JUSTITSMINISTERIET
Politi- og Strafferetsafdelingen

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 6. januar 2014
Kontor: Sikkerheds- og Forebyggelseskontoret
Sagsbeh: Jean Elisabeth Hørdum
Sagsnr.: 2013-0030-1545
Dok.: 830614

Hermed sendes endelig besvarelse af spørgsmål nr. 957 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 1. juli 2013. Spørgsmålet er stillet efter ønske fra Dennis Flydtkjær (DF).

Karen Hækkerup

/

Anette Arnsted

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 957 (Alm. del) fra Folketingets Retsudvalg:

> ”Vil ministeren oplyse, hvor mange og hvilke angreb/sikkerhedshuller Datatilsynets kontrol og Rigspolitiets egne revisioner af statens it-systemer tidligere har afsløret?”

Svar:

Justitsministeriet har til brug for besvarelsen af spørgsmålet indhentet udtalelser fra Rigspolitiet og Datatilsynet.

Rigspolitiet har oplyst følgende:

> ”Rigspolitiet kan til brug for besvarelsen oplyse, at en række af politiets registre som bekendt blev udsat for et hackerangreb, da uautoriseret adgang til CSC's systemer fandt sted primo april 2012, hvor en sårbarhed blev benyttet til adgang til et mainframesystem fra en IP-adresse registreret i Cambodja. Undersøgelser viste, at der i den forbindelse havde været aktivitet mod CPR-registerets miljø på mainframen fra politiets miljø på mainframen.
>
> Rigspolitiet fører løbende tilsyn med CSC og med it-systemer, som drives af politiet selv. Antallet af revisioner og kontroller afstemmes løbende i forhold til den aktuelle situation.
>
> Herudover kan det oplyses, at der i forbindelse med Rigspolitiets løbende tilsyn er blevet identificeret systemsvagheder og sårbarheder. Der træffes i den forbindelse løbende passende modforanstaltninger i form af f.eks. systemopdateringer eller kompenserende kontroller.
>
> Politiets Efterretningstjeneste kan oplyse, at efter Statsministeriets cirkulære nr. 204 af 7. december 2001 vedrørende sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO, EU eller WEU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt (sikkerhedscirkulæret) er Politiets Efterretningstjeneste (PET) national sikkerhedsmyndighed. I forbindelse med regeringsdannelsen i september 2011 blev det besluttet at udpege Forsvarets Efterretningstjenestes Center for Cybersikkerhed som national it-sikkerhedsmyndighed, dog således at PET varetager denne funktion for Justitsministeriets område, herunder for politiet.
>
> Det følger af sikkerhedscirkulærets § 26, at alle former for elektroniske informationssystemer og netværk beregnet til frembringelse, bearbejdning, kommunikation eller lagring af informationer klassificeret HEMMELIGT eller FORTROLIGT

skal sikkerhedsgodkendes af den relevante it-sikkerhedsmyndighed, dvs. for Justitsministeriets område af PET.

Det følger endvidere af sikkerhedscirkulærets § 56, at den nationale sikkerhedsmyndighed fører tilsyn med overholdelsen af de sikkerhedsmæssige foranstaltninger, som Danmark er forpligtet til at gennemføre, og foretager periodiske inspektioner. I forhold til it-systemer fører PET således tilsyn med Justitsministeriets område.

Som det fremgår af sikkerhedscirkulærets § 26, omfatter cirkulæret alene it-systemer, der behandler mv. klassificerede informationer. Det indebærer, at en række af it-systemerne på Justitsministeriets område ikke er omfattet af reglerne i sikkerhedscirkulæret og følgelig heller ikke omfattet af PET's godkendelses- og kontrolvirksomhed. Det gælder også det mainframe-anlæg hos CSC, der har været udsat for hackerangreb.

For så vidt angår de it-systemer på Justitsministeriets område, der er omfattet af PET's kontrol, har PET kun i få tilfælde fundet alvorlige svagheder. Disse problemer vedrører navnlig tilfælde, hvor systemer til behandling mv. af klassificerede oplysninger kobles til internettet. I sådanne tilfælde giver PET påbud om ændringer af systemet og anbefalinger til styrkelse af informationssikkerheden."

Datatilsynet har oplyst følgende:

"I forhold til statslige myndigheders it-systemer sker Datatilsynets tilsyn – som på andre områder – i forbindelse med anmeldelser fra statslige myndigheder[1], behandling af konkrete klager fra borgere og som egen drift undersøgelser. Dertil kommer, at Datatilsynet jævnligt giver anvisning om persondatalovens[2] krav til datasikkerheden i forbindelse med høringer over forslag til love og bekendtgørelser.

Egen drift undersøgelser omfatter både inspektionsbesøg og undersøgelser på skriftligt grundlag. Egen drift undersøgelser sker i forhold til den dataansvarlige for registrene, og siden persondatalovens ikrafttræden i 2000 har Datatilsynet bl.a. gennemført ca. 160 inspektionsbesøg hos statslige myndigheder[3].

[1] En dataansvarlig myndighed skal efter persondatalovens §§ 43-45 anmelde behandling af fortrolige og følsomme personoplysninger til Datatilsynet, der skal afgive en udtalelse om den påtænkte behandling. Anmeldelserne er offentliggjort i "Fortegnelsen" på tilsynets hjemmeside www.datatilsynet.dk.
[2] Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer.
[3] Oversigt over Datatilsynets inspektioner findes i tilsynets årsberetninger, som er offentliggjort på tilsynets hjemmeside www.datatilsynet.dk under "Publikationer".

Datatilsynets tilsyn med statslige myndigheders behandling af personoplysninger har karakter af et legalitetstilsyn – dvs. tilsynets fokus er på, at behandlingen af personoplysninger er i overensstemmelse med reglerne i persondataloven og evt. anden relevant lovgivning, og at reglerne om registreredes rettigheder overholdes. Sagsbehandlingsprocedurer, håndtering af anmodninger fra registrerede personer og sletterutiner mv. gennemgås derfor typisk på et møde med den dataansvarlige.

I forhold til datasikkerhed stiller Datatilsynet typisk spørgsmål inden for de emner, som fremgår af sikkerhedsbekendtgørelsen[4]. Det kan vedrøre myndighedernes uddybende sikkerhedsregler eller mere specifikke sikkerhedsforanstaltninger, herunder f.eks. procedurer for autorisation af brugere og/eller logning. Tilsynet foretager imidlertid ikke en mere omfattende it-revision eller en fuldstændig gennemgang af de etablerede sikkerhedsforanstaltninger.

I relation til hyppigheden af Datatilsynets kontrol kan det oplyses, at persondataloven og databeskyttelsesdirektivet ikke nærmere fastlægger, i hvilket omfang tilsynet skal foretage inspektioner og andre kontrolforanstaltninger. Det er forudsat, at der skal være tale om en løbende inspektionsvirksomhed, men der er ikke opstillet nærmere krav til antallet af inspektioner.

Datatilsynet har – ud af de ca. 160 inspektionsbesøg hos statslige myndigheder – foretaget en del inspektionsbesøg hos politiet, både i politikredsene og hos Rigspolitiet.

Derudover har inspektionerne på det statslige område siden 2000 fordelt sig på inspektionsbesøg hos mange forskellige statslige myndigheder, herunder forskellige statsadvokaturer, fængsler, statsforvaltninger, enheder inden for SKAT samt forskellige ministerier og underliggende styrelser.

Ud over inspektioner hos statslige myndigheder har Datatilsynet tillige gennemført en lang række inspektionsbesøg hos kommuner og amter/regioner samt hos private virksomheder og forskere.

I 2012 har Datatilsynet udarbejdet en inspektionsstrategi for perioden 2013-2015, hvor tilsynet af statslige myndigheder har udvalgt lokale politiembeder og Rigspolitiet som en særlig prioritet.

Datatilsynet har ikke en samlet oversigt eller statistik over de forhold, som tilsynet har påpeget i forbindelse med inspektioner og andre tilsynssager. Tilsynet konstaterer jævnligt mang-

[4] Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning, som ændret ved bekendtgørelse nr. 201 af 22. marts 2001.

lende overholdelse af persondataloven og/eller sikkerhedsbekendtgørelsen. Datatilsynet har derimod ikke afsløret egentlige angreb på it-systemer i forbindelse med tilsynets kontrol af statslige myndigheder.

Datatilsynet har til brug for dette bidrag bl.a. foretaget en gennemgang af konklusionerne på inspektioner, som tilsynet har foretaget hos Rigspolitiet, og inspektioner, som tilsynet har foretaget hos politikredsene, siden politireformen trådte i kraft i 2007. Derudover har tilsynet gennemgået konklusionerne på inspektioner foretaget hos statslige myndigheder de seneste tre år.

Datatilsynet kan på den baggrund nævne følgende eksempler på konstaterede forhold, der ikke var i overensstemmelse med persondatalovens og sikkerhedsbekendtgørelsens sikkerhedskrav.

På inspektioner i flere politikredse har Datatilsynet bl.a. konstateret manglende eller mangelfulde uddybende sikkerhedsregler, manglende retningslinjer vedrørende hjemmearbejdspladser og mobile arbejdspladser, manglende kryptering af kontaktformularer på hjemmesider og manglende eller mangelfuld kontrol med afviste adgangsforsøg.

I forbindelse med en inspektion af overtrædelsesregisteret hos Erhvervs- og Selskabsstyrelsen i 2010 konstaterede Datatilsynet bl.a., at der ikke var implementeret en adgangsløsning, der levede op til sikkerhedskravene.[5]

Afslutningsvis kan det oplyses, at Datatilsynet også på andre måder har fået kendskab til tilfælde, hvor statslige myndigheder ikke har overholdt persondatalovens regler. Det kan f.eks. være ved henvendelser fra borgere, omtale i medierne, oplysninger i klagesager, søgning på internettet mv.

Som eksempler kan nævnes sager om utilsigtet offentliggørelse af personoplysninger, herunder oplysninger af følsom karakter, og andre sager om utilsigtet videregivelse af sådanne oplysninger, manglende kryptering af kontaktformularer på hjemmesider, uberettiget opslag i register samt utilsigtet adgang for uvedkommende virksomheder til skatteoplysninger om andre virksomheders ansatte."

Justitsministeriet kan supplerende henvise til besvarelserne af 27. juni 2013 af spørgsmål nr. 903 og 904 (Alm. del) fra Folketingets Kommunaludvalg.

[5] Datatilsynets udtalelse af 28. september 2010 i sagen (2009-621-0045) er tilgængelig på tilsynets hjemmeside www.datatilsynet.dk under punktet "Afgørelser" → "Arkiv over afgørelser".