

Pressemeddelelse
18. juni 2011

IT-SIKKERHEDSRÅD: VENT MED OFFENTLIGE CLOUD-LØSNINGER

Cloud-løsninger giver store muligheder for effektiviseringer, men de er stadig ikke gode nok til danske offentlige it-systemer, når det gælder it-sikkerhed og sikring af borgernes privatliv.

Sådan siger Rådet for IT-Sikkerhed som kommentar til en række sager hvor blandt andet danske kommuner har forsøgt sig med øget brug af cloud-computing. Blandt de offentligt omtalte sager er Odense Kommunes projekt med at benytte Google Apps til registrering af følsomme personoplysninger om skoleelever. Senest har der været lækage af følsomme personoplysninger fra det køreprøvebooking- system som kommunerne via Kommunernes Landsforening havde lagt ud i Microsofts Azure cloud-løsning. Begge sager er blevet behandlet af Datatilsynet som har påtalt og bedt om yderligere dokumentation for en række forhold. Sagen vedrørende læk fra køreprøvebooking- systemet er endnu ikke afsluttet.

Christian Wernberg-Tougaard, formand for Rådet for Større IT-Sikkerhed, siger: "Den nye cloud-teknologi giver mulighed for betydelige besparelser, også for det offentlige. Det springende punkt er om cloud-løsninger både på kort og langt sigt er lige så sikre og stabile som det offentliges nuværende it-løsninger."

Rådet for Større IT-Sikkerhed mener at cloud-ydelser til offentlige it-systemer skal opfylde alle eksisterende lovbestemmelser og de bedste gængse standarder for it-sikkerhed, og Rådets vurdering er at teknologierne stadig ikke er modne nok. Rådet konstaterer at det i cloud-løsninger typisk ikke længere er muligt at fastslå præcist, hvor bestemte data er lagret fysisk, og at dette giver en række nye udfordringer i forhold til både datasikkerhed og beskyttelse af data, specielt fortrolige og følsomme personoplysninger.

Christian Wernberg Tougaard uddyber: "Tidligere har man kunnet inspicere en fysisk lokalitet, og måske endda nogle bestemte harddiske hvor nogle givne data blev opbevaret. Med cloud-computing begynder computerkraft og datalagring at ligne det vi kender fra el-produktion. Det kan være svært at sige hvor den strøm, vi trækker ud af kontakten, er produceret - og noget lignende gælder i stigende grad for it-ydelser. Det giver en lang række nye udfordringer, specielt for myndigheder som jo skal tjene en hel befolknings interesser."

Rådet for Større IT-Sikkerhed vurderer at datasikkerhed og databeskyttelse med den øgede brug af cloud-computing fremover i langt højere grad skal baseres på certificering og generelle kvalitetsnormer. Derfor har den overordnede lovgivning stor betydning, og Rådet mener at den gældende EU- og danske lovgivning udgør et solidt fundament for fremtidens cloud-løsninger.

Før regeringen giver grønt lys for nye cloud-løsninger i offentligt regi, mener Rådet for Større IT-Sikkerhed at blandt andet følgende centrale krav skal kunne opfyldes:

o Sikkerhedsforhold skal kunne verificeres via fysisk inspektion og certificering hos cloud-leverandørerne, og cloud-løsninger skal overholde alle gældende EU- og dansk lovgivning samt de bedste gængse standarder for it-sikkerhed.

o Der skal være løsninger i forhold til nødberedskab som opfylder præcist samme krav til datasikkerhed og databeskyttelse, som gælder for drift af de almindelige it-systemer.

o Der skal være klare aftaler som sikrer, at data forbliver i myndighedernes varetægt og inden for EU's grænser, også hvis en cloud-leverandør bliver opkøbt eller lukker ned. En del af Rådets medlemmer mener, at eneste farbare vej er, at det offentlige laver sine egne afgrænsede cloud-løsninger lokaliseret i Danmark, og på den måde har det direkte ejerskab og ansvar for både fysisk infrastruktur, stabilitet, it-sikkerhed og beskyttelse af privatlivsoplysninger.

o Kritiske it-tjenester og infrastruktur for forsvar, politi og CPR bør ligge fuldstændig under statens kontrol. Data der er vitale for statens sikkerhed skal kunne verificeres via fysisk inspektion og certificering inden for Danmarks grænser og må ikke komme uden for Danmarks grænser.

Rådet støtter som udgangspunkt de intentioner, der er meldt ud fra både opposition og regering om øget brug af cloud-computing i offentligt regi, men først når de nævnte krav er opfyldt. Rådet ser ingen problemer i, at det offentlige arbejder med konkrete målsætninger i forhold til udbredelse og effektiviseringsgevinster, forudsat at Datatilsynet og andre relevante myndigheder får de fornødne ressourcer til at sikre kvalitet, stabilitet og sikkerhed i nye cloud-løsninger.

Endvidere mener Rådet at det offentliges brug af cloud-computing skal kædes sammen med at alle databrud fremover bliver offentlig- gjort. Rådet opfordrede allerede i 2009 daværende videnskabs- minister Helge Sander til at indføre krav om offentliggørelse af databrud hos både myndigheder og private, og påpegede at det vil være det initiativ, som med mindst mulig indsats vil have størst mulig effekt i forhold til at højne it-sikkerhed og beskyttelse af følsomme persondata.

"Når it-løsningerne bliver mere komplekse, er der brug for mere transparens omkring de problemer, der faktisk opstår. Kun på den måde kan vi sikre, at borgerne fortsat har tillid til de offentlige it-systemer," siger Christian Wernberg-Tougaard.

OM RÅDET FOR STØRRE IT-SIKKERHED

Rådet for Større IT-sikkerhed består af repræsentanter for private og offentlige organisationer samt forskere. Rådet er uafhængigt af såvel politiske, erhvervsmæssige og fagorganisatoriske interesser. Rådets opgave er helhedsorienteret at vurdere mulig- heder og trusler i det digitale servicesamfund, og at være med til at skabe sikre rammer for udvikling af en digital kultur. Rådets arbejdsfelt omfatter blandt andet sikkerhed i forhold til teknik og infrastruktur, sårbarheder i den offentlige it-infrastruktur og adfærdsmæssige problemstillinger i forhold til internettet.

Yderligere oplysninger:

Christian Wernberg-Tougaard, formand

mail: christian@wernberg.org

mobil: 31 22 83 37

Charlotte Bagger Tranberg, næstformand

mail: cbt@law.aau.dk

mobil: 27 77 73 00

Bjørn Kassøe Andersen, kommunikationschef

mail: bka@direction.dk

mobil: 42 44 03 30