
TJENESTEBRUG
AFKLASSIFICERET den 2013-12-13
CENTER FOR
CYBERSIKKERHED
Årsrapport for
sikkerhedsbrud hos
Juli 2013
AFKLASSIFICERET, den
TIL TJENESTEBRUG

CENTER FOR CYBERSIKKERHED

Indhold

1. Sammenfatning

Dette er den første af tre rapporter fra Center fra Cybersikkerhed, der tager udgangspunkt i angrebet mod den statslige it-leverandør CSC.

På baggrund af en foreløbig it-sikkerhedsteknisk undersøgelse af hackerangrebet mod CSC vurderer Center for Cybersikkerhed:

- At der er tale om en omfattende og alvorlig kompromitteringen af visse statslige myndigheders data hos CSC
- At hackerne har haft adgang til at tilgå, kopiere, slette og ændre i data, men det er endnu uvist, i hvilket omfang denne adgang er udnyttet
- At det endnu ikke er klart, om CSC har implementeret et passende sikkerhedsniveau i det pågældende mainframemiljø
- At der på kort sigt bør iværksættes en række it-sikkerhedstekniske tiltag, der kan styrke systemets it-sikkerhedsniveau

Center for Cybersikkerhed vil i samarbejde med relevante myndigheder indsamle og analysere yderligere materiale om kompromitteringen, således at udestående spørgsmål i størst muligt omfang kan besvares. Center for Cybersikkerhed vil på den baggrund i løbet af efteråret 2013 udarbejde en opdateret rapport omkring hackerangrebet mod CSC.

I samarbejde med Digitaliseringsstyrelsen vil Center for Cybersikkerhed inden årets udgang udarbejde en mere fremadrettet rapport med anbefalinger til, hvordan sikkerheden i forhold til offentlige it-systemer og data på baggrund af erfaringerne med den aktuelle sag kan styrkes.

2. Indledning

Den 6. juni 2013 offentliggjorde Rigspolitiet, at flere af politiets it-systemer var blevet kompromitteret ved et hackerangreb mod et mainframemiljø hos it-leverandøren CSC. Angrebet omtales som det hidtil største hackerangreb i Skandinavien.

Forsvarets Efterretningstjenestes Center for Cybersikkerhed er Danmarks nationale it-sikkerhedsmyndighed, og siden begyndelsen af juni har centret i et samarbejde med de relevante offentlige myndigheder, herunder PET, der varetager opgaven som national it-sikkerhedsmyndighed inden for Justitsministeriets ansvarsområde, arbejdet på at klarlægge omfang og eventuelle konsekvenser af kompromitteringen hos CSC.

Denne rapport er den første af tre rapporter, som Center for Cybersikkerhed forventer at udarbejde om hændelsen hos CSC. Rapporten har til formål at skabe et foreløbigt overblik over hændelsen. Rapporten bygger på de analyser, det har været muligt at foretage og på det materiale, Center for Cybersikkerhed har fået adgang til frem til den 28. juni 2013, hvor arbejdet med rapporten blev afsluttet. Målgruppen for rapporten er de berørte myndigheder inden for centrets ansvarsområde.

En opdateret udgave af denne rapport vil foreligge, når Center for Cybersikkerhed har modtaget yderligere materiale, og har haft mulighed for at analysere materialet. Målgruppen for den opdaterede rapport er ligeledes de berørte myndigheder.

Endelig vil Center for Cybersikkerhed udarbejde en rapport, der indeholder centrets overordnede anbefalinger til, hvordan sikkerheden i forhold til offentlige it-systemer og data på baggrund af erfaringerne fra den aktuelle sag kan styrkes. Denne rapport vil blive udarbejdet i samarbejde med Digitaliseringsstyrelsen m.fl.

Det bemærkes, at PET har haft rapporten til gennemgang, og at afsnit, som PET af efterforskningsmæssige hensyn har ønsket fjernet, er markeret med sort.

3. Overblik over hændelsen og Center for Cybersikkerheds indsats

3.1. Center for Cybersikkerheds indsats

Primo juni blev Center for Cybersikkerhed som national it-sikkerhedsmyndighed inddraget i den it-sikkerhedsmæssige undersøgelse af sagen om hackerangreb mod CSC med henblik på at klarlægge konsekvenser af kompromitteringen af de it-systemer, som CSC driver for CPR-kontoret, SKAT og Moderniseringsstyrelsen.

Udgangspunktet var en begrundet mistanke om, at der i en periode i 2012 havde været uautoriseret adgang til en række offentlige myndigheders følsomme data hos CSC Danmark, herunder at politiets kørekortregister og registre over efterlyste m.v. i Schengen var blevet kompromitteret, og at data var blevet kopieret fra CSC's systemer.

Center for Cybersikkerheds indledende indsats er især fokuseret på at foretage en nærmere vurdering af sikkerhedsbruddet og at sikre, at alle uautoriserede adgange til de relevante it-systemer og data hos CSC er lukket. Center for Cybersikkerhed har endvidere fokus på at belyse omfanget af kompromitteringen hos de ramte myndigheder, samt at komme med anbefalinger til sikkerhedstiltag med henblik på at styrke sikkerheden i mainframemiljøet på kort sigt.

Funktionen som national it-sikkerhedsmyndighed inden for Justitsministeriets ansvarsområde, herunder i forhold til politiet, varetages af PET, der foretager en tilsvarende undersøgelse på dette område.

Den strafferetlige efterforskning af sagen varetages af Københavns Politi i samarbejde med NITES og PET.

3.2. Overordnet beskrivelse af hændelsen

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

[redacted]

3.3. CSC's tiltag for indeværende

CSC sendte den 6. juni 2013 en kort redegørelse til CPR-kontoret under Økonomi- og Indenrigsministeriet. Denne redegørelse var et svar på CPR-kontorets forespørgsel af 5. juni 2013 til CSC om en nærmere redegørelse for sagen, herunder:

- hvilke implikationer, sårbarheden kunne have haft på CPR-registret,
- hvilke forholdsregler, CSC havde taget for at standse indbruddet, og
- hvilke tiltag, CSC ville tage som følge af hændelsen.

SKAT har oplyst, at de har modtaget en tilsvarende redegørelse.

I redegørelsen til CPR-kontoret anfører CSC følgende om sagens forløb:

> *"Den 26. februar 2013 blev CSC af det danske politi gjort opmærksom på, at IBM mainframen hos CSC som bl.a. indeholder Rigspolitiets systemer, var blevet kompromitteret i perioden februar 2012 til august 2012. CSC iværksatte øjeblikkeligt undersøgelser for at sikre beviser og for at afhjælpe trusler i tæt samarbejde med Politiet*
>
> *Efterfølgende har CSC undersøgt alle relevante logs fra systemet* [...].
>
> *Gerningsmanden benyttede en hidtil ukendt sårbarhed. Denne sårbarhed blev lukket ved hjælp af nye retningslinjer fra IBM den 10. marts 2013".*

I forhold til at minimere risikoen for tilsvarende angreb har CSC ifølge redegørelsen gjort følgende:

> *"Søgt efter yderligere spor på ulovlig indtrængen*
>
> *Øget fokus på overvågningssystemer*
> *Fordoblet den periode relevante logs gemmes i*
>
> *Yderligere har CSC planlagt følgende yderligere præventive tiltag:*

Revision af funktionsbrugere

Center for Cybersikkerhed har ikke haft mulighed for at kontrollere validiteten af disse oplysninger. Ligeledes har Center for Cybersikkerhed ikke mulighed for at vurdere, om der i dag er et passende sikkerhedsniveau hos CSC.

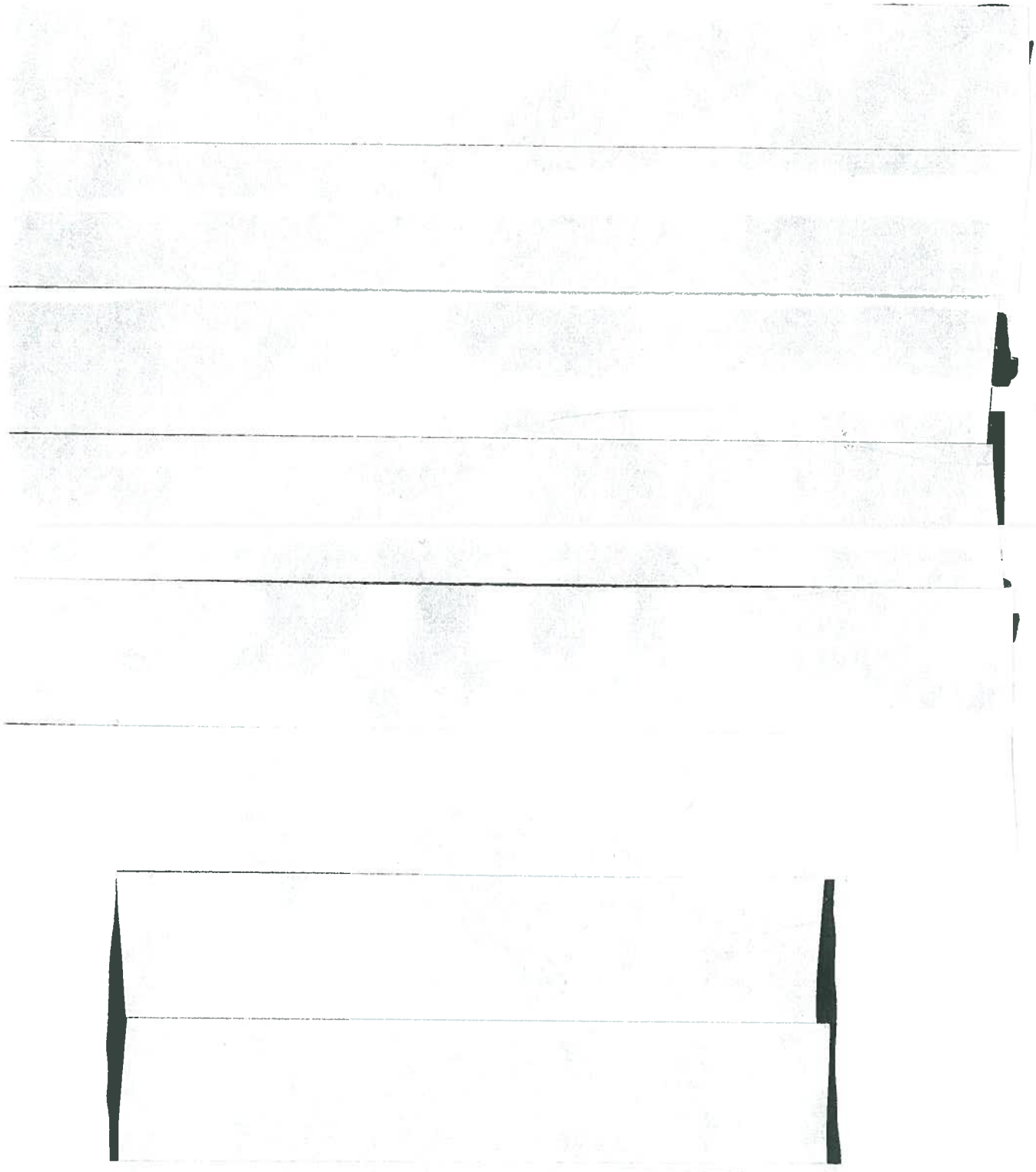
Center for Cybersikkerhed er i dialog med politiet om at sikre, at hensynet til bevissikring i forbindelse med den igangværende strafferetlige efterforskning ikke forhindrer, at der træffes de nødvendige foranstaltninger for at øge sikkerheden på de kompromitterede it-systemer hos CSC.

4. Teknisk beskrivelse af kompromitteringen

4.1. Kompromitteringen af CSC's mainframemiljø

[redacted]

[1] Se bilag 1 for en nærmere beskrivelse af system og terminologi samt figuren på næste side.



Hverken CSC eller de berørte myndigheder har været opmærksomme på kompromitteringen, før dansk politi kontaktede CSC. Ifølge CSC ophørte aktiviteten kort før den formodede hacker blev anholdt i en anden sag.

4.2. Øvrige sårbare mainframemiljøer

[redacted]

5. Data- og kildemateriale

I anledning af sagen om angrebet på CSC har Københavns Politi iværksat efterforskning, og en person er varetægtsfængslet i sagen. Efterforskningen varetages af Københavns Politi i samarbejde med Politiets Efterretningstjeneste (PET) og Rigspolitiets Nationale It-efterforskningssektion (NITES). Det er aftalt med Københavns Politi og PET, at Center for Cybersikkerhed fra PET løbende modtager materiale, der tilvejebringes fra CSC, og som indgår i efterforskningen af sagen, dog således at oplysningerne af hensyn til den verserende efterforskning ikke kan offentliggøres eller videregives til andre myndigheder uden samtykke fra PET. For at undgå kompromittering af den verserende efterforskning er det således ikke muligt i denne rapport at omtale alle de oplysninger, som Center for Cybersikkerhed er i besiddelse af.

[redacted]

Center for Cybersikkerhed har endnu ikke fra CSC fået udleveret dokumentation for, hvilke tiltag CSC har gennemført for at sikre it-systemet, eller på anden måde at validere eventuelle sikkerhedstiltag hos CSC. Center for Cybersikkerhed har derfor ikke mulighed for at be- eller afkræfte, om kompromitteringen er standset fuldstændigt eller om det aktuelle sikkerhedsniveau på CSC's mainframemiljø er passende.

På den baggrund skal det understreges, at det mangelfulde datagrundlag medfører, at Center for Cybersikkerheds vurderinger i denne rapport kun er foreløbige. Centret mangler således flere vigtige brikker, som vil kunne bidrage til mere fyldestgørende og endelige konklusioner. Center for Cybersikkerhed vil fortsat arbejde på at modtage alt relevant materiale, så det kan indgå i centrets arbejde med den opdaterede udgave af denne rapport.

6. Center for Cybersikkerheds foreløbige anbefalinger

På baggrund af kontakt til myndighederne er det centrets vurdering, at det i en række tilfælde er væsentlige it-systemer for det danske samfund, der kan være kompromitteret.

De enkelte myndigheders vurdering af en eventuel kompromittering varierer fra "ikke kritisk" til "alvorlige og vidtrækkende konsekvenser for det danske samfund".

Center for Cybersikkerhed kan med udgangspunkt i ovenstående og på baggrund af de foreløbige undersøgelser give en række foreløbige anbefalinger, til implementering på kort sigt, og som vurderes at kunne give en mærkbar forbedring af sikkerheden i de berørte it-systemer.

6.1. Konsekvensvurdering

Som national it-sikkerhedsmyndighed henstiller Center for Cybersikkerhed til, at de myndigheder, inden for centrets ansvarsområde, der er berørt af CSC-sikkerhedshændelsen, dvs. SKAT, CPR-kontoret og Moderniseringsstyrelsen hver især udarbejder en samlet konsekvensvurdering. I konsekvensvurderingen skal myndigheden vurdere, hvilke konsekvenser en kompromittering af myndighedens data kan have, både i relation til fortrolighed og integritet, samt de imagemæssige følger. På baggrund af konsekvensvurderingen kan myndigheden, under fornøden hensyntagen til lovgivningen, træffe beslutning om, hvilke forholdsregler der skal tages for at beskytte sig mod kompromittering. Da det aldrig vil være muligt at beskytte sig 100 % mod en kompromittering, skal ledelsen acceptere den restrisiko, der vil være efter beskyttelsesforanstaltningerne er implementeret.

Myndighederne bør desuden overveje en strategi for det tilfælde, at der sker brud på informationssikkerheden, herunder en kommunikationsstrategi.

6.2. Systemopdateringer

[redacted]

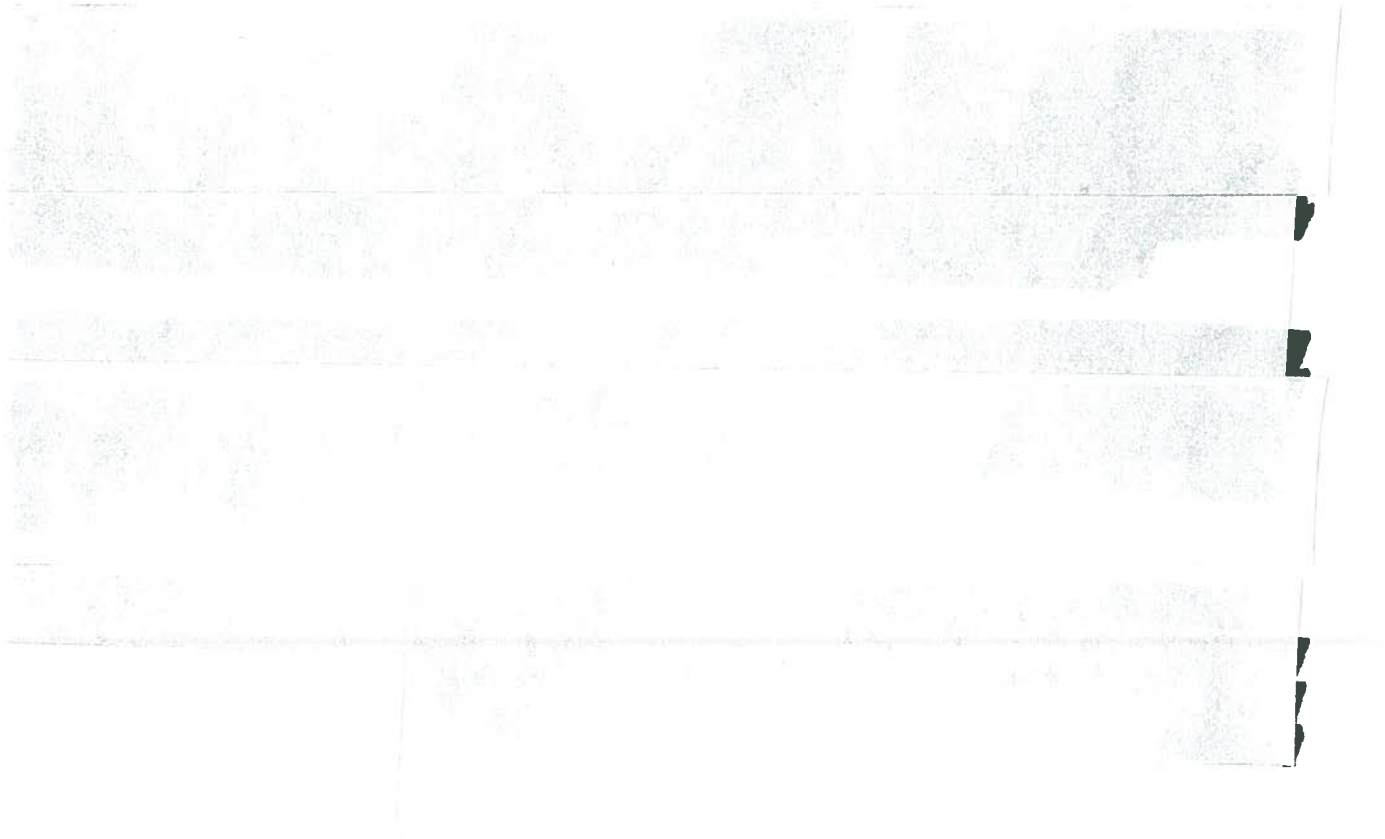
Retningslinjerne bør dog fastlægges på baggrund af en afvejning mellem på den ene side den øgede sikkerhed, som opnås ved hurtige opdateringer, og på den anden side de omkostninger i form af f.eks. personaletimer, som altid er forbundet med systemopdateringer, og ulempen i form af ekstra perioder, hvor it-systemerne ikke kan anvendes af kunden.

Det bemærkes, at CSC i den konkrete sag var ca. tre måneder om at patche IBM's mainframemiljø, uanset at de patches, som IBM havde udsendt, var markeret som kritiske.

Selv om et it-system i videst muligt omfang er opdateret, vil det i sagens natur stadig ikke være sikret mod sårbarheder, som softwareproducenterne endnu ikke har kendskab til. Retningslinjer, som sikrer en beskyttelse mod udnyttelse af allerede kendte sårbarheder, betyder dog, at en vellykket kompromittering vil være væsentligt mere tids- og ressourcekrævende for eventuelle hackere.

6.3. Adgang til mainframemiljøet fra internettet

6.4. Logning



6.5. Integritetscheck

Hvis der identificeres processer, der kan validere integriteten af data, kan de samme processer ofte bruges fremadrettet til at sikre, at brud på integriteten konstateres på et tidligt tidspunkt.

6.6. Konkret forebyggelse af udnyttelse af sårbarheder

De følgende konkrete forebyggende tiltag er udvalgt på baggrund af den viden, som Center for Cybersikkerhed på nuværende tidspunkt har indhentet om sikkerhedsbruddet.

Nr.	Hændelse	Kendt udnyttet sårbarhed pr. juni 2013	Forslag til forebyggelse
1.	[redacted]	[redacted]	[redacted]
2.	[redacted]	[redacted]	[redacted]
3.	[redacted]	[redacted]	[redacted]
4.	[redacted]	[redacted]	[redacted]
5.	[redacted]		[redacted]
6.	[redacted]	[redacted]	[redacted]

6.7. Udsendte varslinger

Center for Cybersikkerhed har udsendt varslinger til centrets kunder, herunder de potentielt berørte myndigheder. Disse varslinger indeholder specifikke forslag til tekniske sikkerhedsforbedringer i mainframemiljøet. Ligeledes er der udsendt en generel varsling om sårbarheder i mainframemiljøet til udenlandske samarbejdspartnere.

Såfremt udviklingen i sagen betyder, at centret kommer i besiddelse af yderligere oplysninger, som er af betydning for myndighederne, vil centret udsende yderligere varslinger.

7. Foreløbig konklusion

Det kan konstateres, at CSC's mainframemiljø har været udsat for en omfattende kompromittering, hvor en eller flere hackere har haft mulighed for at tilgå, kopiere, ændre og slette stærkt følsomme data tilhørende offentlige myndigheder. Det er på det foreliggende grundlag ikke muligt at klarlægge det fulde omfang af kompromitteringen, men visse data – primært tilhørende politiet – er med sikkerhed kompromitterede, og det kan ikke kan udelukkes, at også de øvrige myndigheders data er kompromitterede.

Det er ikke muligt at fastslå, om de sårbarheder, der muliggjorde den konstaterede kompromittering, på nuværende tidspunkt er fjernet, ligesom det ikke er muligt at fastslå, om CSC vil kunne forhindre forsøg på lignende kompromitteringer. Det er ligeledes ikke muligt at fastslå, om der i dag generelt er et passende sikkerhedsniveau i CSC's mainframemiljø.

Center for Cybersikkerhed vil i samarbejde med relevante myndigheder fortsætte indsatsen med henblik på mere fyldestgørende analyser af hændelsen, således at de udestående spørgsmål i størst muligt omfang kan besvares.

8. Bilag

Bilag 1

Mainframemiljø

Et mainframemiljø er betegnelsen for et antal større computere, hvis regnekraft, lagerkapacitet m.m. deles af mange brugere. Det berørte mainframemiljø hos CSC deles af en række organisationer, både private virksomheder og offentlige myndigheder, i alt ca. organisationer. Mainframemiljøet består af maskinel fra IBM og anvender i hovedsagen styresystemet z/OS.

Mainframemiljøet er delt op i en række logiske partitioner (LPAR), der hver især fungerer som en selvstændig maskine i form af en virtuel computer, hvorpå der afvikles selvstændigt styresystem, selvstændige applikationer og databaser. Det berørte mainframemiljø er opdelt i mere end partitioner

- Rigspolitiet: Bl.a. kørekortregisteret, Schengen Information Systemet og e-mail-konto-oplysninger
- SKAT: Et meget stort antal systemer
- CPR-kontoret: CPR-registret
- Moderniseringsstyrelsen: Bl.a. Statens Lønsystem.

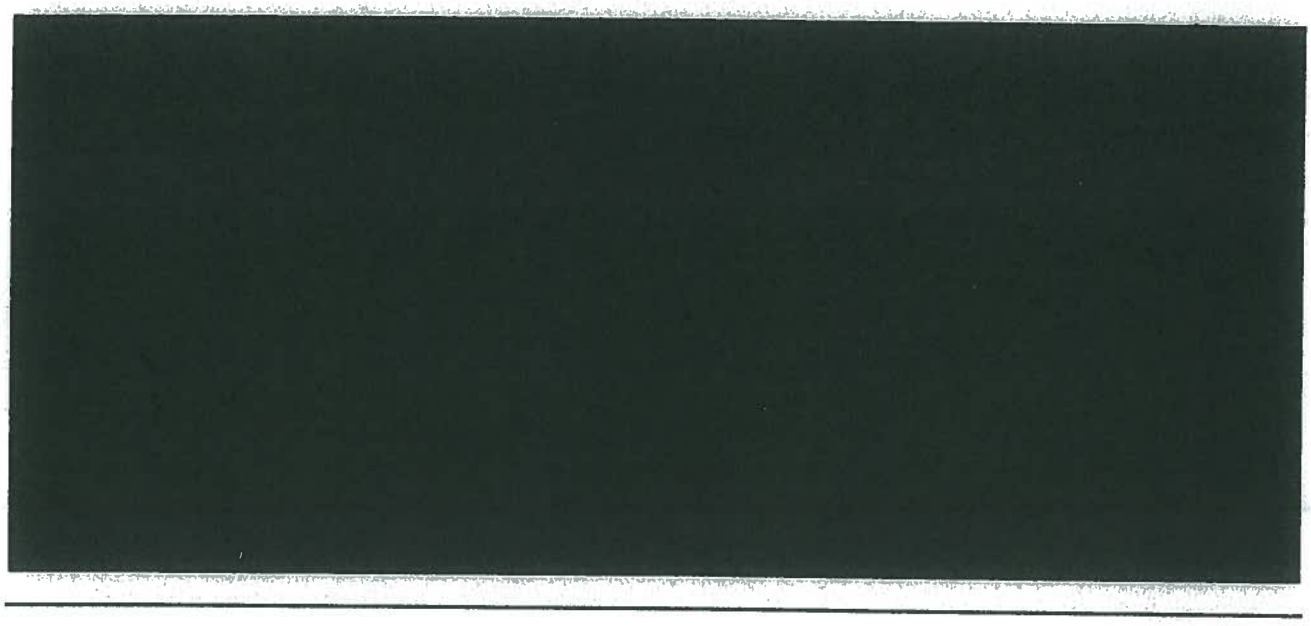
En række LPAR i mainframemiljøet har installeret [redacted] med mulighed for at tilbyde adgang til systemer og data via internettet.

Adgangskontrol

[redacted] Rettigheder til ressourcer kan betyde, at det er muligt for et system at anvende andre systemer, databaser o. lign. direkte, uden interaktion fra en bruger. Hvis et system skal hente data i en database eller anvende en proces i et andet system, skal systemet have de rette rettigheder til at gøre det, ligesom en bruger skal.

Bilag 2

Sikkerhedsteknisk tidslinje over CSC-hændelsen



Oktober 2012: IBM bliver opmærksom på sikkerhedsbristerne i selskabets mainframesoftware

IBM udsender meddelelse om to patches, der skal lukke sårbarheder,

21. december 2012: IBM udsender to patches, som de markerer som kritiske.

4. marts 2013: CSC bliver opmærksom på, at patches udsendt i december af IBM, som CSC på dette tidspunkt endnu ikke har implementeret, udbedrer en væsentlig sårbarhed i mainframesoftwaren.

10. marts 2013: De udnyttede sårbarheder på rettes (patches) af CSC.

17. marts 2013: De udnyttede sårbarheder på hvor CPR-registret findes) rettes (patches) af CSC.