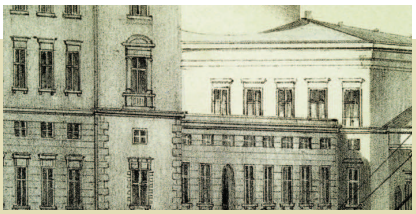
3/2013

STATSREVISORERNE

Beretning om forebyggelse af hackerangreb



3/2013

Beretning om forebyggelse af hackerangreb

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 2013

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.
Finansministeren og klima-, energi- og bygningsministeren afgiver en redegørelse til beretningen.
Rigsrevisor afgiver et notat med bemærkninger til ministrenes redegørelser.
På baggrund af ministrenes redegørelser og rigsrevisors notat tager Statsrevisorerne endelig stilling til beretningen, hvilket forventes at ske ultimo januar 2014.
Ministrenes redegørelser, rigsrevisors bemærkninger og Statsrevisorernes eventuelle bemærkninger samles i Statsrevisorernes Endelig betænkning over statsregnskabet, som årligt afgives til Folketinget i april måned – i dette tilfælde Endelig betænkning over statsregnskabet 2013, som afgives i april 2015.

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-Schultz Distribution
Herstedvang 10
2620 Albertslund
Telefon: 43 22 73 00
Fax: 43 63 19 69
E-mail: distribution@rosendahls-schultzgrafisk.dk
Hjemmeside: www.rosendahls-schultzgrafisk.dk

ISSN 2245-3008
ISBN 978-87-7434-415-5

Statsrevisorernes bemærkning

BERETNING OM FOREBYGGELSE AF HACKERANGREB

Statslige virksomheder opbevarer store mængder fortrolige digitale data og er ansvarlige for at beskytte disse oplysninger. Det drejer sig bl.a. om kommercielt fortrolige og personfølsomme data. Disse data skal opbevares sikkert, og der bør etableres tekniske sikringstiltag, som kan styrke sikkerheden, forebygge hackerangreb og mindske risikoen for misbrug af it-systemer og fortrolige data.

Behovet for beskyttelse mod hackerangreb understreges af, at der i de senere år har været flere hackerangreb på statslige virksomheders it-systemer.

Statsrevisorerne finder det foruroligende, at der i de undersøgte statslige virksomheder har været utilstrækkelig sikring mod hackerangreb og utilstrækkelig beskyttelse af it-systemer og fortrolige digitale data.

Statsrevisorerne finder det utilfredsstillende:

- at ledelsen i de undersøgte virksomheder i Finansministeriet og Klima-, Energi- og Bygningsministeriet ikke har foretaget tilstrækkelige risikovurderinger
- at der på undersøgelsestidspunktet var en unødig stor risiko for hackerangreb, som kunne føre til misbrug af it-systemer og fortrolige data i Finansministeriet og Klima-, Energi- og Bygningsministeriet
- at Statens It – der er it-driftsleverandør for ca. 80 statslige virksomheder – ikke i tilstrækkelig grad har undersøgt, om et hackerangreb mod en virksomhed med utilstrækkelige sikringstiltag kunne sprede sig til andre statslige virksomheder.

Statsrevisorerne,
den 9. oktober 2013

Peder Larsen
Henrik Thorup
Helge Adam Møller
Kristian Jensen
Klaus Frandsen
Magnus Heunicke

RIGSREVISIONEN

Beretning til Statsrevisorerne om forebyggelse af hackerangreb

Rigsrevisionen afgiver hermed denne beretning til Statsrevisorerne i henhold til § 17, stk. 2, i rigsrevisorloven, jf. lovbekendtgørelse nr. 101 af 19. januar 2012. Beretningen vedrører finanslovens § 7. Finansministeriet og § 29. Klima-, Energi- og Bygningsministeriet.

Indholdsfortegnelse

I. Introduktion og konklusion 1

II. Statslige virksomheders forebyggelse af hackerangreb 3
A. Indledning 3
B. Formål, afgrænsning og metode 3
C. Undersøgelse af de 3 sikringstiltag 5
D. Undersøgelse af særlige sikringstiltag i Statens It 7
E. Ansvaret for virksomhedernes sikring 8

Bilag 1. Ordliste 10
Bilag 2. Kildehenvisninger 12

Beretningen vedrører finanslovens § 7. Finansministeriet og § 29. Klima-, Energi- og Bygningsministeriet.

I undersøgelsesperioden har der været følgende ministre:

Finansministeriet:
Bjarne Corydon: 3. oktober 2011 -

Klima-, Energi- og Bygningsministeriet:
Martin Lidegaard: 3. oktober 2011 -

I. Introduktion og konklusion

1. Denne beretning handler om, hvad en række statslige virksomheder gør for at forebygge hackerangreb. En fornuftig adfærd på internettet er vigtig for at undgå angreb, men det er i dag også nødvendigt at supplere med tekniske sikringstiltag, der kan medvirke til at styrke sikkerheden og forebygge angreb.

2. Den stigende digitalisering af den statslige forvaltning øger behovet for, at statslige virksomheder beskytter sig mod hackerangreb og risikoen for misbrug af it-systemer og fortrolige data. Behovet tydeliggøres af, at der i de senere år har været angreb på flere statslige virksomheder.

3. Internationale undersøgelser har vist, at 3 centrale sikringstiltag kan forebygge hovedparten af de på nuværende tidspunkt kendte typer af hackerangreb:

- teknisk begrænsning af download af programmer fra internettet
- begrænsning af brugen af lokaladministratorer
- systematisk sikkerhedsopdatering af programmer.

Rigsrevisionen har derfor vurderet, om de undersøgte statslige virksomheder har håndteret risikoen for hackerangreb, herunder implementeret de 3 sikringstiltag. Virksomhederne er Statens It, Digitaliseringsstyrelsen, Klima-, Energi- og Bygningsministeriets departement og Energistyrelsen.

Rigsrevisionen har desuden undersøgt, om Statens It har håndteret risikoen for, at et hackerangreb på én virksomhed med utilstrækkelige sikringstiltag kan sprede sig til andre virksomheder, fx via de delte servicer (fælles løsninger). Statens It blev etableret som it-driftsleverandør i 2010 og har i dag ca. 80 statslige virksomheder tilsluttet, herunder de 3 andre virksomheder, som indgår i denne undersøgelse.

4. Boks 1 viser eksempler på succesfulde hackerangreb, der kunne have været forebygget eller reduceret med de 3 sikringstiltag.

Hacking *henviser i denne beretning til den ulovlige handling, at en ukendt og uautoriseret person i det skjulte anvender 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 internettets svagheder.*

Sikringstiltag *henviser i denne beretning til en praksis eller mekanisme, der forbedrer it-sikkerheden, dvs. bestræbelser, der tages i anvendelse for at modvirke fejl, tab og misbrug af data og sikre tilgængelighed til it-systemer og data.*

BOKS 1. EKSEMPLER PÅ SUCCESFULDE HACKERANGREB

Der har inden for det seneste år været succesfulde angreb, som har berørt flere af de statslige virksomheder, der er tilsluttet Statens It. Rigsrevisionen anser et angreb som succesfuldt, når ingen af virksomhedens eller Statens It's interne sikringstiltag har forebygget eller detekteret angrebet, og hvor det ikke efterfølgende er muligt at afvise, at it-systemer eller data er blevet misbrugt. Angrebene er alene afsløret, fordi Center for Cybersikkerhed har kunnet konstatere kommunikation med hjemmesider, der er kendt eller mistænkt for skadelig aktivitet.

Ifølge Center for Cybersikkerhed kunne nogle af angrebene have været undgået, hvis de 3 sikringstiltag, der behandles i denne beretning, havde været implementeret i virksomhederne. Center for Cybersikkerhed vurderer også, at konsekvenserne af hovedparten af angrebene ville have været væsentligt mindre, hvis de 3 sikringstiltag havde været implementeret.

5. Undersøgelsen baserer sig på it-revisioner udført som led i årsrevisionen i foråret 2013 og er igangsat på eget initiativ. Rigsrevisionen har valgt at afgive en beretning, da vi vurderer, at undersøgelsens resultater om utilstrækkelig sikring af data er af principiel betydning. Hertil kommer, at det er Rigsrevisionens vurdering, at alle statslige virksomheder bør forholde sig til undersøgelsens anbefaling om at håndtere risikoen for hackerangreb.

UNDERSØGELSENS HOVEDKONKLUSION

Rigsrevisionen finder, at de data, som de undersøgte statslige virksomheder var ansvarlige for, på undersøgelsestidspunktet ikke var tilstrækkeligt beskyttet, og at der med det konstaterede sikkerhedsniveau var en unødig stor risiko for hackerangreb og misbrug af it-systemer og fortrolige data. Undersøgelsen viste, at ingen af de undersøgte virksomheder i deres risikovurderinger havde håndteret den risiko, de udsatte sig for. Rigsrevisionen vurderer desuden, at opgavesplittet mellem Statens It og virksomhederne – hvad angår sikring mod hackerangreb – ikke er klart.

Konkret viste undersøgelsen, at de undersøgte virksomheder ikke systematisk havde forebygget hackerangreb ved teknisk at begrænse download af programmer fra internettet og brugen af lokaladministratorer, ligesom det kun var 2 ud af 4 virksomheder, der systematisk sørgede for at sikkerhedsopdatere deres programmer. Der var endvidere ikke i virksomhedernes risikovurderinger dokumentation for, at ledelsen havde taget stilling til den risiko, virksomheden udsatte sig for ved ikke at have implementeret de 3 sikringstiltag.

Rigsrevisionen vurderer, at Statens It ikke i tilstrækkelig grad havde undersøgt risikoen for, at et hackerangreb på én virksomhed med utilstrækkelige sikringstiltag kunne sprede sig til andre virksomheder, fx via driftscentrets delte services (fælles løsninger). Rigsrevisionen vurderer endvidere, at Statens It's udbredte brug af domæneadministratorer øgede risikoen for spredning af et angreb.

Det er Rigsrevisionens vurdering, at undersøgelsens resultater kan være gældende for en større kreds af statslige virksomheder end de netop undersøgte.

Rigsrevisionens anbefaler derfor:

- **at alle statslige virksomheder i deres risikovurdering forholder sig til risikoen for et hackerangreb, herunder om de i tilstrækkelig grad teknisk har begrænset download af programmer fra internettet og brugen af lokaladministratorer, og om anvendte programmer mv. systematisk sikkerhedsopdateres.**

På baggrund af undersøgelsen skal Rigsrevisionen endvidere anbefale:

- **at Finansministeriet præciserer opgavesplittet mellem Statens It og virksomhederne, hvad angår sikring mod hackerangreb fra internettet**
- **at Finansministeriet ved Digitaliseringsstyrelsen eller Forsvarsministeriet ved Center for Cybersikkerhed udarbejder vejledning til alle statslige virksomheder om, hvilke sikringstiltag en statslig virksomhed bør overveje for at imødegå aktuelle trusler om hackerangreb.**

II. Statslige virksomheders forebyggelse af hackerangreb

A. Indledning

6. Den teknologiske udvikling medfører en stigende digitalisering af samfundet, som også har resulteret i en effektivisering af den offentlige sektor gennem nye digitale løsninger og servicer. I dag opbevarer statslige virksomheder store mængder digitale data, som i varierende grad er fortrolige. Det drejer sig fx om kommercielt fortrolige data, som private virksomheder, der er underlagt kontrol i henhold til konkurrencelovgivningen, er forpligtede til at aflevere til staten. Desuden er hovedparten af de statslige virksomheder ansvarlige for at beskytte oplysninger, der er omfattet af persondataloven. Disse data kan omfatte personers helbredsoplysninger, politiske og religiøse overbevisning, etniske baggrund, strafbare forhold, sociale problemer og andre rent private forhold, fx skatteoplysninger samt ansættelses- og indkomstforhold.

Med den stigende brug af informationsteknologi øges risikoen for angreb fra internettet – også kaldet hacking. Et nyligt eksempel er fra forsommeren 2013, hvor hackere ved et angreb på bl.a. politiets kørekortregister fik adgang til en lang række borgeres cpr-oplysninger. Rigsrevisionen har konstateret, at også andre statslige virksomheder, fx under Erhvervs- og Vækstministeriet og Finansministeriet, har været udsat for hackerangreb.

Center for Cybersikkerhed, som i de senere år har bistået flere private og statslige virksomheder med håndteringen af hackerangreb, vurderer, at problemet er stigende. Et eventuelt brud på fortroligheden af de data, staten opbevarer, kan have væsentlige negative konsekvenser for borgere og private virksomheder samt for de berørte statslige virksomheder.

Center for Cybersikkerhed *er en del af Forsvarets Efterretningstjeneste under Forsvarsministeriet. Centrets mission er at beskytte Danmark mod cybertrusler, fx hackerangreb, spionage og tyveri over internettet.*

B. Formål, afgrænsning og metode

7. Formålet med revisionen var at vurdere, om udvalgte statslige virksomheder i tilstrækkelig grad reducerede risikoen for hackerangreb. Virksomhederne var Statens It og Digitaliseringsstyrelsen, som hører under Finansministeriet, og på Klima-, Energi- og Bygningsministeriets område var det departementet og Energistyrelsen. Disse virksomheder blev udvalgt blandt virksomheder, som er tilsluttet Statens It.

8. På baggrund af erfaringer fra tidligere it-revisioner er det Rigsrevisionens vurdering, at undersøgelsens resultater kan gøre sig gældende for en større kreds af statslige virksomheder end de 4 omtalte.

9. Sikring af informationssikkerhed, herunder reduktion af risikoen ved hackerangreb, er en kontinuerlig proces. Regeringen besluttede i 2004, at statslige virksomheder skulle implementere informationssikkerhedsstandarden DS 484. De senere år har virksomhederne måttet bruge enten DS 484 eller den internationale standard ISO 27001. Fremadrettet har regeringen besluttet, at staten skal følge ISO 27001, når den nye udgave af standarden foreligger i dansk oversættelse, hvilket forventes at være i oktober 2013. Begge standarder stiller krav om, at virksomhederne skal udarbejde en risikovurdering, som skal medtænke alle relevante risici, og at resultatet af risikovurderingen omsættes til konkrete sikringstiltag.

DS 484 *og* ***ISO 27001*** *er begge informationssikkerhedsstandarder. DS 484 er en dansk standard, mens ISO 27001 er internationalt anerkendt. Der er forskel på indholdet i sikkerhedsstandarderne, men for dem begge gælder det, at efterlevelse af standarden er en metode til at sikre virksomhedernes informationer.*

Formålet med risikovurderingen er at prioritere resurserne effektivt i forhold til, hvor de gør mest gavn, og sikre, at virksomheden ikke udsætter sig for større risici, end hvad ledelsen finder acceptabelt.

Sikkerhedstruslerne på fx internettet udvikler sig hurtigt og bliver stadigt mere komplekse, mens en risikovurdering er et øjebliksbillede af situationen på det tidspunkt, hvor vurderingen udarbejdes. Sikkerhedsstandarderne forudsætter derfor, at der mindst én gang årligt gennemføres en risikovurdering, så ledelsen i de enkelte virksomheder kan holde sig informeret om det aktuelle risikobillede.

Da antallet af hackerangreb er stigende, og langt hovedparten af de statslige virksomheder i dag opbevarer store mængder følsomme og fortrolige data digitalt, er det relevant for statslige virksomheder i deres risikovurdering at forholde sig til risikoen for et angreb, herunder vurdere, om virksomhedens aktuelle it-sikkerhed er passende.

10. Ud fra internationale undersøgelser om hackerangreb er det Rigsrevisionens vurdering, at følgende 3 sikringstiltag kan forebygge hovedparten af de på nuværende tidspunkt kendte typer af angreb:

*Tildelingen af rettighed som **lokaladministrator** giver medarbejderen det højeste niveau af adgang og kontrol over den computer, som medarbejderen arbejder ved.*

- teknisk begrænsning af download af programmer fra internettet
- begrænsning af brugen af lokaladministratorer
- systematisk sikkerhedsopdatering af programmer.

I overført betydning svarer de 3 sikringstiltag til nogle af de mest effektive låse på markedet, som kan forebygge hovedparten af alle forsøg på indbrud.

Rigsrevisionen finder, at det i dag bør være god praksis at implementere de 3 sikringstiltag, medmindre der er en tilstrækkelig forretningsmæssig begrundelse for ikke at gøre det.

11. Det australske forsvarsministerium vurderede i oktober 2012, at 85 % af alle hackerangreb kan forebygges med nogle få sikringstiltag. Andre internationale organisationer udgiver lignende anbefalinger vedrørende forebyggelse af hackerangreb, som opdateres i henhold til udviklingen i sikkerhedstruslerne, fx den britiske myndighed for teknisk informationssikkerhed, Communications-Electronics Security Group (CESG), og SANS Institute. SANS Institute er et amerikansk privat forsknings- og uddannelsesinstitut, som samarbejder med den amerikanske efterretningstjeneste (National Security Agency) foruden en lang række andre offentlige og private aktører.

Ud over forebyggende tiltag omfatter de omtalte undersøgelser andre tekniske og organisatoriske sikringstiltag. De 3 sikringstiltag i Rigsrevisionens undersøgelse omfatter 3 af det australske forsvarsministeriums vigtigste anbefalinger om forebyggelse, ligesom de også indgår i CESG's anbefalinger. De 3 sikringstiltag er desuden indeholdt i SANS Institute's højest prioriterede *quick wins*, som instituttet vurderer er de p.t. mest effektive måder at reducere risikoen for hackerangreb væsentligt og øjeblikkeligt på, uden at virksomheder skal foretage omfattende proceduremæssige eller tekniske ændringer.

Der er forskelle i beskrivelsen af de 3 sikringstiltag i de 3 nævnte undersøgelser og i Rigsrevisionens undersøgelse. Fx omtaler undersøgelserne *whitelisting*, som har til formål at sikre, at kun på forhånd godkendte programmer kan anvendes. Vi har undersøgt, om virksomhederne teknisk har begrænset medarbejdernes download af programmer, som er et mindre resursekrævende sikringstiltag, der har samme formål.

Det er Rigsrevisionens vurdering, at de 3 nævnte undersøgelser sammen med andre internationale undersøgelser understøtter væsentligheden af de 3 forebyggende sikringstiltag, som vi behandler i denne undersøgelse. Ifølge Center for Cybersikkerhed kan konklusionerne fra den australske undersøgelse og andre tilsvarende undersøgelser umiddelbart overføres til danske forhold.

12. Det skal bemærkes, at de 3 forebyggende tiltag ikke kan stå alene som god praksis. Et effektivt forsvar mod hackerangreb indebærer flere tekniske og organisatoriske sikringstiltag, som ikke er behandlet i denne undersøgelse.

13. Ud over at undersøge, om virksomhederne havde implementeret de 3 sikringstiltag, undersøgte vi, om risikoen ved eventuelt at fravælge implementeringen af sikringstiltagene var beskrevet i virksomhedernes risikovurdering, så det fremgik, at virksomhedernes ledelse havde forholdt sig til risikoen og muligheden for at forebygge hackerangreb.

Særligt i forhold til Statens It undersøgte vi, om Statens It havde risikovurderet og testet, om et hackerangreb på én af de virksomheder, som var tilsluttet driftscentret, kunne sprede sig til andre af de tilsluttede virksomheder. Rigsrevisionen finder, at sikkerheden i Statens It og i de virksomheder, som var tilsluttet driftscentret, skal ses i sammenhæng, da der var en risiko for, at svagheder hos én af virksomhederne potentielt kunne påvirke andre virksomheder. I forlængelse heraf undersøgte vi, om Statens It havde begrænset anvendelsen af domæneadministratorer, som kan øge risikoen for spredning af et angreb.

*En **domæneadministrator** har markant flere rettigheder end en lokaladministrator. En domæneadministrator har det højeste niveau af rettigheder, adgang og kontrol over alle it-systemer og data i en virksomhed. En hackers overtagelse af en domæneadministrators rettigheder øger derfor risikoen for spredning af angrebet.*

Endelig gennemgik Rigsrevisionen den standardkundeaftale, der var indgået mellem Statens It og alle de tilsluttede virksomheder, for at vurdere opgavesplittet mellem Statens It og virksomhederne vedrørende de 3 sikringstiltag.

Rigsrevisionen gennemgik endvidere virksomhedernes sikkerhedspolitik og andet relevant materiale, og vi interviewede medarbejdere i virksomhederne. Rigsrevisionen modtog desuden en rapport fra Statens It, som viste det aktuelle niveau af sikkerhedsopdatering på alle virksomhedernes computere. Vi gennemgik rapporten for at vurdere, om virksomhedernes sikkerhedsopdatering var tilstrækkelig.

14. Beretningen har i udkast været forelagt Finansministeriet, Klima-, Energi- og Bygningsministeriet, Statens It, Digitaliseringsstyrelsen, Energistyrelsen og Center for Cybersikkerhed, hvis bemærkninger i videst muligt omfang er indarbejdet.

15. Bilag 1 indeholder en ordliste, der forklarer udvalgte ord og begreber. Bilag 2 indeholder kildehenvisninger til de omtalte internationale undersøgelser i beretningen.

C. Undersøgelse af de 3 sikringstiltag

16. Rigsrevisionen har undersøgt, om de udvalgte virksomheder har implementeret de 3 anbefalede sikringstiltag.

Tabel 1 viser resultatet af Rigsrevisionens undersøgelse af praksis i de udvalgte virksomheder.

Tabel 1. Sikkerhedspraksis i udvalgte virksomheder

	Statens It	Digitaliserings-styrelsen	Klima-, Energi- og Bygnings-ministeriets departement	Energi-styrelsen
Begrænser download af programmer fra internettet	Nej	Nej	Nej	Nej
Begrænser brugen af lokaladministratorer	Nej	Nej	Nej	Nej
Sikkerhedsopdaterer systematisk programmer	Ja	Nej	Nej	Ja

Note: ”Nej” betyder, at virksomheden i enkelte tilfælde følger god praksis, men at det ikke sker systematisk.
”Ja” betyder, at virksomheden systematisk følger god praksis, men at der forekommer afvigelser.

Nedenfor følger en uddybning af de 3 sikringstiltag og undersøgelsens resultater, som de er præsenteret i tabel 1.

*At **downloade** et program vil sige at kopiere et program fra internettet ned på sin egen computer. For at programmet kan tages i brug, kræves det, at man efterfølgende installerer programmet på sin computer.*

Download af programmer fra internettet

17. En virksomhed kan opsætte it-systemerne, så medarbejderne ikke selv kan downloade programmer fra internettet (denne opsætning forhindrer ikke download af fx billeder, dokumenter og grafiske præsentationer). Dermed kan medarbejderne kun benytte de programmer, som virksomheden anser for relevante for medarbejdernes arbejdsopgaver, fx tekstbehandling, regneark og internetadgang. Virksomheden kan også vælge at opsætte systemerne, så medarbejderne selv kan downloade programmer fra internettet. Hermed øges risikoen for, at medarbejderen downloader skadelige programmer, fx en hackers fjernstyringsprogram, uden at vide det. Rigsrevisionen har undersøgt, om virksomhederne har implementeret tekniske begrænsninger, så medarbejderne ikke selv kan downloade programmer fra internettet.

18. Rigsrevisionens undersøgelse viste, at ingen af de undersøgte virksomheder havde implementeret tekniske begrænsninger, så medarbejderne ikke kunne downloade programmer fra internettet. Det første sikringstiltag om teknisk at begrænse download af programmer fra internettet var dermed ikke implementeret.

Ingen af de 4 virksomheder havde i deres risikovurdering begrundet fraværet af tekniske begrænsninger for download af programmer fra internettet. Rigsrevisionen finder, at der bør være dokumentation for, at ledelsen har taget stilling til den risiko, virksomheden udsætter sig for ved ikke teknisk at begrænse download af programmer fra internettet.

Brug af lokaladministratorer

19. En virksomhed kan vælge at opsætte computerne, så medarbejderne ikke er lokaladministratorer. En virksomhed kan også vælge at 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 på computeren og andre funktioner, der har til formål at begrænse hacking, og bevæge sig videre i virksomhedens it-systemer. Som lokaladministrator kan hackeren desuden installere forskellige skadelige programmer på computeren. Rigsrevisionen har undersøgt, om de udvalgte virksomheder har begrænset brugen af lokaladministratorer.

20. Rigsrevisionens undersøgelse viste, at alle de undersøgte virksomheder havde valgt at lade medarbejderne være lokaladministrator på deres egen computer. Det andet sikringstiltag om at begrænse brugen af lokaladministratorer var dermed heller ikke implementeret.

Ingen af de 4 virksomheder havde i deres risikovurdering begrundet brugen af lokaladministratorer. Rigsrevisionen finder, at der bør være dokumentation for, at ledelsen har taget stilling til den risiko, virksomheden udsætter sig for ved ikke at begrænse brugen af lokaladministratorer.

Sikkerhedsopdatering af programmer

21. Hackere kan udnytte svagheder i programmer som fx Adobe Reader, Adobe Flash Player, Java og browsere (fx Internet Explorer), der findes på langt størstedelen af alle medarbejderes computere. Disse svagheder kan dog minimeres, hvis programmerne systematisk sikkerhedsopdateres. Producenterne af programmerne udsender regelmæssigt nye sikkerhedsopdateringer. Hyppigheden af sikkerhedsopdateringer afhænger bl.a. af, hvornår producenten bliver opmærksom på en sikkerhedsbrist. Det er ikke ualmindeligt, at der udsendes sikkerhedsopdatering til et program et par gange om måneden. Rigsrevisionen har undersøgt, om virksomhederne systematisk har sikkerhedsopdateret de 4 udvalgte programmer.

22. Rigsrevisionens undersøgelse viste, at Statens It og Energistyrelsen systematisk sikkerhedsopdaterede deres programmer, mens det ikke var tilfældet i de 2 andre virksomheder. Det tredje sikringstiltag om systematisk at sikkerhedsopdatere anvendte programmer var dermed ikke implementeret i 2 ud af de 4 undersøgte virksomheder.

Undersøgelsen viste videre, at virksomhederne i deres risikovurdering ikke havde begrundet deres praksis vedrørende sikkerhedsopdatering af deres programmer. Rigsrevisionen finder, at der bør være dokumentation for, at ledelsen i virksomhederne har taget stilling til den risiko, virksomheden udsætter sig for ved ikke systematisk at sikkerhedsopdatere sine programmer.

Undersøgelsen viste dog også, at praksis på området var ved at blive ændret. Statens It var ved at udrulle nye computere til alle virksomheder, som er tilsluttet Statens It. Denne udrulning, der netop var gennemført hos Energistyrelsen, vil medføre en bedre sikkerhed, da virksomhederne får systematiske sikkerhedsopdateringer, som svarer til niveauet i Statens It. Statens It forventer at afslutte opgaven inden årets udgang.

23. Rigsrevisionen forventer umiddelbart, at Statens It's udrulning af nye computere vil løse en væsentlig del af problemet med mangelfulde sikkerhedsopdateringer. Rigsrevisionen har dog fået oplyst, at nogle af de i alt ca. 1.500 fagsystemer, som Statens It drifter for de tilsluttede virksomheder, vanskeliggør sikkerhedsopdatering af computerne. Det skyldes, at nogle fagsystemer kan være udviklet til en bestemt version af fx browseren på computerne. En ny version af browseren kan medføre, at et fagsystem ikke umiddelbart kan afvikles. I disse tilfælde vil en sikkerhedsopdatering i stedet medføre nedsat eller helt manglende funktionalitet.

Statens It og flere af de tilsluttede virksomheder savner overblik over, hvilke fagsystemer der vanskeliggør sikkerhedsopdateringer på computerne, eller hvor store omkostninger der samlet set vil være forbundet med en løsning, som også sikkerhedsmæssigt er tilfredsstillende. Der er således på nuværende tidspunkt ikke indsamlet tilstrækkelig information til at kunne vurdere opgavens omfang. På den baggrund er det for tidligt at vurdere, om denne særlige udfordring vedrørende sikkerhedsopdateringer bliver løst med Statens It's udrulning af de nye computere.

D. Undersøgelse af særlige sikringstiltag i Statens It

Risiko for spredning af hackerangreb

24. Statens It er baseret på at dele servicer mellem de tilsluttede virksomheder for at kunne minimere omkostningerne pr. transaktion (fx gennemførelse af en betaling eller en søgning i en database) ved it-anvendelsen. Fx kan samme server håndtere opdatering af antivirus på alle computere. Fælles harddiske kan bruges på tværs af virksomheder og ministerier, og samme medarbejder kan arbejde på tværs af it-systemer og data.

Stigende anvendelse af delte servicer kan dog også udgøre en større risiko for en ringere sikkerhed for de tilsluttede virksomheder. En risiko ved brugen af delte servicer er, at virksomheden med den svageste it-sikkerhed kan påvirke sikkerhedsniveauet i andre virksomheder. Et hackerangreb på en virksomhed med utilstrækkelige sikringstiltag kan indebære, at hackerne har nemmere adgang til fortrolige data hos driftscentrets øvrige virksomheder. De virksomheder, der er tilsluttet Statens It, er således afhængige af it-sikkerheden hos hinanden.

Center for Cybersikkerhed har oplyst, at der er eksempler på, at et hackerangreb på en statslig virksomhed har spredt sig til andre virksomheder inden for samme ministerområde. Rigsrevisionen finder det væsentligt, at Statens It forholder sig aktivt til risikoen for spredning inden for samme ministerområde såvel som på tværs af ministerområder. Det forudsætter bl.a. en forudgående risikovurdering og en efterfølgende test af, om det ønskede sikkerhedsniveau er opnået.

25. Rigsrevisionen undersøgte, om Statens It har vurderet risikoen for, at et hackerangreb på én virksomhed kan kompromittere it-sikkerheden i andre virksomheder. Rigsrevisionen undersøgte desuden, om Statens It havde testet, om kompromitterede it-systemer i én virksomhed kunne sprede sig til andre virksomheder, der er tilsluttet Statens It.

Undersøgelsen viste, at Statens It ikke havde vurderet risikoen for, at et hackerangreb på én virksomhed kan kompromittere it-sikkerheden i andre virksomheder, der er tilsluttet Statens It. Desuden havde Statens It ikke udført test, som viste, om et angreb på én virksomhed kan kompromittere andre virksomheders it-systemer inden for driftscentret. Statens It har oplyst, at driftscentret har et passende sikkerhedsniveau, men anerkender behovet for afdækning af risikoen for spredning af angreb og en efterfølgende test heraf.

Risiko ved udbredt brug af domæneadministratorer

26. Rigsrevisionen undersøgte Statens It's anvendelse af domæneadministratorer. En domæneadministrator har det højeste niveau af rettigheder, adgang og kontrol over alle it-systemer og data i en virksomhed. En hackers overtagelse af en domæneadministrators rettigheder øger derfor risikoen for spredning af hackerangrebet.

27. Det er Rigsrevisionens vurdering, at Statens It havde en meget udbredt anvendelse af domæneadministratorrettigheder, som udgør en væsentlig risiko i relation til et eventuelt hackerangreb.

28. Statens It har oplyst, at antallet af domæneadministratorer i Statens It er nedbragt væsentligt. Statens It finder det vanskeligt at begrænse brugen af domæneadministratorer yderligere, uden at det påvirker driftscentrets evne til at levere stabil drift til tilsluttede virksomheder. Statens It er dog enig med Rigsrevisionen i, at Statens It ved ændrede metoder og med en styrket overvågning af administratorerne kan opnå en mere tilfredsstillende sikkerhed.

Statens It har oplyst, at virksomhedernes it-sikkerhed samlet set er forbedret med tilslutningen til Statens It, men at etableringen af et driftscenter også medfører, at der opstår nye risici, fx vedrørende hackerangreb.

E. Ansvaret for virksomhedernes sikring

*Statens It's **infrastruktur** omfatter bl.a. servere, netværk, computere og generelle programmer, fx kontorpakker, mail/kalender og brugerrettighedsstyringssystemer.*

29. Det fremgår af standardkundeaftalen, der er indgået mellem Statens It og alle de tilsluttede virksomheder, at Statens It skal håndtere drift og sikkerhed i infrastrukturen, mens virksomhederne skal håndtere drift og sikkerhed i fagsystemerne. Kundeaftalen omtaler desuden forholdet vedrørende sikkerhedsopdateringer, men ikke download af programmer eller brugen af lokaladministratorer. Rigsrevisionen finder, at man på baggrund af kundeaftalen ikke entydigt kan afgøre opgavesplittet vedrørende de sikringstiltag, der er behandlet i denne beretning.

***Fagsystemerne** er de tilsluttede virksomheders fagspecifikke systemer, som anvendes til virksomhedernes opgaveløsning, og som afvikles oven på Statens It's infrastruktur.*

I praksis påvirker den enkelte virksomheds valg vedrørende fagsystemerne Statens It's mulighed for at udarbejde en sikker infrastruktur og påvirker dermed også de andre virksomheders sikkerhed. Omvendt påvirker Statens It's valg vedrørende sikkerheden i infrastrukturen virksomhedernes forretningsmæssige muligheder.

30. Private virksomheder er forpligtede til at aflevere digitale oplysninger til staten, og borgere registreres uden nødvendigvis at ønske det. Det er Rigsrevisionens vurdering, at ansvaret for, at oplysningerne forbliver fortrolige, i sidste ende ligger hos det ministerium, som indsamler og registrerer oplysningerne. Heraf følger, at det er virksomhederne, der som dataejere har ansvaret for, at informationssikkerheden er tilstrækkelig.

Rigsrevisionen, den 2. oktober 2013

Lone Strøm

/Peder Juhl Madsen

Bilag 1. Ordliste

Adobe Flash	Et tilføjelsesprogram, der kan downloades fra internettet, og som bruges til at vise grafiske elementer, fx en filmtrailer eller andre små videoer og hele hjemmesider.
Adobe Reader	Et tilføjelsesprogram, der kan downloades fra internettet, og som giver mulighed for sikker visning, udskrivning, signering og kommentering af pdf-dokumenter.
Antivirusprogram	Beskytter en computer ved at skanne aktiviteten og dermed afsløre og fjerne vira (skadelige programmer), før de kommer ind og/eller spredes. Antivirusprogrammer indeholder ofte en funktion, som filtrerer trafikken mellem computeren og internettet for at forhindre, at skadelige programmer kommer ind eller ud af computeren.
Browser	Et program, som installeres på computeren, så brugeren kan gå på internettet og søge på forskellige hjemmesider. Den hidtil mest udbredte browser er Microsoft Internet Explorer, som mange computere leveres med.
Center for Cybersikkerhed	En del af Forsvarets Efterretningstjeneste under Forsvarsministeriet. Centrets mission er at beskytte Danmark mod cybertrusler, fx hackerangreb, spionage og tyveri over internettet.
Dataejer	Har ansvaret for at sikre data ved hjælp af de nødvendige tekniske og organisatoriske tiltag. Ved overdragelse af opgaver vedrørende databehandling (herunder indsamling, registrering og lagring) har dataejer fortsat ansvaret for, at sikkerheden er tilstrækkelig.
Delte servicer (fælles løsninger)	Oversat fra den engelske betegnelse "shared services", som indebærer at samle administrative funktioner, der tidligere har eksisteret i flere enheder (fx ministerier), i én enhed og standardisere og effektivisere opgaveløsningen, fx vedrørende it.
Digitalisering	Omsætning af fx data, lyd eller billeder til digital form samt udbredelse af elektroniske medier og computerbaserede forretningsgange.
Domæneadministrator	Har det højeste niveau af rettigheder, adgang og kontrol over alle it-systemer og data i en virksomhed. En domæneadministrator har dermed markant flere rettigheder end en lokaladministrator.
Download	Det at kopiere en fil, fx et program eller lyd- og billedfiler fra internettet ned på sin egen computer.
DS 484 og ISO 27001	Er begge informationssikkerhedsstandarder. DS 484 er en dansk standard, mens ISO 27001 er internationalt anerkendt. Der er forskel på indholdet i sikkerhedsstandarderne, men for dem begge gælder det, at efterlevelse af standarden er en metode til at sikre virksomhedernes informationer.
Fagsystem	De tilsluttede virksomheders fagspecifikke systemer, som anvendes til virksomhedernes opgaveløsning, og som afvikles oven på Statens It's infrastruktur.
Hacking (hackerangreb)	Betegner i denne beretning den ulovlige handling, at en ukendt og uautoriseret person i det skjulte anvender 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 internettets svagheder.
Harddisk	Den del i computeren hvor alle data, dvs. programmer, dokumenter, spil, musik, fotos mv., bliver gemt.
Informationssikkerhed	Dækker sikkerhed i relation til alle it-bårne informationer, men også ikke-it-bårne som bl.a. fysiske rammer og fysiske dokumenter.
Infrastruktur	Statens It's infrastruktur omfatter servere, netværk, computere og generelle programmer, fx kontorpakker, mail/kalender og brugerrettighedsstyringssystemer.
Internet Explorer	Én blandt mange browsere. Internet Explorer produceres af Microsoft.

Java	Et tilføjelsesprogram, der kan downloades fra internettet, og som hjælper computerens browser med at vise særlige formater, fx Adobe Flash. Mange almindeligt kendte hjemmesider og funktioner vil ikke kunne anvendes uden Java, fx Google Maps og NemID.
Lokaladministrator	Tildelingen af rettighed som lokaladministrator giver medarbejderen det højeste niveau af adgang og kontrol over den computer, som medarbejderen arbejder ved.
Sikkerhedsopdatering	Hackere udnytter svagheder i kendte programmer til at skaffe sig adgang til computeren. En sikkerhedsopdatering lukker en kendt svaghed i et program.
Sikringstiltag	Betegner i denne beretning en praksis eller mekanisme, der forbedrer it-sikkerheden, dvs. bestræbelser, der tages i anvendelse for at modvirke fejl, tab og misbrug af data og sikre tilgængeligheden til it-systemer og data.
Statslige virksomheder	En forvaltningsenhed inden for et ministerområde, hvis ledelse er budget- og regnskabsansvarlig for et eller flere områder på finansloven.
Whitelisting	En liste af godkendte programmer. Whitelisting fungerer ved, at et program automatisk kontrolleres, når det forsøges anvendt, og programmet kan kun anvendes, hvis det står på listen. At implementere whitelisting kræver vedligeholdelse af information om alle computerbrugernes opgaver og de programmer, der er nødvendige for opgaveløsningen, herunder de eksakte versioner af programmerne.
Årsrevision	Rigsrevisionens årsrevision består af løbende revision af bl.a. forretningsgange og interne kontroller, herunder it-revision og afsluttende revision af bl.a. årsregnskabet. Resultatet af den løbende revision afrapporteres almindeligvis til den pågældende virksomhed og ministeriet.

Bilag 2. Kildehenvisninger

Australian Government, Department of Defence, Intelligence and Security, the Defence Signals Directorate (2012): *Strategies to Mitigate Targeted Cyber Intrusions:* www.dsd.gov.au/publications/Top_35_Mitigations_2012.pdf

British Government Communications Headquarters, Communications-Electronics Security Group (2012): *10 steps to Cyber Security*: www.bis.gov.uk/assets/biscore/business-sectors/docs/0-9/12-1121-10-steps-to-cyber-security-advice-sheets

SANS Institute (2013): *Critical Controls for Effective Cyber Defense:* www.sans.org/critical-security-controls/cag4-1.pdf