicious software. Malware er en fællesbetegnelse for ondsindede computerprogrammer, der gør skadelige eller uønskede handlinger på brugerens computer.
Misbrug og kompromittering af it-systemer og data	Indebærer, at en person uretmæssigt kan få adgang til en række af institutionens it-systemer og data. Der kan fx være tale om, at personen uretmæssigt afbryder eller ændrer datakørsler, eller at personen uretmæssigt ændrer, sletter eller læser/stjæler data.
Personhenførbar	Det er muligt at se, hvilken bruger der har foretaget en given handling i institutionens it-systemer.
Risikobillede	Risikoen for misbrug og kompromittering af it-systemer og data (både risikoen for hackerangreb, spionage og tyveri af data over internettet samt truslen fra ansatte, der ubevidst eller bevidst bryder sikkerheden på deres arbejdsplads).
Segmentering af netværk	Betyder, at institutionen har opdelt netværket i afgrænsede områder. Det medvirker fx til at sikre, at hackerangreb og malware ikke kan sprede sig til alle it-systemer og data, men kun rammer en begrænset del af netværket.

Sikkerhedsbrud	Betyder, at en intern eller en ekstern person forsætligt eller uforsætligt har foretaget en handling, der truer it-sikkerheden.
Sikkerhedsforanstaltninger	Skal bidrage til at forhindre eller opdage misbrug og kompromittering af it-systemer og data. Det er fx tekniske regler i it-systemerne, der kan forhindre uønskede handlinger.
Sikkerhedsgrupper	Grupper i AD, hvorigennem institutionen tildeler og administrerer rettigheder til it-systemer og data.
Sikkerhedshændelse	En uventet hændelse i it-miljøet, der indikerer, at der er eller kan være noget galt.
System- og servicekonti	Anvendes bl.a. til automatiserede kørsler i it-driften. Det kan fx være periodiske overførsler af store mængder data, backupkørsler og overvågning af it-driften. System- og servicekonti har tilknyttet nogle rettigheder, som bestemmer, hvad kontoen kan bruges til. De system- og servicekonti, der er omfattet af undersøgelsen, har udvidede administratorrettigheder. System- og servicekonti er brugeruafhængige. Hver system- og servicekonto har ét password, som betroede it-medarbejdere har kendskab til. System- og servicekonti anvendes dermed ikke med personlige passwords. Al anvendelse af system- og servicekonti, herunder misbrug, er derfor ikke personhenførbar.
Systemunderstøttelse	En regel i AD, der ikke kan afviges. Hvis institutionen fx har implementeret systemunderstøttelse af en passwordlængde på mindst 8 karakterer, er det ikke muligt at formulere passwords på færre karakterer.
Udvidede administrator-rettigheder	Det højeste niveau af rettigheder, adgang og kontrol over institutionens it-systemer og data, der styres i AD. Desuden kan de udvidede administratorrettigheder give mulighed for at omgå institutionens sikringsforanstaltninger. I nogle tilfælde kan de udvidede administratorrettigheder – afhængigt af institutionens systemopbygning – også give adgang til andre væsentlige it-systemer og data. Udvidede administratorrettigheder betegner i denne beretning de it-medarbejdere og/eller system- og servicekonti, der er medlem af ”Domain Admins-gruppen” i AD.