Cloud tjekliste

- din sikre vej ud i skyen

En samling operationelle tjeklister, der tager højde for, at dit it-arbejde foregår i en ny verden:

- Kontrakten med cloud-udbyderen er omdrejningspunktet
- Tilgængeligheden er SLA'en, og SLA'en er produktet
- Din eneste sikkerhed er backup!

KomplexIT

makes complexity simple

Tjekliste for en sikker og ansvarlig cloud-service og -infrastruktur

Cloud er rykket ind i de danske virksomheder, store som små. Overvejelserne går ikke længere så meget på, *om* man skal basere sin it-infrastruktur på cloud, men snarere *hvordan* og *hvor meget.*

Mange virksomheder sender deres it-infrastruktur ud i skyen i den tro, at cloud-udbyderne leverer en samlet pakke af sikker infrastruktur. Men det gør de som udgangspunkt ikke. Uden at vide det lader virksomhederne ansvaret forsvinde den samme vej som deres it-infrastruktur: ud i det blå.

Hvis du vil udnytte det enorme potentiale i cloud på en sikker og ansvarlig måde, skal du være opmærksom på en række forretningsmæssige, juridiske og sikkerhedsmæssige forhold. Den helt korte konklusion er:

- **Kontrakten med cloud-udbyderen er omdrejningspunktet**
- **Tilgængeligheden er SLA'en, og SLA'en er produktet**
- **Din eneste sikkerhed er backup.**

Vi uddyber ovenstående bullets på de følgende sider i en række tjeklister, som kan klæde dig på til at gøre dig de nødvendige overvejelser og stille de kritiske spørgsmål, så din virksomhed kan udnytte potentialet i cloud på en sikker og ansvarlig måde.

Kontrakten med cloud-udbyderen er omdrejningspunktet

Cloud er et paradigmeskifte fra at eje til at leje software og hardware. Virksomheder har i årtier tænkt it inden for nogle givne rammer og forudsætninger, men med cloud er verden ikke længere den samme.

Cloud kræver et nyt mindset. Det forretningsmæssige beslutningsgrundlag for at vurdere, om man skal udnytte cloud, og hvordan og hvor meget, baserer sig nu på, at du ikke er ejer, men lejer. Og kontrakten med din cloud-leverandør er blevet omdrejningspunktet.

Jo højere modenhed og professionalisme hos cloud-udbyderen, jo mere optimeret og standardiseret et det maskinrum, du får adgang til. Forretningsbetingelser og procedurer er optimeret og standardiseret. Derfor kan du som regel ikke ændre på kontrakten med din cloud-leverandør – men se det som et sundhedstegn og vælg så den leverandør, der passer bedst til jer.

For at vælge den rette cloud-leverandør og -løsning skal du indledningsvist afklare, om I har særlige, ufravigelige krav til jeres cloud-løsning, og om kravene kan opfyldes af den pågældende leverandør. Så undgår du at investere unødig tid og ressourcer i at undersøge en cloud-løsning, som i sidste ende alligevel ikke kan opfylde jeres behov.

Tjekliste for indledende overvejelser ved valg af cloud-leverandør

Understøttelse af forretningen

- Er jeres formål med og ønsker til cloud-løsningen klare?
- Hvis it er forretningskritisk – deponerer I jeres competitive edge ved at vælge en – standard-/branche-løsning i skyen?
- Hvad har forretningen brug for, at løsningen leverer af funktionalitet?
- Har I garanti for, at løsningen bliver ved med levere lige netop det, som er vigtigt for jer?
- Kan I risikere, at løsningen bliver udviklet i en retning, hvor den ikke længere opfylder jeres behov?

Krav til serviceniveau

- Afgør med jer selv, hvad der er *need to have*, og hvad der er *nice to have*
- Afvej risici og omkostninger.

It-arkitektur og integration

- Byg it-services sammen, ikke it-arkitekturer
- Hvis I lægger workloads ud, som er afhængige af internettet, så husk at internettet er *best effort*, ikke *best quality*
- Fokuser ikke kun på services, fokuser også på netværk og datacenterfundamentet.

Økonomisk kalkule

- Evaluer cloud-løsningens reelle pris over 3 eller 5 år for at vurdere, om det er en god investering. Medtag også risiko for prisstigninger
- Hvis I overvejer at vælge en cloud-løsning pga. omkostningsreducering, skal I sikre jer, at det reelt er muligt at opnå besparelserne.

Sikkerhed

- Krav til sikkerhed – er der tale om særligt forretningskritiske eller sensitive data?
- Hvordan opnås sikkerhed – hvilket sikkerhedsniveau tilbyder leverandøren?
- Kender I grænsefladerne – hvor overtager leverandøren ansvaret for jeres data?
- Behov for ændring af interne processer – overvej om det ønskede sikkerhedsniveau kan opnås ved at ændre egne, interne procedurer
- Vurder leverandørens sikkerhed både før aftaleindgåelse og efterfølgende – er det muligt at få adgang til erklæringer fra uafhængig tredjemand om sikkerhed? Hvordan sikres det, at I modtager besked om sikkerhedsbrud?
- Kan leverandøren redegøre for, hvor jeres data er?
- Får leverandøren adgang til data – i så fald, hvordan kontrolleres denne proces?

Compliance

- I kan kun vurdere, om I kan/må bruge en bestemt leverandør, hvis I kender jeres egne risici og dermed jeres krav til sikkerhedsniveau og de deraf afledte kontrolmål:
  - Pas på, hvis der er tale om brug af cloud, initieret af et moderselskab, men reelt på vegne af hele koncernen, som kan bruge tjenesten
  - Sikkerhed: ekstern sikkerhed, intern sikkerhed
  - Lovkrav
  - Særlige vilkår stillet af Datatilsynet i en tilladelse, eller af andre myndigheder
- I har pligt til at foretage en vurdering af compliance og sikkerhed hos leverandøren, før I begynder at bruge tjenesten, og der er krav om, at I løbende følger op på aftalen, både i forhold til compliance og sikkerhed
- I har pligt til at overholde danske krav, selv om I bruger en leverandør uden for Danmark
- I skal vide, hvor jeres data opbevares fysisk – dvs. I skal kende den præcise beliggenhed af datacentre. Et servicecenter er også et datacenter – læseadgang svarer til opbevaring

Hvis cloud-løsningen behandler persondata, skal I sikre, at persondataloven overholdes:

- **Leverandøren skal handle inden for rammerne af en instruks – også hvor der er tale om ren opbevaring af data**
- **Der skal foreligge en skriftlig databehandleraftale**
- **Behandlingen hos leverandøren skal opfylde de krav, som I selv skal opfylde, og I skal føre kontrol med opfyldelse af kravene.**
- I skal kende til og godkende cloud-leverandørens eventuelle brug af underleverandører, som skal leve op til alle formelle og materielle krav
- Overførsel af data til lande uden for EU/EØS kræver et særligt grundlag
- Er der tale om bogføringsdata, kan I placere sådanne data i skyen uden tilladelse fra Erhvervsstyrelsen, hvis en række vilkår er opfyldt
- Vær opmærksom på eventuelle relevante myndighedskrav.

Exit

- Kan ydelsen hjemtages eller nemt leveres af tredjepart?
- Har leverandøren en procedure for exit – og har leverandøren vellykkede eksempler på exits?
- Har I behov for behandling af opbevarede data efter kontraktens udløb, fx af lovgivnings-mæssige eller forretningsmæssige grunde
- Kan I få data ud i et format, så I kan gemme dem?

Tilgængeligheden er SLA'en, og SLA'en er produktet

Med cloud sker der et skifte fra at eje til at leje: du begynder nu at leje dig ind på en softwareløsning, på en platform eller i en infrastruktur. Produktet er ikke længere noget fysisk, men en service, og SLA'en er udslagsgivende for tilgængeligheden til den pågældende service.

Når din leverancemodel ændrer sig fra at eje til at leje, sker der samtidig et tab af kontrol. Vurdér derfor kontrakten i et samlet risikoperspektiv, hvor tab af kontrol og de potentielle risici herved holdes op mod den potentielle gevinst.

Indledningsvist har du vurderet din potentielle cloud-leverandør i forhold til understøttelse af din forretning, krav til serviceniveau, it-arkitektur og integration, økonomisk kalkule, sikkerhed, compliance og exit (jf. tjekliste for indledende overvejelser ved valg af cloud-leverandør).

Med vurdering af implementeringsrisiko, produktrisiko, leverancerisiko og modpartsrisiko får du afdækket 80-90 % af de forhold, I bør afdække. I kan have særlige behov, som bør afdækkes særskilt.

Tjekliste for implementeringsrisiko

- Understøtter cloud-løsningen jeres processer?
- Kan et gap håndteres?
- Er der behov for særlig implementering, herunder med andre systemer?
- Hvordan sikres integrationer?
- Hvordan håndteres ansvarsfordelingen ved implementering – eksempelvis hvis implementeringen ikke lykkes?
- Kan I komme ud af cloud-kontrakten, hvis implementeringen mislykkes (udtrædelsesret)?

Tjekliste for produktrisiko

- Hvad er produktet, hvordan udvikles det, og forbliver produktet det samme?
- Kan I få indflydelse på, hvordan produktet udvikles i fremtiden?
- Er produktets funktionalitet baselined i cloud-kontrakten?
- Hvad er inkluderet, og hvad er tilkøb?

- Nyudvikling – er det et selvstændigt modul eller udvidelse af den bestående løsning?
- Er roadmap tilgængeligt og ligger det fast, hvem der bestemmer?
- Har I mulighed for at deltage i leverandørens udviklingsfora?
- Fortrolighed og competitive edge – især vigtigt at overveje, hvis jeres forretning differentierer sig på it-løsninger.

Tjekliste for leverancerisiko

- Tilgængeligheden er SLA'en
- SLA'en er produktet
- Ofte er det ikke muligt (og ikke ønskeligt) at ændre på servicemål og måle-metoder, men konsekvenserne af manglende overholdelse kan i et vist omfang godt adresseres individuelt
- Priser og fiksering af disse er et centralt emne, som også bør tænkes ind
- Forsikring som mitigering af risiko?
- Hvilke servicemål (om nogen) garanteres i forhold til oppetid, tilgængelighed og svartid, og hvordan og hvor måles performance?
- Hvilke sanktioner har du, hvis leverandøren ikke overholder servicemålene?
- Bed om oplysninger om leverandørens performance-historik.

Tjekliste for modpartsrisiko

- Er det en 'solid' leverandør?
- Back up og adgang til data?
- Hvordan er I stillet, hvis leverandøren går konkurs, eller adgangen til cloud-løsningen på anden vis ophører?
- Escrow (sikring af source code, hvis leverandøren eksempelvis går konkurs) – hvordan, hvornår og af hvem?
- En escrow-aftale skal omfatte udvikling, vedligeholdelse og drift
- Escape pod eller 'den sikre vej ud', fx spejling på en ekstra lokation.

Din eneste sikkerhed er backup

Ransomware, malware, phishing... fortsæt selv listen over ubudne gæster og uønsket adgang til virksomhedens it-systemer og -infrastruktur. Lige så mange måder, hvorpå uønskede gæster kan skaffe sig adgang til jeres data, næsten lige så mange bud er der på, hvordan du kan købe dig til sikkerhed og tryghed.

Men reelt er der kun én måde at sikre jeres data: backup. De rette backup-procedurer og -politikker er dit eneste, reelle værn. Firewall, kryptering, betaling af løsepenge eller eksterne konsulenter kan ikke redde hverken data eller pc'er ved et angreb. Hverken før, under eller efter.

Det betyder dog ikke, at du kan nøjes med backup for at sikre jeres data. Du bør sikre, at antivirus er opdateret, og at brugerne kun har rettigheder til de data, de skal bruge. Jeres brugere bør ikke være lokale administratorer på deres pc, medmindre de har absolut behov for det. Og så skal du sørge for løbende at informere brugerne om risikobilledet i erkendelse af, at brugerne er det vigtigste – og det svageste – led i jeres sikkerhedskæde.

Udviklingen inden for ransomware og malware er et kapløb, hvor virksomhederne hele tiden ligger bagerst i feltet. Forrest ligger en industri af it-kriminelle, og de løber stærkt. Derfor: Din eneste reelle sikkerhed er backup pakket ind i de rette backup-procedurer og -politikker.

På næste side finder du vores tjekliste for data, remote backup og beredskabsplaner, så du kan sikre dine data bedst muligt – i skrivende stund.

Tjekliste for data

Indsigt i den fysiske sikkerhed i udbyderens datacenter

- Hvem kan få adgang til datacenteret – kunder, gæster, leverandører?
- Hvor mange lag af fysisk sikkerhed er der implementeret – kort, kode, biometric scannere og sluser?
- Power supply – N+X og gerne redundant by-strøm?
- Avanceret brandbekæmpelse og vanddetektorer?
- Vagt/bemanding 24/7?

Hvor opbevarer cloud-leverandøren jeres data?

- Hvor er datacenteret placeret geografisk?

Opbevarer cloud-leverandøren data inden for EU/EØS?

- Sørg for at lave en skriftlig aftale – ofte kaldet en 'databehandleraftale'.

Udbyderens overholdelse af kvalitetsstandarder?

- Overholder leverandøren de mest gængse standarder – 3402, 27001 / ISO22301, SOC 2?

Hvor godt kender I jeres leverandør – personligt, renommé?

- Har I allerede et kunde-/leverandørforhold, har I besøgt jeres leverandør og set faciliteterne?
- Eller kender I dem overhovedet ikke?

Hvilken type storage benytter udbyderen?

- JBOD-diske eller RAID
- Interne diske eller enterprise storage systemer
- Easy Tier/SSD som JBOD eller RAID
- Garanti for IO/performance på storage
- Spejling af data til sekundært datacenter.

Virtuelle servere hos udbyder, hvem tager backup af dem?

- Ansvaret er oftest todelt, udbyderen sikrer jer som oftest mod disaster, dvs. hardware- og datacenterfejl – men det er ikke en selvfølge
- Det er altid virksomhedens ansvar at sikre data, fx i Office 365, OneDrive, Hosted SQL eller lign.

Hvem har adgang til data?

- Hvilket personale drifter jeres servere?
- Benyttes der underleverandører?
- Screening for it-kriminalitet hos udbyderens personale?

Har udbyderen både adgang til backupdata og live data?

- Hvis udbyderen også tager backup af jeres data, har driftspersonalet så adgang til både klienter og backup-systemer?

Generelle sårbarheder, bl.a. SSL v2-protokollen på hostede servere

- DROWN (Decrypting RSA using Obsolete and Weakened eNcryption)

RDP (Remote Desktop Protocol)/SSH (Secure Shell) direkte fra internettet uden ACL (access control list)?

Firewall foran hostede servere, findes/findes ikke?

Kryptering af data på hostede servere?

Løbende patch management af hostede servere?

Tjekliste for remote backup

- Backup-frekvens, hvor hyppigt skal der tages backup af jeres data: dagligt, ugentligt, hver 2. time?
- What's in/what's out - sikre at der er backup af alle nødvendige filtyper, drev, volumes, databaser m.m.
- Backup-historik, hvor lang tid skal data gemmes, for at I overholder evt. krav fra revision?
- Transport af backup-data – er data krypteret under transport mellem jer og udbyderen?
- Opbevaring af backup data – gemmes data i krypteret format hos udbyderen?
- Spejling af backup data – er data placeret i flere brandceller/datacentre hos udbyderen?
- Hvem har adgang til backup-data, og har udbyderen både adgang til backup-data og live data?
- Hvem kan restore jeres data, og hvilken sikkerhed er implementeret i forbindelse med restore?
- Restore-tid – hvor hurtigt kan I restore jeres data i forbindelse med fx servernedbrud?
- Restore-test – kan I restore de data, som I forventer?
- Har leverandøren en beredskabsplan for håndtering af virusangreb?

Tjekliste for beredskabsplaner

- Har I lavet en nødplan for, hvad der skal gøres, når det sker? Oftest skal der handles hurtigt – 'stands ulykken'
- Har I testet, om planen virker i praksis? Hvordan får I fat i planen, hvis virksomhedsdata nu er krypteret – er den tilgængelig offline?
- Løbende restore tests fra backup, også de komplicerede systemer, fx SQL, Oracle, DB2, Exchange?
- Awareness om beredskabsplaner, nødplaner og procedurer – er alle medarbejdere bekendt med de procedurer, der er beskrevet, og hvor de findes?
- Eskalation og informationsprocedurer – hvem skal have hvad at vide, og hvor hyppigt skal der gives en opdatering på problemløsningen?

Næste skridt

Vil du vide, om du har en sikker og ansvarlig cloud-service og -infrastruktur? Med en udvidet ransomware-analyse fra Komplex it får du:

- Overblik over virksomhedens sikkerhedsværktøjer og hvilke områder af din infrastruktur, der er beskyttet, og hvilke der muligvis ikke er
- En vurdering af virksomhedens beredskabsplaner og eventuelle faldgruber
- En gennemgang af virksomhedens backup-politikker og forventet nedetid i tilfælde af virusangreb, samt forslag til eventuelle ændringer
- Gennemgang og dokumentation af brugernes privilegier
- Afdækning af brugernes adfærd og trykprøvning af virksomhedens sikkerheds-politikker i forbindelse med virustrusler
- Gennemgang af cloud-kontrakter og tilhørende SLAen for at afdække virksom-hedens sårbarhed.

Kontakt Komplex it for at høre mere om, hvordan du sikrer din cloud-service og -infrastruktur bedst muligt.

Tjeklisten er udarbejdet den 20. april 2016 i forlængelse af vores halvdagsseminar 'Hvem har ansvaret for din sky?' afholdt i samarbejde med Plesner Advokater og IBM Softlayer i marts 2016.

Tilmeld dig Komplex it's nyhedsbrev for at holde dig opdateret med vores anbe-falinger inden for storage-, server- og backup-løsninger i skyen.

KomplexIT

makes complexity simple

Komplex it A/S - Øst
Lyskær 13B
2730 Herlev
Telefon: 7027 7330

Komplex it A/S - Vest
Klamsagervej 35
8230 Åbyhøj
Telefon: 7027 7330

Hos Komplex it er vi alle specialister, der på hvert vores område udelukkende fokuserer på at lave det absolut bedste og mest økonomiske fundament til jeres it-løsning. Vi designer, leverer og drifter server, storage og backup, så alle medarbejdere i jeres virksomhed - it-ansvarlige, slutbrugere og ledelse - får præcis det it-grundlag, de har behov for til at kunne levere en optimal arbejdspræstation, hver dag, året rundt.

Når vi leverer din it-infrastruktur, bestemmer du selv, om udstyret skal stå hos os, hos dig, eller om vi skal levere som en hybridløsning.

Sammen med Komplex it kommer tingene ned på jorden, og I får en gennemtænkt, overskuelig og fremtidssikret server-, storage- og backup-løsning.