Valby, 6. juni 2013

CPR-kontoret
Att.: Carsten Grage

Finsensvej 15
2000 Frederiksberg

Kære Carsten,

Vedr. Sikkerhedshændelse på Politiet's IT system

CPR-kontoret har ved mail af 5. juni 2013, samt mundtligt på Forretningsgruppemødet 6. juni 2013, bedt om CSC's redegørelse for, hvorfor CPR ikke tidligere af CSC er blevet orienteret om ovenstående problemstilling.

CSC har i tæt samarbejde med Rigspolitiets IT afdeling, støttet Politiets efterforskning. Dette arbejde har ikke resulteret i nogen indikation af, at CPR-Registeret skulle have været berørt eller truet af det oplevede angreb af CSCs mainframe. CSC har derfor ikke har haft anledning til en specifik orientering af CPR-kontoret, ligesom CSC er blevet påbudt af Rigspolitiet ikke at informere tredjeparter om den igangværende efterforskning eller angrebet i øvrigt, hvorfor CSC ikke har haft mulighed for at give en generel orientering af hensynet til Politiets efterforskning.

Det skal desuden bemærkes, at CSC ikke af egen drift er berettiget til at informere kunder om øvrige kunders fortrolige forhold.

CSC stiller sig naturligvis til rådighed for afklaring af alle spørgsmål, som CPR-kontoret måtte have vedrørende CPR-kontorets data og informationer.

Venlig hilsen

Henning Søby
Account General Manager

CSC Danmark A/S | Retortvej 8 | 2500 Valby
tt +45 3614 4000+45 3614 4000 | **ff** +45 3614 4011+45 3614 4011 | csc-dk@csc.com | **www.csc.com/dk**
CVR nr.: 15 23 15 99

Valby, 6. juni 2013

CPR-kontoret
Att.: Carsten Grage

Finsensvej 15
2000 Frederiksberg

Kære Carsten,

Vedr. Sikkerhedshændelse på Politiets it-systemer

CPR-kontoret har ved mail af 5. juni 2013, samt mundtligt på Forretningsgruppemødet 6. juni 2013, anmodet om CSC's nærmere redegørelse for ovennævnte sag, hvilke implikationer sårbarheden kunne have haft på CPR-systemet, samt hvilke forholdsregler CSC har taget og agter at tage som følge af sikkerhedshændelsen.

Sagsforløb

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, herunder også CPR systemet.

Gerningsmanden benyttede en hidtil ukendt sårbarhed. Denne sårbarhed blev lukket ved hjælp af nye retningslinier fra IBM den 10. marts 2013.

Mulige implikationer af sårbarheden i forhold til CPR-systemet

Sårbarheden kunne have medført adgang til CPR registerets data. Imidlertid har CSC i tæt samarbejde med Rigspolitiets IT afdeling, støttet Politiets efterforskning, og undersøgt alle dele af den berørte mainframe. Dette arbejde har ikke resulteret i nogen indikation af, at CPR-Registereret skulle have været berørt eller truet af det oplevede angreb af CSCs mainframe.

Mitigerende tiltag

CSC har sammen med Politiet og Rigspolitiets IT afdeling allerede foretaget følgende tiltag for at minimere risiko for tilsvarende angreb som det ovenfor beskrevne:

- Søgt efter yderligere spor på ulovlig indtrængen
- [redacted]
- Øget fokus på overvågningssystemer
- Fordoblet den periode relevante logs gemmes i

CSC Danmark A/S | Retortvej 8 | 2500 Valby
t +45 3614 4000 | f +45 3614 4011 | csc-dk@csc.com | **www.csc.com/dk**
CVR nr.: 15 23 15 99

Yderligere has CSC planlagt følgende yderligere præventive tiltag:

- [redacted]
- [redacted]
- Revision af funktionsbrugere
- [redacted]
- [redacted]

Som nævnt i dag, bedes CPR rette henvendelse til Rigspolitiets Sikkerhedschef, Politikommisær Lars Borgeskov, for eventuelle yderligere oplysninger om sikkerhedshændelsen, idet CSC ikke har tilladelse til at videregive yderligere oplysninger herom grundet den igangværende efterforskning.

Venlig hilsen

Henning Søby
Account General Manager