4/2017

STATSREVISORERNE
RIGSREVISIONEN

Rigsrevisionens beretning om

3 regioners beskyttelse af adgangen til it-systemer og sundhedsdata

afgivet til Folketinget med Statsrevisorernes bemærkninger

November 2017

4 /
2017

Beretning om 3 regioners beskyttelse af adgangen til it-systemer og sundhedsdata

Statsrevisorerne fremsender denne beretning med deres bemærkninger til Folketinget og vedkommende minister, jf. § 3 i lov om statsrevisorerne og § 18, stk. 1, i lov om revisionen af statens regnskaber m.m.

København 2017

Denne beretning til Folketinget skal behandles ifølge lov om revisionen af statens regnskaber, § 18:
Statsrevisorerne fremsender med deres eventuelle bemærkninger Rigsrevisionens beretning til Folketinget og vedkommende minister.
Sundhedsministeren afgiver en redegørelse til beretningen. Ministerens kommentarer til de indhentede udtalelser fra regionsrådene indgår i redegørelsen.
Rigsrevisor afgiver et notat med bemærkninger til ministerens redegørelse.
På baggrund af ministerens redegørelse og rigsrevisors notat tager Statsrevisorerne endelig stilling til beretningen, hvilket forventes at ske i februar 2018.
Ministerens redegørelse, rigsrevisors bemærkninger og Statsrevisorernes eventuelle bemærkninger samles i Statsrevisorernes Endelig betænkning over statsregnskabet, som årligt afgives til Folketinget i februar måned – i dette tilfælde Endelig betænkning over statsregnskabet 2017, som afgives i februar 2019.

Henvendelse vedrørende
denne publikation rettes til:

Statsrevisorerne
Folketinget
Christiansborg
1240 København K
Telefon: 33 37 59 87
Fax: 33 37 59 95
E-mail: statsrevisorerne@ft.dk
Hjemmeside: www.ft.dk/statsrevisorerne

Yderligere eksemplarer kan
købes ved henvendelse til:

Rosendahls Lager og Logistik
Herstedvang 10
2620 Albertslund
Telefon: 43 22 73 00
Fax: 43 63 19 69
E-mail: distribution@rosendahls.dk
Hjemmeside: www.rosendahls.dk

ISSN 2245-3008
ISBN trykt 978-87-7434-535-0
ISBN pdf 978-87-7434-536-7

Statsrevisorernes bemærkning

BERETNING OM 3 REGIONERS BESKYTTELSE AF ADGANGEN TIL IT-SYSTEMER OG SUNDHEDSDATA

Center for Cybersikkerhed vurderer, at offentlige myndigheder i Danmark i stigende grad er truet af cyberangreb. Sundhedssektorens it-systemer er udsat for en specifik trussel. Fx har der i Danmark været flere angreb på sygehuse i Region Syddanmark, som kan have haft konsekvenser for patientbehandlingen.

Regionerne har ansvaret for at beskytte sundhedsdata i Danmark. Beretningen handler om, hvordan 3 regioner – Region Syddanmark, Region Midtjylland og Region Hovedstaden – beskytter adgangen til it-systemer og sundhedsdata.

Statsrevisorerne finder, at de 3 regioners beskyttelse af adgangen til it-systemer og sundhedsdata ikke er tilfredsstillende. Hermed er der risiko for, at følsomme og fortrolige persondata kommer i hænderne på uvedkommende eller ikke er pålidelige og tilgængelige, når der er brug for dem.

Statsrevisorerne bemærker:

- At grundlæggende sikringstiltag mod hackerangreb ikke i tilstrækkelig grad er implementeret i nogen af de 3 regioner. Særligt kritisk er det, at 27.000 medarbejdere i Region Syddanmark har lokaladministratorrettigheder, da det øger risikoen for hackermisbrug.
- At styring og kontrol af medarbejdere med privilegerede rettigheder er mangelfuld i alle 3 regioner, herunder at der er utilstrækkelig begrænsning af muligheder for at tilgå internettet, når der logges på med privilegerede rettigheder.
- At Region Syddanmark og Region Hovedstaden har passwords til system- og servicekonti, der ikke har været skiftet i lang tid – op til 9 år – og passwords, der ikke lever op til god praksis.
- At alle 3 regioners logningstiltag er mangelfulde, hvilket gør det vanskeligt at opdage og opklare hackerangreb og misbrug af rettigheder. Region Midtjylland har ikke implementeret nogen af de undersøgte logningstiltag, selv om regionen har udarbejdet en politik for området.

STATSREVISORERNE,
den 15. november 2017

Peder Larsen
Henrik Thorup*)
Klaus Frandsen
Søren Gade
Henrik Sass Larsen
Villum Christensen

*) *Statsrevisor Henrik Thorup har ikke deltaget ved behandlingen af denne sag på grund af inhabilitet.*

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.

Rigsrevisionen har gennemgået regnskaberne efter § 4, stk. 1, nr. 1, jf. § 6 i rigsrevisorloven.

Beretningen vedrører finanslovens § 16. Sundheds- og Ældreministeriet.

I undersøgelsesperioden har der været følgende ministre:

Ellen Trane Nørby: november 2016 -
Karen Ellemann: februar 2017 - maj 2017 (fungerende minister)

Beretningen har i udkast været forelagt Sundheds- og Ældreministeriet, Region Hovedstaden, Region Syddanmark og Region Midtjylland, hvis bemærkninger er afspejlet i beretningen.

1. Introduktion og konklusion

1.1. FORMÅL OG KONKLUSION

1. Denne beretning handler om, hvad 3 regioner – Region Syddanmark, Region Midtjylland og Region Hovedstaden – gør for at beskytte adgangen til it-systemer, der indeholder sundhedsdata om borgerne. Rigsrevisionen har selv taget initiativ til undersøgelsen, der bygger på it-revisioner, som Rigsrevisionen har udført i 1. halvår 2017.

2. Regionerne har ansvaret for det danske sygehusvæsen. Regionerne har dermed også ansvaret for at beskytte sundhedsdata, der indeholder følsomme persondata om borgernes helbred. Regionerne skal sikre, at disse data er fortrolige, men også at de er tilgængelige og pålidelige, så patienter kan få den rette behandling til den rette tid. Derfor skal regionerne beskytte borgernes sundhedsdata mod at komme i hænderne på uvedkommende.

3. I takt med den øgede digitalisering i regionerne og samfundet i øvrigt vokser truslen mod regionernes it-systemer og data, hvilket stiller større krav til it-sikkerheden. Regionerne er truet af udefrakommende hackerangreb, ligesom medarbejderne i regionerne kan udgøre en risiko, hvis de bevidst eller ubevidst misbruger deres adgang til it-systemer og data.

Derfor bør regionerne dels have etableret grundlæggende sikringstiltag, der beskytter mod hackerangreb, dels styre og kontrollere medarbejdernes adgang til it-systemer og data. Det gælder særligt i forhold til de medarbejdere, der har privilegerede rettigheder og dermed fuld adgang til og kontrol med it-systemerne, idet et hackerangreb mod disse medarbejdere vil give hackeren samme adgang og kontrol. De grundlæggende sikringstiltag kan sammen med styring og kontrol af privilegerede rettigheder i væsentlig grad reducere risikoen for, at regionernes it-systemer og data kompromitteres.

4. Formålet med undersøgelsen er at vurdere, om de 3 regioner har en tilfredsstillende beskyttelse af adgangen til it-systemer og data, der er med til at sikre fortroligheden, tilgængeligheden og pålideligheden af borgernes sundhedsdata.

HACKERANGREB

Hackerangreb dækker over udefrakommende angreb på digitale systemer eller netværk, der giver hackerne mulighed for at få uautoriseret adgang til it-systemer og data.

Hackerangreb omtales også som cyberangreb og sikkerhedshændelser.

GRUNDLÆGGENDE SIKRINGSTILTAG

Grundlæggende sikringstiltag bruges i denne beretning som en samlet betegnelse for følgende sikringstiltag:

- begræns download af programmer
- undgå afvikling af ikke-godkendte programmer
- sikkerhedsopdatér programmer og styresystemer
- undgå at give medarbejdere lokaladministratorrettigheder
- begræns muligheden for, at malware kan sprede sig ubegrænset.

KONKLUSION

Det er Rigsrevisionens vurdering, at beskyttelsen af adgangen til it-systemer og sundhedsdata ikke er tilfredsstillende i de 3 regioner. Hermed er der risiko for, at følsomme og fortrolige persondata kommer i hænderne på uvedkommende, og at vigtige sundhedsdata, der indgår i behandlingen af borgere i sygehusvæsenet, ikke er pålidelige eller tilgængelige, når der er brug for dem. På baggrund af undersøgelsens resultater og det nuværende trusselsbillede finder Rigsrevisionen, at de grundlæggende tiltag mod hackerangreb og beskyttelse af adgangen til it-systemer og sundhedsdata bør prioriteres højt i alle landets regioner.

Der er mangler i regionernes grundlæggende tiltag mod hackerangreb. Rigsrevisionen finder det særligt kritisk, at alle ca. 27.000 medarbejdere i Region Syddanmark er lokaladministratorer. Det øger markant risikoen for, at hackere kan misbruge medarbejdernes rettigheder og dermed kan tiltvinge sig adgang til og kompromittere it-systemer og sundhedsdata. I Region Midtjylland og Region Hovedstaden er der et stort antal computere med forældede styresystemer, der ikke længere bliver sikkerhedsopdateret. Hermed udsætter de 2 regioner sig for en øget risiko for hackerangreb.

Rigsrevisionen finder det derudover særligt kritisk, at ledelsen i Region Syddanmark ikke har udstukket helt overordnede rammer for it-sikkerheden på de undersøgte områder. Hermed mangler der en klar retning for, hvordan ledelsen vil prioritere og håndtere it-sikkerheden, så borgernes sundhedsdata beskyttes. God it-sikkerhed kræver forankring og prioritering i topledelsen – især i store organisationer som regionerne.

De 3 regioner bør generelt være bedre til at styre og kontrollere medarbejdere med privilegerede rettigheder, fx ved løbende kontrol af, hvilke medarbejdere der skal have disse rettigheder. De undersøgte regioner har ikke i tilstrækkelig grad begrænset medarbejdernes mulighed for at tilgå internettet, når de logger på med de privilegerede rettigheder. Når det sammenholdes med, at ingen af de 3 regioner i tilstrækkelig grad begrænser medarbejdernes mulighed for at downloade programmer, medfører det en øget risiko for, at medarbejderne uforvarende henter og åbner skadeligt indhold, der inficerer it-systemerne og udsætter sundhedsdata for fare.

Region Hovedstaden og Region Syddanmark har passwords til system- og servicekonti, der ikke er skiftet i lang tid. Rigsrevisionen fandt således passwords, der er 6-9 år gamle, og som ikke lever op til god praksis for antallet af karakterer i et password. Hermed øges risikoen for internt og eksternt misbrug af adgangen til it-systemer og data. Undersøgelsen viser dog, at alle 3 regioner har et klart fokus på at nedbringe antallet af system- og servicekonti med privilegerede rettigheder.

De 3 regioners logningstiltag på det undersøgte område er mangelfulde. Manglende logning gør det vanskeligt eller umuligt for regionerne at opdage og opklare hackerangreb og misbrug af rettigheder. Fx har Region Hovedstaden ikke etableret en systematisk gennemgang af logfiler, mens Region Midtjylland ikke har nogen af de undersøgte logningstiltag, selv om regionen har udarbejdet en politik for området.

De 3 regioner har oplyst, at de efterfølgende har iværksat konkrete initiativer i forhold til de undersøgte områder, der imødekommer flere af Rigsrevisionens kritikpunkter.

1.2. BAGGRUND

5. De offentlige myndigheder er i stigende grad truet af cyberangreb. Det viser en vurdering af cybertruslen mod Danmark, som er udarbejdet af Center for Cybersikkerhed i februar 2017. Det fremgår af vurderingen, at truslen fra cyberangreb mod danske myndigheder er meget høj, og at den er stigende i omfang og kompleksitet.

Det fremgår endvidere af vurderingen, at der er en specifik trussel mod sundhedssektorens it-systemer. Det er bl.a. baseret på, at sundhedssektoren i udlandet i stigende grad har været udsat for angreb. I USA, England og Tyskland er der set eksempler på, at hackere har krypteret mails og patientjournaler, hvilket i nogle tilfælde har haft direkte konsekvenser for patientbehandlingen. I Danmark har der været flere angreb mod sygehuse i Region Syddanmark – senest i maj og juni 2017, hvor 20-30 medarbejdere blev låst ude af deres computere. Et af de seneste – og hidtil største – globale hackerangreb, der ramte i maj 2017, gik blandt andre ud over britiske hospitaler, der måtte aflyse behandlingen af patienter.

6. Danske Regioner har beskrevet nødvendigheden af, at der arbejdes for at styrke regionernes it-sikkerhed og dermed beskyttelsen af borgernes sundhedsdata. Det fremgår af Danske Regioners publikation *Regionernes politiske linje for informationssikkerhed* fra 2015, at sundhedsdata er personlige, og at der således følger et særligt ansvar med, når regionerne anvender sundhedsdata.

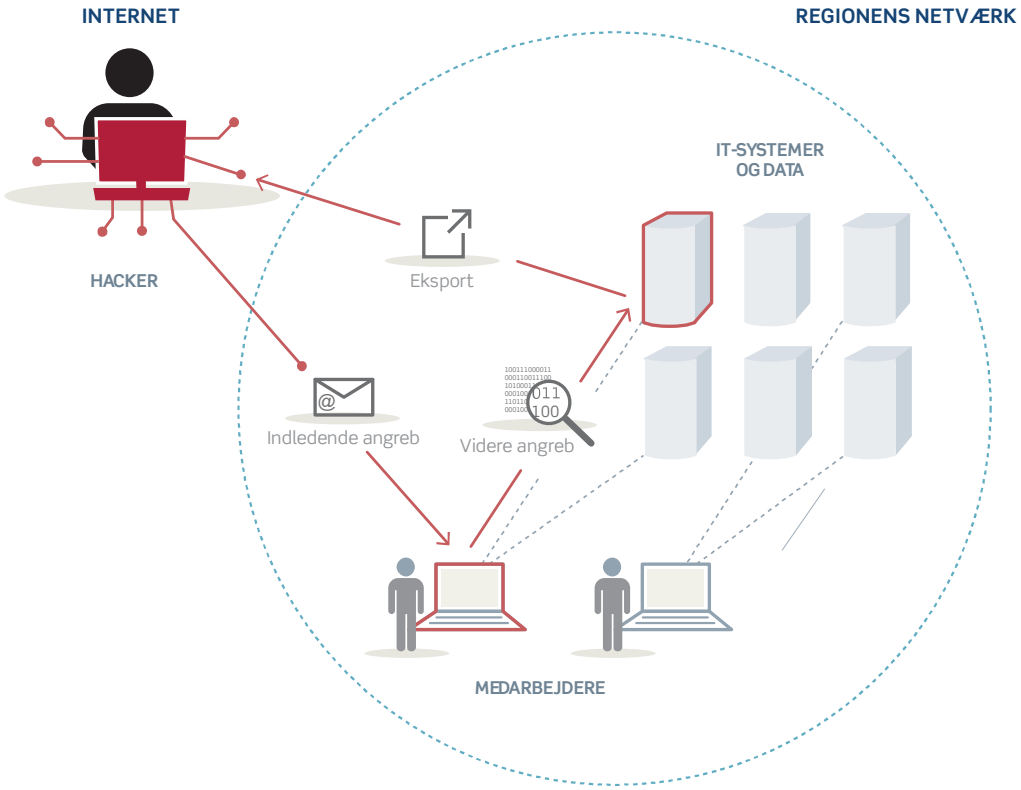
7. Ofte vil det være en kombination af fx svagheder i it-systemer og forkert medarbejderadfærd, der medfører brud på it-sikkerheden og dermed risiko for, at sundhedsdata kompromitteres. Dette er illustreret i figur 1, der viser, at en hacker typisk kan forsøge at udnytte svagheder i it-systemer og indlede et angreb ved at sende en mail til en medarbejder, der uforvarende åbner det skadelige indhold. Hackeren kan på den måde via medarbejderen fortsætte det videre angreb og få adgang til it-systemer og data, så hackeren afslutningsvist fx kan eksportere de ønskede data. Herved er der risiko for, at fortrolige persondata havner i de forkerte hænder, og at data ændres, slettes eller gøres utilgængelige, hvilket vanskeliggør den fortsatte drift og opgavevaretagelse i regionen.

CENTER FOR CYBERSIKKERHED

Center for Cybersikkerhed er en del af Forsvarets Efterretningstjeneste under Forsvarsministeriet. Centret er sat i verden for at hjælpe danske myndigheder og virksomheder med at forebygge, imødegå og beskytte sig mod cyberangreb.

FIGUR 1

ET TYPISK HACKERANGREB



Kilde: Rigsrevisionen.

Regionerne bør derfor ikke kun have fokus på at sikre it-systemerne mod udefrakommende angreb, fx ved at opdatere systemerne, men også på at styre og kontrollere medarbejdernes adgang til it-systemer og data, så hackere ikke kan udnytte medarbejdernes adgang og rettigheder. Styring og kontrol af adgangen til it-systemer og data reducerer omfanget af og skaderne ved et hackerangreb og begrænser risikoen for, at medarbejdere bevidst eller ubevidst misbruger deres adgang.

8. Rigsrevisionen har tidligere gennemført undersøgelser af it-sikkerhed og beskyttelse af persondata i staten: beretning om forebyggelse af hackerangreb fra 2013, beretning om statens behandling af fortrolige oplysninger om personer og virksomheder fra 2014 og senest beretning om adgangen til it-systemer, der understøtter samfundsvigtige opgaver fra 2015. Alle 3 undersøgelser viste, at der var utilstrækkelig beskyttelse af it-systemer og fortrolige data i staten.

1.3. REVISIONSKRITERIER, METODE OG AFGRÆNSNING

Revisionskriterier

9. Undersøgelsen er særligt baseret på revisionskriterier, som Rigsrevisionen tidligere har brugt i beretningen om adgangen til it-systemer, der understøtter samfundsvigtige opgaver, og i beretningen om forebyggelse af hackerangreb. Revisionskriterierne lægger sig tæt op ad vejledninger udarbejdet af Center for Cybersikkerhed. Særlig relevant er vejledningen *Cyberforsvar der virker* fra januar 2017 (1. version fra 2013). Vejledningen beskriver sikringstiltag, som giver en høj grad af beskyttelse, og som reducerer risikoen for angreb væsentligt. Herudover har Center for Cybersikkerhed udarbejdet en passwordvejledning og en logningsvejledning, der beskriver god praksis for brug af passwords og logning.

10. Undersøgelsen omhandler 4 udvalgte områder, som reducerer risikoen for, at it-systemer og data bliver kompromitteret. Det er vigtigt, at der er udarbejdet en politik for it-sikkerheden, og at den er forankret i topledelsen. Derfor har vi som det første undersøgt, om regionerne har ledelsesforankrede politikker på de 4 områder. En politik sætter de overordnede rammer og bør være udmøntet i konkrete retningslinjer og procedurer i de relevante afdelinger. Derfor har vi også undersøgt, i hvilket omfang regionerne har retningslinjer og procedurer på områderne.

De 4 områder er:

- grundlæggende sikringstiltag mod hackerangreb
- styring og kontrol af medarbejdere med privilegerede rettigheder
- styring og kontrol af system- og servicekonti med privilegerede rettigheder
- logning af konti med privilegerede rettigheder.

Vi har undersøgt, om regionerne har implementeret grundlæggende sikringstiltag, der i væsentlig grad reducerer risikoen for hackerangreb. De grundlæggende sikringstiltag, fx sikkerhedsopdatering af programmer og operativsystemer og begrænsning af administratorrettigheder, er baseret på anbefalingerne fra Center for Cybersikkerhed og på Rigsrevisionens vurdering af, hvilke tiltag der er grundlæggende for god it-sikkerhed. Hvis de grundlæggende sikringstiltag ikke er på plads, kan øvrige tekniske tiltag og foranstaltninger få reduceret deres virkning.

De privilegerede rettigheder giver en omfattende adgang til og kontrol med it-systemer og data. Det er derfor vigtigt, at brugen af privilegerede rettigheder styres og kontrolleres for at undgå misbrug internt og eksternt. De privilegerede rettigheder kan knytte sig til enkelte medarbejdere, men også til system- og servicekonti, som flere medarbejdere typisk kan administrere. Styring og kontrol af privilegerede rettigheder vil derfor blive undersøgt både for medarbejdere og for system- og servicekonti.

Herudover har vi undersøgt, om regionerne logger udvalgte handlinger, som udføres af konti med privilegerede rettigheder. Det er vigtigt, fordi logning kan øge regionernes mulighed for at opdage og opklare hackerangreb og misbrug af adgangen til data.

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.

LOGNING

Logning øger chancen for at kunne undersøge et angreb til bunds. Alle handlinger på regionens it-systemer genererer et digitalt fingeraftryk, som kan opsamles i en log. Logning af konti med privilegerede rettigheder kan fx vise, om personer har logget sig på it-systemer, og hvad de har brugt rettighederne til.

11. De grundlæggende sikringstiltag giver sammen med styring, kontrol og logning af privilegerede rettigheder en god beskyttelse mod misbrug af adgangen til regionernes it-systemer og data. Rigsrevisionen understreger dog, at revisionskriterierne og de anbefalinger, de har afsæt i, ikke er statiske. Da risikobilledet ændrer sig løbende, vil anbefalinger til god praksis også ændre sig. Opfyldelsen af revisionskriterierne er dermed ikke ensbetydende med et tilstrækkeligt it-sikkerhedsniveau fremover.

12. I undersøgelsen har vi inden for de 4 udvalgte områder vurderet, om regionerne opfylder (grøn), delvist opfylder (gul) eller ikke opfylder (rød) revisionskriterierne.

Vi har for revisionskriterierne, der handler om antallet af medarbejdere med permanente privilegerede rettigheder og om system- og servicekonti med privilegerede rettigheder, valgt at fastsætte en grænse på 10. Det er en generel anerkendt anbefaling, at antallet bør begrænses, og på baggrund af vores erfaringer fra it-revisionen generelt har vi vurderet, at grænsen er rimelig. Kriteriet er således efter vores opfattelse udtryk for god praksis på området, hvor regionerne bør bestræbe sig på at have så få medarbejdere og konti med permanente privilegerede rettigheder som muligt. Hvis der er behov for at have et højere antal medarbejdere eller konti med permanente privilegerede rettigheder, bør ledelsen løbende forholde sig til og godkende dette.

Metode

13. Undersøgelsen tager udgangspunkt i 3 udvalgte regioner – Region Syddanmark, Region Midtjylland og Region Hovedstaden. Undersøgelsen dækker hermed de 3 største regioner, som har ansvaret for en væsentlig del af sundhedsvæsenet. Samlet dækker de 3 regioner ca. 4,3 mio. af landets ca. 5,7 mio. borgere.

14. Vurderingen af regionernes it-sikkerhed og beskyttelse mod hackerangreb tager udgangspunkt i den enkelte regions centrale netværk, som giver adgang til de it-systemer og databaser, der indeholder borgernes sundhedsdata. Da indgangen til sundhedsdata går gennem regionens centrale netværk, er det som udgangspunkt det netværk, vi har undersøgt it-sikkerheden på.

15. Vurderingen af regionernes segmentering og brug af logning af konti med privilegerede rettigheder er testet ved hjælp af en gennemgang af udvalgte it-systemer i de 3 regioner. De udvalgte systemer indeholder alle sundhedsdata og er alle koblet op på det centrale netværk i hver region.

ACTIVE DIRECTORY
Active Directory (AD) er et af de mest anvendte brugeradministrationssystemer, hvori regionen styrer og kontrollerer adgange og rettigheder til it-systemer og data.

16. Medarbejdernes rettigheder styres i brugeradministrationssystemet Active Directory (AD). Vurderingen af, om regionerne i tilstrækkelig grad styrer og kontrollerer de privilegerede rettigheder, tager derfor udgangspunkt i en gennemgang af regionernes AD.

17. Undersøgelsen er baseret på resultaterne af Rigsrevisionens it-revision i Region Syddanmark, Region Midtjylland og Region Hovedstaden i 1. halvår 2017. Resultaterne afspejler tilstanden i regionerne på revisionstidspunktet. På flere områder har regionerne efter it-revisionens udførelse oplyst, at de har ændret eller taget initiativ til at ændre forholdene. Disse oplysninger er ikke gennemgået og revideret og indgår derfor ikke i Rigsrevisionens vurdering, men oplysningerne er omtalt i gennemgangen af de enkelte områder.

Afgrænsning

18. De tiltag vedrørende beskyttelse af adgangen til it-systemer og data, som indgår i denne undersøgelse, er væsentlige og effektive, men ikke udtømmende i forhold til god it-sikkerhed. Vi har ikke undersøgt andre supplerende sikringstiltag som fx fysisk sikkerhed eller sikring af brug af mobile enheder og medicoteknisk udstyr.

Vi har valgt udelukkende at fokusere på beskyttelsen af adgangen til it-systemer, der indeholder følsomme persondata. Vi har således ikke undersøgt beskyttelsen af regionernes administrative data, fx løndata. Vi har ikke undersøgt, om regionernes behandling af personlige oplysninger følger persondataloven.

19. Revisionen er foretaget med udgangspunkt i regionernes centrale it-afdeling, der har ansvaret for at fastsætte rammerne for it-sikkerheden og for driften og håndteringen af det centrale netværk, som alle sygehuse i den pågældende region er tilkoblet.

20. Revisionen er udført i overensstemmelse med standarderne for offentlig revision, jf. bilag 1.

21. I bilag 1 er undersøgelsens metodiske tilgang beskrevet. I bilag 2 er en oversigt over resultaterne af it-revisionerne. Bilag 3 indeholder en ordliste, der forklarer udvalgte ord og begreber.

2. Regionernes beskyttelse af adgangen til it-systemer og data

2.1. POLITIK FOR IT-SIKKERHED PÅ UDVALGTE OMRÅDER

22. Vi har undersøgt, om regionerne har en politik for, hvordan it-systemer og data beskyttes gennem konkrete sikringstiltag. Baggrunden herfor er, at ledelsen bør have fastsat overordnede rammer, der gør det tydeligt for de relevante medarbejdere i organisationen, hvordan de skal agere for at imødegå misbrug af og angreb på it-systemer og sundhedsdata. Skriftlige politikker, retningslinjer og procedurer på områderne mindsker også risikoen for, at relevant viden og oplysninger er knyttet til få medarbejdere og dermed kan gå tabt, og kan være med til at sikre en mere ensartet praksis i store organisationer som regionerne.

Politikkerne på området skal være godkendt af ledelsen for at sikre, at ledelsens prioritering er tydelig og er med til at understøtte, at der er overensstemmelse mellem det it-sikkerhedsniveau, som regionens ledelse ønsker, og den faktiske it-sikkerhed.

23. Tabel 1 viser resultatet af vores undersøgelse af, om regionerne har udarbejdet en politik, retningslinjer og procedurer for it-sikkerheden på de 4 udvalgte områder.

TABEL 1

POLITIK, RETNINGSLINJER OG PROCEDURER FOR IT-SIKKERHEDEN PÅ DE 4 UDVALGTE OMRÅDER

	Region Syddanmark	Region Midtjylland	Region Hovedstaden
Regionen har udarbejdet en politik, retningslinjer og procedurer for grundlæggende sikringstiltag mod hackerangreb	●	●	●
Regionen har udarbejdet en politik, retningslinjer og procedurer for tildeling af privilegerede rettigheder til medarbejdere	●	●	●
Regionen har udarbejdet en politik, retningslinjer og procedurer for system- og servicekonti med privilegerede rettigheder	●	●	●
Regionen har udarbejdet en politik, retningslinjer og procedurer for logning af konti med privilegerede rettigheder	●	●	●

● Ikke opfyldt
● Delvist opfyldt
● Opfyldt

Kilde: Rigsrevisionen.

Det fremgår af tabel 1, at niveauet for politikker, retningslinjer og procedurer på området er forskelligt mellem regionerne. Region Hovedstaden har udarbejdet både politik, retningslinjer og procedurer på alle 4 udvalgte områder.

Region Midtjylland har udarbejdet en politik, retningslinjer og procedurer på næsten alle områder. Regionen har kun i nogen grad udarbejdet en politik, retningslinjer og procedurer for system- og servicekonti med privilegerede rettigheder, da der kun er få, overordnede beskrivelser af system- og servicekonti i regionens øvrige politikker og retningslinjer. Regionen har oplyst, at der efterfølgende er udarbejdet retningslinjer for system- og servicekonti.

Region Syddanmark har ikke udarbejdet en politik, retningslinjer og procedurer på 3 af områderne. Regionen har kun i nogen grad udarbejdet en politik, retningslinjer og procedurer for tildeling af privilegerede rettigheder, da regionen kun har en retningslinje på området, der er udarbejdet af it-afdelingen, og som derved ikke er ledelsesgodkendt. Regionen har oplyst, at regionen efterfølgende har udarbejdet politikker, retningslinjer og procedurer for brugen af privilegerede rettigheder tilknyttet medarbejdere og system- og servicekonti, og at regionen fremadrettet vil sikre yderligere dokumentation og forankring af it-sikkerhedsområdet.

2.2. GRUNDLÆGGENDE SIKRINGSTILTAG MOD HACKERANGREB

MALWARE
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.

24. Vi har undersøgt, om regionerne har implementeret grundlæggende sikringstiltag mod hackerangreb. Regionerne skal forhindre, at hackere eller malware kommer ind og spreder sig i it-systemerne. Derfor er det vigtigt, at regionerne implementerer grundlæggende sikringstiltag, da de i væsentlig grad reducerer risikoen for hackerangreb.

25. Tabel 2 viser resultatet af vores undersøgelse af, om regionerne har implementeret grundlæggende sikringstiltag mod hackerangreb.

TABEL 2

GRUNDLÆGGENDE SIKRINGSTILTAG MOD HACKERANGREB

	Region Syddanmark	Region Midtjylland	Region Hovedstaden
Regionen har begrænset download af programmer	🟡	🟡	🟡
Regionen har sikret, at kun godkendte programmer kan afvikles	🟡	🟢	🟡
Regionen har sikret, at regionen kan hente sikkerhedsopdateringer fra producenterne af relevante produkter	🟢	🟡	🟡
Regionen har løbende gennemført sikkerhedsopdateringer af relevante produkter, der kan opdateres	🟢	🟢	🟢
Regionen har sikret, at ingen medarbejdere har lokaladministratorrettigheder	🔴	🟢	🟢
Regionen har etableret tiltag, fx segmenteret netværket, så en inficering i form af hackere eller malware ikke kan sprede sig ubegrænset	🟡	🟡	🟡

🔴 Ikke opfyldt
🟡 Delvist opfyldt
🟢 Opfyldt

Kilde: Rigsrevisionen.

Begrænsning af download af programmer

DOWNLOAD kendetegner den proces, hvor et program hentes fra internettet.

INSTALLATION kendetegner den proces, hvor et program pakkes ud og klargøres til brug på computeren.

26. Det er muligt at opstille begrænsninger, så medarbejderne ikke selv kan downloade programmer fra internettet. Hermed undgås det, at medarbejderne bevidst eller ubevidst downloader skadelige programmer, fx en hackers program. Vi har derfor undersøgt, om regionerne har implementeret tekniske begrænsninger, så medarbejderne ikke selv kan downloade programmer fra internettet.

27. Det fremgår af tabel 2, at ingen af de 3 regioner i tilstrækkelig grad har begrænset medarbejdernes mulighed for at downloade programmer fra internettet.

Region Midtjylland har ikke begrænset download af programmer, men har sikret, at kun godkendte programmer kan afvikles, hvilket mindsker risikoen for, at regionens it-systemer bliver inficeret med malware.

Region Hovedstaden og Region Syddanmark har implementeret en løsning, hvor downloadet materiale undersøges i et begrænset og lukket miljø, inden det afleveres til medarbejderen. I begge regioner viser undersøgelsen dog, at det er muligt at downloade almindelige filtyper, der typisk kan være årsag til, at skadeligt indhold inficerer it-systemer.

AFVIKLING kendetegner den proces, hvor et program åbnes og kører på computeren.

Der findes programmer, som kan afvikles uden at være installeret. Det er typisk tilfældet for malware – altså skadelige programmer, som hackere benytter sig af.

Sikring af, at kun godkendte programmer kan afvikles

28. Ved at begrænse medarbejdernes muligheder for at afvikle programmer begrænses hackernes muligheder for at trænge ind i it-systemerne. Det er derfor vigtigt for it-sikkerheden, at regionerne sikrer, at kun godkendte programmer kan afvikles af medarbejderne.

Den sikreste model er en såkaldt whitelisting, dvs. en systemunderstøttet liste over godkendte programmer. En sådan liste vil medføre, at de programmer, der ikke er på listen, ikke kan blive afviklet. En anden – men mindre sikker model – er blacklisting, hvor regionen forhindrer afvikling af en række programmer, som regionen ved er skadelige. Ulempen ved denne model er, at den ikke fanger ukendte, skadelige programmer, og at den kræver høj grad af regelmæssig opdatering for at være virksom.

29. Det fremgår af tabel 2, at det kun er Region Midtjylland, der har implementeret en whitelisting-teknologi, som sikrer, at kun godkendte programmer kan afvikles af medarbejderne.

Undersøgelsen viser, at Region Hovedstaden og Region Syddanmark ikke har etableret en whitelisting-løsning, men at de har sikret, at kendte, skadelige programmer ikke kan afvikles (blacklisting). Der er dog stadig en risiko for, at skadelige programmer, som ikke er kendte, afvikles, og dermed øges risikoen for hackerangreb. Region Hovedstaden har oplyst, at regionen er ved at indføre en whitelisting-løsning.

Sikring af, at regionen kan hente sikkerhedsopdateringer fra producenterne af relevante produkter

30. Hackere kan udnytte svagheder i computerens styresystem. De kan også udnytte svagheder i computerens programmer som fx Adobe Reader, Adobe Flash Player, Java og browsere, der findes på langt størstedelen af alle medarbejderes computere. Disse svagheder kan dog minimeres, hvis programmerne systematisk sikkerhedsopdateres. Producenterne udsender regelmæssigt nye sikkerhedsopdateringer. Hyppigheden afhænger bl.a. af, hvornår producenten bliver opmærksom på en sikkerhedsbrist. Vi har derfor undersøgt, om regionerne systematisk kan hente sikkerhedsopdateringer til udvalgte programmer og operativsystemer.

WINDOWS XP

Windows XP er et styresystem, som ikke længere opdateres. I forbindelse med hackerangrebet i maj 2017 udsendte producenten helt ekstraordinært sikkerhedsopdateringer til styresystemet.

31. Det fremgår af tabel 2, at det kun er Region Syddanmark, der henter sikkerhedsopdateringer til alle relevante produkter. Region Hovedstaden har ca. 800 computere med Windows XP på netværket, som ikke længere sikkerhedsopdateres. Regionen har oplyst, at computerne er beskyttet bag ekstra firewalls og løbende bliver udfaset, så antallet pr. 1. juli 2017 er reduceret til 497 computere med Windows XP.

Region Midtjylland har ca. 7.000 computere med Windows XP og ca. 250 servere med et operativsystem, som producenten ikke længere supporterer. Regionen har dog etableret kompenserende foranstaltninger, fx begrænsning af afvikling af programmer, der bidrager til at mindske risikoen for inficering med malware. Regionen har i øvrigt oplyst, at regionen har planer om, at hovedparten af computerne afvikles i løbet af 2017, så regionen har ca. 500 computere med Windows XP tilbage, og at disse vil være skærmet og indkapslet.

Løbende gennemførelse af sikkerhedsopdateringer af relevante produkter, der kan opdateres

32. Det er vigtigt, at regionerne løbende gennemfører sikkerhedsopdateringer af relevante programmer og operativsystemer.

33. Det fremgår af tabel 2, at alle 3 regioner løbende gennemfører sikkerhedsopdateringer af de programmer og operativsystemer, der kan sikkerhedsopdateres.

Sikring af, at ingen medarbejdere har lokaladministratorrettigheder

34. Regionerne kan opsætte computerne, så medarbejderne er lokaladministratorer og dermed har det højeste niveau af adgang og kontrol over computeren. Ved at overtage lokaladministratorens rettigheder kan en hacker fx lukke antivirusfunktionen og andre funktioner på computeren, der har til formål at begrænse hacking, og bevæge sig videre i regionens it-systemer. Som lokaladministrator kan hackeren desuden installere forskellige skadelige programmer på computeren. Vi har derfor undersøgt, om regionerne har begrænset brugen af lokaladministratorer.

35. Det fremgår af tabel 2, at Region Hovedstaden og Region Midtjylland har sikret, at medarbejderne ikke er lokaladministratorer på de computere, de har adgang til.

I Region Syddanmark har alle ca. 27.000 medarbejdere i regionen lokaladministratorrettigheder. Hermed udsætter regionen sig for en markant øget risiko for, at medarbejdere – bevidst eller ubevidst – installerer og afvikler skadelige programmer på deres computere, som kan sprede sig og kompromittere regionens netværk. Regionen har oplyst, at regionen har foretaget en række kompenserende handlinger for at reducere de trusler, som adgangen til selv at kunne installere programmer medfører, bl.a. gennem monitorering af al ind- og udgående trafik, hvilket efter regionens opfattelse er en mere moderne tilgang til it-sikkerhed. Regionens kompenserende tiltag vedrørende overvågning og detektering er reaktive og ikke forebyggende. Derfor er det vores opfattelse, at disse tiltag ikke bør stå alene, og at regionen uanset tiltagene bør begrænse brugen af lokaladministratorer, da det er et grundlæggende og forebyggende sikringstiltag. Regionen har endvidere oplyst, at regionen er gået i gang med et projekt, der bl.a. omfatter nedlæggelse af lokaladministratorrettigheder.

Etablering af tiltag, fx segmenteret netværket, så en inficering i form af hackere eller malware ikke kan sprede sig ubegrænset

36. Hvis det lykkes en hacker at trænge ind i it-systemerne, er det vigtigt, at skaderne fra hackerangrebet begrænses. Det kan fx opnås ved, at regionerne segmenterer – altså adskiller – de mest kritiske systemer fra det øvrige netværk. På den måde begrænses hackerens eller malwarens muligheder for at sprede sig i systemerne, og skaderne af et angreb mindskes.

SEGMENTERING AF NETVÆRK

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, men kun rammer en begrænset del af netværket.

37. Det fremgår af tabel 2, at ingen af de 3 regioner har segmenteret netværket omkring de it-systemer, vi har undersøgt.

Region Midtjylland har segmenteret netværket delvist, idet ét af de undersøgte it-systemer er adskilt fra det øvrige netværk. De øvrige undersøgte it-systemer er ikke segmenteret. Regionen har i øvrigt etableret kompenserende foranstaltninger, herunder firewalls, på computerne, der i nogen grad mindsker spredning af skadeligt indhold.

Region Hovedstaden har ikke adskilt de udvalgte it-systemer, men har etableret kompenserende foranstaltninger, der i en vis udstrækning modvirker, at skadeligt indhold kan sprede sig, fx ved at beskytte computere med avanceret antivirus. Regionen har oplyst, at Sundhedsplatformen er på et segmenteret netværk, og at der er iværksat et projekt, der vil få alle de kritiske systemer på segmenterede netværk.

Region Syddanmark har ikke etableret segmentering af regionens netværk, men har etableret kompenserende foranstaltninger, der i en vis udstrækning begrænser kommunikationen mellem computerne i regionens netværk, og som dermed også i nogen grad begrænser spredning af skadeligt indhold.

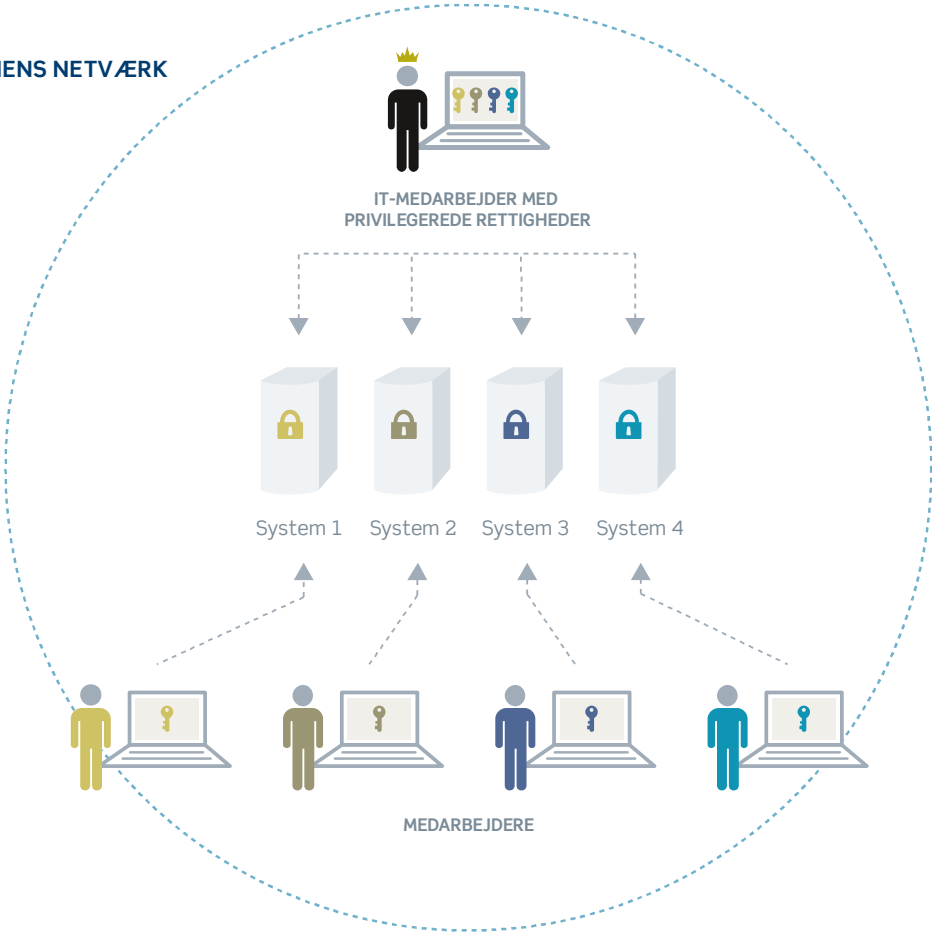
2.3. STYRING OG KONTROL AF MEDARBEJDERE MED PRIVILEGEREDE RETTIGHEDER

38. Vi har undersøgt regionernes kontrol og styring af medarbejdere med privilegerede rettigheder. Medarbejdere med privilegerede rettigheder (typisk betroede it-medarbejdere) har udvidet adgang til og kontrol med it-systemer og data. Det er nødvendigt med sådanne medarbejdere for at vedligeholde og sikre driften af it-systemer og netværk. Det er dog vigtigt for it-sikkerheden, at antallet af disse medarbejdere begrænses, da de er et oplagt mål for hackere, der vil misbruge medarbejdernes rettigheder til at få adgang til it-systemer og data. Hvis det er nemt for en medarbejder med privilegerede rettigheder at bevæge sig rundt i systemerne, er det også nemt for en hacker. Derfor er det også vigtigt at styre og kontrollere de privilegerede rettigheder, da det reducerer omfanget af og skaderne ved et hackerangreb. Herudover mindskes risikoen for, at medarbejdere bevidst eller ubevidst misbruger deres rettigheder.

39. Figur 2 viser, hvordan medarbejdernes adgang til it-systemer og data er afhængig af tildeling af rettigheder (nøgler) til systemerne. Almindelige medarbejdere får kun adgang (nøgle) til specifikke it-systemer og data. Betroede it-medarbejdere med privilegerede rettigheder har i kraft af deres tildelte rettigheder adgang (nøgler) til mange af regionens it-systemer og data.

FIGUR 2

RETTIGHEDER OG ADGANG TIL IT-SYSTEMER OG DATA



Kilde: Rigsrevisionen.

40. Tabel 3 viser resultatet af vores undersøgelse af, hvordan regionerne har styret og kontrolleret medarbejdernes privilegerede rettigheder.

TABEL 3

STYRING OG KONTROL AF MEDARBEJDERE MED PRIVILEGEREDE RETTIGHEDER

	Region Syddanmark	Region Midtjylland	Region Hovedstaden
Regionen har et begrænset antal medarbejdere, der permanent har privilegerede rettigheder	🟡	🟢	🟡
Regionen har sikret, at alle medarbejdere med privilegerede rettigheder anvender en personlig administratorkonto	🟢	🟢	🟢
Regionen har implementeret en regelmæssig kontrol af medarbejdere med privilegerede adgangsrettigheder	🟡	🔴	🟡
Regionen har sikret, at personlige passwords til konti med privilegerede rettigheder følger god praksis og er systemunderstøttede	🟢	🔴	🟡
Regionen har sikret, at medarbejdere med privilegerede rettigheder ikke kan tilgå internettet, når de er logget på med disse rettigheder	🔴	🟡	🔴

🔴 Ikke opfyldt
🟡 Delvist opfyldt
🟢 Opfyldt

Kilde: Rigsrevisionen.

Begrænsning af antal medarbejdere, der permanent har privilegerede rettigheder

41. Jo flere medarbejdere, der permanent har fået tildelt privilegerede rettigheder, desto større er risikoen for misbrug af rettighederne alt andet lige. Derfor bør regionerne tilstræbe at have så få medarbejdere, der permanent har privilegerede rettigheder, som muligt. På den baggrund har vi undersøgt, om regionerne har et begrænset antal (under 10) betroede it-medarbejdere med permanente, privilegerede rettigheder, medmindre ledelsen har forholdt sig til og godkendt et højere antal. Ledelsens godkendelse bør være en formel, årlig godkendelse fra regionens øverste ledelse, hvoraf det fremgår, hvad der konkret begrunder tildelingen af rettigheder til den enkelte medarbejder.

42. Det fremgår af tabel 3, at det kun er Region Midtjylland, der har færre end 10 medarbejdere med permanente, privilegerede rettigheder.

Region Syddanmark havde på undersøgelsestidspunktet 11 medarbejdere med permanente, privilegerede rettigheder. Antallet var dog ikke godkendt af den øverste ledelse, men på et lavere niveau. Regionen har efterfølgende oplyst, at regionen har reduceret antallet til 8.

Region Hovedstaden har siden 2013 reduceret antallet af medarbejdere med privilegerede rettigheder væsentligt. Regionen har 28 medarbejdere med permanente, privilegerede rettigheder, men antallet er ikke ledelsesgodkendt siden 2013, og der foreligger således ikke nogen aktuel godkendelse. Regionen har oplyst, at ledelsen efterfølgende har godkendt antallet af medarbejdere med permanente privilegerede rettigheder.

Sikring af, at alle medarbejdere med privilegerede rettigheder anvender en personlig administratorkonto

43. Det er vigtigt at kunne kontrollere de ændringer, der foretages af medarbejdere med privilegerede rettigheder, så eventuelt misbrug kan spores tilbage til den ansvarlige medarbejder. Derfor er det nødvendigt, at medarbejdere med privilegerede rettigheder anvender en personlig administratorkonto.

44. Det fremgår af tabel 3, at alle 3 regioner har sikret, at medarbejdere med privilegerede rettigheder anvender en personlig administratorkonto, så det sikres, at alle ændringer foretaget af disse medarbejdere er personhenførbare.

Implementering af en regelmæssig kontrol af medarbejdere med privilegerede adgangsrettigheder

45. Regionerne bør sikre, at medarbejderne ikke har rettigheder og adgang til flere it-systemer og data, end de har et arbejdsbetinget behov for. Det betyder, at de privilegerede rettigheder bør inddrages, når der ikke længere er behov for dem. Regionerne bør derfor regelmæssigt foretage en dokumenteret kontrol af de tildelte rettigheder.

46. Det fremgår af tabel 3, at ingen af de 3 regioner foretager en regelmæssig kontrol af medarbejdere med privilegerede rettigheder. Region Hovedstaden og Region Syddanmark fører delvist en regelmæssig kontrol. Undersøgelsen viser dog, at kontrollen i begge tilfælde ikke er fuldstændig. FX omfatter kontrollen ikke alle medarbejdere med udvidede rettigheder. Region Hovedstaden har oplyst, at regionen har iværksat en systematisk kontrol af medarbejdere med privilegerede rettigheder.

Region Midtjylland har ikke implementeret en regelmæssig kontrol af medarbejdere med privilegerede rettigheder. Regionen har oplyst, at regionen fører en uformel kontrol, og at der er iværksat et arbejde med at sikre en regelmæssig kontrol.

Sikring af, at personlige passwords til konti med privilegerede rettigheder følger god praksis og er systemunderstøttede

47. Regionerne bør ved hjælp af systemunderstøttelse sikre, at passwords til konti med privilegerede rettigheder følger god praksis for antal karakterer, kompleksitet og regelmæssige skift. Hermed kan regionerne mindske risikoen for, at passwords brydes, og uvedkommende derved kan tiltvinge sig adgang til it-systemer og data. Passwords til personlige konti med privilegerede rettigheder bør have en længde på mindst 9 karakterer, være komplekse, fx små og store bogstaver og tal, og skiftes inden 90 dage. Hvis regionens ledelse har fastsat skærpede krav til passwordkvaliteten, er det disse krav, vi har lagt til grund.

SYSTEMUNDERSTØTTELSE AF PASSWORDS

Systemunderstøttelse af passwords er en regel i AD, der ikke kan afviges. Hvis institutionen fx har implementeret systemunderstøttelse af en passwordlængde på mindst 9 karakterer, er det ikke muligt at anvende passwords på færre karakterer.

48. Det fremgår af tabel 3, at det kun er Region Syddanmark, der lever op til passwordkravene. Region Midtjylland følger ikke god praksis for længden af passwords. Derudover følger regionen ikke egne krav til, hvor ofte passwords skal skiftes. Hermed er der risiko for, at sikkerhedsniveauet er lavere, end regionens ledelse har besluttet. Regionen har oplyst, at passwords nu følger god praksis og er systemunderstøttede.

Region Hovedstaden har kun en mundtlig aftale om at anvende lange passwords, men denne politik er ikke systemunderstøttet, så rent teknisk er det muligt at bruge kortere passwords. Regionen har oplyst, at regionen efterfølgende har indført systemunderstøttelse, der sikrer, at passwords følger god praksis.

Sikring af, at medarbejdere med privilegerede rettigheder ikke kan tilgå internettet, når de er logget på med disse rettigheder

49. Hackerangreb kan fx ske via hjemmesider, der er inficeret med malware, som spreder sig til de besøgende på hjemmesiden. Hvis en medarbejder logger på med sine privilegerede rettigheder og tilgår en inficeret hjemmeside, kan hackere overtage rettighederne og få adgang til regionens it-systemer og data. Derfor bør regionerne sikre, at medarbejdere ikke kan tilgå internettet, når de er logget på med de privilegerede rettigheder.

50. Det fremgår af tabel 3, at Region Midtjylland delvist har forhindret, at medarbejdere med privilegerede rettigheder kan tilgå internettet, når de er logget på med disse rettigheder, idet halvdelen af regionens medarbejdere med privilegerede rettigheder ikke kunne tilgå internettet. Regionen har oplyst, at det ikke længere er muligt at tilgå internettet med privilegerede rettigheder.

Region Hovedstaden og Region Syddanmark har ingen sikringsforanstaltninger i forhold til at forhindre internetadgangen for medarbejdere med privilegerede rettigheder, når de er logget på med disse rettigheder. Region Syddanmark har oplyst, at regionen arbejder på at etablere denne sikring inden udgangen af året.

2.4. STYRING OG KONTROL AF SYSTEM- OG SERVICEKONTI MED PRIVILEGEREDE RETTIGHEDER

51. Vi har undersøgt regionernes styring og kontrol af system- og servicekonti med privilegerede rettigheder. System- og servicekonti med privilegerede rettigheder giver samme omfattende adgang og beføjelser til it-systemer og data, som de privilegerede rettigheder, der knytter sig til medarbejdere. System- og servicekonti kan – i modsætning til personlige administratorkonti – typisk administreres af flere medarbejdere og er derfor ikke personhenførbare. Dermed er det også vanskeligere at spore brugen af rettigheder tilbage til konkrete medarbejdere. Regionerne bør derfor ud fra et it-sikkerhedshensyn styre og kontrollere system- og servicekonti med privilegerede rettigheder.

52. Tabel 4 viser resultatet af vores undersøgelse af, hvordan regionerne har styret og kontrolleret de privilegerede rettigheder, der knytter sig til system- og servicekonti.

TABEL 4

STYRING OG KONTROL AF SYSTEM- OG SERVICEKONTI MED PRIVILEGEREDE RETTIGHEDER

	Region Syddanmark	Region Midtjylland	Region Hovedstaden
Regionen har et begrænset antal system- og servicekonti med privilegerede rettigheder	●	●	●
Regionen har sikret, at passwords til system- og servicekonti med privilegerede rettigheder følger god praksis og er systemunderstøttede	●	●	●

● Ikke opfyldt
● Delvist opfyldt
● Opfyldt

Kilde: Rigsrevisionen.

Begrænsning af antal system- og servicekonti med privilegerede rettigheder

53. I lighed med de privilegerede rettigheder, der er knyttet til medarbejdere, bør regionerne begrænse antallet af system- og servicekonti med privilegerede rettigheder. Vi har derfor undersøgt, om regionerne har et begrænset antal (under 10) system- og servicekonti med privilegerede rettigheder, medmindre ledelsen har forholdt sig til og godkendt et højere antal.

54. Det fremgår af tabel 4, at 2 af de 3 regioner har et begrænset antal system- og servicekonti med privilegerede rettigheder. Region Midtjylland og Region Syddanmark havde på undersøgelsestidspunktet begge 3 system- og servicekonti med privilegerede rettigheder. Region Syddanmark har efterfølgende oplyst, at regionen har reduceret antallet fra 3 til 0.

Region Hovedstaden har 29 system- og servicekonti med privilegerede rettigheder. Regionen har oplyst, at det skyldes historiske årsager, og at nye system- og servicekonti som udgangspunkt ikke får tildelt disse rettigheder. Undersøgelsen viser, at regionens ledelse i 2013 blev orienteret om og godkendte antallet af system- og servicekonti. Ledelsen er siden regelmæssigt orienteret om antallet af system- og servicekonti. Der har dog ikke været en årlig, formel godkendelse fra ledelsen, hvor det fremgår, hvad der konkret begrunder tildelingen af de privilegerede rettigheder til disse konti. En sådan formel godkendelse foreligger ikke siden 2013. Regionen har oplyst, at ledelsen efterfølgende har godkendt antallet af system- og servicekonti med privilegerede rettigheder.

Sikring af, at passwords til system- og servicekonti med privilegerede rettigheder følger god praksis og er systemunderstøttede

55. Regionerne bør ved hjælp af systemunderstøttelse sikre, at passwords til system- og servicekonti med privilegerede rettigheder følger god praksis med hensyn til antal karakterer og kompleksitet. Hermed kan regionerne mindske risikoen for, at passwords brydes, og uvedkommende derved kan tiltvinge sig adgang til it-systemer og data. Passwords til system- og servicekonti med privilegerede rettigheder bør have en længde på mindst 15 karakterer og være komplekse, fx små og store bogstaver samt tal. Hvis regionens ledelse har fastsat skærpede krav til passwordkvaliteten, er det disse krav, vi har lagt til grund.

56. Det fremgår af tabel 4, at det kun er Region Midtjylland, der har sikret, at passwords til privilegerede system- og servicekonti lever op til god praksis. Alle regionens passwords til system- og servicekonti er maskingenererede og længere end 15 karakterer.

I Region Syddanmark er 2 ud af 3 passwords til system- og servicekonti fra 2008, og de lever ikke op til regionens gældende passwordpolitik, da passwordene kun er på 8 karakterer. Den gældende politik indebærer, at nye passwords til system- og servicekonti genereres automatisk, og at de er komplekse og på minimum 24 karakterer. Autogenererede passwords er typisk komplicerede og lange og er derfor vanskelige at bryde. Regionen har oplyst, at passwordene er blevet ændret og nu lever op til regionens passwordpolitik.

Region Hovedstaden har de seneste 3 år autogenereret passwords til system- og servicekonti. Disse passwords er komplekse og på mindst 16 karakterer. Undersøgelsen viser dog, at kun 4 passwords er fra denne periode. De øvrige passwords er primært fra 2010 og 2011, mens et enkelt er fra 2009. Regionen har oplyst, at disse passwords som udgangspunkt ikke følger regionens gældende passwordpolitik.

2.5. LOGNING AF KONTI MED PRIVILEGEREDE RETTIGHEDER

57. Vi har undersøgt regionernes logning af konti med privilegerede rettigheder. Regionerne kan ikke forvente at forhindre alle angreb. Derfor er det vigtigt, at regionerne er i stand til at opdage sikkerhedshændelser hurtigst muligt, hvilket logning bl.a. bidrager til. Logning kan fx vise, om uvedkommende – både interne og eksterne – har haft adgang til it-systemer, og hvilke handlinger og ændringer der er foretaget i systemerne.

De privilegerede rettigheder giver som nævnt det højeste niveau af rettigheder og adgang til regionernes it-systemer og data. Det er derfor særligt vigtigt, at regionerne sikrer en tilstrækkelig logning af anvendelsen af disse rettigheder med henblik på at kunne opdage og opklare misbrug og sikkerhedshændelser.

58. Tabel 5 viser resultatet af vores undersøgelse af, om regionerne har sikret logning af konti med privilegerede rettigheder.

TABEL 5

LOGNING AF KONTI MED PRIVILEGEREDE RETTIGHEDER

	Region Syddanmark	Region Midtjylland	Region Hovedstaden
Regionen har sikret, at konti med privilegerede rettigheder logges, når de starter programmer, så sporbarheden sikres	●	●	●
Regionen har sikret, at logfiler gennemgås regelmæssigt med henblik på at opdage uautoriserede ændringer eller uhensigtsmæssigheder i it-miljøet	●	●	●
Regionen har sikret, at medarbejdere med privilegerede rettigheder, der logges, ikke har adgang til loggen	●	●	●

● Ikke opfyldt
● Delvist opfyldt
● Opfyldt

Kilde: Rigsrevisionen.

Sikring af, at konti med privilegerede rettigheder logges, når de starter programmer, så sporbarheden sikres

59. Vi har undersøgt, om konti med privilegerede rettigheder bliver logget, når de starter programmer i udvalgte it-systemer, der indeholder følsomme persondata. Det er vigtigt, at regionerne logger konti med privilegerede rettigheder, når de starter et program, fordi det giver mulighed for at se, om der fx er startet programmer, webbrowsere eller andet, som kan have kompromitteret it-systemet.

60. Det fremgår af tabel 5, at ingen af de 3 regioner har sikret, at konti med privilegerede rettigheder logges, når de starter programmer.

I Region Hovedstaden logges konti med privilegerede rettigheder, når der logges på og af it-systemerne, men ikke når de starter programmer, dvs. at man ikke kan se, hvis andre programmer er åbnet og brugt. Det er derfor ikke lige så tydeligt, hvad der er foretaget i systemerne. Regionen har oplyst, at regionen har igangsat et arbejde med at etablere logning ved start af programmer, og at denne form for logning er slået til på de nyeste systemer, herunder Sundhedsplatformen.

Region Midtjylland har oplyst, at logning ved start af programmer er en del af regionens igangværende logningsprojekt og de tilhørende handlingsplaner. Region Syddanmark har oplyst, at regionen i 2017 vil implementere denne form for logning.

Sikring af, at logfiler gennemgås regelmæssigt med henblik på at opdage uautoriserede ændringer eller uhensigtsmæssigheder i it-miljøet

61. Regionerne bør gennemgå logfiler regelmæssigt – enten via medarbejdere, der er uddannet i at gennemgå logfiler, eller via automatiserede overvågningssystemer. På den måde kan regionerne opdage adfærd og hændelser i it-miljøet, der ikke er, som de bør eller plejer at være.

62. Det fremgår af tabel 5, at 1 af de 3 regioner i tilstrækkelig grad har sikret, at logfiler gennemgås regelmæssigt. I Region Syddanmark bliver logfiler automatisk opsamlet og gennemgået.

Region Hovedstaden opsamler og gennemgår logfiler automatisk, men der er kritiske it-systemer, som indgår i vores undersøgelse, som endnu ikke er tilsluttet den automatiske opsamling og gennemgang af logfiler. Regionen har oplyst, at regionen arbejder på at få alle de kritiske systemer sat op til at blive logget.

Region Midtjylland gennemgår ikke regelmæssigt logfiler for de systemer, der indgår i vores undersøgelse. Regionen har oplyst, at regionen i forbindelse med et logningsprojekt er i gang med at etablere en løsning, som på sigt vil gøre det muligt at gennemføre central overvågning af logfiler.

Sikring af, at medarbejdere med privilegerede rettigheder, der logges, ikke har adgang til loggen

63. Hvis en person – enten en medarbejder med privilegerede rettigheder eller en hacker, der har overtaget disse rettigheder – har misbrugt it-systemer eller data, vil vedkommende typisk forsøge at sløre eller slette sine spor i logfilerne. Regionerne bør derfor sikre, at der er funktionsadskillelse i loggen, dvs. at privilegerede rettigheder ikke giver adgang til logfilerne. Logfilerne bør hurtigst muligt sikres mod ændringer og sletning, så der opnås de bedste muligheder for opklaring af sikkerhedshændelsen.

64. Det fremgår af tabel 5, at det kun er Region Syddanmark, der i tilstrækkelig grad har sikret, at medarbejdere med privilegerede rettigheder, der logges, ikke har adgang til loggen, dvs. har adskilt funktionerne.

Region Hovedstaden har delvist adskilt funktionerne, men én medarbejder med privilegerede rettigheder kan i nogle tilfælde tilgå logfilerne. Region Midtjylland har slet ikke sikret funktionsadskillelse i adgangen til loggen, hvilket øger risikoen for, at logfilerne ændres eller slettes, hvis rettighederne er blevet misbrugt. I så fald kan de ikke anvendes til at opklare sikkerhedshændelser. Regionen har oplyst, at funktionsadskillelse vil blive etableret i forbindelse med regionens logningsprojekt.

Rigsrevisionen, den 8. november 2017

Lone Strøm

/Mads Nyholm Jacobsen

BILAG 1. METODISK TILGANG

Formålet med undersøgelsen er at vurdere, om 3 udvalgte regioner har en tilfredsstillende beskyttelse af adgangen til it-systemer og data, der er med til at sikre fortroligheden, tilgængeligheden og pålideligheden af borgernes sundhedsdata.

Undersøgelsen er baseret på it-revisioner i de 3 regioner, som vi har udført i perioden januar - marts 2017. De 3 regioner er Region Syddanmark, Region Midtjylland og Region Hovedstaden. Undersøgelsen dækker således de 3 største regioner, som har ansvaret for en væsentlig del af sundhedsvæsenet. Samlet dækker de 3 regioner 4,3 millioner af landets 5,6 millioner borgere.

I forbindelse med it-revisionen har vi besøgt de 3 regioner.

Revisionskriterier

Undersøgelsen er baseret på revisionskriterier, som Rigsrevisionen tidligere har brugt i beretningen om adgangen til it-systemer, der understøtter samfundsvigtige opgaver (2015) og beretningen om forebyggelse af hackerangreb (2013). Revisionskriterierne lægger sig tæt op ad vejledninger udarbejdet af Center for Cybersikkerhed. Særlig relevant er vejledningen *Cyberforsvar der virker* fra januar 2017 (1. version fra 2013). Vejledningen beskriver sikringstiltag, som giver en høj grad af beskyttelse og reducerer risikoen for angreb væsentligt. Herudover har Center for Cybersikkerhed udarbejdet en passwordvejledning og en logningsvejledning.

Undersøgelsen tager udgangspunkt i 4 udvalgte områder, som reducerer risikoen for, at it-systemer og data bliver kompromitteret:

- grundlæggende sikringstiltag mod hackerangreb
- styring og kontrol af medarbejdere med privilegerede rettigheder
- styring og kontrol af system- og servicekonti med privilegerede rettigheder
- logning af konti med privilegerede rettigheder.

Vi understreger, at revisionskriterierne 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 ensbetydende med et tilstrækkeligt it-sikkerhedsniveau fremover.

Gennemgang af it-systemer

De it-systemer, der indgår i vurderingen af regionernes it-sikkerhed og beskyttelse mod hackerangreb, tager udgangspunkt i den enkelte regions centrale netværk, som giver adgang til de it-systemer og databaser, der indeholder borgernes sundhedsdata. Da indgangen til sundhedsdata går gennem regionens centrale netværk, er det som udgangspunkt det netværk, vi har undersøgt it-sikkerheden på.

Vurderingen af regionernes segmentering og brug af logning af konti med privilegerede rettigheder er baseret på regionernes praksis i forhold til udvalgte it-systemer.

Udvælgelsen af disse it-systemer er baseret på følgende 4 kriterier:

- Systemerne er inkluderet på regionernes liste over vigtige systemer.
- Systemerne er koblet til det centrale netværk.
- Systemerne indeholder følsomme persondata.
- Systemerne drives af regionerne selv.

Hvor flere it-systemer kvalificerede sig ifølge kriterierne, har vi udvalgt tilfældigt.

I forhold til Region Hovedstaden bør det nævnes, at Sundhedsplatformen, der er et omfattende it-projekt med centrale patientdata, ikke er udvalgt til gennemgang, da systemet fortsat var under udrulning på undersøgelsestidspunktet.

Vi har undersøgt, om der foretages logning af, om medarbejdere med privilegerede konti starter programmer op, der kan anvendes til at tilgå it-systemerne på uautoriseret vis. Herudover har vi undersøgt, om logningen i forhold til systemerne gennemgås, og om regionerne har segmenteret – altså adskilt – de udvalgte systemer på netværket, så malware ikke spredes til alle systemer ved et hackerangreb. Formålet har dermed ikke været at foretage en egentlig systemrevision af systemerne.

Medarbejdernes rettigheder styres i brugeradministrationssystemet Active Directory (AD). Vurderingen af, om regionerne i tilstrækkelig grad styrer og kontrollerer de privilegerede rettigheder, tager derfor udgangspunkt i AD.

Standarderne for offentlig revision

Revisionen er udført i overensstemmelse med standarderne for offentlig revision. Standarderne fastlægger, hvad brugerne og offentligheden kan forvente af revisionen, for at der er tale om en god faglig ydelse. Standarderne er baseret på de grundlæggende revisionsprincipper i rigsrevisionernes internationale standarder (ISSAI 100-999).

BILAG 2. OVERSIGT OVER REVISIONSRESULTATERNE

	Region Syddanmark	Region Midtjylland	Region Hovedstaden
Politik, retningslinjer og procedurer for it-sikkerheden på udvalgte områder			
Regionen har udarbejdet en politik, retningslinjer og procedurer for grundlæggende sikringstiltag mod hackerangreb	🔴	🟢	🟢
Regionen har udarbejdet en politik, retningslinjer og procedurer for tildeling af privilegerede rettigheder til medarbejdere	🟡	🟢	🟢
Regionen har udarbejdet en politik, retningslinjer og procedurer for system- og servicekonti med privilegerede rettigheder	🔴	🟡	🟢
Regionen har udarbejdet en politik, retningslinjer og procedurer for logning af konti med privilegerede rettigheder	🔴	🟢	🟢
Grundlæggende sikringstiltag mod hackerangreb			
Regionen har begrænset download af programmer	🟡	🟡	🟡
Regionen har sikret, at kun godkendte programmer kan afvikles	🟡	🟢	🟡
Regionen har sikret, at regionen kan hente sikkerhedsopdateringer fra producenterne af relevante produkter	🟢	🟡	🟡
Regionen har løbende gennemført sikkerhedsopdateringer af relevante produkter, der kan opdateres	🟢	🟢	🟢
Regionen har sikret, at ingen medarbejdere har lokaladministratorrettigheder	🔴	🟢	🟢
Regionen har etableret tiltag, fx segmenteret netværket, så en inficering i form af hackere eller malware ikke kan sprede sig ubegrænset	🟡	🟡	🟡
Styring og kontrol af medarbejdere med privilegerede rettigheder			
Regionen har et begrænset antal medarbejdere, der permanent har privilegerede rettigheder	🟡	🟢	🟡
Regionen har sikret, at alle medarbejdere med privilegerede rettigheder anvender en personlig administratorkonto	🟢	🟢	🟢
Regionen har implementeret en regelmæssig kontrol af medarbejdere med privilegerede adgangsrettigheder	🟡	🔴	🟡
Regionen har sikret, at personlige passwords til konti med privilegerede rettigheder følger god praksis og er systemunderstøttede	🟢	🔴	🟡
Regionen har sikret, at medarbejdere med privilegerede rettigheder ikke kan tilgå internettet, når de er logget på med disse rettigheder	🔴	🟡	🔴

🔴 Ikke opfyldt
🟡 Delvist opfyldt
🟢 Opfyldt

	Region Syddanmark	Region Midtjylland	Region Hovedstaden
Styring og kontrol af system- og servicekonti med privilegerede rettigheder			
Regionen har et begrænset antal system- og servicekonti med privilegerede rettigheder	●	●	●
Regionen har sikret, at passwords til system- og servicekonti med privilegerede rettigheder følger god praksis og er systemunderstøttede	●	●	●
Logning af konti med privilegerede rettigheder			
Regionen har sikret, at konti med privilegerede rettigheder logges, når de starter programmer, så sporbarheden sikres	●	●	●
Regionen har sikret, at logfiler gennemgås regelmæssigt med henblik på at opdage uautoriserede ændringer eller uhensigtsmæssigheder i it-miljøet	●	●	●
Regionen har sikret, at medarbejdere med privilegerede rettigheder, der logges, ikke har adgang til loggen	●	●	●

● Ikke opfyldt
● Delvist opfyldt
● Opfyldt

Kilde: Rigsrevisionen.

BILAG 3. ORDLISTE

Active Directory (AD)	Et brugeradministrationssystem, hvori institutionen styrer og kontrollerer adgang og rettigheder til it-systemer og data.
Applikationer	Computerprogrammer, der tjener et brugerformål. De mest anvendte applikationer (apps) til kontorbrug er fx tekstbehandlingsprogrammer, regneark og webbrowsere.
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.
Hackerangreb	Angreb på digitale systemer eller netværk, der giver hackerne mulighed for at få uautoriseret adgang til it-systemer og data. Et hackerangreb kan fx have til formål at stjæle data og udnytte disse til berigelsesformål, spionage, destruktion eller aktivistiske aktioner. Hackerangreb omtales flere steder som cyberangreb og sikkerhedshændelse.
Logfiler	De filer, hvori institutionen gemmer registreringerne af oplysninger om anvendelse af og hændelser i institutionens it-systemer og data.
Logning	Alle handlinger på regionens it-systemer genererer et digitalt fingeraftryk, som kan opsamles i en log. Logning af konti med privilegerede rettigheder kan fx vise, om personer har logget sig på it-systemer, og hvad de har brugt rettighederne til. Logning øger chancen for at kunne undersøge et angreb til bunds.
Lokaladministrator	Tildelingen af rettighed som lokaladministrator giver medarbejderen det højeste niveau af adgang og kontrol over den computer, som medarbejderen arbejder ved.
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.
Privilegerede rettigheder	Det højeste niveau af rettigheder, adgang og kontrol over institutionens it-systemer og data. Desuden kan de privilegerede rettigheder give mulighed for at omgå institutionens sikringsforanstaltninger. I nogle tilfælde kan de privilegerede rettigheder – afhængigt af institutionens systemopbygning – også give adgang til andre væsentlige it-systemer og data. Privilegerede rettigheder betegner i denne beretning de it-medarbejdere og/eller system- og servicekonti, der er medlem af "Domain Admins-gruppen" i AD.
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.
Sikkerhedshændelse	En uventet hændelse i it-miljøet, der indikerer, at der er eller kan være noget galt.

System- og service-konti	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 privilegerede rettigheder. System- og servicekonti er brugeruafhængige. Hver system- og servicekonto har ét password, som betroede it-medarbejdere typisk har kendskab til. System- og servicekonti anvendes dermed ikke med et personligt password. Al anvendelse af system- og servicekonti, herunder misbrug, er derfor ikke personhenførbar.
Systemunderstøttelse	En regel, der ikke kan afviges. Hvis institutionen fx har implementeret systemunderstøttelse af en passwordlængde på mindst 9 karakterer, er det ikke muligt at formulere passwords på færre karakterer.