

Compliance Management som SaaS og Open Source

af Frederik Helweg-Larsen, CISM, fhl@policyenforcer.dk

Cloud Computing, Open Source og Software-as-a-Service (SaaS) er begreber der tales meget om for tiden, men hvad betyder det for de virksomheder, der skal anvende teknologierne, og er det vejen at gå med følsomme emner som Informationssikkerhed og Compliance? Her er nogle betragtninger.

Vi er i gang med et paradigmeskifte, hvor vi ændrer hele vores opfattelse af softwarelicenser, dataopbevaring og informationssikkerhed. Vi har været vant til, at hardware og software var placeret på virksomhedens lokationer, hvor det var forholdsvis enkelt at gøre status på aktiverne. Alle udgifter vejede tungt ved anskaffelsen og blev så afskrevet over en årrække, samtidig med at der blev betalt for vedligeholdelsen. Sikkerhed var fokuseret på adgangen til virksomhedens netværk og blev håndteret af firewalls og indholdssikkerhed, som også stod placeret i serverrummet.

Alt sammen noget der er omkostningstungt ved anskaffelse og kræver ressourcer og kompetencer at vedligeholde. Dertil kommer, at eventuelle fejlinvesteringer kan sætte deres spor i økonomien i lang tid.

Skiftet fra Licenser til SaaS og Cloud Computing

Vi ser nu, at mange teknologier bliver flyttet over til services man abonnerer på uden opstartsomkostninger. Det kender vi allerede fra e-mail, website systemer, økonomisystemer, salgsstyring med mere. Google er vel den mest kendte udbyder af både applikationer, sikkerhed og services, der alle ligger i "skyen".

SaaS er en delmængde af begrebet Cloud Computing^{*)}. Cloud Computing er et udtryk for, at (alle) data og services er hosted uden for virksomhedens netværk. De tre mest udbredte komponenter i cloud computing er SaaS, PaaS og IaaS. En variant af SaaS går på at modtage software, der implementeres på virksomhedens interne servere og afregne licensen med leverandøren på månedlig basis.

Hele tankegangen med SaaS er, at udgifterne følger den værdi, man får af at anvende den applikation eller service, som man betaler leje til. Der er ingen stor startudgift, ofte er der heller ikke nogen bindingsperiode, og man betaler en fast månedlig ydelse, der er kendt på forhånd. Dette betyder, at leverandøren hele tiden skal være sikker på, at kunderne er tilfredse med ydelserne, da de ellers forsvinder. Samtidig kan man som kunde opsige sin aftale, såfremt udbyttet ikke var som forventet. Det stiller altså større krav til leverandørerne.

Hvad så med Open Source?

Det er også "hot" at tale om Open Source for tiden, navnlig inden for staten, hvor det er en målsætning at løse flere opgaver med Open Source software. Man kan være tilbøjelig til at tro, at Open Source betyder gratis software, der ikke er forbundet med nogen omkostninger at anvende. Sådan er det dog ikke. De fleste leverandører af Open Source applikationer har velfungerende virksomheder, der skal tjene penge for at overleve, så man skal holde godt øje med de betingelser, der er forbundet med anvendelse af produkterne.

Open Source produkter er altid underlagt en licensaftale ^{**) der beskriver reglerne for anvendelse. Sådanne licensvilkår giver altid ret til at afvikle programmet, se kildekoden, lave ændringer heri og videredistribuere såvel original som ændret kode. Ofte vil der tillige gælde en forpligtelse til, at alle de ændringer til kildekoden, som man selv har lavet, ved videredistribution skal medfølge selv som Open Source, og at ingen dele af koden må videresælges. Vil man arbejde videre med Open Source, er det dermed til fællesskabets bedste. Leverandøren af den oprindelige kildekode kan derimod godt beslutte at videreudvikle Open Source versionen og frigive resultatet som en betalt licens. Det kaldes ofte dual licensing. Leverandøren (licensgiveren) i modsætning til licenstagere har altså særlige rettigheder på grund af ophavsretten.}

Der er sjældent support på Open Source fra andre end andre brugere af samme software, men der kan ofte tegnes en supportaftale med leverandøren, og i det hele taget er det altid godt at sætte ind licensvilkårene. ^{***)}

Hos Policy Enforcer har vi valgt at anvende begge modeller, og har således en Open Source version der leveres uden beregning til én bruger, og en SaaS løsning til virksomheder der ønsker support og altid opdateret software. Da begge løsninger deler platform og data, så kan man altså frit flytte informationerne efter behov. På den måde dækker vi alles behov bredest muligt, og modtager kun betaling for service, vedligeholdelse og support af SaaS løsningen der er målrettet virksomheder.

Tør man lægge sikkerheden ud i skyen?

Når man afgiver kontrol over sikkerheden, og i stedet skal stole på en leverandørs sikkerhed, så kan det give anledning til bekymring. Det bliver man nødt til at tage stilling til, hvis Cloud Computing skal være en fremtidig platform. I forvejen har de fleste tillid til deres leverandører af IT sikkerhed, og om man stadig har det, når teknikken er placeret uden for eget netværk, bør bero på en individuel risikovurdering.

Jeg mener, at man bør stille krav til sin leverandør om fortrolighed, integritet og tilgængelighed af data med den interne sikkerhedspolitik som udgangspunkt. I mange tilfælde vil en leverandør af *Cloud Computing Services* kunne stå inde for en aftale, der er bedre, end hvad der ville være rentabelt at håndtere internt.

Hvad skal man så være opmærksom på?

Inden indgåelse af en SaaS-aftale bør man tage stilling til nogle spørgsmål vedrørende kvalitet og sikkerhed. Her er nogle punkter til inspiration:

- **Service Level Agreement (SLA)**

Denne aftale bør beskrive forhold som oppe-tider, sikkerhed, backup-services o.l.

- **Bindinger**

På samme måde som vi kender det fra teleselskaber, kan der være bindinger i aftalen, der betyder, at der som minimum er udgift til drift i en fastsat periode. Der kan også være opsigelsesfrister, der påvirker økonomien. Tag disse forhold med i overvejelserne og det samlede regnestykke.

- **Sikkerhed**

Vurder sikkerheden i forhold til krypteret trafik, sikkerhed ved login og en generel vurdering af udbyderens troværdighed. Det kan være svært at foretage en konkret test af leverandørens sikkerhed, så der er ikke nogen enkel løsning på dette spørgsmål.

- **Dataejerskab**

Man bør sikre sig at dataejerskabet ligger hos en selv som kunde, og at det er muligt at eksportere

data på en enkel måde. Så vil der altid være mulighed for at flytte data hjem igen, hvis den hostede løsning ikke lever op til forventningerne.

- **Support**

Det er altid vigtigt med god support. Hvilke svartider har leverandøren og kan de kontaktes på andre måder end e-mail? Bed eventuelt om referencer og tal med andre der anvender samme service.

Der kan findes flere oplysninger om sikkerhedsovervejelser i forbindelse med cloud computing i "DI ITEK og DIs vejledning om cloud computing" ****).

Compliance som service

Hos Policy Enforcer har vi valgt at ændre vores salgsmode til udelukkende at være en SaaS ydelse. Der er nu kun et valg mellem en OnSite løsning (installeret på lokalnettet) og en OnLine løsning (Cloud Computing). Vi ved af erfaring, at værdien af et system til Compliance Management virker moderat i starten, og bliver betydelig mere markant over tid. Jo længere man anvender systemet, jo mere værdi giver det. Derfor var det oplagt at tilpasse prissætningen, så den modsvarer den oplevede værdi.

Derudover har vi frigivet Policy Enforcer version 2.0 som Open Source med et udvalgt DS484 indhold. Denne version er tiltænkt udviklere af nyt indhold inden for f.eks. miljøregler, CO2-udledning, arbejdspladsvurderinger eller personalepolitikker. Anvendelsesmulighederne er mange.

Compliance Management giver ledelsen et overblik over de interne politikkers efterlevelse og er med til at identificere og minimere risici. Interne processer kan effektiviseres og virksomhedens troværdighed kan styrkes. Der er mange gode grunde til at have systemer til at styre compliance, så hvis det er på tide at skifte regnearket ud så overvej en SaaS løsning.

Prøv det...

Den bedste måde at få erfaringer på er ved at kaste sig ud i en test af de SaaS/Cloud løsninger der er relevante for jeres virksomhed. Stil spørgsmål og få en fornemmelse af kvalitet og service.

De fleste tilbyder prøveperioder på deres services, og vil gerne hjælpe mulige nye kunder i gang.

Hvis du er interesseret i mere information om Policy Enforcer SaaS – så klik ind på www.policyenforcer.dk

Link:

*) Se en video der forklarer mere om Cloud Computing på <http://vimeo.com/8309586>

**) Læs mere om Open Source licenser på www.opensource.org

***) Kontakt advokat Martin von Haller Grønæk vedr. Open Source og licensregler på <http://www.bvhd.dk/>

****) <http://di.dk/shop/publikationer/produktside/Pages/Produktside.aspx?productid=8036>