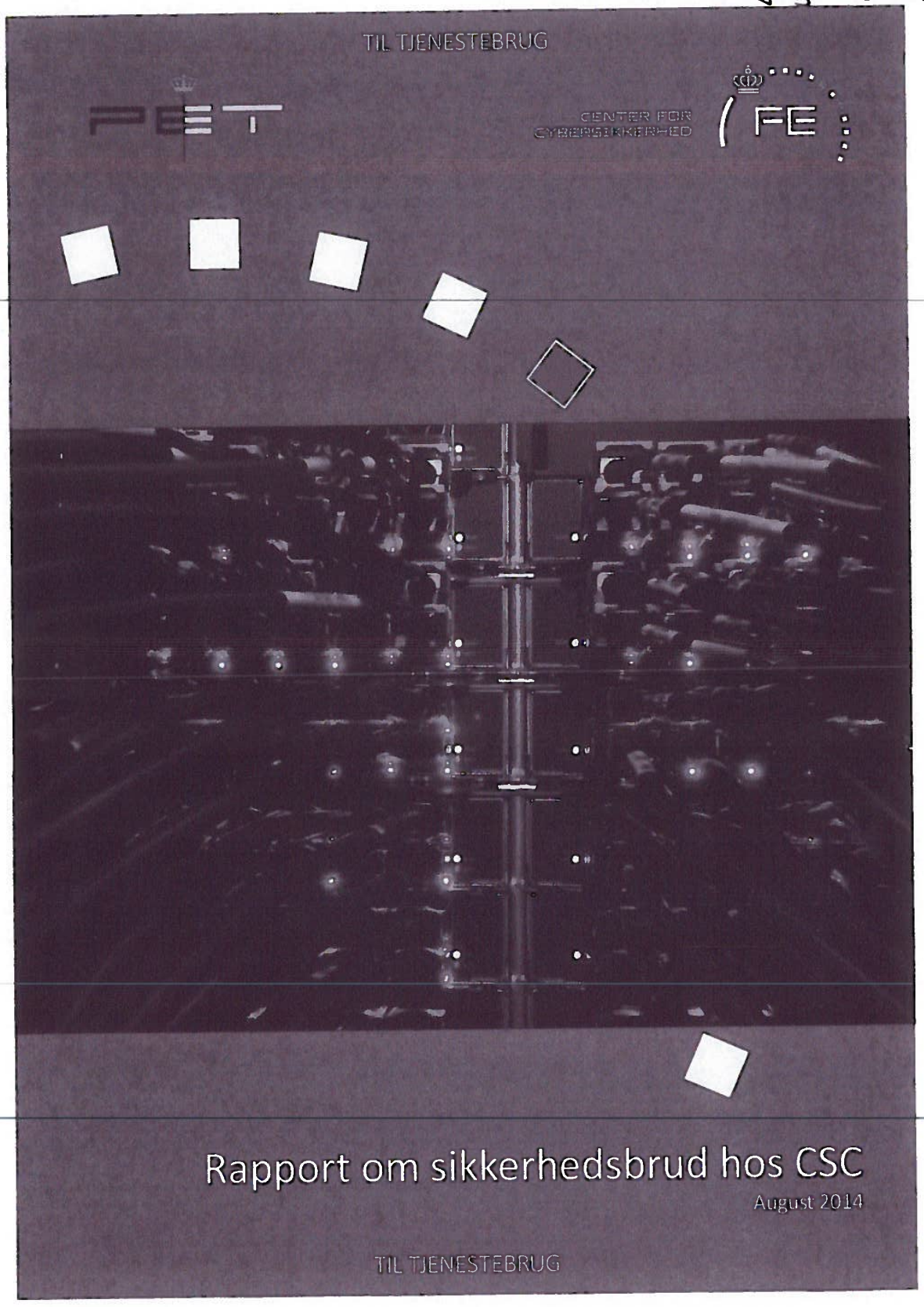


INDHOLD

1. SAMMENFATNING

I januar 2013 blev dansk politi af svensk politi gjort opmærksom på, at flere af dansk politis it-systemer muligvis var blevet kompromitteret ved et angreb mod et fællesoffentligt mainframemiljø (et mainframemiljø, der anvendes af en række statslige myndigheder) hos it-leverandøren CSC. CSC varetager driften af vigtige it-systemer for en række danske myndigheder. Dansk politis undersøgelser viste, at der havde været angreb mod CSC, som havde medført, at en eller flere personer havde kompromitteret dele af CSC's systemer.

I juni 2013 blev Center for Cybersikkerhed inddraget i sagen, og centeret har sammen med Politiets Efterretningstjeneste (PET) udarbejdet denne rapport om kompromitteringen. Center for Cybersikkerhed er Danmarks nationale it-sikkerhedsmyndighed, og PET varetager funktionen som it-sikkerhedsmyndighed inden for Justitsministeriets område.

Center for Cybersikkerhed og PET har indsamlet og analyseret store mængder materiale om kompromitteringen. Det har imidlertid ikke været muligt at skabe et fuldstændigt overblik over kompromitteringens omfang, da ikke alt relevant materiale hos det svenske politi har været tilgængeligt for danske myndigheder.

På baggrund af de it-sikkerhedstekniske undersøgelser af kompromitteringen af det fællesoffentlige mainframemiljø hos CSC samt en uafhængig konsulentundersøgelse fra revisionsfirmaet PwC vurderer Center for Cybersikkerhed og PET:

- At der har været tale om en omfattende og alvorlig kompromittering af de dele af CSC's mainframemiljø, som indeholder data fra politiet, CPR-kontoret, SKAT og Moderniseringsstyrelsen.
- At en eller flere personer har haft adgang til og mulighed for at tilgå, kopiere, slette og ændre i myndighedernes data hos CSC.
- At der med sikkerhed er kopieret data fra politiets systemer.
- At der ikke er fundet indikationer på, at der er kopieret data fra hverken SKAT, Moderniseringsstyrelsen eller CPR-kontorets systemer. Tilsvarende er der dog heller ikke fundet indikationer, der gør det muligt at fastslå, at der ikke er kopieret data fra de nævnte myndigheders systemer.
- At det ikke er muligt at give et komplet overblik over hvilke data, der med sikkerhed er (eller ikke er) kopieret fra mainframemiljøet.

Center for Cybersikkerhed, PET og de berørte myndigheder har – udover at vurdere omfanget af kopiering af data – også set på risikoen for, at data er blevet ændret. Center for Cybersikkerhed og PET vurderer, at det ikke er sandsynligt, at dataintegriteten hos de berørte myndigheder er kompromitteret.

De nævnte offentlige myndigheder deler en række it-serviceydelser og ressourcer hos CSC på et fællesoffentligt mainframemiljø, der er en del af CSC's samlede mainframemiljø. Efter kompromitteringen har CSC implementeret en række væsentlige informationssikkerhedstiltag i det pågældende mainframemiljø. Der er dog fortsat forbedringspotentialer, og der bør derfor iværksættes yderligere informationssikkerhedsmæssige tiltag på såvel serviceudbyder- som kundesiden, der kan styrke informationssikkerhedsniveauet i det fællesoffentlige mainframemiljø hos CSC. Center for Cybersikkerhed og PET vil fortsat være i tæt dialog med de berørte myndigheder og CSC vedrørende implementering af sådanne tiltag.

Center for Cybersikkerhed og PET betragter kompromitteringen som en af de alvorligste kompromitteringer mod it-systemer i Danmark til dato.

2. INDLEDNING

Denne rapport bygger på det materiale, som Center for Cybersikkerhed og PET har haft adgang til frem til april 2014. Rapporten indeholder de overordnede resultater af de analyser af informationssikkerheden, det har været muligt at foretage på det foreliggende datagrundlag.

Efter Center for Cybersikkerheds indledende it-sikkerhedstekniske analyser afholdt centeret en række møder med CSC i efteråret 2013 med henblik på at indsamle yderligere informationer om det fællesoffentlige mainframemiljø, som var blevet kompromitteret. Efter aftale med CSC gennemførte PwC på vegne af Center for Cybersikkerhed i november 2013 en uafhængig sikkerhedsgennemgang af det fællesoffentlige mainframemiljø hos CSC.

Rapportens vurdering af det aktuelle informationssikkerhedsniveau på det fællesoffentlige mainframemiljø hos CSC bygger på PwC's uafhængige gennemgang af sikkerheden samt Center for Cybersikkerheds og PET's egne analyser. Hverken Center for Cybersikkerhed eller PET har haft direkte adgang til at undersøge CSC's systemer og sikkerhedsopsætning, men har baseret sig på CSC's oplysninger. Oplysningerne er i størst muligt omfang søgt valideret af Center for Cybersikkerhed og PET gennem dialog med de berørte myndigheder, PwC og CSC.

Center for Cybersikkerhed og PET's analyser har givet anledning til at udarbejde nogle fremadrettede anbefalinger, der kan styrke informationssikkerheden i danske myndigheders digitale systemer. Anbefalingerne, der er udarbejdet af Center for Cybersikkerhed i samarbejde med Digitaliseringsstyrelsen, indeholder overordnede beskrivelser af, hvordan myndigheder kan styrke den sikkerhedsmæssige håndtering af statens outsourcede it-drift. Anbefalingerne bliver offentliggjort i en selvstændig rapport, der udgives af Center for Cybersikkerhed og Digitaliseringsstyrelsen. PET har, i kraft af sin rolle som it-sikkerhedsmyndighed inden for Justitsministeriets område, endvidere udarbejdet et bilag til indeværende rapport med anbefalinger til, hvordan informationssikkerheden specifikt kan styrkes i politiets systemer.

Center for Cybersikkerhed og PET betragter med denne rapport den it-sikkerhedsmæssige undersøgelse af kompromitteringen som afsluttet.

3. DATAGRUNDLAG FOR RAPPORTEN

3.1. Materiale fra svensk og dansk politi

Svensk politi orienterede i januar 2013 dansk politi om, at der på it-udstyr tilhørende en svensk statsborger var fundet materiale, der tydede på, at den pågældende havde haft adgang til danske data hos CSC i Danmark. Materialet blev fundet under en efterforskning, som det svenske politi havde indledt for at undersøge, om den svenske statsborger havde kompromitteret et mainframemiljø i Sverige.

Som følge af kompromitteringen blev der i Danmark iværksat en efterforskning, der varetages af Københavns Politi i samarbejde med PET og Rigspolitiets Nationale It-efterforskningssektion (NITES). Center for Cybersikkerhed har som national it-sikkerhedsmyndighed varetaget den it-sikkerhedsmæssige undersøgelse af sagen med henblik på at klarlægge konsekvenserne af kompromitteringen af it-systemer, som CSC drifter for en række offentlige myndigheder.

Af hensyn til den verserende efterforskning samt de krav til fortrolighed, som disse oplysninger er underlagt, kan dette materiale ikke offentliggøres. Det er således ikke muligt i denne rapport at omtale alle de oplysninger, som Center for Cybersikkerhed og PET er i besiddelse af og som rapportens konklusioner er baseret på.

Hovedparten af datagrundlaget for denne rapport stammer fra it-udstyr, der er i svensk politis varetægt. Dansk politi har over flere omgange modtaget dele af det datamateriale, som svensk politi har til sin rådighed. Herefter er dette datamateriale blevet overdraget til Center for Cybersikkerhed til brug for centerets it-sikkerhedsmæssige undersøgelse af sagen. Center for Cybersikkerhed og PET har således udelukkende haft adgang til at undersøge en delmængde af det fulde datamateriale, som er i svensk politis varetægt.

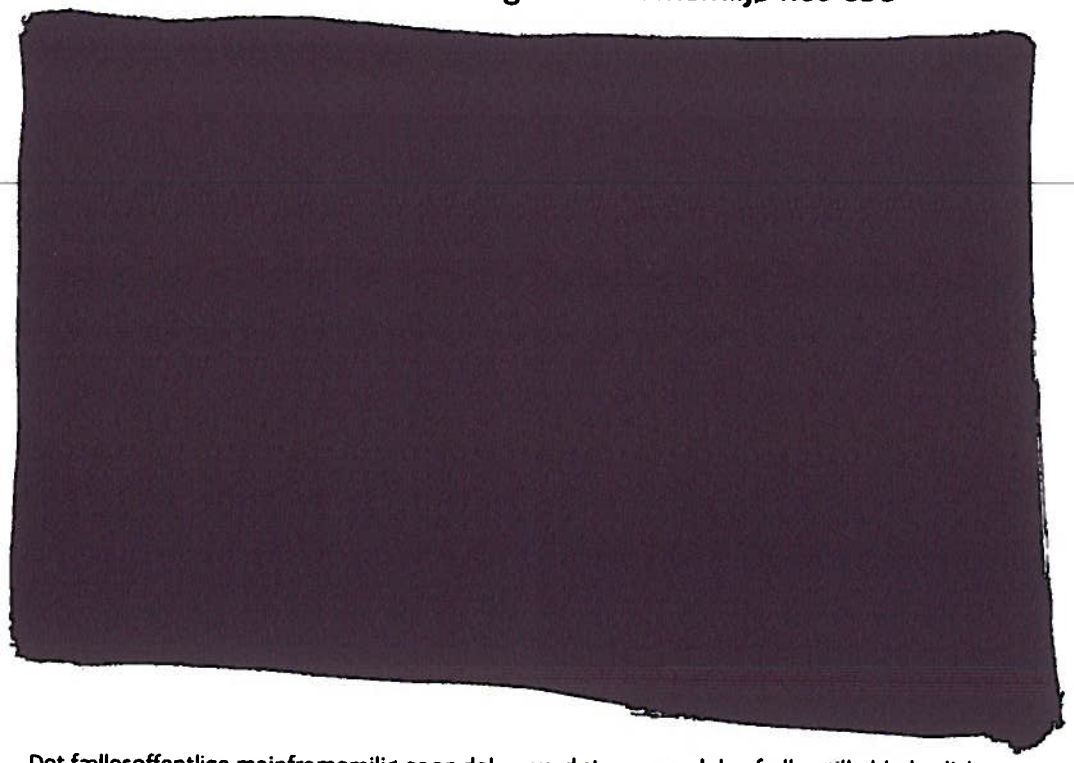
Det modtagne datamateriale har været af så stort et omfang, at Center for Cybersikkerhed og PET har været nødsaget til at prioritere de it-sikkerhedstekniske undersøgelser ud fra en væsentlighedsvurdering. Konkret har Center for Cybersikkerhed modtaget data svarende til et tocifret antal terabyte, hvilket i A4-papir svarer til en stak, der minimum kan nå fra jorden til månen og tilbage igen. Desuden har dele af datamaterialet været krypteret, således at adgang har været vanskeliggjort. Slutteligt har de it-sikkerhedstekniske analyser været besværliggjort af, at dele af kompromitteringen ikke blev logget. Det har således ikke været muligt at skabe et komplet overblik over kompromitteringen.

Derfor mangler Center for Cybersikkerhed og PET potentielt væsentlige informationer, som kunne bidrage til yderligere belysning af sikkerhedskompromitteringen. Det er alligevel Center for Cybersikkerhed og PET's vurdering, at det er mindre sandsynligt, at adgang til de manglende informationer ville ændre væsentligt på rapportens konklusioner, da en meget stor og meget væsentlig del af kompromitteringen har kunnet klarlægges.

3.2. Materiale indsamlet hos CSC

Det materiale, der er indsamlet hos CSC – både af PET, Center for Cybersikkerhed og PwC – stammer fra interview med CSC-medarbejdere og udskrifter fra CSC's systemer. Medarbejdere fra PET, Center for Cybersikkerhed eller PwC har således ikke på noget tidspunkt haft direkte adgang til CSC's systemer. Det bemærkes, at CSC har bidraget aktivt til undersøgelsen og udleveret det efterspurgte materiale.

3.3. Beskrivelse af det fællesoffentlige mainframemiljø hos CSC



Det fællesoffentlige mainframemiljø er en del af et større mainframemiljø hos CSC. Det er placeret på flere lokationer og omfatter flere servere, hvis regnekraft, lagerkapacitet m.m. deles af mange it-systemer og brugere. Mainframemiljøet består af maskinel fra IBM og anvender i hovedsagen styresystemet z/OS, der ligeledes er fra IBM.

CSC's mainframemiljø består af flere logiske partitioner (LPAR), der hver især fungerer som en selvstændig virtual maskine, hvorpå der bl.a. afvikles selvstændigt styresystem, applikationer og databaser.

Det berørte fællesoffentlige mainframemiljø hos CSC består af [redacted] der indeholder it-systemer og data fra Rigspolitiet, SKAT, CPR-kontoret og Moderniseringsstyrelsen. De [redacted] er sammenkoblet på tværs via forskellige net værkstyper og deler fælles tilkoblede diske, hvor det er muligt for dem at dele data. Det bemærkes, at [redacted] ikke eksisterede på gerningstidspunktet.

Det fællesoffentlige mainframemiljø indeholder data fra bl.a. Kørekortregisteret, Schengen Information Systemet, CPR-registret, Statens Lønsystem og en række systemer fra SKAT.

Det fællesoffentlige mainframemiljø deler et fælles sikkerhedssystem, RACF, som er en database, der deles og tilgås af de fem virtuelle maskiner. Se faktaboks på side 9.

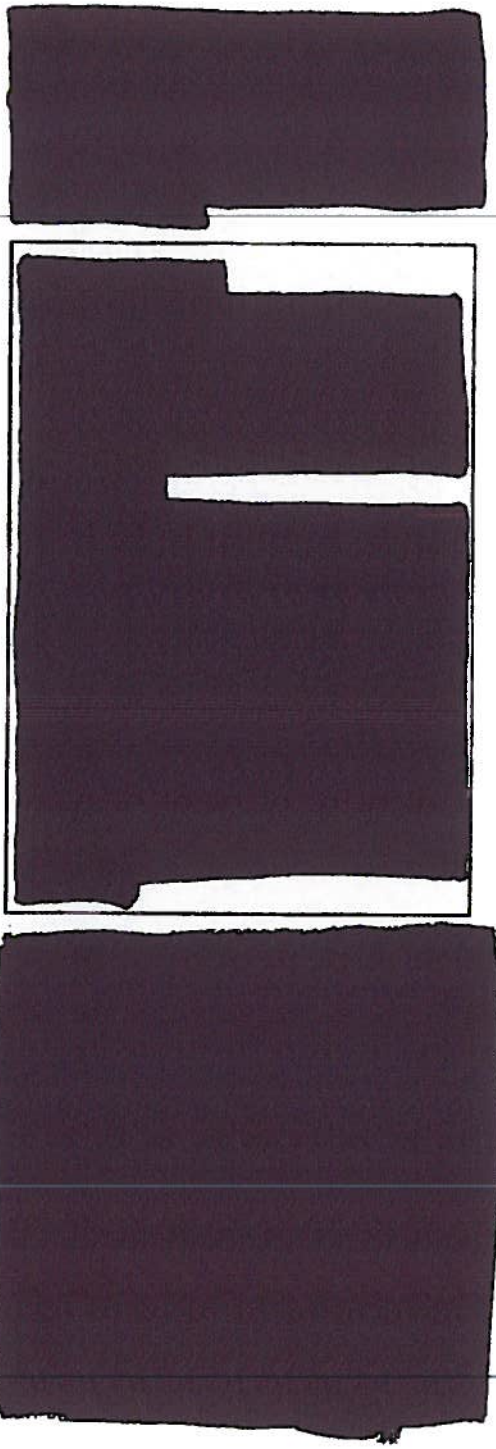
Et antal LPAR er forbundet til internettet. På [redacted] er installeret flere webservere, der giver de offentlige myndigheders brugere af it-systemerne mulighed for tilgå og anvende disse fra internettet.

4. BESKRIVELSE AF KOMPROMITTERINGEN

Dansk politi underrettede i februar 2013 CSC om, at dele af deres mainframemiljø var kompromitteret. Hverken CSC eller de øvrige danske myndigheder, der anvendte mainframemiljøet, var forud for orienteringen fra svensk politi opmærksom på, at mainframemiljøet var blevet kompromitteret. CSC fik efter anbefaling fra politiet efterfølgende udarbejdet en konsulentrapport fra det svenske rådgivningsfirma Robert Malmgren AB (Romab) vedrørende hændelsesforløbet og omfanget af kompromitteringen, ligesom CSC selv udarbejdede en rapport om hændelsen. CSC modtog i foråret 2013 Romab-rapporten til kommentering, mens Center for Cybersikkerhed modtog rapporten i juni 2013. Rapporten konkluderede, at et mainframemiljø hos CSC i perioden fra april 2012 til august 2012 var blevet kompromitteret fra internettet. Ifølge rapporten var det sket ved, at angriberen udnyttede sårbarheder i en webserver installeret i [redacted] i mainframemiljøet. Efter at være brudt ind i mainframemiljøet opnåede angriberen systemadministratorrettigheder ved at udnytte andre sårbarheder.

Center for Cybersikkerhed og PET's gennemgang af de logfiler, der har været til rådighed, viser de første tegn på rekognosceringsaktivitet fra angriberen den 11. februar 2012. Fra forskellige IP-adresser i flere lande undersøgte angriberen dele af CSC's infrastruktur, der var tilgængelig via internettet, før selve angrebet blev sat ind.

På angriberens it-udstyr, som er i det svenske politis varetægt, blev der fundet logfiler, som har gjort det muligt at rekonstruere dele af angrebsaktiviteterne. Ifølge CSC's egne undersøgelser viste de fundne logfiler, at der blev overført store mængder data til servere i tre lande. Ifølge oplysninger fra CSC ophørte aktiviteterne den 27. august 2012.



[redacted]

Resource Access Control Facility (RACF)
For at styre adgangen til data og systemer på mainframen er der implementeret en Resource Access Control Facility (RACF) fra IBM. RACF er en database, der indeholder alle oplysninger om brugernavn, password og de enkelte brugeres og systemers rettigheder. RACF styrer brugere og andre systemers adgang. Hvis et system skal hente data i en database eller anvende en proces i et andet system, skal systemet tildeles passende rettigheder ligesom en bruger. Rettighederne vedligeholdes af systemadministratorer, der har et udvidet sæt rettigheder, som indebærer, at systemadministratorer kan oprette, nedlægge samt ændre brugere og systemers rettigheder.

[redacted]

Som følge af angriberens mulighed for at omgå logning, er det ikke muligt at give et komplet overblik over, hvilke data, der med sikkerhed er kopieret fra mainframemiljøet. Center for Cybersikkerhed og PET kan dog fastslå, at i hvert fald store mængder data tilhørende politiet er blevet kopieret fra CSC's systemer.

På grund af den verserende efterforskning kan Center for Cybersikkerhed og PET ikke gå i detaljer med, hvilke data, der uretmæssigt er kopieret, eller hvilket motiv, der ligger bag kompromitteringen. Center for Cybersikkerhed og PET kan dog overordnet konkludere, at det som minimum drejer sig om data fra Kørekortregistret, politiets registre, der indeholder oplysninger fra CPR- og CVR-registre-

ne om personer og virksomheder i Danmark, Schengen Information Systemet og registret for Efterlyste Køretøjer. På baggrund af de foretagende undersøgelser vurderer Center for Cybersikkerhed og PET, at alle data er kopieret fra politiets systemer på det fælles offentlige mainframemiljø.

Center for Cybersikkerhed og PET anser det ikke for sandsynligt, at [redacted] er kompromitteret, da hverken Center for Cybersikkerhed eller PET har fundet indikationer herpå i de analyserede data fra henholdsvis svensk politi og CSC.

4.1. Kompromittering af data på HSM

[redacted]

4.2. Validering af dataintegritet i det fællesoffentlige mainframemiljø

Angriberens adgang til myndighedernes data hos CSC gav potentielt angriberen adgang til at ændre i, tilføje eller slette data. Den mulige kompromittering af dataintegriteten foranledigede Center for Cybersikkerhed og PET til at opfordre de myndigheder, der havde data på de berørte systemer, til at sætte undersøgelser i gang for at validere, om data var blevet ændret i forbindelse med kompromitteringen.

Myndighederne anvendte flere forskellige metoder til at gennemføre valideringerne. En metode, der blev anvendt, var at sammenligne sikkerhedskopier taget før kompromitteringen startende med de aktuelle data på systemerne. Denne metode var dog ikke i alle tilfælde tilstrækkelig, idet data i de fleste systemer er meget dynamiske, men den gav en indikation af, om mængden af data var uændret. Desuden har myndighederne foretaget stikprøvevise udtræk af data, der er blevet gennemgået med henblik på at bedømme validiteten.

Derudover blev også tekniske valideringsmekanismer, f.eks. monitorering af pludselige eller abnorme ændringer i mængder, indhold eller værdier af data, implementeret i nogle systemer. Derigennem ville systemerne generere alarmer ved anormalitet.

Endelig har myndighederne overfor Center for Cybersikkerhed og PET oplyst, at de har været særligt opmærksomme på fejlrapporteringer fra borgere, samarbejdspartnere og kunder, og at de ikke har kunnet konstatere ændringerne i antallet af fejl i data rapporteret af brugere eller andre berørte parter.

De myndigheder, der var berørt af angrebet mod CSC, har overfor Center for Cybersikkerhed og PET sammenfattende oplyst, at de ikke har fundet indikationer på, at sikkerhedskompromitteringen havde konsekvenser for integriteten af de myndighedsdata, der befandt sig i det fællesoffentlige mainframemiljø.

På baggrund af myndighedernes gennemgang vurderer Center for Cybersikkerhed og PET, at det ikke er sandsynligt, at dataintegriteten hos de berørte myndigheder er kompromitteret. Samtidig bemærker Center for Cybersikkerhed og PET dog, at enkeltstående dataændringer i store databaser kan være særdeles svære at detektere.

5. OPFØLGNING PÅ CENTER FOR CYBERSIKKERHEDS ANBEFALINGER

I en foreløbig rapport om sikkerhedsbruddet hos CSC fra juli 2013 gav Center for Cybersikkerhed en række anbefalinger til de berørte offentlige myndigheder og CSC om tiltag, der kunne implementeres hurtigt, og som vurderedes at kunne føre til en mærkbar forbedring af informationssikkerhedsniveauet i det fællesoffentlige mainframemiljø.

Det er Center for Cybersikkerhed og PET's vurdering, at de berørte myndigheder i vid udstrækning har fulgt op på centerets anbefalinger. De berørte myndigheder, der anvender det fællesoffentlige mainframemiljø, har alle foretaget en konsekvensvurdering samt et dataintegritetscheck som anbefalet af Center for Cybersikkerhed i den foreløbige rapport fra juli 2013.

Center for Cybersikkerheds foreløbige anbefalinger til forbedring af informationssikkerhedsniveauet i det fællesoffentlige mainframemiljø rettede sig også mod CSC. CSC's opfølgning på og implementering af disse indgår som en væsentlig del af grundlaget for PwC's analyse af og konklusioner om sikkerhedsniveauet i det fællesoffentlige mainframemiljø, der behandles i det følgende afsnit.

6. PwC'S ANALYSE AF DET FÆLLESOFFENTLIGE MAINFRAMEMILJØ HOS CSC (UDARBEJDET I NOVEMBER 2013)

Som følge af sikkerhedskompromitteringen blev Center for Cybersikkerhed som national it-sikkerhedsmyndighed anmodet om at stå i spidsen for en analyse af informationssikkerhedsniveauet i det fællesoffentlige mainframemiljø hos CSC.

Gennem interview med medarbejdere fra CSC og analyse af materiale fra CSC og politiet har Cen-ter for Cybersikkerhed fået grundlag for at vurdere dele af informationssikkerhedsniveauet i det fællesoffentlige mainframemiljø. Desuden har Center for Cybersikkerhed efter aftale med CSC anmodet revisionsfirmaet PwC om at gennemgå de tiltag, som CSC har foretaget og påtænker at foretage med henblik på at styrke informationssikkerheden i det fællesoffentlige mainframemiljø. PwC's gennemgang, der fandt sted i efteråret 2013, danner grundlag for Center for Cybersikkerheds og PET's vurdering af, om sikkerhedsniveauet hos CSC kan anses for at være betryggende.

PwC's arbejde er primært foretaget ved interview med medarbejdere fra CSC samt stikprøvevis vurdering af konfigurationsudtræk fra de [redacted] På den baggrund har PwC udarbejdet en rapport, der beskriver det fællesoffentlige mainframemiljø hos CSC primo november 2013. Rapportens oversigt over CSC's plan for håndtering af sikkerhedsbrudene er optaget som bilag til denne rapport.

Formålet har været at gennemføre en uafhængig test af, om sikkerheden vedrørende de offentlige myndigheders mainframemiljø hos CSC er tilrettelagt og implementeret på en hensigtsmæssig måde primo november 2013. Det er ledelsen hos de offentlige myndigheder, der i samarbejde med CSC har ansvaret for at sikre tilrettelæggelse af et betryggende niveau.

På grund af begrænsninger i ethvert kontrolsystem kan der opstå fejl eller besvigelser, som ikke afdækkes af analysen. Endvidere vil en anvendelse af resultatet af analysen på efterfølgende perioders transaktioner være undergivet en risiko for, at der foretages ændringer af systemer eller kontroller, hvorved resultatet muligvis ikke længere vil være gældende.

Det bemærkes, at analysen ikke er udtryk for en revision eller et review i overensstemmelse med danske revisionsstandarder, og gennemgangen er udelukkende gennemført med det formål at foretage en vurdering af, om sikkerheden i relation til de [redacted] er på et betryggende niveau.

6.1. Informationssikkerhedsmæssige tiltag hos CSC

Efter CSC blev opmærksom på sikkerhedskompromitteringen, blev der gennemført en række it-sikkerhedsmæssige tiltag, som omfatter både procesmæssige og tekniske forhold. PwC har gennem interview med medarbejdere fra CSC samt stikprøvevis vurdering af systemkonfiguration vurderet relevansen og styrken af de sikkerhedsmæssige tiltag.

PwC har ved deres gennemgang opdelt de sikkerhedsmæssige tiltag således: Tiltag, der afdækker meget betydelige svagheder (prioritet 1), tiltag, der afdækker betydelige svagheder (prioritet 2), og tiltag, der afdækker en svaghed (prioritet 3). I nedenstående gennemgang er der fokuseret på prioritet 1 og 2.

6.1.1. Gennemførte sikkerhedstiltag hos CSC

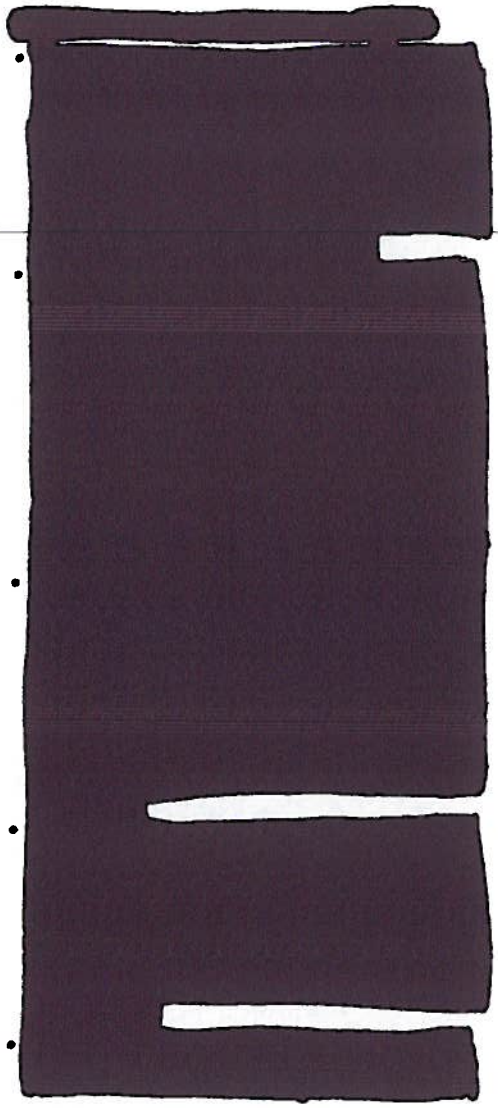
Efter CSC blev opmærksom på sikkerhedsbruddet, er der gennemført en række sikkerhedsmæssige tiltag i relation til de områder, som er omfattet af PwC's gennemgang. PwC har af CSC fået oplyst, at de gennemførte sikkerhedstiltag pr. november 2013 omfatter:

[redacted]

6.1.2. Planlagte og delvist gennemførte sikkerhedstiltag hos CSC

I tilknytning til ovenstående sikkerhedstiltag, der efter det til PwC oplyste allerede er gennemført, har PwC på møder med CSC fået oplyst, at nedenstående sikkerhedstiltag pr. november 2013 er planlagte eller delvist gennemførte:

[redacted]



Sammenfatning af planlagte og delvist gennemførte sikkerhedstiltag hos CSC

CSC har oplyst, at der er sikkerhedstiltag, som er planlagt og delvist gennemførte. De ikke-gennemførte sikkerhedstiltag er primært af teknisk karakter og indeholder to tiltag, som PwC anser for at kunne afdække en meget betydelig svaghed (prioritet 1).

PwC bemærker hertil, at selv om grunden til, at sikkerhedstiltag er forsinket eller hindret i deres implementering i en række tilfælde kan henføres til vanskeligheder med koordination med kunderne, er de ikke-afdækkede risici på undersøgelsestidspunktet [primo november 2013] væsentlige, og implementeringen bør derfor efter PwC's opfattelse færdiggøres snarest muligt.

PwC sammenfatter CSC's tiltag således:
"Med de gennemførte sikkerhedstiltag er det forsøgt på hensigtsmæssig måde at etablere et sikkert udgangspunkt for den fortsatte drift, forstærke den aktive sikkerhed samt i forøget omfang at muliggøre løbende opfølgning på sikkerhedsmæssige hændelser. Styrken af de enkelte sikkerhedsmæssige tiltag, der er gennemført, vurderes tillige at være relevant."

"Det er vores opfattelse, at de gennemførte sikkerhedstiltag er korrekt tidsmæssigt prioriteret, idet seks af de otte tiltag, som vi har anset for de mest væsentlige (prioritet 1) alle er gennemført. Vi skal dog samtidig bemærke, at det har taget forholdsvis lang tid at få en række af disse implementeret, og at der stadig er en række udestående tiltag."
(November 2013)

CSC har efterfølgende oplyst til Center for Cybersikkerhed og PET, at alle sikkerhedstiltag med prioritet 1 er gennemført, og at der på tidspunktet for udarbejdelsen af nærværende rapport kun er ét sikkerhedstiltag med prioritet 2, der ikke er implementeret. CSC afventer yderligere dialog med kunderne, før det sidste sikkerhedstiltag med prioritet 2 kan betragtes som gennemført, hvilket forventes at kunne ske i indeværende år.

6.1.3. Yderligere væsentlige sikkerhedsmæssige forbedringspotentialer

PwC påpeger også, at der er et væsentligt potentiale for forbedringer i relation til sikkerheden indenfor en række områder. En del af disse forbedringer vil kræve, at den tilhø-

rende ydelse bliver rekvireret af kunden, og at kunden deltager aktivt i sikkerhedsarbejdet.

6.2. PwC's konklusion vedr. informationssikkerhedsniveauet hos CSC

Det er PwC's vurdering november 2013, at der hos CSC er ydet en væsentlig indsats for at modvirke, at det fællesoffentlige mainframemiljø igen kan udsættes for en sikkerhedskompromittering i lighed med den, der fandt sted i perioden april til august 2012. CSC's indsats er gennemført efter en relevant prioritering, men er endnu ikke tilendebragt, hvorfor der fortsat er sikkerhedsmæssige forbedringsmuligheder.

PwC har ikke under sin gennemgang fået kendskab til forhold, der efter PwC's opfattelse udgør meget væsentlige it-risici, der ikke er tilstrækkeligt afdækkede, eller som enkeltvis bevirker, at sikkerheden på det offentlige

mainframemiljø ikke kan betragtes som betryggende.

Det er imidlertid PwC's vurdering, at der på sigt er et væsentligt potentiale for forbedringer i relation til sikkerheden inden for en række områder. En del af disse forbedringer vil kræve, at den tilhørende ydelse bliver rekvireret af kunden, og at kunden deltager aktivt i sikkerhedsarbejdet.

7. KONKLUSION

Center for Cybersikkerhed og PET modtog PwC's rapport i november 2013, og har efterfølgende foretaget en række analyser med det formål at opnå en større forståelse af sammenhængen mellem kompromitteringen, de udnyttede sårbarheder og det nuværende sikkerhedsniveau hos CSC. På det grundlag betragter Center for Cybersikkerhed og PET angrebet mod det fællesoffentlige mainframemiljø hos CSC som et af de hidtil alvorligste angreb mod it-systemer i Danmark. Center for Cybersikkerhed og PET kan konkludere, at der var tale om en omfattende og alvorlig kompromitteringen af politiet, CPR-kontoret, SKAT og Moderniseringsstyrelsens it-systemer i det fællesoffentlige mainframemiljø hos CSC, da angriberen havde mulighed for at tilgå, kopiere, slette og ændre i myndighedernes data.

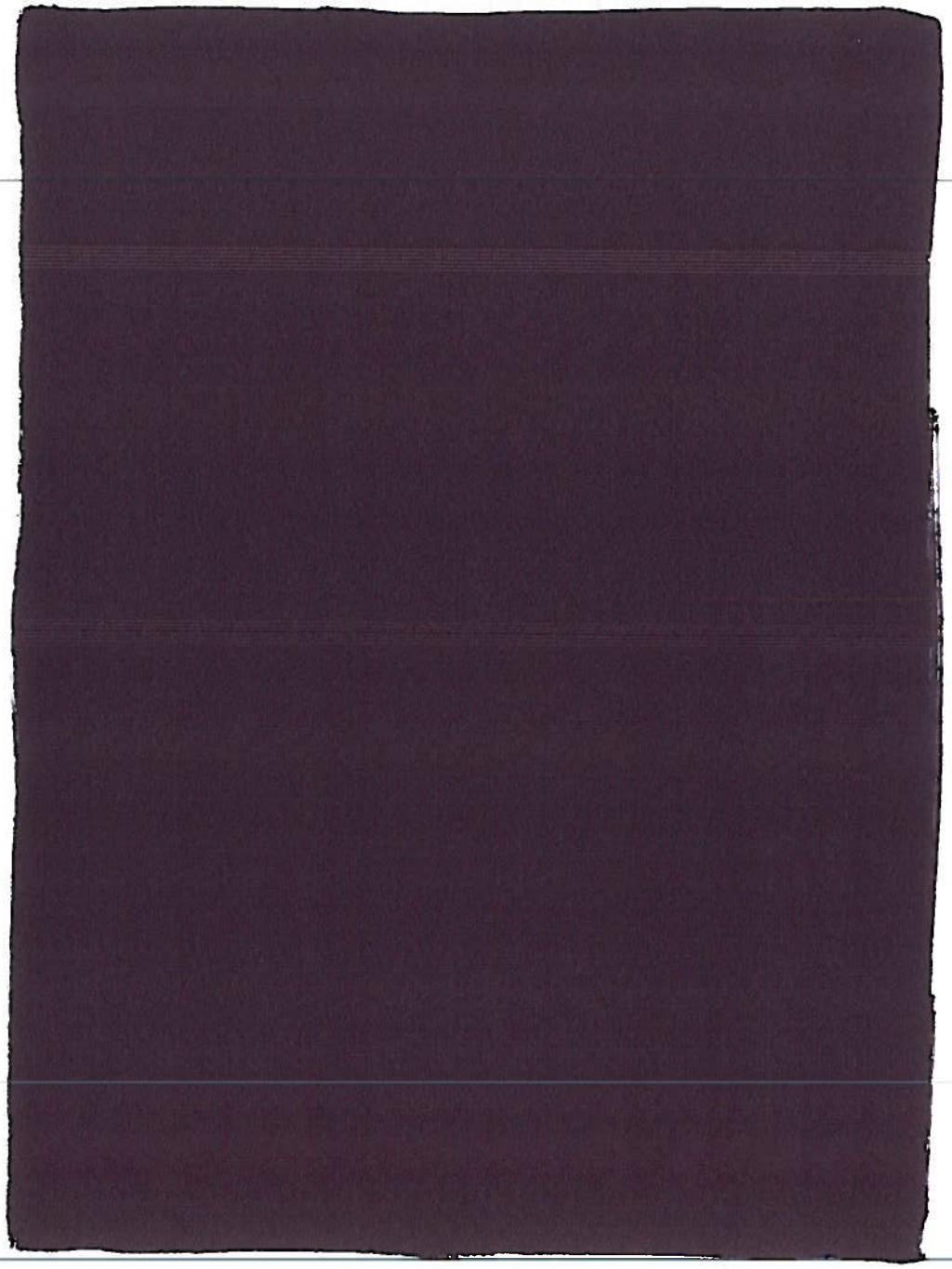
Center for Cybersikkerhed og PET anerkender, at CSC har gennemført en række relevante informationssikkerhedstiltag, der styrker informationssikkerheden i det fællesoffentlige mainframemiljø. CSC har oplyst, at alle højt prioriterede sikkerhedstiltag er gennemført, og at der på tidspunktet for udarbejdelsen af denne rapport kun er ét sikkerhedstiltag af lavere prioritet, der ikke er implementeret. CSC afventer yderligere dialog med kunderne, før det sidste sikkerhedstiltag kan betragtes som gennemført. Tiltagene tager bl.a. hånd om de foreløbige anbefalinger til forbedring af informationssikkerhedsniveauet i det fælles offentlige mainframemiljø, som Center for Cybersikkerhed identificerede i den foreløbige rapport om sikkerhedsbruddet hos CSC fra juli 2013. De identificerede og udnyttede sårbarheder i det fællesoffentlige mainframemiljø er ifølge CSC fjernet, men Center for Cybersikkerhed og PET kan ikke udelukke, at andre sårbarheder vil kunne udnyttes ved et nyt angreb. Det ændrer imidlertid ikke på, at Center for Cybersikkerhed og PET på baggrund af PwC's analyse vurderer, at informationssikkerheden i det fællesoffentlige mainframemiljø hos CSC er væsentligt forbedret.

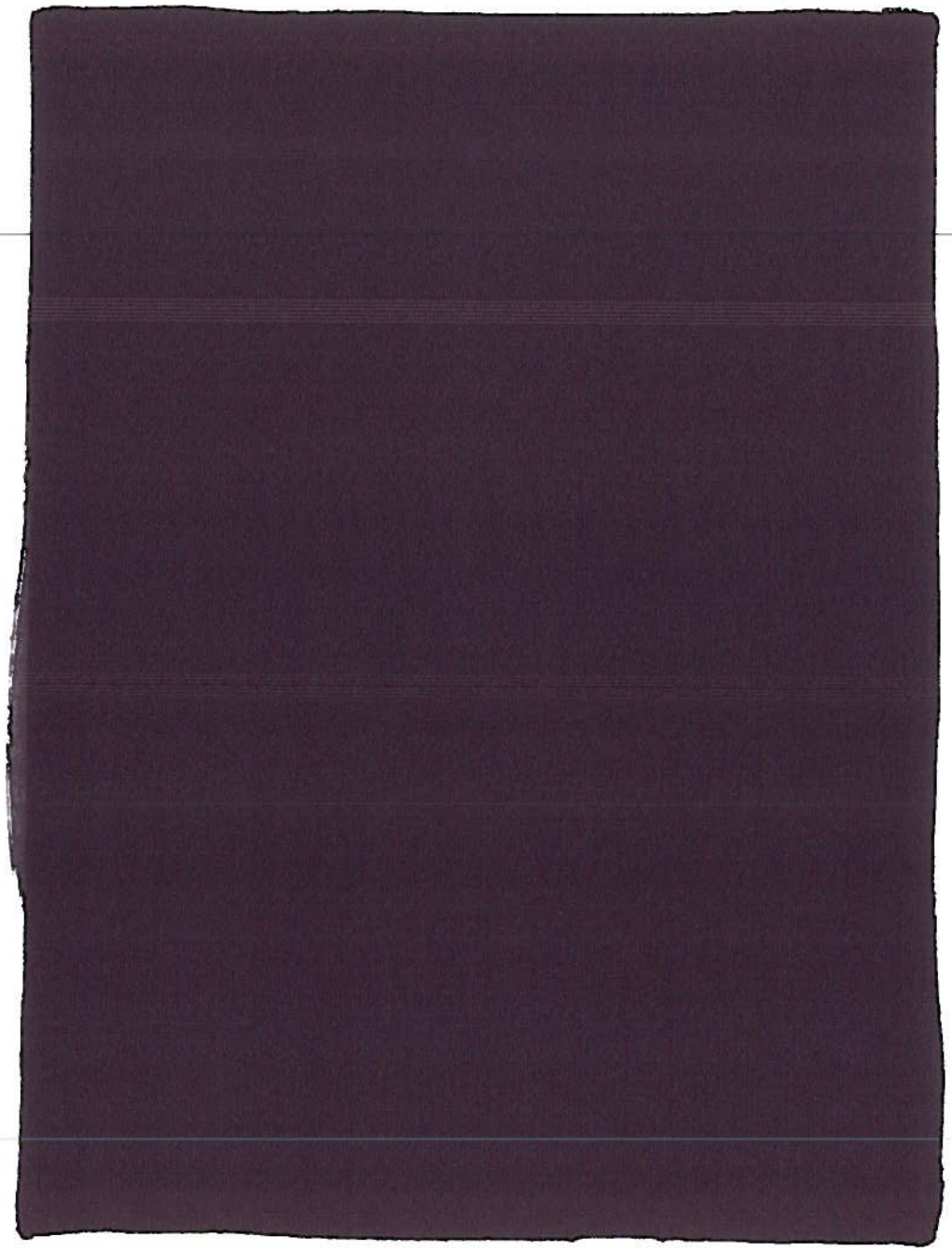
Center for Cybersikkerhed og PET bemærker, at der fortsat eksisterer informationssikkerhedsmæssige forbedringspotentialer i forhold til det fællesoffentlige mainframemiljø, og der bør derfor iværksættes yderligere en række informationssikkerhedstekniske tiltag på både serviceudbyder- og kundesiden. Center for Cybersikkerhed og PET vil fortsat være i tæt dialog med de berørte myndigheder og CSC vedrørende implementering af disse tiltag.

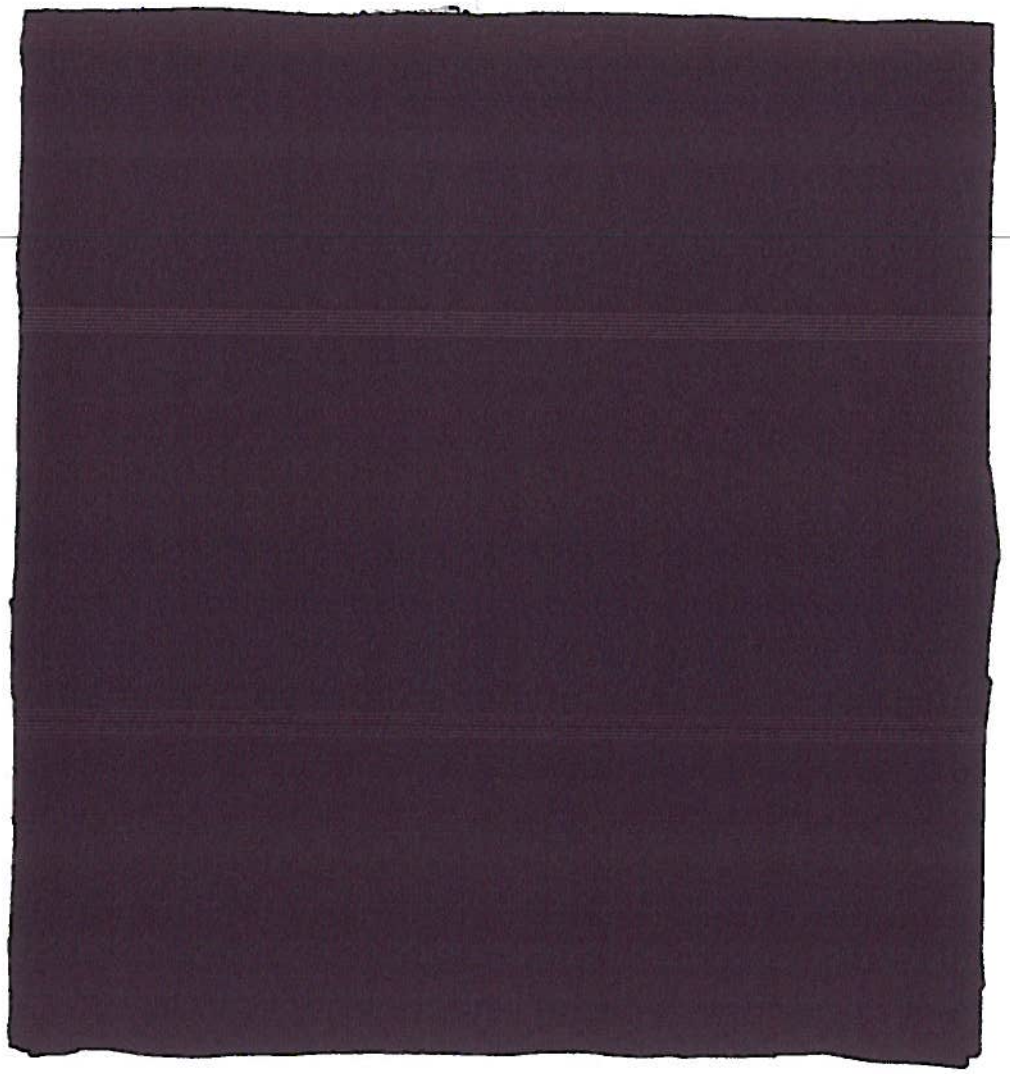
Afslutningsvis skal Center for Cybersikkerhed og PET understrege, at de udnyttede sårbarheder ikke er begrænset til det fællesoffentlige mainframemiljø hos CSC. Tilsvarende systemer fra IBM med samme opsætning og softwareversioner er potentielt sårbare over for den samme type kompromittering og kan, såfremt de ikke er blevet sikkerhedsopdaterede, stadig være sårbare for den samme type angreb. Det illustreres af, at Center for Cybersikkerhed og PET har kendskab til mindst to vellykkede kompromitteringer af andre virksomheder end CSC, hvor de samme sårbarheder blev udnyttet. Det drejer sig om kompromitteringer af Nordea i sommeren 2012 og af det svenske firma Logica i vinteren 2011-2012. I forlængelse heraf forventer Center for Cybersikkerhed i 2014 at udgive en vejledning, der giver en række konkrete anbefalinger om, hvordan myndigheder og virksomheder kan styrke informationssikkerheden i mainframeinstallationer. Dermed kan risikoen for gentagelse af hackerangreb med den samme modus operandi, der tidligere har været anvendt ved hackerangreb mod mainframeinstallationer i Danmark og Sverige, reduceres.

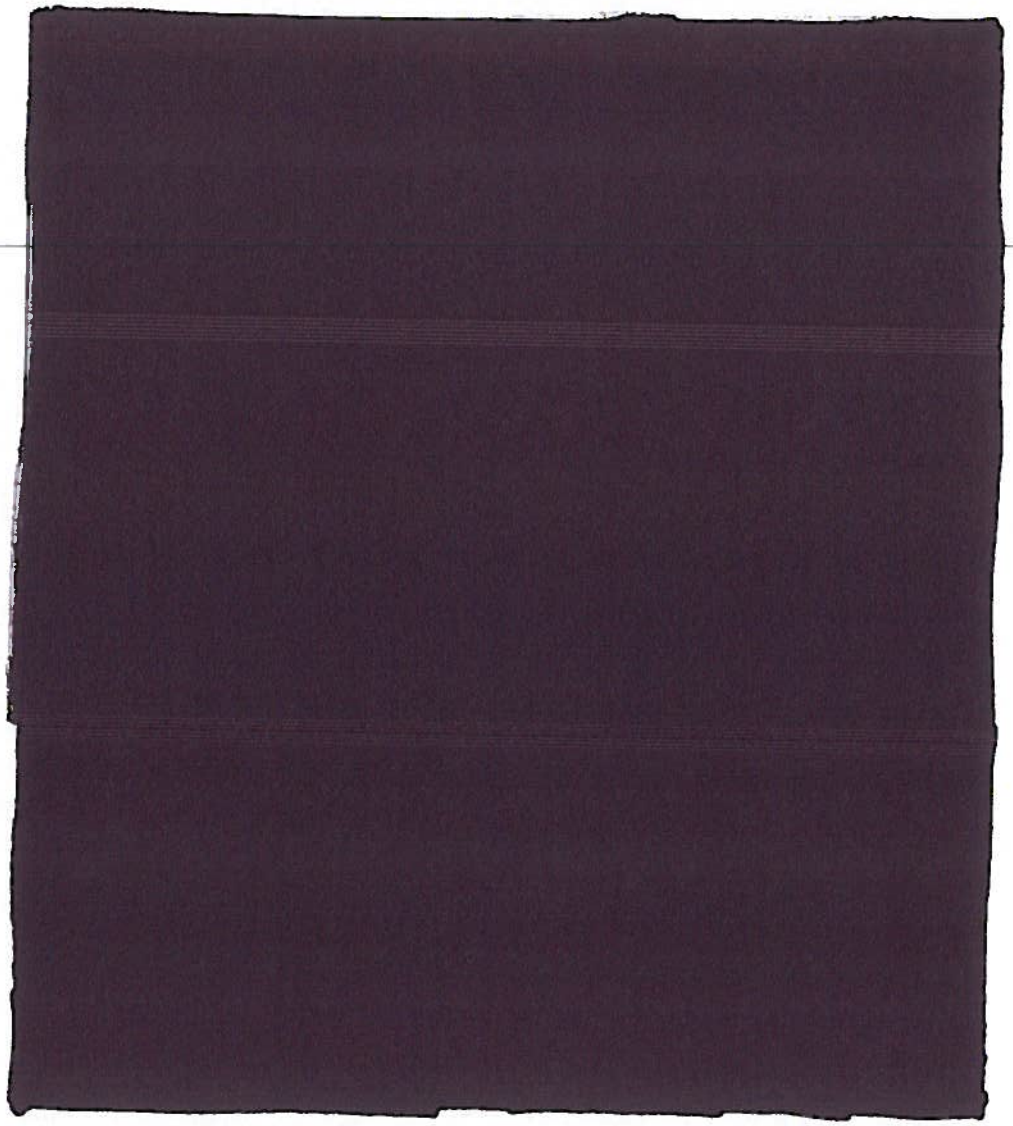
8. BILAG 1. PWC-RAPPORTENS OVERSIGT OVER CSC'S PLAN FOR HÅNDTERING AF SIKKERHEDSBRUDDENE

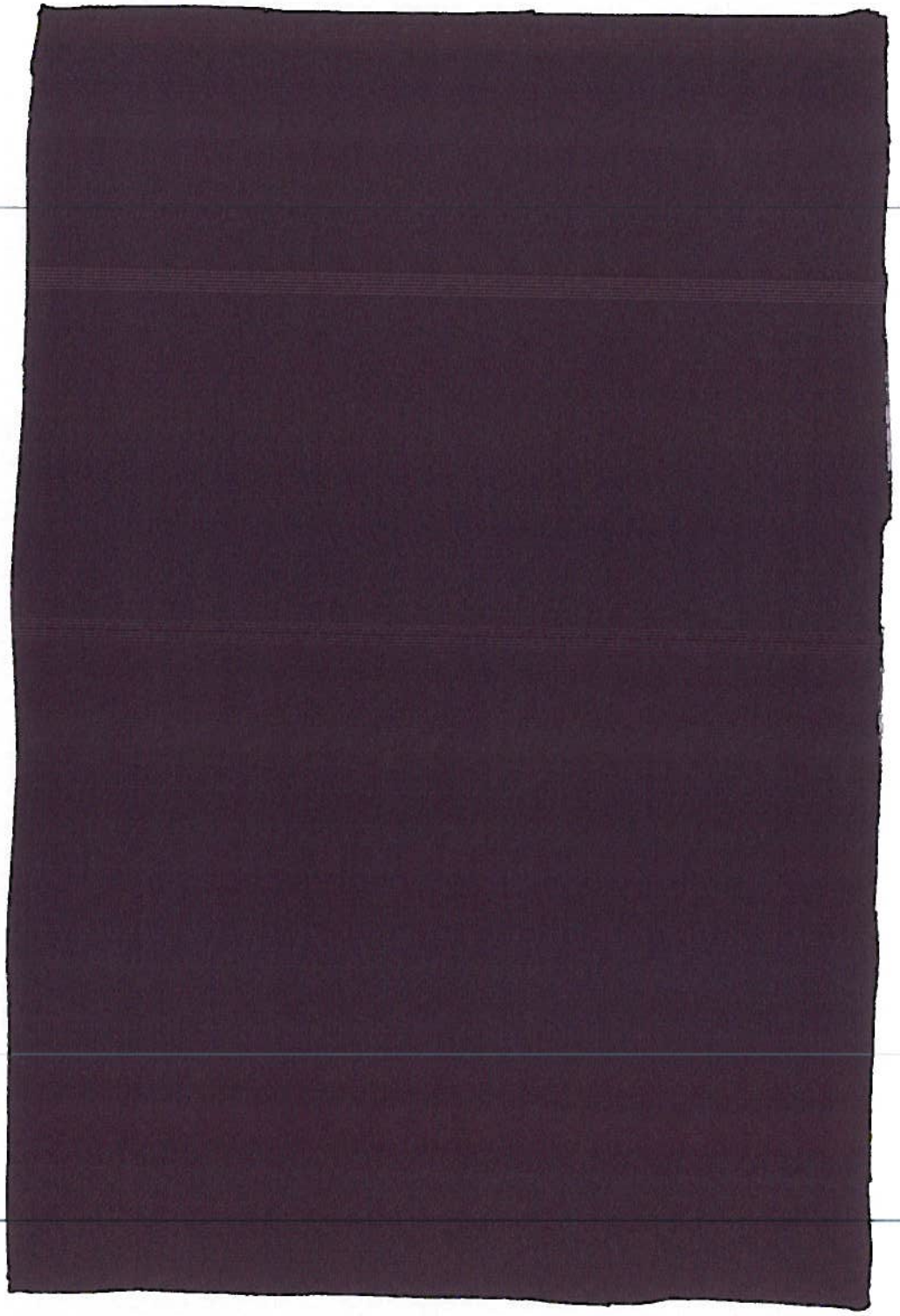
Status primo december 2013 på CSC's plan for håndtering af sikkerhedsbrud

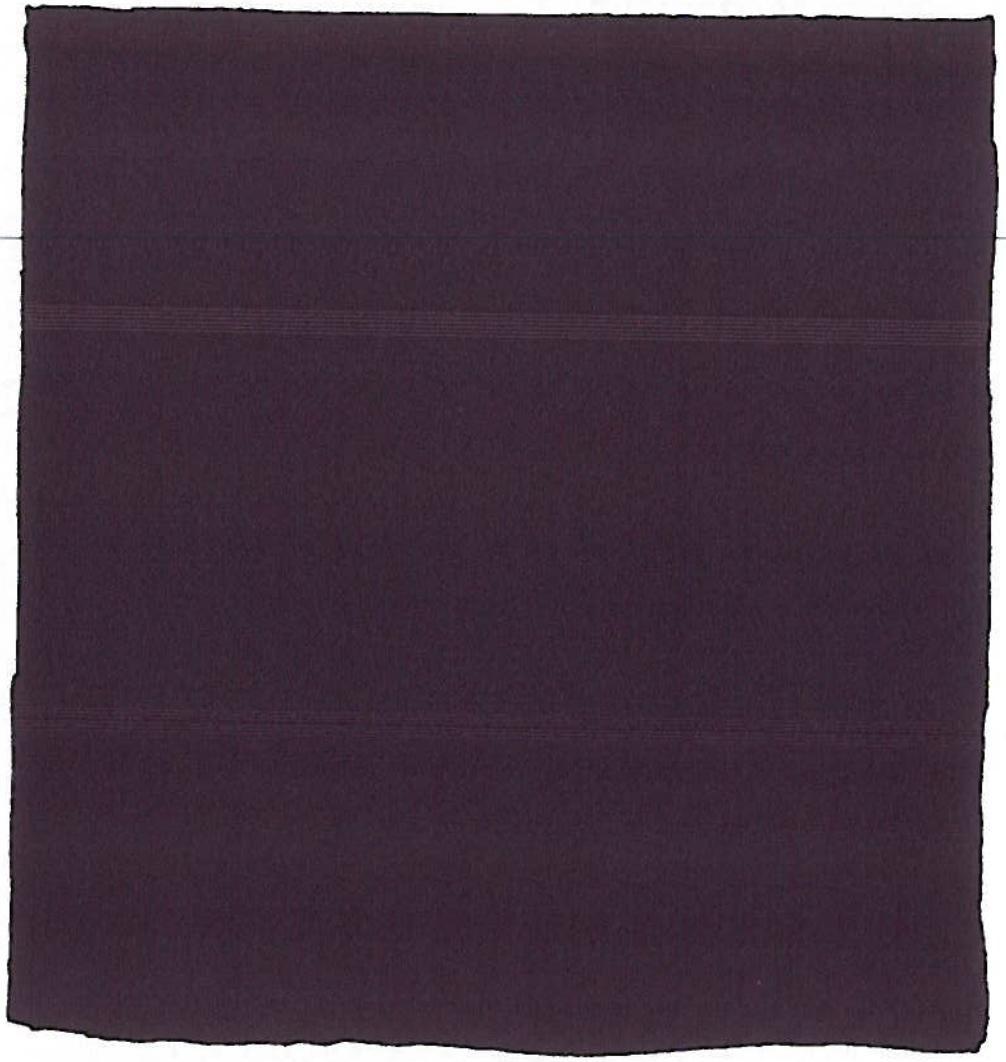












9. BILAG 2. PET'S ANBEFALINGER TIL DANSK POLITI OG JUSTITS-MINISTERIET I FORBINDELSE MED HACKERANGREBET PÅ POLITIETS SYSTEMER HOS CSC

POLITIETS EFTERRETNINGSTJENESTE
DANISH SECURITY AND INTELLIGENCE SERVICE

Dato: 12.06.2014
Jour Nr. 0402-03-1

Bilag 2. PET's anbefalinger til Dansk Politi og Justitsministeriet i forbindelse med hackerangrebet på politiets systemer hos CSC

1. Indledning

Politiets Efterretningstjeneste (PET) afgav den 19. juli 2013 en indledende rapport om hackerangrebet på politiets systemer hos CSC. Rapporten indeholdte en række indledende anbefalinger rettet mod at forbedre sikkerheden for politiets systemer. I forlængelse af rapporten af 19. juli 2013 samt nærværende rapport følger nedenfor PET's anbefalinger til forbedring af sikkerheden for politiets systemer. Anbefalingerne vedrører forhold af betydning i relationen mellem kunde (politiet) og driftsleverandør af IT-ydelser, forhold vedrørende separation af systemer, forhold vedrørende indgåelse af kontrakter og driftsaftaler, forhold vedrørende systemkompleksitet, håndtering af sikkerhedshændelser, samt monitorering af systemer.

PET vurderer, at nedenstående anbefalinger er relevante og nødvendige i forhold til alle politiets systemer, hvorpå der håndteres følsom information og ikke blot for systemer hostet af CSC. PET vurderer endvidere, at anbefalingerne bør gennemføres snarest.

2. Relationen mellem kunde og driftsleverandør

I en situation, hvor der er indgået en IT-driftsaftale mellem politiet og en driftsleverandør, anbefaler PET, at aftalen jævnligt gennemgås med henblik på at vurdere, om de aftalte sikkerhedsforanstaltninger fortsat er tidssvarende og effektive. Aftaler bør altid gennemgås i forbindelse med systemændringer. Ansvaret for at dette sker påhviler såvel kunden som driftsleverandøren.

TIL TJENESTEBRUG

PET anbefaler, at indgåede aftaler sikrer, at politiet til enhver tid informeres om ændringer af betydning for fortrolighed, integritet eller tilgængelighed af data på politiets systemer.

PET anbefaler, at der etableres processer, som sikrer, at politiet opretholder et overblik over sikkerhedsniveau og løbende forholder sig til, om sikkerhedsniveauet er passende. Det kræver, at kunde og leverandør samarbejder og prioriterer at deltage i samarbejdet. Både kunde og leverandør skal sikre sig, at relevante kompetencer er til stede.

PET anbefaler, at det skal være muligt at ændre sikkerhedsniveauet i forhold til politiets systemer i takt med udviklingen i trusselsbilledet og uafhængigt af andre kunders kontrakter og forhold.

3. Manglende separation

Hos CSC deler de berørte kunder et fælles mainframemiljø. Det har den konsekvens, at det ikke er muligt at differentiere sikkerhedsniveauet, og dermed er den enkelte kunde henvist til et fælles sikkerhedsniveau. Behov for et differentieret sikkerhedsniveau kan opstå som følge af differentierede behov for enten fortrolighed, integritet og/eller tilgængelighed i de forskellige systemer.

Såfremt der ikke er mulighed for at differentiere sikkerhedsniveauerne, anbefaler PET, at der skabes en bedre koordination mellem myndighederne på det fælles mainframemiljø. Én myndighed må ikke ensidigt kunne træffe beslutninger, der påvirker andre myndigheders sikkerhedsniveau i negativ retning.

PET anbefaler, at systemer bliver opdelt i sikkerhedszoner, hvor der etableres sikkerhedsforanstaltninger, der svarer til risikobilledet for de pågældende systemer og data.

PET anbefaler, at politiets systemer og data evalueres for sensitivitetsniveau med henblik på at få etableret differentierede sikkerhedsniveauer for data med forskellig sensitivitet. Det bemærkes i den forbindelse, at klassificerede data udelukkende

må behandles og opbevares på dertil godkendte systemer. Arbejdet kan med fordel bygge videre på de indledende kortlægninger udført i regi af Rigspolitiets igangværende projekt SAFE.

4. Fokus på sikkerhed i forbindelse med indgåelse af kontrakter og driftsaftaler

Ved indgåelse af kontrakter og driftsaftaler mellem offentlige myndigheder og driftsleverandører sker en afvejning af hensynet til driftssikkerhed og pris mod hensynet til sikkerhed.

PET kan konstatere, at der for politiets systemer generelt har været nogen fokus på sikkerhed ved indgåelse af kontrakter.

PET anbefaler, at der ved indgåelse af kontrakter skal være styrket fokus på sikkerhed, herunder at der altid tages særskilt stilling til, hvorvidt det foreslåede sikkerhedsniveau er passende.

5. Kompleksitet af systemer

Systemer, der i dag afvikles på en mainframe, er ofte udviklet for en række år siden. Med tiden er der i mange af disse systemer foretaget større eller mindre ændringer, så kompleksiteten er blevet meget stor. Mange af systemerne er af den årsag blevet vanskelige at vedligeholde, og sikkerheden i systemerne er ikke i tilstrækkelig grad blevet revurderet undervejs.

PET anbefaler, at der udføres en gennemgang af arkitektur og processer i forhold til politiets systemer. Særligt for systemer med meget lang levetid, som f.eks. det kompromitterede mainframesystem. I denne forbindelse bør det sikres, at der løbende implementeres "best practice" for f.eks. opdateringsprocedurer, systemadskillelse, lukning af unødvendige services og processer, lukning af unødvendige IP-adresser og porte samt revision af eksisterende processer.

PET anbefaler at sikkerhedsniveauet for politiets systemer dokumenteres og verificeres helhedsorienteret i sammenhæng med alle forbundne systemer.

TIL TJENESTEBRUG

6. Håndtering af sikkerhedshændelser

PET anbefaler, at der i forbindelse med indgåelse af kontrakter og driftsaftaler stilles krav om, hvordan eventuelle sikkerhedshændelser håndteres. Det skal specificeres, hvordan ansvaret for håndtering af hændelser fordeles, hvornår hændelser rapporteres til kunden samt kriterier for eskalering af tiltag til behandling af hændelser. Aftaler om håndtering og behandling af hændelser skal revideres med jævne mellemrum og i takt med den generelle udvikling i risikobilledet.

PET anbefaler, at der sker opbygning og test af kapacitet til at håndtere sikkerhedshændelser, der berører politiets systemer, særligt for så vidt angår systemtyper, der ikke er i almen drift i det offentlige eller i det private erhvervsliv.

7. Systemmonitorering

I den konkrete sag er det konstateret, at CSC ikke har været i stand til at detektere hackerangrebet. Systemer bør altid monitoreres på en måde, så det er muligt at detektere, hvis der forekommer usædvanlig trafik eller usædvanlige trafikmønstre samt vurdere om det pågældende trafikmønster indikerer et hackerangreb.

[redacted]

TIL TJENESTEBRUG