DATATILSYNET

CPR-kontoret
Holmens Kanal 22
1060 København K

INDGÅET I
21 DEC. 2015
CPR KONTORET

17. december 2015

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-mail
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2014-632-0084
Sagsbehandler
Kasper Frederiksen
Direkte 3319 3235

Vedrørende hackerangrebet på CSC i forhold til CPR-kontoret

1. Baggrunden for sagen

Datatilsynet vender hermed tilbage til sagen om hackerangrebet i forhold til personoplysninger, som behandledes hos CSC på vegne af det daværende Økonomi- og Indenrigsministerium, IT og CPR (nu CPR-administrationen i Social- og Indenrigsministeriet, i det følgende "CPR-kontoret").

Efter anmodning fra Datatilsynet er CPR-kontoret fremkommet med udtalelser til sagen ved breve af 27. marts og 1. oktober 2014.

Datatilsynet har i forbindelse med sagen modtaget "Foreløbig rapport om sikkerhedsbrud hos CSC" fra juli 2013 fra Center for Cybersikkerhed. Tilsynet er ligeledes i besiddelse af "Rapport om sikkerhedsbrud hos CSC" fra august 2014 fra PET og Center for Cybersikkerhed (omtalt som Rapport II).

Datatilsynet har den 31. juli 2015 truffet afgørelse i sagen om hackerangrebet i forhold til Rigspolitiet[1]. Tilsynet fokuserede i den forbindelse sine undersøgelser på forholdene omkring Schengen-informationssystemet. Undersøgelserne afdækkede imidlertid en række forhold omkring indretningen af den berørte mainframe, som også er af relevans for den nærværende sag.

2. Sagens omstændigheder

Datatilsynet kan overordnet[2] beskrive sagen således:

2.1. CPR-kontorets it-systemer hos CSC

CPR-kontoret benyttede CSC som databehandler. I den forbindelse indgik de personoplysninger, som CPR-kontoret er dataansvarlig for, i et mainframe-

[1] Datatilsynets udtalelse af 31. juli 2015 til Rigspolitiet er tilgængelig her: http://www.datatilsynet.dk/nyheder/nyhedsarkiv/artikel/vedroerende-uvedkommendes-adgang-til-personoplysninger-rigspolitiets-jnr-2013-079-76/

[2] Datatilsynet har modtaget en større mængde oplysninger i de rejste sager i forlængelse af hackerangrebet, herunder oplysninger, som er klassificerede eller af forskellige årsager undtaget fra aktindsigt efter offentlighedsloven

Social- og Indenrigsudvalget 2015-16
SOU Alm.del Bilag 117
Offentligt

miljø hos CSC. Mainframiljøet indeholdt ud over CPR-kontorets it-systemer også it-systemer fra Moderniseringsstyrelsen, SKAT og Rigspolitiet.

Om mainframemiljøet foreligger følgende oplysninger, jf. Datatilsynets brev af 31. juli 2015 til Rigspolitiet:

"2.2. Det konkrete system
2.2.1. Om mainframens indretning
Hackerangrebet er foregået mod én fysisk computer, en såkaldt mainframe af fabrikat IBM. Mainframen var konfigureret i fire partitioner, såkalte LPAR's (Logical Partitions). De fire LPAR's er benævnt D11, D12, D13 og D14.

I en LPAR kan der driftes systemer, programmer og services.

Mainframen var konfigureret således, at de tilsluttede lagringsmedier (diske) var delte og fysisk kunne tilgås fra alle fire LPAR'er. I det følgende benyttes betegnelsen '*det delte disk-system*' for disse lagringsmedier.

RACF er et mainframe sikkerhedssystem udviklet af IBM. RACF anvendes bl.a. til at kontrollere bruger-id og password for brugere og administratorer, samt disses autorisationer til at anvende data, programmer og andre ressourcer på mainframes.

Den aktuelle mainframe var konfigureret med ét RACF sikkerhedssystem, som var fælles for hele mainframen inklusiv de fire LPAR'er. Dette RACF kontrollerede således i den aktuelle situation bruger-id og password for alle brugere og administratorer samt disses autorisationer til at anvende data, systemer, programmer og services og andre ressourcer i alle fire LPAR'er på mainframen.

De oplysninger om bruger-id, password og autorisationer, som RACF i det aktuelle tilfælde anvendte, fandtes lagret i krypteret form i en database/fil på det delte disksystem, som var tilsluttet mainframen. I det følgende omtales denne database/fil som '*RACF-databasen*'.

I LPAR D11 var der installeret en aktiv webserverservice, som kunne tilgås fra det åbne internet. Det var en sårbarhed i denne webserver, som hackeren benyttede til at skaffe sig den indledende adgang til mainframen.

2.2.2. Om mainframens anvendelse
I mainframen driftedes bl.a. informationssystemer for Rigspolitiet, SKAT, Økonomi- og Indenrigsministeriet og Moderniseringsstyrelsen.

De informationssystemer, der blev driftet for Rigspolitiet, omfattede bl.a. Schengen-informationssystemet, Kriminalregisteret, Kørekortregisteret, Pasregisteret og Index-registeret.

Schengen-informationssystemet indeholdt bl.a. oplysninger om personer, der var eftersøgt, havde indrejseforbud i Schengen-området eller var under diskret overvågning af politi eller efterretningstjenester i henhold til artiklerne 95-99 i Schengenkonventionen.

Kriminalregisteret indeholdt bl.a. oplysninger om straffede personer og disses strafbare forhold.

Kørekortregisteret indeholdt bl.a. oplysninger om alle personer, der har dansk kørekort, herunder kørekortindehaverens personnummer og kørekortnummer.

Pasregisteret indeholdt bl.a. oplysninger om alle personer, der har et dansk pas, herunder bl.a. indehaverens personnummer og pasnummer.

Index-registeret indeholdt bl.a. oplysninger fra CPR-registeret om alle borgere i Danmark med et personnummer.

Rigspolitiet har oplyst, at Rigspolitiets systemer blev driftet i LPAR D11 og D14.

På forespørgsel har Rigspolitiet oplyst, at den implicerede webserver, som var installeret og aktiv i LPAR D11, havde til formål at give adgang fra internettet til portalen www.tjenestemandspension.dk.

Moderniseringsstyrelsen er dataansvarlig for internetportalen www.tjenestemandspension.dk. Portalen retter sig mod alle tjenestemænd med tjenestemandspension. På portalen kan den enkelte tjenestemand finde relevante oplysninger om egen tjenestemandspension.

Datatilsynet har specifikt spurgt Rigspolitiet om, hvem (f.eks. Rigspolitiet eller CSC), der har truffet beslutning om, at webserveren skulle kunne tilgås fra internettet af brugere udenfor CSC's lokalitet. I to omgange har Rigspolitiet ikke besvaret spørgsmålet.

Datatilsynet lægger i det følgende til grund, at LPAR D11 er blevet anvendt af både Moderniseringsstyrelsen og Rigspolitiet. Dette understøttes af oplysningerne i de rapporter, som Datatilsynet er i besiddelse af, hvoraf det fremgår, at både Rigspolitiet og Moderniseringsstyrelsen benyttede LPAR D11.

RACF sikkerhedssystemet på mainframen var fælles for de fire ovennævnte LPAR'er D11, D12, D13 og D14. RACF sikkerhedssystemets database (RACF-databasen) indeholdt oplysninger om ca. 85.000 bruger- og administrator-id'er, samt oplysninger om de hertil knyttede password og autorisationer til at anvende programmer, services og data på hele mainframen. Det høje antal bruger- og administrator-id'er i RACF-databasen hænger sammen med, at RACF-sikkerhedssystemet kontrollerede brugere og administratorer af systemerne fra såvel Rigpolitiet, Økonomi- og Indenrigsministeriet, SKAT og Moderniseringsstyrelsen. En kopi af RACF-databasen blev fundet på hackerens computer."

2.2. Hackerangrebet

Om hackerangrebet er oplyst følgende, jf. Datatilsynets brev af 31. juli 2015 til Rigspolitiet:

"Hackerangrebet blev foretaget ved bl.a. at udnytte to sårbarheder i IBM softwaren på mainframen. Begge sårbarheder var såkaldte zero-day sårbarheder, hvilket betyder, at der ikke eksisterer rettelser til afhjælpning af sårbarhederne. IBM udsendte først rettelser til afhjælpning af de to zero-day sårbarheder, efter at angrebet var ophørt. Den aktuelle udnyttelse af sårbarhederne kunne derfor ikke have været afværget ved patchning.

Hackeren har skaffet sig adgang til mainframen via en webserver, som kunne tilgås fra det åbne internet. Ved at udnytte den ene zero-day sårbarhed, som fandtes i IBM webserversoftwaren, har hackeren opnået en indledende og begrænset adgang til mainframen.

Ved derefter at udnytte den anden zero-day sårbarhed i mainframens systemsoftware, har hackeren trinvis kunnet øge sine beføjelser og tiltage sig mere kontrol med mainframen. Forløbet førte til, at hackeren opnåede ubegrænset adgang til alle data og dermed adgang til at kopiere, slette, ændre og tilføje data. Der er undervejs i forløbet blevet installeret et eller flere programmer, som har kunnet benyttes til at udtrække data fra mainframen. Undervejs i forløbet har hackeren opnået så store rettigheder, at hackeren har kunnet stjæle og kopiere (downloade) hele RACF-databasen fra mainframen. Endvidere er der opnået adgang til at omgå logning af de udførte handlinger, hvorefter hackeren har kunnet operere "stealth".

....."

Der foreligger ikke et fuldstændigt overblik over, hvilke data der med sikkerhed er kopieret fra mainframemiljøet. Det er imidlertid konstateret, at store mængder data tilhørende politiet er kopieret og trukket ud fra systemet, ligesom RACF-databasen er blevet kopieret og downloadet.

2.3. CPR-kontorets håndtering af hackerangrebet

CPR-kontoret har bl.a. oplyst, at det daværende Økonomi- og Indenrigsministerium med bistand fra Center for Cybersikkerhed igangsatte en nærmere undersøgelse af, om der var grund til at tage yderligere forholdsregler for CPR-systemet på baggrund af den konkrete sag, og at CPR-kontoret følger ISO 27001 og træffer løbende sikkerhedsforanstaltninger i forhold til den aktuelle risikovurdering for CPR-systemet, ligesom kontoret har fulgt de anbefalinger til yderligere sikkerhedsforanstaltninger, som er fremkommet under den iværksatte undersøgelse af hackerangrebet.

Endvidere har CPR-kontoret bl.a. oplyst, at CPR-systemet siden marts 2014 ikke længere driftsafvikles på den fællesoffentlige mainframe hos CSC eller anvender den fælles RACF, og at CPR-systemet er flyttet til en selvstændig platform, hvor der anvendes et andet adgangskontrolsystem. CPR-kontoret har også oplyst, at der i forbindelse med flytningen af CPR-systemet blev foranstaltet en ekstraordinær, uvildig it-revision og gennemført en sikkerhedsvurdering af den nye platform i samarbejde med Center for Cybersikkerhed.

Herudover oplyste CPR-kontoret ved sit brev af 27. marts 2014, at det daværende Økonomi- og Indenrigsministerium ikke havde konstateret, at personoplysninger, som behandledes hos CSC på vegne af CPR-kontoret, var blevet uautoriseret tilgået, modificeret, misbrugt eller offentliggjort som følge af hackerangrebet, at CPR-kontoret i perioden siden februar 2012 ikke havde modtaget henvendelser eller indikationer på, at CPR's data skulle være blevet uautoriseret modificeret, misbrugt eller offentliggjort som følge af hackerangrebet, at Økonomi- og Indenrigsministeriet løbende vurderede, om der var anledning til at informere konkrete borgere eller grupper af borgere om sikkerhedsbruddet, men indtil videre ikke havde fundet anledning til dette, og at Økonomi- og Indenrigsministeriet bemærkede, at politiet den 6. juni 2013 offentliggjorde en vejledning til borgerne efter sikkerhedsbristen.

I forhold til den kopierede og downloadede RACF-database har CPR-kontoret bl.a. oplyst, at databasen for CPR-systemets vedkommende indeholdt oplysninger om bl.a. brugernavne og passwords for ca. 38.000 brugere, at 25.000 af disse brugere var aktive, mens de resterende var blokerede og ikke kunne anvendes, og at databasen for ca. 11.000 af brugernavnene bl.a. også indeholdt oplysninger om fornavn og efternavn på brugeren samt i visse tilfælde e-mailadresse.

3. Datatilsynets udtalelse

3.1. For så vidt angår RACF-systemet og det disksystem, der var tilknyttet den omhandlede mainframe, konkluderede Datatilsynet i afgørelsen af 31. juli 2015 bl.a.:

"Sikkerhedssystemet RACF styrer og kontrollerer adgang og autorisationer til systemer for brugere og administratorer. Den aktuelle mainframe var indrettet med ét RACF, som dækkede hele mainframen, dvs. alle fire LPAR'er D11, D12, D13 og D14, brugere og administratorer af systemerne samt data for såvel Rigspolitiet som SKAT, Økonomi- og Indenrigsministeriet og Moderniseringsstyrelsen. Ved at dele RACF påførte de fire dataansvarlige hinanden forøgede risici, både fordi den enkelte dataansvarlige, f.eks. Rigspolitiet, eksponeres for visse former for sikkerhedshændelser hos de øvrige dataansvarlige, og fordi konsekvenserne af visse sikkerhedshændelser kan sprede sig fra én dataansvarlig til de øvrige dataansvarlige. Rigspolitiet har på forespørgsel oplyst, at der i RACF-databasen eksisterede (eller kunne oprettes) bruger- eller administrator-id med autorisationer til at kunne tilgå og udføre handlinger på data, som Rigspolitiet ikke er dataansvarlig for. Rigspolitiet har endvidere oplyst, at det drejer sig om data, som SKAT, Moderniseringsstyrelsen eller Økonomi- og Indenrigsministeriet er dataansvarlige for.

På computeren, som blev beslaglagt i Cambodia, blev fundet en kopi af en RACF-database. Det er fastslået, at der er tale om en kopi af RACF-databasen, som fandtes på den aktuelle mainframe. RACF-databasen indeholdt adgangskoder og autorisationer for ca. 85.000 bruger- og administrator-id'er hidrørende fra forskellige myndigheder. Datatilsynet må anse det for overvejende sandsynligt, at hackeren har været i stand til at bryde den kryptering, der var på RACF-databasens indhold, og dermed tilgå indholdet.

På denne baggrund - og fordi hackeren vides at have tilegnet sig ubegrænsede rettigheder til at tilgå alle data på mainframen - må alle data på mainframen og hele det delte disksystem anses for eksponeret og potentielt kompromitteret ved hackerangrebet."

og:

"Den aktuelle mainframe var indrettet med ét delt disksystem, som kunne tilgås fra alle fire LPAR'er D11, D12, D13 og D14. Det delte disksystem blev benyttet til at lagre data for informationssystemerne, som blev driftet i alle fire LPAR'er, dvs. for Rigspolitiet, SKAT, Økonomi- og Indenrigsministeriet og Moderniseringsstyrelsen. Ved at dele disksystemet påførte de fire dataansvarlige hinanden forøgede risici, både fordi den enkelte dataansvarlige, f.eks. Rigspolitiet, eksponeredes for visse former for sikkerhedshændelser hos de øvrige dataansvarlige, og fordi konsekvenserne af visse sikkerhedshændelser kunne sprede sig fra én dataansvarlig til de øvrige dataansvarlige. Delingen af disksystemet er med hensyn til adskillelse af dataansvarlige og adskillelse af de dataansvarliges data risikabel og undergraver tillige forsvar i dybden for alle de dataansvarlige."

3.2. Datatilsynets vurdering i forhold til CPR-kontoret

Datatilsynet må lægge til grund, at angriberen potentielt har haft adgang til at ændre i, tilføje eller slette data, som befandt sig i systemer, som på vegne af CPR-kontoret blev håndteret hos CSC.

Datatilsynet har i den forbindelse noteret sig, at det er anført i Rapport II, at de berørte myndigheder har foretaget dataintegritetscheck (og konsekvensvurdering) som anbefalet af Center for Cybersikkerhed i den foreløbige rapport fra juli 2013.

Hertil kommer, at de oplysninger om personlige brugere, der indgik RACF-databasen, efter Datatilsynets opfattelse i sig selv udgør personoplysninger omfattet af persondataloven. Tilsynet lægger herved vægt på, at oplysningerne omfattede navne og andre personoplysninger.

Efter Datatilsynets opfattelse er der således tale om, at personoplysninger, som CPR-kontoret er dataansvarlig for, er kommet til uvedkommendes kendskab, da RACF-databasen er blevet kopieret og downloadet.

Det forhold, at mainframemiljøet hos CSC var delt mellem flere myndigheder, medvirkede efter Datatilsynets opfattelse til, at en angriber via en webserver, som én myndighed var dataansvarlig for, kunne tilgå både data, som den pågældende myndighed var dataansvarlig for, og data, som andre myndigheder var dataansvarlige for.

Det forhold, at RACF-databasen var delt mellem flere myndigheder, forøgede desuden angriberens mulighed for at skaffe sig adgang til CPR-kontorets systemer via uberettiget adgang til andre myndigheders systemer.

Efter Datatilsynets opfattelse har CPR-kontoret derfor ikke haft tilstrækkelig kontrol med sikkerheden omkring de personoplysninger, som på myndighedens vegne blev håndteret hos CSC. Datatilsynet finder således, at CPR-kontoret ikke har levet op til kravet i persondatalovens § 41, stk. 3[3], om de fornødne sikkerhedsforanstaltninger.

Datatilsynet tager ved sin vurdering af sagen også i betragtning, at CPR-kontoret fik håndteret CPR-systemet i det pågældende mainframemiljø hos CSC, og at kompromittering af oplysningerne kunne få alvorlige skadevirkninger for såvel CPR-kontoret, andre myndigheder, som bruger CPR-systemet, som de personer, der behandles oplysninger om.

På den baggrund er det efter Datatilsynets opfattelse meget alvorligt, at en udenforstående potentielt har haft mulighed for at tilgå, kopiere, slette og ændre i CPR-systemet hos CSC, og at personoplysninger i RACF-databasen er blevet kopieret og downloadet.

Datatilsynet finder derfor CPR-kontorets manglende efterlevelse af persondatalovens sikkerhedskrav **kritisabel**.

Datatilsynet har noteret sig det oplyste om de skridt, som CPR-kontoret har taget til at forbedre beskyttelsen af CPR-systemet.

---

[3] Ifølge persondatalovens § 41, stk. 3, skal der træffes de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven

3.3. Underretning af de berørte personer

Hvis personoplysninger er kommet til uvedkommendes kendskab, er det Datatilsynets opfattelse og faste praksis, at reglen i persondatalovens § 5, stk. 1, om god databehandlingsskik medfører, at den dataansvarlige skal vurdere, om og i givet fald hvordan de berørte personer skal underrettes.

Ved vurderingen af spørgsmålet om underretning må den dataansvarlige blandt andet tage oplysningernes karakter og de mulige konsekvenser for de berørte personer i betragtning.

I et tilfælde, hvor en brugerdatabase er blevet kompromitteret, må det også tages i betragtning, om såvel brugernavne som passwords er berørt, om passwords var krypteret, og om det må frygtes, at angriberen har brudt krypteringen.

Tilsynet vurderer umiddelbart, at der i sådanne situationer som oftest vil være behov for underretning ganske hurtigt. Ud over nulstilling af passwords i de berørte løsninger kan der således være brugere, der har behov for at ændre passwords andre steder eller at ændre en metodik til opbygning af passwords, som kan være blotlagt.

Datatilsynet skal på denne baggrund opfordre CPR-kontoret til at fastsætte retningslinjer for håndtering af sikkerhedsbrud – både for myndigheden selv og som led i aftalerne med de relevante databehandlere – såfremt sådanne retningslinjer ikke allerede er fastsat.

3.4. Afsluttende bemærkninger

Datatilsynet foretager sig herefter ikke yderligere i sagen.

Tilsynet forventer at offentliggøre denne udtalelse på sin hjemmeside.

Med venlig hilsen

Lena Andersen
Kontorchef