VEJLEDNING

Sikkerhedsmæssige overvejelser ved cloud computing og outsourcing

DI ITEK
1787 København V.
3377 3377
itek.di.dk
itek@di.dk

DI ITEK – et branchefællesskab i Dansk Industri for virksomheder inden for it, tele, elektronik og kommunikation

Udgivet af: DI ITEK

Redaktion: Henning Mortensen

ISBN: 978-87-7144-045-4

0.03.15

VEJLEDNING

Sikkerhedsmæssige overvejelser ved cloud computing og outsourcing

BAGGRUND

Digitalisering er helt centralt for, at danske virksomheder kan øge produktiviteten og konkurrenceevnen i en global verden. Derfor er det vigtigt, at virksomhederne tager moderne teknologier og metoder som big data, internet of everything, cloud computing, sociale medier og mobile løsninger til sig.

Cloud computing er af de teknologier, som europæiske virksomheder anser som særligt lovende. Ifølge et studie fra EU Kommissionen[1] brugte 19% af alle europæiske virksomheder cloud computing i 2014. Af disse bruger knapt halvdelen avancerede cloud løsninger til at styre regnskaber, kunder og andre forretningskritiske programmer. Danmark er med til at trække det europæiske gennemsnit op, idet 38% af danske virksomheder bruger cloud computing under en eller anden form.

Nogle af teknologierne ændrer på de behov, der er til sikkerheden for, at data og systemer er til rådighed, når de skal være det (tilgængelighed), er sikre således, at kun dem, der skal have adgang, får adgang (fortrolighed), og således at data kun ændres af dem, der må (integritet).

39% af dem, der bruger cloud computing, betragter risikoen for en sikkerhedsbrist som en begrænsende faktor. 42% af de virksomheder, der ikke bruger cloud computing i dag, betragter manglende viden om cloud computing - herunder sikkerhed - som en begrænsende faktor. Der er derfor god grund til at hæve vidensniveauet om cloud computing og sikkerhed.

Denne vejledning giver anbefalinger til informationssikkerheden, når virksomhederne lader eksterne parter drive og vedligeholde nogle af virksomhedens it-systemer.

I denne vejledning gennemgås det indledningsvis, hvad outsourcing og cloud computing er. Herefter gennemgås de sikkerhedskrav, som en virksomhed bør opstille,

[1] http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises

når de bruger eksterne leverandører. Der konkluderes med en tjekliste for god leverandørsikkerhed.

OUTSOURCING

Outsourcing betyder, at virksomhed køber en ydelse, som den tidligere selv har stået for, hos en underleverandør. Formålet er ofte at opnå en bedre pris eller en bedre kvalitet, ved at anvende en specialiseret leverandør. Outsourcing anvendes af næsten alle virksomheder - f.eks. ved at lægge produktion til fjernøsten eller ved at hyre et rengøringsselskab.

Outsourcing af opgaver i it-afdelingen eller evt. udskillelse af hele it-afdelingen til en serviceleverandør er også meget udbredt. It-outsourcing betyder, at en virksomhed indgår en kontrakt med it-leverandør om at stå for drift og vedligehold af (dele af) virksomhedens it-systemer. Outsourcingpartneren stiller dermed noget it-infrastruktur i form af hardware, software og service til rådighed for kunden. Kunden er typisk i dialog med hostingprovideren om, hvordan han ønsker opgaven skal gennemføres. Kunden kan dermed i et betydeligt omfang påvirke udformningen af løsningen.

CLOUD COMPUTING

Der findes mange forskellige definitioner af cloud computing. Cloud computing defineres af den amerikanske standardiseringsorganisation, NIST, som en software og hardware infrastruktur, der giver let adgang til it-mæssige ressourcer overalt med en minimal indsats[2]. Det Europæiske agentur for Netværks og Informationssikkerhed (ENISA), definerer cloud computing som en servicemodel for efterspørgsel af it-løsninger, der ofte er baseret på virtualisering og distribuerede it-teknologier[3]. Cloud computing vil ofte samtidig indebære outsourcing.

Cloud computings karakteristika

Cloud computing har ifølge NIST fem grundliggende karakteristika: For det første er der tale om efterspørgselsorienteret selvbetjening, hvor kunderne kan tilvælge og fravælge it-ressourcer efter behov. For det andet er ressourcerne typisk direkte tilgængelige over et netværk, og de kan derfor tilgås fra platforme med meget forskellige karakteristika. For det tredje er ressourcerne poolet, således at der ofte serviceres flere kunder på den samme infrastruktur med høj grad af uafhængighed af fysisk lokation. For det fjerde er løsningen fleksibel således, at der kan skrues op og ned for efterspørgslen uden varsel. For det femte måles ressourceforbruget løbende, og der betales kun for de ressourcer, man bruger.

---

[2] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
[3] https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security

ENISA opsummerer karakteristikaene som abstrakte ressourcer, let skalerbarhed og høj grad af fleksibilitet, øjeblikkelig anskaffelse, delte ressourcer, efterspørgselsbaseret service kombineret med at der kun betales for det der bruges og endelig programmerbar styring af de efterspurgte ressourcer.

Cloud computing servicemodeller

Cloud computing har flere forskellige servicemodeller. For det første har vi Software as a Service (SaaS), hvor den software, kunden har købt adgang til, kører på en cloud computing infrastruktur. Kunden skal således ikke selv håndtere hardware, styresystemer, lagerplads osv. Eksempler inkluderer webmail, ERP og CRM-systemer. For det andet har vi Platform as a Service (PaaS), hvor kunden kan placere sit eget software på en cloud infrastruktur. Cloud udbyderen stiller dermed en programmeringsplatform til rådighed - f.eks. en .net eller en javaplatform. For det tredje har vi Infrastructure as a Service (IaaS), hvor kunden får adgang til en hardware infrastruktur, men selv har kontrol med styresystemer, applikationer og lager. Nogle gange nævnes også en fjerde servicemodel, Unified Communication as a Service, som er kommunikationsservices på tværs af forskellige typer af platforme.

Cloud computings implementeringstyper

Der er flere forskellige typer af implementeringer af cloud computing. Den mest almindeligt omtalte er en public cloud, hvor cloud infrastrukturen ejes og drives af en cloud udbyder. En variant er, når en sammenslutning af interessenter (community) sammen ejer og driver en cloud infrastruktur. Det er også muligt at have en privat cloud, som bruges af een kunde, og som enten ejer og driven clouden selv eller får den drevet hos en tredjepart (serviceleverandør cloud). Den private cloud kan fysisk være placeret hos kunden, men kan også være tilgængelig via nettet. Hybrid cloud, er en sammensætning af flere forskellige af de tre førstnævnte cloud infrastrukturer. Ved flere af de forskellige former for cloud computing, er der ikke altid klarhed over, hvor data befinder sig geografisk, hvilket kan skabe juridiske udfordringer. Beskrivelsen af de forskellige former for cloud computing kan sammenfattes som følger:

Traditionel deployment	Privat cloud	Community	Public Cloud
Traditionel deployment er den typiske it-implementering, som de fleste virksomheder benytter idag. Denne deployment kan køre hos kunden og være styret af kunden eller en partner i kundens eget data center. I de fleste tilfælde, sker det altså som en enkelt implementering for en enkelt kunde.	Privat Cloud er cloud computing hos een specifik virksomhed. Med privat cloud, får man mange af fordelene fra Public cloud og med øget control og fleksibilitet gennem dedikerede virksomhedsressourcer. Til gengæld har man typisk selv driften af miljøet og omkostningerne forbundet dermed.	En Community Cloud er når en sammenslutning af interessenter sammen ejer og driver en cloud infrastruktur. En community cloud oprettes typisk, når der skal samarbejdes på tværs af organisationer om konkrete projekter eller om forskning.	Public Cloud er cloud computing med globalt delte ressourcer. Online tjenester som giver fordele som: hurtig skalering, automatiske opdateringer af software, forbrugsafhængig omkostningsstruktur, så kunder kun betaler, for det de bruger.
Hybrid løsning			
Kunder ønsker ofte udvikling af hybride løsninger, hvor man kombinerer de bedste elementer fra privat og public løsninger. Det gør det muligt at beslutte lokation og hvilke roller, der ønskes tildelt henholdsvis de private og de public dele af en løsning.			

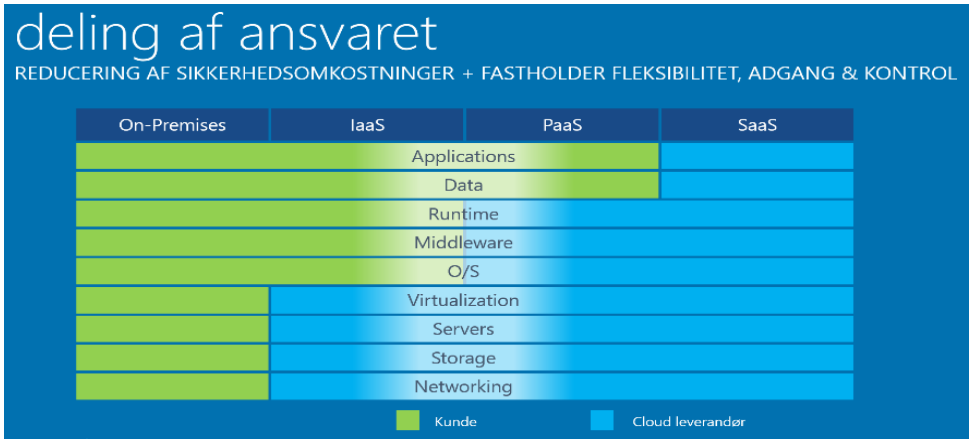
SIKKERHEDSOVERVEJELSER

I tilgift til de ofte klare økonomiske incitamenter, oplever virksomheder der anvender outsourcing- eller cloudleverandører, at der gennem adgangen til specialiserede kompetencer også opnås øget kvalitet i it-systemerne. Outsourcing vil typisk betyde mere direkte dialog med leverandøren og de specialiserede kompetencer, denne er i besiddelse af. Der er også større mulighed for at få skræddersyet systemer. Indenfor cloud computing tilbydes ofte mere standardiserede løsninger, der så til gengæld er billige og skalerbare i betydningen, at man kan skrue op og ned for behovet for ressourcer. Kunden har ved cloud computing ofte ikke mulighed for at komme direkte i dialog med leverandørens specialister. For begge gælder, at de specialiserede kompetencer hos leverandøren betyder, at sikkerheden typisk vil være bedre, end hvad virksomheden selv kan tilvejebringe, hvis virksomheden stiller de krav til leverandøren, som beskrives i denne vejledning. Når virksomheden overvejer at lade andre overtage driften og vedligeholdelsen af sine it-systemer, er det vigtigt, at virksomheden samtidig gør sig nogle overvejelser om sikkerheden. Mindre virksomheder, der hidtil ikke har haft fokus på sikkerhed, vil typisk få forbedret sikkerhed ved at outsource eller bruge cloudløsninger, mens virksomheder, med god fokus på sikkerhed, skal håndtere de ændringer i trusselsbilledet, som følger af at lagre data uden for virksomheden.

Ansvar og kompetencer

Virksomheden kan ikke skille sig af med ansvaret for it-systemerne ved at udskille drift og vedligehold. Virksomheden har stadig ansvaret for, at lovgivningen er overholdt, og at risiko håndteres fornuftigt.

Der er forskellig sikkerhed tilknyttet de forskellige servicemodeller: Ved SaaS kan man således stille krav om at få dokumentation for sikkerhedsniveauet, men ved IaaS har kunden selv langt mere kontrol med it-systemerne og dermed også selv en langt mere aktiv rolle at spille for at skabe et fornuftigt sikkerhedsniveau. Når kunden har systemerne kørende in-house i en såkaldt privat cloud, har man også en meget aktiv rolle at spille. Outsourcingleverandøren kan fungere som mellemmand og skabe hybride løsninger mellem drift on-premise og drift i clouden. Heller ikke i denne situation kan kunden dog skille sig af med ansvaret.



Det er derfor vigtigt, at virksomheden beholder visse it-kompetencer, således at man på et fagligt grundlag kan gå i dialog med sin leverandør. Særlig vigtigt er det, at virksomheden har kompetencer indenfor informationssikkerhed således, at virksomheden kan stille de rette krav til sin leverandør og sikre, at de aftaler, som fremgår af kontrakten mellem de to parter, efterleves. Det er også vigtigt, at virksomheden har kompetencer til at kunne reagere på henvendelser fra leverandøren om eventuelle sikkerhedshændelser. De jurister, som er involveret i kontraktforhandlingerne, skal forstå at beskrive den fordeling af rollerne, som virksomheden selv og dens leverandør skal spille.

Risikoanalyse og dataklassifikation

Inden virksomheden vælger en leverandør, bør der foretages en risikoanalyse og en dataklassifikation.

Risikoanalysen skal kortlægge de risici, som virksomheden står overfor. Der bør altid foretages en risikoanalyse årligt - uanset om der skal vælges en ekstern leverandør eller ej. Risici afhænger af konsekvenser og sandsynlighed for at trusler, som f.eks. hacking og virus, fejl på it-systemer og tyveri af data fra medarbejdere eller andre, får konsekvenser. Der kan med fordel tages udgangspunkt i OCTAVE-

modellen[4], når der skal tilvejebringes et overblik over truslerne. En model for selve risikoanalysen kan findes i ISO27005.

Risikoanalysen skal foruden at adresserer virksomhedens egne risici også kortlægge hvilke risici, der er ved at vælge en ekstern leverandør fremfor selv at drive it-systemerne. Så snart virksomhedens data forlader virksomheden, opstår der nye former for risici - f.eks. kabelbrud, leverandørens manglende evne til at forsætte sin forretning, leverandørens oppetid, leverandørens sikkerhedsniveau set i forhold til hvad virksomheden selv ville kunne tilvejebringe, fremmede landes adgang til data med domstolskendelse og opsnapning af data på internettet på vej til leverandørens datacenter. Omvendt vil andre risici forsvinde, når der vælges en ekstern leverandør. Når der bruges en kombination af servicemodeller, f.eks. en SaaS, der kører på en IaaS, skal risikoanalysen sikre, at der kortlægges risici og stilles sikkerhedskrav, som også tager højde for kombinationen af risici hos de forskellige leverandører. Det europæiske agentur for netværks- og informationssikkerhed har lavet en risikovurdering af nogle af de mest almindelige risici, der er ved at anvende en ekstern leverandør[5].

Desuden skal der på baggrund af risikoanalysen foretages en dataklassifikation. På baggrund af de risici, der findes ved at beholde systemer og data inhouse eller hos en ekstern leverandør, skal det afgøres, hvilke data man vil lægge ud til en ekstern part. Særligt opmærksom skal man være på data, som er forretningskritiske - f.eks. forskningsdata - tillige med data som kan være omfattet af lovkrav - f.eks. personoplysninger eller bogføringsdata.

Sikkerhedsstandarder og best practises

Når man skal vurdere eksterne leverandørers sikkerhed, er det ofte relevant at se på, hvilket holistisk sikkerhedsniveau de kan tilbyde. Der findes flere meget omfattende standarder og best practises, som kan bruges til at foretage en sikkerhedsmæssig vurdering. Vi kan ikke gennemgå dem alle og fokuserer derfor på ISO, NIST, ISAE, CSA og EU.

ISO27001 opstiller krav til, hvordan sikkerheden hos en leverandør styres. Leverandøren skal have implementeret et såkaldt Information Security Management System (ISMS), som sikrer, at sikkerheden er på et konstant højt niveau og løbende forbedres. Som kunde bør man kræve, at standarden efterleves af både cloud- og outsourcingleverandører.

ISO27002 opstiller en række kontrolmål og operationelle kontroller, som leverandøren bør implementere eller argumentere for, hvorfor han ikke implementerer. Kontrollerne sikrer f.eks., at personalet har de rette kompetencer, at sårbarheder i software patches, og at hændelser på systemerne logges. Som kunde bør man kræve, at standarden efterleves af både cloud- og outsourcingleverandører.

---

[4] http://di.dk/Shop/Publikationer/Produktside/Pages/Produktside.aspx?productId=2793

[5] https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security

ISO27001 og ISO27002 bør i forvejen være kendt af virksomhederne, fordi de også typisk bruges til at etablere et forsvarligt sikkerhedsniveau på inhouse it-løsninger. Samlet set stiller standarderne følgende krav:

- Ledelsens ansvar og rolle skal præciseres
- Der skal udarbejdes sikkerhedspolitikker med retningslinjer
- Der skal fastlægges roller og ansvar til forskellige aktører i organisationen
- Der skal ske håndtering af risici og muligheder - herunder risikoanalyse og etablering af kontroller i forhold til: politikker, organisering, personalesikkerhed, styring af aktiver (herunder klassifikation), adgangsstyring, kryptering, fysisk sikring, driftssikkerhed (herunder malware, logning, sårbarheder), kommunikationssikkerhed, anskaffelse, udvikling og vedligeholdelse af udstyr, styring af leverandører, styring af nedbrud, beredskab og compliance med lovgivning
- Der skal laves en målsætning for informationssikkerheden og laves planer for opfyldelse af mål
- Ressourcer, kompetencer og bevidsthed skal tilvejebringes hos organisationens medarbejdere
- Der skal laves planer for, hvordan kommunikation håndteres, herunder hvem der må sige hvad hvornår til hvem
- Det skal dokumenteres, hvilke tiltag der er sat i værk for at understøtte informationssikkerheden
- Der skal ske planlægning og styring af it-driften - herunder vurdering af og håndtering af risici
- Der skal løbende ske overvågning, måling, analyse og evaluering
- Sikkerhedskontroller skal løbende revideres og godkendes af ledelsen
- Der skal være en proces, der løbende sikrer forbedringer

I overordnede termer er det disse krav, som kunderne bør stille til cloud og outsourcingleverandørerne.

NIST har i standarden 800-53r4[6] ligesom ISO opstillet en række krav og kontroller, som bør være på plads for at skabe god sikkerhed. Der er et betydeligt overlap mellem de krav, der stilles i de standarderne, hvorfor de ikke gennemgås detaljeret her. Pointen er, at en leverandør, der er certificeret efter den ene eller anden standard, må forventes at have fornuftig styr på sikkerheden.

Når man skal bruge en cloudleverandør, vil det typisk være vanskeligt at få adgang til de fysiske lokationer, hvor systemer og data kører. Det vil simpelthen være en sikkerhedsbrist for de øvrige kunder at lukke en kunde ind i et datacenter. Derfor lukker man i praksis en ekstern revisor ind, som så på vegne af alle kunderne kan sikre sig, at sikkerhedsniveauet er som ønsket. Den eksterne revisor udarbejder på baggrund af inspektion og dialog med leverandøren en revisionserklæring. Erklæringen dokumenterer, at en række kontroller er implementeret og fungerer. For de almindelige it-kontroller hedder revisionserklæringen ISAE3402[7] (tidligere SAS 70). Erklæringen bruges både af cloud- og outsourcingleverandører, og man bør

[6] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[7] http://www.ifac.org/sites/default/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf

som kunde stille krav om forevisning af disse erklæringer. En sådan revisionserklæring kan være et krav fra den revisionsvirksomhed, der udarbejder kundens eget årsregnskab. I forhold til outsourcingleverandører kan man også i kontrakten stille eksplicitte krav om at få adgang til datacenteret. I forhold til danske outsourcingleverandører har brancheforeningen BFIH lavet et hostingmærke, som udstedes til de leverandører, der lever op til forskellige krav, der går ud over revisionserklæringen.

Som supplement til en ISAE3402 kan man også få en SSAE 16 SOC 2 erklæring. SSAE-erklæringen ser mere på risiko ved, at outsourcing eller cloud leverandørens eget personale udfører bevidst skadelige handlinger end ISAE-erklæringen.

Cloud Security Alliance (CSA) er en organisation af cloud interessenter og brugere, som har lavet en sikkerhedsguide til cloudløsninger, Security Guidance for Critical Areas of Focus in Cloud Computing[8]. Guiden opstiller en række sikkerhedsmæssige krav til styring og drift af en cloud, som cloududbydere og deres kunder bør være opmærksomme på. Guiden indeholder også en del overvejelser om og kortlægger fordele og ulemper ved cloud-løsninger i forskelligt perspektiv. Igen er der et væsentligt overlap med de krav og kontroller, der stilles i ISO- og NIST-standarderne. Guiden er dog mere cloud specifik end de øvrige standarder. CSA har lavet en rigtig god mapping af sine egne kontroller op mod ISO, NIST og en række andre standarder og lovkrav, CSAs Cloud Control Matrix[9].

CSA har også tilvejebragt en certificering af personalets cloud computing kompetencer, CCSK. Hvis man skal i dialog med konsulenter indenfor cloud computing, kan det være værd at se efter denne certificering.

På europæisk plan har der været stor politisk interesse for at få udnyttet de effektiviseringsmuligheder, der ligger i at anvende eksterne leverandører. Foruden ENISAs risikovurdering har EU Kommissionen lavet en strategi for cloud computing. I den forbindelse er der nedsat en række arbejdsgrupper, der skal levere en række produkter, som bidrager til at nedbryde nogle af de sikkerhedsmæssige barrierer ved cloud anvendelse[10]. Produkterne er (i de udkast som i skrivende stund foreligger) meget cloud specifikke og for en dels vedkommende tæt relateret til at skabe compliance med europæisk lovgivning og fortolkningspraksis. Blandt produkterne forventes der at komme:

- en samlet indstilling vedrørende alle de forskellige sikkerhedsstandarder, der berører området
- standard service level agreements, som kan tilknyttes kontrakten mellem kunde og leverandør
- certificering af cloud leverandører
- et code of conduct for cloudleverandører, som bl.a. vil stille krav til behandling af personoplysninger, sikkerhedskrav og kontroller (som igen er

[8] https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf
[9] https://cloudsecurityalliance.org/research/ccm/
[10] https://ec.europa.eu/digital-agenda/en/cloud-computing-strategy-working-groups

meget i overensstemmelse med de kontroller, standarderne peger på) og governance.

Når kunden stiller de ovenfor nævnte krav om dokumentation af sikkerheden hos leverandøren, er det vigtigt at være opmærksom på, om den fremviste dokumentation er gældende for hele den service, kunden køber af leverandøren. Dette er særlig relevant, når leverandørens ydelse er baseret på en kombination af servicemodeller. Hvis der ikke er dokumentation for løsningens helhed, må kunden give sig i kast med en mere manuel risikovurdering af løsningen.

Særlige sikkerhedskrav

Alle rimelige sikkerhedskrav vil blive efterlevet, hvis leverandøren kan dokumentere efterlevelse af en eller flere af de ovenfor nævnte standarder. Nogle virksomheder kan have behov for yderligere præcis dokumentation af efterlevelse af visse kontroller. Man kan derfor undersøge, om der fra leverandøren foreligger eller kan rekvireres:

- resultatet af en penetrationstest
- beskrivelse af sikkerhedsorganisation og - politikker
- beskrivelse af anvendelsen af kryptering af transmitterede og lagrede data, herunder hvordan nøgler opbevares tillige med mulighederne for at anvende sin egen kryptering med egne nøgler
- beskrivelse af hvilke underleverandører der behandler data
- beskrivelse af hvor data befinder sig, herunder indenfor EU
- beskrivelse af hvordan data slettes - herunder på backup, f.eks. jf. standarden for sletning, NIST 800-88r1[11].
- beskrivelse af hvad der logges
- beskrivelse af hvordan håndtering af autentifikation og autorisation hos såvel leverandør som kunde foregår, med henblik på at sikre at der er præcis den adgang til data og systemer, som der er brug for
- beskrivelse af hvordan man kommer i kontakt med leverandører, hvis man har forskellige typer af spørgsmål
- beskrivelse af hvad der sker hvis leverandøren går konkurs, skifter forretningsområde eller bliver solgt, herunder beskrivelse af om kurator holder datacenteret kørende
- beskrivelse af hvordan man bliver orienteret af leverandøren, hvis der er opstået sikkerhedsbrister
- beskrivelse af under hvilket lands lovgivning eventuelle tvister løses
- beskrivelse af hvem der ejer data og hvordan virksomhedens data evt. må bruges af leverandøren, f.eks. til at forbedre tekniske filtre.

Lovkrav til behandling af personoplysninger

Der er en række særlige forhold, som skal iagttages, når de data, der behandles hos leverandøren, er personoplysninger. I Danmark er behandlingen af personoplysninger reguleret i Lov om behandling af personoplysninger (persondataloven)[12]. Denne lov implementerer EU direktiv 95/46/EF, som regulerer behandlingen af

[11] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
[12] https://www.retsinformation.dk/forms/r0710.aspx?id=828

personoplysninger i EU[13]. Outsourcing og cloudleverandører, som behandler personoplysninger om danske borgere, skal iagttage disse regler. I praksis giver dette anledning til, at der er nogle juridiske forhold, som skal håndteres og sikres gennem kontraktuelle og praktiske implementeringer - f.eks. med hensyn til eventuel behandling af data i lande udenfor EU, fordeling af rollerne som dataansvarlig og databehandler samt de øgede sikkerhedskrav til it-løsningen, hvis der behandles personoplysninger.

Da flere af cloududbyderne opererer udenfor EU eller har tredjepartsleverandører, som opererer udenfor EU, skal der være aftaler om udveksling af data.

Der er i retsgrundlaget flere forskellige muligheder for, at personoplysninger kan forlade EU. For det første er de cloududbydere, som er omfattet af Safe Harbour-reglerne, i princippet godkendt. Flere EU-lande stiller dog spørgsmål ved denne godkendelse, fordi der er tale om udfyldelse af en self-assessment. Der pågår pt. forhandlinger mellem USA og EU om at revidere grundlaget for Safe-Harbour reglerne. Et alternativ er at lave Binding Corporate Rules. Men disse regler bruges alene indenfor koncerner og kan typisk ikke anvendes i forbindelse med cloud computing. Et bedre alternativ er at vælge cloud udbydere, som efterlever EU's model clauses[14], der er EU Kommissionens standardkontrakt for udveksling af data med visse lande udenfor EU. Det danske datatilsyn har udtalt sig om betingelserne for at anvende cloud computing løsninger ved behandling af personoplysninger og henviser netop til anvendelse af EU Kommissionens model clauses[15].

Fordelingen af de juridiske roller som henholdsvis dataansvarlig (controller) og databehandler (processor) skal være præcist defineret i kontrakten. Som udgangspunkt vil kunden være dataansvarlig og leverandøren være databehandler. Imidlertid vil der være visse behandlinger, som kræver en konkret juridisk vurdering. F.eks. vil leverandøren ofte kunne anskues som dataansvarlig for administrative processer knyttet til behandlingen[16].

De enkelte lande har fastsat særlige nationale regler, som understøtter fortolkningen af EU direktivet i den nationale lovgivning. I Danmark er der en række bekendtgørelser, som uddyber fortolkningen af persondataloven. En særlig vigtig bekendtgørelse er sikkerhedsbekendtgørelsen[17], som udmønter sikkerhedskravene til it-systemer, der behandler personoplysninger. Bekendtgørelsen gælder kun for den offentlige sektor, men det må anbefales, at også private virksomheder stiller krav om, at deres leverandør efterlever - eller i det mindste lader sig inspirere af - bestemmelserne i bekendtgørelsen.

---

[13] http://eur-lex.europa.eu/legal-content/DA/ALL/?uri=CELEX:31995L0046
[14] http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm
[15] http://www.datatilsynet.dk/afgoerelser/seneste-afgoerelser/artikel/behandling-af-personoplysninger-i-cloud-loesningen-office-365/
[16] http://www.datatilsynet.dk/afgoerelser/seneste-afgoerelser/artikel/behandling-af-personoplysninger-i-cloud-loesningen-office-365/
[17] https://www.retsinformation.dk/Forms/R0710.aspx?id=842

ISO27018 uddyber og supplerer ISO27002 og opstiller nogle ekstra kontroller, som leverandører af cloud computing løsninger bør efterleve, når der behandles personoplysninger. Der er bl.a. tale om følgende kontroller: styring af adgangskontrol, muligheder for anvendelse af kryptering, krav til underleverandører og information under leverandører, log af hændelser, logning af behandling af personoplysninger og håndtering af sikkerhedshændelser. Kunderne kan overveje at stille krav til leverandøren om en fuld implementering af ISO27018, når der behandles personoplysninger.

I den danske fortolkningspraksis stilles der på en række områder krav om anvendelse af kryptering, når personoplysninger transmitteres over internettet, herunder på vej mellem virksomhed og outsourcing eller cloudleverandør. I hovedtræk går Datatilsynets praksis på, at det er obligatorisk at kryptere følsomme personoplysninger og CPR-nummer. Desuden skal der krypteres, hvis det er meddelt som vilkår af Datatilsynet[18]. I en række andre tilfælde er det kun en anbefaling fra Datatilsynet, at der bruges kryptering. I relation til anvendelsen af cloud computing blev det af Datatilsynet meddelt som et vilkår, at der bruges kryptering. Kryptering findes i mange former. Virksomheden skal tage stilling til, om den vil bruge sin egen kryptering, eller om den vil bruge en eventuel kryptering fra cloudleverandøren. Virksomheden skal desuden tage stilling til, hvor kraftig kryptering der skal bruges.

Retsgrundlaget for behandling af personoplysninger i EU stammer tilbage fra 1995, og er derfor i skrivende stund under revision. EU Kommissionen er kommet med et udspil til ny regulering, der har til formål at modernisere, harmonisere og effektivisere reglerne samtidig med, at der gives en bedre beskyttelse af personoplysninger. Når reglerne er vedtaget, vil der komme en to års implementeringsfrist. Vi må derfor forvente, at de i dette afsnit omtalte regler vil blive ændret. Et element i de nye regler, som formodentlig vil blive vedtaget, er kravet om at gennemføre en privacy impact assessment, PIA. En PIA er en risikovurdering ved, at der behandles personoplysninger - set fra den registreredes synspunkt. Det vil være at udvise rettidig omhu at sikre sig, at en sådan analyse laves for de it-systemer, der i væsentligt omfang behandler personoplysninger. Ved anvendelse af meget standardiserede løsninger (SaaS, public cloud) bør det undersøges, om leverandøren har lavet en PIA. Desuden bør virksomheden selv lave en PIA for virksomhedens egen behandling af personoplysninger. DI har lavet en skabelon[19], som med fordel kan anvendes, når man skal lave en PIA.

Kontrakten

Kontrakten mellem virksomheden og cloud- eller outsourcingleverandøren er afgørende for, hvilke services der leveres, og dermed også for hvilket sikkerhedsniveau der aftales. Der kan stilles helt konkrete krav til de enkelte kontroller til outsourcingleverandører - men ikke til cloudleverandører. Derfor stilles de sikkerhedsmæssige krav ofte som henvisninger til efterlevelse af standarder, hvor man så evt. i et vist omfang kan henvise til kontroller, som virksomhedens risikoanalyse har fremhævet som særligt vigtige. Af kontrakten bør det derfor fremgå, at (dele af) de ovenstående standarder efterleves. Desuden bør det fremgå, hvor ofte og i hvilket

[18] http://www.datatilsynet.dk/erhverv/internettet/krav-og-anbefalinger-ifm-overfoersel-af-personoplysninger-via-internettet/
[19] http://itek.di.dk/SiteCollectionDocuments/Vejledninger/DI's%20skabelon%20for%20Privacy%20Impact%20Assessment.pdf

omfang der gennemføres revision og kan forelægges revisionserklæringer. Det er virksomhedernes ansvar løbende kontrollere, at der ikke er bemærkninger i revisionserklæringerne, og at sikkerheden derfor til stadighed er på det aftalte niveau. Kontrakterne bør også indeholde bestemmelser om, hvordan sikkerhedshændelser håndteres samt et krav om løbende rapportering af sikkerhedsniveauet. Virksomheden bør have kompetencer inhouse til at kunne forstå disse erklæringer og reagere på dem. Kontrakter bør udarbejdes af advokatfirmaer med erfaring på dette område.

TJEKLISTE

Cloud computing og outsourcing kan forbedre virksomhedernes produktivitet og konkurrenceevne betydeligt. Det er derfor vigtigt, at virksomhederne adresserer denne nye teknologi. For at gøre brug af teknologien og samtidig fortsat kunne leve op til sit ansvar for behandlingen af data bør virksomheden selv have fokus på sikkerhed og gennemføre en risikoanalyse og en dataklassifikation. Desuden bør virksomheden stille en række sikkerhedsmæssige krav til sine leverandører.

Grundet den høje grad af standardiserede løsninger vil det i en række sammenhænge ikke være muligt at stille specifikke krav om bestemte kontroller til leverandøren. Kunderne er derfor henvist til at stille generelle krav og bør vurdere om leverandørerne kan:

- Fremlægge en ISAE3402-erklæring uden bemærkninger
- Efterleve en eller flere af standarderne:
    - Efterlevelse af eller certificering efter ISO27001 og ISO27002
    - Efterlevelse af eller certificering efter NIST800-53
    - Efterlevelse af eller certificering efter CSA Security Guidance for Critical Areas of Focus in Cloud Computing
- Fremlægge en SSAE 16 SOC 2 erklæring uden bemærkninger
- Fremlægge dokumentation for specifikke sikkerhedstiltag som f.eks. penetrationstests

Hvis leverandøren kan dokumentere efterlevelse af en eller flere af de tre standarder tillige med en ISAE3402-klæring uden bemærkninger, er der rimelig grund til at tro, at sikkerheden er på plads.

Når der behandles personoplysninger i en cloud løsning, skal det desuden undersøges, om leverandøren kan dokumentere:

- Efterlevelse af eller certificering efter ISO27018
- Anvendelse af EUs model clauses ved indgåelse af kontrakt, alternativt at der henvises til en safe harbour godkendelse i kontrakten
- Gennemførelse af en privacy impact assessment
- Efterlevelse af fremtidige guidelines fra EU Kommissionen, som omtalt i denne vejledning.

Hvis leverandøren kan efterleve de punkter, er der rimelig grund til at tro, at der kan behandles personoplysninger i overensstemmelse med dansk lovgivning.

Hverken ved outsourcing eller ved cloud computing er sikkerheden på plads ved at stille krav til leverandøren. Virksomheden skal i kontrakten sikre sig, at det er præciseret, hvilke sikkerhedstiltag leverandøren tager, og dermed hvilke resterende sikkerhedstiltag virksomheden selv skal udføre. Virksomheden bør sikre sig, at den i virksomheden har kompetencer til at stille krav til leverandørerne, være i dialog med leverandøren om eventuelle sikkerhedshændelser og udføre eventuelle egne supplerende sikkerhedstiltag.