En praktisk och lite enklare checklista för införskaffande, användning och lämnande av molntjänster

Version: 1.0
Publiceringsdatum: 2015-08-24

Förord

Syftet med denna praktiska och lite enklare checklista är att hjälpa beslutsfattare, främst hos slutanvändarorganisationer, på strategisk, taktisk och operativ nivå vid införskaffande, användande och lämnande av molntjänster. Checklistan innehåller en del av de säkerhetsfrågor som behöver ställas och redas ut. En mer utförlig och avancerad checklista runt molnsäkerhet [1] finns för övrigt att tillgå på CSA Swedish Chapters hemsida[1].

Om du som läsare har idéer till förbättringar av skriften så tag gärna kontakt med kontaktpersonen för den senaste versionen av dokumentet.

Versionshistoria

Version	Skribenter	Publicerad
1.0 första versionen	**Projektledare/Editor**: John Lindström (LTU) **Skribenter**: Lars Magnusson, Patric Sporrong, Ulf Berglund, Jan A Andersson, Ove Bristrand, Jan Wellergård, Karl-Mårten Karlsson, Nada Kapidzic Cicovic, Lars Perhard, Christina Arrhult Björk och Maria Nyrén-Ivarsson. **Kontaktperson**: john.lindstrom@ltu.se	2015-08-24

Innehållsförteckning

1. Introduktion 4
2. Kort orientering om lagar, regleringar, standarder, etc. som berör molntjänster 5
3. Praktisk checklista för säkerhet i molntjänster 7
4. Sammanfattning 12
5. Källhänvisning 12

Ordlista och förkortningar

XaaS	X-as-a-Service – används för att benämna "något" eller "allting" som en tjänst.
IaaS	Infrastructure-as-a-Service.
PaaS	Platform-as-a-Service.
SaaS	Software-as-a-Service.
SECaaS	Security-as-a-Service.
AD	Active Directory. En katalogtjänst där man förvarar och kan hämta information om resurser i en domän, såsom t.ex. användare, datorer och annan utrustning. AD kan även ge tillgång till flera tjänster.
ADFS	Active Directory Federation Services. En tjänst som bidrar med single sign-on funktionalitet där federerade identiteter kan användas.
API	Application Programming Interface. Ett definierat gränssnitt till en tjänst som tillgängliggjorts utåt så att andra skall kunna använda sig av hela eller delar av tjänsten genom att anropa den.
Due diligence	En vanligt förekommande procedur som innebär en genomgång av t.ex. ett företag för att upptäcka fel, brister, svagheter och risker med mera samt även det som är bra och styrkor. Proceduren genomförs vanligen i samband med större/viktiga affärer eller uppköp av företag för att förstå risknivån.
ENISA	EUs centrala organisation för nätverks- och informationssäkerhet.

[1] https://chapters.cloudsecurityalliance.org/sweden/research/

Härdning	Ett begrepp som innebär att en mjukvaruplattform ”härdas” genom att säkerhetshål tätas igen och att alla onödiga tjänster och program som innebär risker eller intrångsmöjligheter tas bort eller inaktiveras.
ISO270xx	ISO är en internationell standardiseringsorganisation och deras 27000-serie berör informationssäkerhet i olika bemärkelser.
OSL	Offentlighets- och sekretesslagen (2009:400).
OWASP	Open Web Application Security Project. Organisation som letar efter och publicerar säkerhetsrelaterade problem och brister i syfte att organisationer skall kunna göra riskbedömningar och avhjälpa eventuella problem och brister.
PCI-DSS	Payment Card Industry Data Security Standard. Standard för att upprätthålla hög säkerhet – främst använd när personlig information och betalkortsinformation är inblandat.
SAML	Security Assessment Markup Language. Ett XML-baserat dataformat för utbyte av autentiserings- och auktorisationsdata mellan parter. Används ofta i single sign-on sammanhang.
Säkerhet	När termen säkerhet eller informationssäkerhet används, så inbegriper den säkerhet för IT, informationssystem och information.

Before you read this document…please read:

This document has been written for use mainly within Sweden, and although most of the aspects discussed are of a general nature, readers should have this fact in mind while reading.

These guidelines should not be construed as technical or legal advice on any specific facts or circumstances. The content is not exhaustive and is intended for limited general informational purposes only. The authors make no representations as to accuracy, completeness, actuality, suitability, or validity of any information and will not be liable for any errors, omissions, or delays in this information or any losses, injuries, or damages arising from its display or use. All information is provided on an as-is basis with no warranties, and confers no rights. Readers should consult appropriate technical, accounting or legal consultants concerning any specific question or the relevance of the subjects discussed herein to particular factual circumstances.

1. Introduktion

Denna skrift berör ett antal vanligt förekommande frågeställningar rörande säkerhet som kan uppkomma vid införskaffande, användning och lämnande av molntjänster. Tanken med checklistan är att den skall vara praktisk och lite enklare att använda än den mer utförliga checklistan[1]. Primärt är syftet är att hjälpa beslutsfattare, främst hos slutanvändarorganisationer, på strategisk, taktisk och operativ nivå att börja ställa rätt säkerhetsfrågor vid rätt tillfälle. Förhoppningen är dock att även andra som arbetar med t ex inköp, drift och olika ledningssystem med fördel kan ta del av skriftens innehåll också. Sålunda önskar den här enkla anvisningen förmedla några goda råd vid anskaffning och användning av molntjänster.

Vanliga IT-tjänster upphandlas oftast via företagets eller myndighetens stödfunktioner och kan kräva både tid och resurser av organisationen. Allt som behövs för att använda en molntjänst, är en mobil, surfplatta, dator eller annan enhet med internetuppkoppling, vilket gör molntjänster attraktiva att använda men kan samtidigt punktera de gängse säkerhetsrutinerna i organisationen såvida inte viss försiktighet tas i beaktande.

Molntjänster [2] kan definieras som en modell för att möjliggöra tillgång till IT-resurser som efter egna önskemål kan anpassas för olika elektroniska tjänster. Det kan handla om tjänster för tillgång till t.ex. säkerhet (SECaaS), nätverk (Network-as-a-Service), virtuella servrar (IaaS), lagring (Storage-as-a-Service), mjukvara som en tjänst (SaaS), eller hela plattformar för utveckling och drift av lösningar (PaaS).

Vad gäller molntjänster så kan en leverantör av molntjänst i sin tur använda sig av molntjänster för att leverera sin helhet. Detta kan skapa en komplexitet ibland annat avtalsstrukturen med många aktörer inblandade och svårighet att få överblick över vad man som beställare faktiskt beställer av en leverantör. Detta kan behöva klarläggas för att förstå vem som verkligen ansvarar för vad och hur.

Molntjänster är attraktiva för användaren eftersom de oftast har låga inträdeskostnader t.ex. för att börja utveckla programvaror eller för att dela information med andra. Användaren behöver inte vare sig köpa in hårdvara eller dyrbar programvara, och det är i vissa fall bara att skapa ett konto i molntjänsten och börja använda den. Kostnadsbilden är också attraktiv eftersom användaren, dock beroende lite på avtal, enbart betalar för den mängd eller volym som efterfrågas för stunden. Om användaren önskar mer, skruvas flödet upp och prislappen för molntjänsten följer med.

Enkelheten och de låga inträdeskostnaderna för användning av molntjänsterna har även en baksida. Attraktionen av enkla och snabba verktyg i molnet för samarbete över organisationsgränser och nationsgränser dygnet runt gör inte sällan att problematiken med säkerhet glöms bort eller nonchaleras. Traditionella rutiner för att implementera nya tjänster i verksamheten åsidosätts. Beslut om användning kan enkelt fattas av enskilda anställda både i stabs- och linjefunktion, och säkerheten kan snabbt riskera att punkteras. Information som hanteras i molnet bör värderas på samma sätt som övrig information värderas i organisationen, d.v.s. efter de lagar, regler och policys som gäller. Analyser för hotbild, risker och sårbarheter samt laglighetskontroll ska göras även för molntjänster så att inte värdet av en användares tillgångar äventyras, t.ex. känslig personlig information, känslig information relaterad till användarens kunder eller det egna företaget och dess varumärke.

Användare av molntjänster kanske inte tänker på att kraven för säkerheten, t.ex. utifrån i ISO 27001-standarden för informationssäkerhet, även bör ställas på molnleverantörer. I den nyligen uppdaterade ISO 27001-standarden från 2013 finns nya kontroller t.ex. informationssäkerhetspolicy för leverantörsrelationer och hantering av informationssäkerhetsincidenter - med bäring på molntjänster. Den kommande ISO 27017-standarden, baserad på 27002, speciellt inriktad mot molnsäkerhet är ett nytt tillskott som även får antas att bli väl använd. Användningen av molntjänster bör kontinuerligt speglas i en uppdaterad och anpassad informationssäkerhetspolicy, i riktlinjerna samt anvisningarna för informationssäkerheten i en organisation.

Integration med molntjänster inblandat kan innebära följande:

- Integration mellan molntjänst samt egna servrar.
- Integration mellan molntjänster från olika leverantörer (se ovan).
- Integration av molntjänster, outsourcade tjänster samt egna system.

- Integration av ovan nämnda samt publika system.

Integration mellan molntjänster och företagens interna system, vilket ofta kallas hybridmolntjänster, har ökat och bedöms att kraftigt öka med lansering av APIer från molntjänstleverantörerna. Integration mellan olika molntjänster bedöms även de att öka kraftigt. Utmaningarna för att bibehålla en god säkerhetsnivå blir större desto mer integration av olika system som införs. Inför en integration bör en analys av säkerhetsbrister helst göras via en risk- och sårbarhetsanalys. En tilltagande utveckling inom området för outsourcing bl.a. vad gäller stat och kommun kan förutses äga rum framöver genom s.k. ”hybridlösningar” där leverantören kommer att tillhandahålla kombinationer av traditionell drift, egenproducerade molntjänster och tredjepartsproducerade molntjänster.

När man har all IT inom sin egen organisation så behöver en organisation ta ett helhetsansvar och kan inte frigöra sig från säkerhetsansvar. Vid outsourcing av hela eller delar av sitt IT-stöd så köper en organisation hjälp med att på olika vis t.ex. sköta och hantera driften av IT-stödet. Även här har en organsation fullt säkerhetsansvar för allt även om det praktiska så att säga delegeras ut till en eller flera externa outsourcingparter. Vid molntjänster så blir det ofta problematiskt då organisationen köper en tjänst. Det kan i vissa fall vara svårt att överblicka och få insyn i hur säkerhetsarbetet går till även om det skrivs att en organisation skall få tillträde och tillgång till säkerhetsrelaterade tester, genomgångar och dokument.

Det finns även en rad andra aspekter som kan behöva tänkas över och undersökas - såsom t.ex. hur skyddet ska hanteras vad gäller personuppgifter, finansiell information och kreditkortsdata, patientdata, bokföringsdata m.m. skall hanteras generellt och i molnet. Mer om vad som gäller beträffande personuppgifter i molnet kan läsas i [3].

2. Kort orientering om lagar, regleringar, standarder, etc. som berör molntjänster

Här lämnas en sammanfattande orientering om de juridiska regelverk utifrån svensk rätt som en potentiell användare av molntjänster har att förhålla sig till. Redogörelsen är inte uttömmande och adresserar inte vissa specialfall som t.ex. finansiella tjänster i den privata sektorn eller registerlagar m.m. i det offentliga (sjuk/hälsovård, utbildning, ordningsmakten och försvaret m.fl.) eller tjänster i andra sektorer som är föremål för särskild lagstiftning.

Först och främst bör en molnkund göra en undersökning av leverantörens tillförlitlighet på längre sikt:

- Vad har leverantören för renommé, bedömd ekonomisk uthållighet m.m. i form av en s.k. due diligence-undersökning.
- Vad gäller en leverantör som inte har resurser för att infria de åtaganden som den åtagit sig – är det risk för att avtalsbestämmelser och andra villkor som erbjudits eller framförhandlats blir verkningslösa.

Ett stöd i denna process kan vara att undersöka utifall leverantören tillhandahåller så kallade Service Organization Control (SOC)-rapporter. Dessa är interna kontrollrapporter som en leverantör kan tillhandahålla för att underlätta bedömning och hantering av risker relaterat till de tjänster som erbjuds. SOC utarbetas av American Institute of Certified Public Accountants (AICPA) och man har i samarbete med Cloud Security Alliance tagit fram ett tredjeparts program för bedömning av de molntjänsteleverantörer som använder sig av AICPAs SOC 2-rapportering. Enligt AICPA[2] så inkluderar SOC 2 kontroller som är relevanta för ”security, availability, processing integrity, confidentiality, or privacy”. Viktigt att notera är att ”privacy” i detta sammanhang inte nödvändigtvis är detsamma som att följa europeisk persondataskyddslagstiftning men rapporterna ger ändå en god inblick i hur leverantören arbetar med olika relevanta frågor. SOC-rapporter tillhandahålls kostnadsfritt till alla leverantörens kunder. Dock kan det krävas att man tecknar ett så kallat Non Disclosure Agreement (NDA) för att få tillgång till rapporterna. Ni som av olika anledningar använder er av molntjänster idag rekommenderas att begära ut dessa rapporter om ni inte redan gjort det. Dessa rapporter innehåller ibland ganska intressant och relevant information.

När denna första fas klarats av kan konstateras att såvitt avser mindre affärer det är omöjligt eller ytterst svårt för en molnkund att förhandla avtalsvillkor med leverantören över huvud taget. I vissa fall har de stora leverantörerna lokala (i Sverige) återförsäljare som kan fungera som implementatörer och tillhanda tilläggslösningar som t.ex. extra support, kryptering m.m. Här återigen är det viktigt att undersöka den lokala återförsäljarens status.

[2] http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SORHome.aspx

Om leverantören inte kan tillhandahålla rapporter från oberoende tredjepartsrevisoner, som t.ex. de tidigare nämnda SOC-rapporterna, så bör man inte gå vidare med avtalet utan att förbehålla sig rätten att utföra egna revisioner av leverantören (vilket tyvärr i många fall är svårt eller omöjligt med en molnleverantör bl.a. p.g.a. att leverantören har så många andra kunder vars information inte får kompromitteras). Detta kan dock medföra extra kostnader som måste ställas i relation till nyttan av tjänsten. Om leverantörerna tillhandahåller rapporter från tredjepartsrevisioner så bör dessa omnämnas i avtalet samt med vilken periodicitet de utförs.

De kontraktuella frågor som sedan skall sättas i fokus är givetvis erbjuden kapacitet relativt pris. En numera ganska välkänd fara vid molntjänster är att leverantören ofta meddelar att kapacitetstaket är nått och vill sälja mer av den varan. Utan adress i avtalet kan det vara svårt för kunden att kontrollera om sådana erbjudanden är motiverade.

SLAer (d.v.s. överenskommelse om servicenivå) kan vara en del av lösningen och sådana delregleringar är i allmänhet mycket viktiga. Här kan man också konstatera att eftersom molntjänster oftast är prismässigt attraktiva – relativt andra lösningar som verksamheten har in-house på egna servrar – så är den ekonomiska kompensation som kan erbjudas ofta begränsad. En aspekt på detta är att större leverantörer eller nischade sådana ofta kan vara så måna om sitt renommé att en bra lösning över tid trots allt är att räkna med. Molnkunden bör emellertid ha analyserat vissa riskscenarion, särskilt som det handlar om att lägga ut affärskritiska rutiner i molnet. Det kan här handla om att försäkra sig om vilken grad av leveranssäkerhet, olika typer av säkerhet, som leverantören kan tillhandahålla. Vissa leverantörer har s.k. distribuerad säkerhet (information speglas över fler lagringslösningar som finns i olika datahallar) och kör inte backup i traditionell bemärkelse. Detta är något som kunden måste förhålla sig till. Kanske etableras en säkerhetsbackup för att data inte skall behöva riskera att förloras, men det orsakar då en extra kostnad som reducerar det attraktiva i hela upplägget.

Det ovan antydda problemet att kunden måste säkerställa att dess data kan åtkommas vid varje given tidpunkt, dels under resans gång, dels i samband med att avtalet upphör av någon av många olika anledningar, skall också behandlas i avtalet. Detta kan föranleda att tester görs under pågående avtalförhållande för att kontrollera att den data som kunden får ut ur molnleverantörens system är aktuell, komplett och i läsbart skick. Detta bör i allmänhet även inbegripa att kunden får tillgång till loggar och olika typer av metadata som bör definieras från fall till fall.

I detta sammanhang kan konstateras att vi ännu inte har några klara standarder för återleverans av data, format m.m. vad gäller molnet. Detta är emellertid en utomordentligt komplex frågeställning eftersom molnleverantörer tillämpar så diversifierade egna standarder och proprietära miljöer. Olika standardiseringsorgan som t.ex. SIS[3] arbetar med detta (bl.a. så är nya ISO/IEC 27017 på gång). I EUs nya dataskyddsförordningen, som kommer röstas om nästa år, öppnas upp för möjligheten att införa dataskyddscertifieringar (Article 39). En ENISA-studie[4] som gjordes under 2013 relaterar till detta.

Personuppgiftslagen (PuL) innehåller regler för hur personuppgifter får behandlas och är baserad på EUs dataskyddsdirektiv och innehåller en hel del regler som molntjänstkunder måste förhålla sig till. Datainspektionen har utfärdat en hel del information som kan sökas på dess hemsida. I den mån kunden, som är personuppgiftsansvarig vad gäller hanteringen av ev. persondata i systemet/tjänst, faktiskt hanterar personrelaterad data måste det säkerställas att leverantören på ett lagligt och säkert sätt hanterar informationen – här måste en risk- och sårbarhetsanalys göras. Datainspektionen ställer även krav på säkerhet i detta sammanhang. Datainspektionen är den myndighet som genom sin tillsynsverksamhet ska bidra till att behandlingen av personuppgifter inte leder till otillbörliga intrång i enskilda individers personliga integritet. På Datainspektionens hemsida[5] finns en hel del information att söka relaterat till PuL.

I förekommande fall då man planerar att använda sig av molntjänster är det viktigt att utröna vem som är personuppgiftsansvarig för de personuppgifter som kommer att behandlas[6]. Det bör framgå tydligt i avtalen mellan parterna vem som är personuppgiftsansvarig och vem som är personuppgiftsbiträde för de personuppgifter som behandlas. Oavsett om du är personuppgiftsansvarig eller personuppgiftsbiträde bör du vara väl insatt i vad PuL kräver och att du kan möta de relevanta kraven innan du börjar använda en molntjänst för behandling av personuppgifter.

[3] Informationsteknik - Molnbaserade datortjänster - Översikt och terminologi (ISO/IEC 17788:2014, IDT) är det som SIS kommit fram med så här långt; dvs berör i princip endast terminologin

[4] https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/security-certification-practice-in-the-eu-information-security-management-systems-a-case-study

[5] www.datainspektionen.se

[6] http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/personuppgiftsansvarig/

Det unika med en molntjänst för både användare och ansvarig för personuppgifter är att det kan vara svårt att avgöra var, rent fysiskt, de personuppgifter man är ansvarig för behandlas och vilka som är involverade i behandlingen av dessa. Informationen kan ”flyta” mellan servrar/lagring placerade i olika länder och således mellan olika jurisdiktioner och ett flertal underleverantörer kan vara inblandade.

Med avstamp i PuL bör du åtminstone säkerställa att följande punkter är uppfyllda vid användande av en molntjänst

- §30 i PuL gör gällande att ”Det skall finnas ett skriftligt avtal om personuppgiftsbiträdets behandling av personuppgifter för den personuppgiftsansvariges räkning. I det avtalet skall det särskilt föreskrivas att personuppgiftsbiträdet får behandla personuppgifterna bara i enlighet med instruktioner från den personuppgiftsansvarige och att personuppgiftsbiträdet är skyldigt att vidta de åtgärder som avses i 31 § första stycket.”
- Inte sällan använder sig en molntjänsteleverantör utav underleverantörer och här gäller det att som personuppgiftsansvarig se till att veta vilka dessa är och att kraven uppfylls i alla led. Om du är en leverantör av tjänster vilka i sin tur baserar sig på en molntjänst och där dina kunder är personuppgiftsansvariga så bör du säkerställa att avtalet med molntjänsten även involverar skydd av dina kunders eventuella personuppgifter. Inte sällan så riktar sig molnleverantörens standardavtal enbart till dig som kund där du är personuppgiftsansvarig.
- § 31 i PuL gör gällande att ”När den personuppgiftsansvarige anlitar ett personuppgiftsbiträde, skall den personuppgiftsansvarige förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna.”
- Som nämnt i den tidigare punkten så måste dessa skyldigheter regleras skriftligt i avtal med molnleverantören. Här kan det underlätta arbetet om molnleverantören kan tillhandahålla oberoende tredjepartsrevisioner såsom de tidigare nämnda SOC-rapporterna och att tillgång till sådana regleras i avtalet. Vilka typer av säkerhetsåtgärder som krävs måste bedömmas från fall till fall i beaktande av hur pass känslig informationen är som skall behandlas.
- Vid överföring av personuppgifter till tredje land, d v s ett annat land utanför EU/EES området krävs bland annat att EU-Model Clauses undertecknas och om överföring av personuppgifter ska ske till USA krävs att Safe Harbour–principerna undertecknas. Undertecknandet behöver vara explicit och tydligt för den berörda personen när det sker.

EU håller på att ta fram en ny dataskyddsförordning vilken kommer att ersätta PuL. När förordningen har antagits av EU har EU-länderna 2 år på sig att anpassa sig till förordningen.

Det finns kostnadsfria och lätt tillgängliga checklistor, som berör juridik i molntjänster mer utförligt, att läsa hos t.ex. Cloud Security Alliance, Cloud Sweden, EuroCloud och ENISA. Vid användning av standardavtal är det dock viktigt att alltid ta hänsyn till den specifika situationen var gäller själva leveransen, parterna och andra aspekter som kan vara unikt för en viss leveranssituation. Man bör därför iaktta en viss försiktighet med att använda standardavtal rakt av. Vidare kräver de flesta standardavtal att parterna lägger till vissa delar såsom tjänstebeskrivning, SLA och vilket ansvar parterna har i förhållande till detta. (I referenslistan finns vidare hänvisningar till litteratur och standardavtal för området).

3. Praktisk checklista för säkerhet i molntjänster

Nedan finns en praktisk checklista, utformad ur ett livscykelperspektiv, för att underlätta kravställning och utvärdering av säkerheten i molntjänster. Det är önskvärt att ta med ett antal olika säkerhetsaspekter i en molntjänsts livscykel vid kravställning och utvärdering. Dessutom underlättas eventuell uppföljning och audit om alla utvärderade krav och leverantörens svar är med i avtalet. En molntjänsts livscykel kan beskrivas med följande steg sett ur ett säkerhetsperspektiv:

- Kravställning.
- Utvärdering.
- Avtal.
- Audit/uppföljning.
- Avslut/exit.

Kravställning

Ta först en ordentlig fundering över vilken information är lämplig att lägga ut i molnet. För om man lägger ut information kommer det att vara tillgänglig för individer utanför din organisation. Utvärdera om det är lämpligt eller inte. Detta är till stor del avgörande om en molntjänst är aktuell eller inte. Om en molntjänst är aktuell finns nedan ett antal punkter som kan vara lämpliga att titta igenom under kravställningen av säkerhet för en molntjänst:

- Molntjänster kan ofta inte garantera var information lagras. Informationen kan vara lagrad i olika delar av världen vid olika tillfällen. Även fjärråtkomst i supportsyftet anses som överföring av information. Är det acceptabelt?
- Vilka lagkrav finns och vad som är relevant för din organisation?
  - **Dataskydd** - PuLsamt EUs förslag till ny dataskyddsförordning COM (2012) 11 från 25 januari 2012 som ännu är ett förslag, men kan vara bra att beakta.
  - **Sekretess (OSL)** – det är tveksamt om myndigheter får lägga ut information i molnet enligt JO beslut[7]
- Vilka standarder som berör säkerhet kan vara lämpliga att titta igenom och se vad de ställer för krav vid en ev. certifiering? Har vi krav på oss från våra kunder (eller leverantörer, myndigheter m.fl.) att vi skall uppfylla eller vara certifierade mot någon av t ex nedan standarder:
  - **ISO/IEC 27000**[8] - kan vara en bra start för att välja ut krav som ska ställas till molntjänstleverantören om man inte redan har Lednings System för Informationssäkerhet implementerat i sin organisation. Kommande ISO/IEC 27017 kan även den vara intressant att se över.
  - **PCI-DSS**[9] – om vår organisation hanterar finansiell data eller kreditkortskortnummer etc. kan denna standard vara tillämplig att molntjänstleverantören (och kanske även vi själva som användare) uppfyller.
  - **CSA** - Cloud Security Alliance har fler dokument som kan användas vid kravställning, t.ex.: Cloud Control Matrix [4] och Consensus Assessments Initiative Questionnaire [5]
- Ett antal mer specifika områden som bör utvärderas från ett molntillämpningsperspektiv är följande:
  - **Användarhanteringsprocess** – är processen för att lägga till och ta bort användare och administratörer i enlighet med våra krav?
  - **Autentisering** – vilken nivå eller vilka nivåer på autentisering av användare och administratörer har vi som krav skall finnas, och vilka erbjuds av molntjänsten?
  - **Behörighetshantering/roller/grupper/auktorisation** – vilka nivåer på behörigheter, roller, grupper och auktorisation av användare/administratörer har vi, och vilka erbjuds av molntjänsten?
  - **Spårbarhet** - finns det stöd för spårbarhet av åtkomst och förändring av informationen? Kan det göras tillgängligt för kunderna, utan att exponera information till andra kunder?
  - **Gallringsrutiner** - finns rutiner för regelbunden gallring av inadekvat eller felaktig information/personuppgifter och hur ser desamma ut?
  - **Kryptering och integritet av information** - stöder tjänsten kryptering och integritetsskydd och för vilken del av informationen som lagras i den?
  - **Nätverkssäkerhet** - vilka mekanismer finns implementerade hos molntjänstleverantören?
  - **Lagring och backup** - innefattas det av tjänsten, eller krävs det separata lösningar för backup?
  - **Avveckling av media** - görs det på ett säkert sätt för all hårdvara som kan innehålla kundens information?
  - **Förstöring av information efter exit** - vad händer med informationen efter att avtal avslutas eller bryts? Kan molntjänstleverantören garantera att det förstörs och lämnas tillbaka?

Utvärdering

Det kan finnas olika/flera nivåer inom en molntjänst:

- SaaS-tjänst, som ligger ovanpå en
  - PaaS-tjänst, som använder en

[7] http://www.jo.se/sv/Om-JO/Press1/Presskatalog/Allvarlig-kritik-mot-vardgivare-for-hanteringen-av-patientjournaler-/
[8] http://www.sis.se/tema/ISO27000/
[9] https://www.pcisecuritystandards.org/security_standards/

- IaaS-tjänst, och
  - dess underleverantörer för fysisk datahall.

Det är därför viktigt är att utvärdera säkerheten i varje nivå. Dessutom är det ofta små spelare som levererar en SaaS-tjänst ovanför en stor PaaS/IaaS-leverantör – och de små har inte alltid alla delar på plats vad gäller säkerhet.

Gruppera krav och ställ till rätt målgrupp:

- Driftkrav (relevant för alla nivåer).
- Säkerhetskrav (SaaS).
- Integrationskrav (SaaS).

Driftkrav (relevanta för alla nivåer):

- **Härdning**[10] – hur härdar leverantören alla komponenter som de levererar i sin driftsmiljö – t.ex. operativsystem, databaser, webbservrar, webbapplikationer?
- **Sårbarhetshantering/patchning** – hur ser leverantören till att alla komponenter testas och patchas (uppdateras) mot kända sårbarheter?
- **Autentiseringssmekanismer** – vilka autentiseringsmekanismer används vid administrationsinloggningar (sysadmin)? Endast autentisering med hjälp av användarnamn och lösenord över Internet, eller någon sorts stark eller multifaktor autentisering? Det sistnämnda är att föredra för administratörsinloggningar.
- **Behörighetsprocesser** – vilka processer har leverantören kring behörighetshantering? Hur ofta görs revisioner av befintliga behörigheter (särskilt viktigt för sysadmin konton)? Vilka processer finns när en administratör slutar sin anställning/uppdrag? Hur snabbt stängs kontot?
- **Tillgänglighet** – vilken tillgänglighet och svarstider garanteras i de olika nivåerna av tjänsten?
- **Lagring och backup** – erbjuds backup och var i så fall lagras backuperna? Vad händer om leverantören går i konkurs eller får problem med sin miljö? Kunden bör överväga att ha egen backup av all information hos sig eller i en annan tjänst – för att förebygga eventuella problem[11].
- **Spårbarhet** – sparas loggar från alla komponenter? I ett centralt behörighetsskyddat system? Får kunden komma åt logginformationen för att utreda säkerhetsincidenter som spänner över interna och molnmiljöer?
- **Gallring** - finns rutiner för regelbunden gallring av inadekvat eller felaktig information/personuppgifter och hur ser desamma ut?
- **Integration av rutiner för säkerhetsincidenter** – kunder får sällan komma åt säkerhetsloggінformationen eftersom molntjänster delas av fler kunder och leverantören inte kan erbjuda en kund att se sina loggar utan att andra kunders information röjs genom detta. För att kunna utreda säkerhetsincidenter behövs därför integration mellan kundens och leverantörens incidenthanteringsprocesser.

Säkerhetskrav (SaaS):

- **Säker utveckling (SDL, OWASP)** – hur är molntjänsten utvecklad? Använder leverantören "Security Development Lifecycle" (SDL[12]) i sin utvecklingsprocess och tar hänsyn till alla hot och risker, samt säkerhetskrav under utvecklingen av tjänsten? Använder leverantören OWASP[13] Top 10 risker under utveckling och test av sina webbtjänster – för att få med de vanligaste bristerna?
- **Säkerhetstester (penetrationstester)** - görs det regelbundna säkerhetstester av SaaS-tjänsten? Får kunderna tillgång till resultatet av testerna? Kan kunden själv genomföra säkerhetstester av sin del av SaaS-tjänsten?
- **Web Application Firewall (WAF)** - skyddar leverantören sin tjänst från attacker genom så kallad WAF eller något annat motsvarande?
- **Autentisering** – vilka autentiseringsmekanismer och nivåer stöds och vilka vill vi ha? Vilka tillitsnivåer för identiteten hos användare och administratörer krävs? Kan vi ha starkare (två-faktor) autentisering för

[10] Härdning är ett sätt att minska antalet gränsytor i olika mjukvaror eller tjänster genom att stänga ner onödiga funktioner som riskerar att påverka funktionalitet negativt och på så vis orsaka driftsstörningar eller sårbarheter.
[11] CodeSpaces råkade ut för intrång som slutade i att all kundinformation blev raderat (http://threatpost.com/hacker-puts-hosting-service-code-spaces-out-of-business/106761)
[12] https://msdn.microsoft.com/en-us/library/windows/desktop/84aed186-1d75-4366-8e61-8d258746bopq.aspx
[13] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

administratörer? Kan SaaS-tjänsten integreras med företagets AD för att slippa administrera konton i flera olika system?

- **Kryptering av information** – vilken kryptering erbjuds och hur stöds den i tjänsten? Vad behöver vi ha och hur?
- **Spårbarhet** - loggas all åtkomst till kundernas information och vart? Till ett centralt loggsystem? Hur länge sparas loggarna? Kan kunderna få tillgång till loggar som är relevanta för deras användning av tjänsten? Kontinuerligt eller endast vid behov?
- **Gallringsrutiner** – finns stöd för gallringsrutiner i mjukvaran?

Integrationskrav (SaaS):

- **Stöd för SAML/ADFS** - har molntjänsten stöd för externa autentiseringstjänster genom ADFS eller federering av biljetter (SAML)?
- **Vilka nätintegrationer krävs** - vilka brandväggsöppningar krävs för att integrera den nya molntjänsten med företagsinterna system? Man vill inte öppna upp för mycket för då exponeras även interna tjänster till den externa parten.
- **Vilken infrastruktur krävs internt för att uppnå säker integration**:
  - API-gateways är ett bra sätt att integrera med externa tjänster, men produkterna inom detta område är ganska dyra och komplexa.
  - Någon variant av integrationsgateway eller en proxylösning behövs för integration.

Integration är väldigt viktig aspekt av användning av molntjänster. Den oftast tas inte med i beräkningen av kostnaden av en molntjänst. Ibland kan integrationskostnaden och nya system som krävs för säker integration vara högre än kostnad för själva molntjänsten. Det är viktigt att planera för det.

Ytterligare en aspekt som man inte får glömma är att ställa säkerhetskrav även mot eventuella tredjepartsintegratörer (de eventuell information som de bearbetat/lagrat behöver förstöras/återlämnas när uppdraget är slutfört). Det är inte sällan man behöver hjälp för att konfigurera den nya molntjänsten och bygga nya komponenter för att uppnå full potential med den. Därför krävs det separata krav:

- **Utveckling** - vilken process används vid utveckling av de nya komponenterna (SDL och OWASP)?
- **Autentisering** – om utvecklarna sitter internt hos oss då autentiseras de på samma sätt som egna anställda. Dock inte så sällan sker utveckling hos integratören själv och då är frågan hur sker åtkomst till företagets utvecklingsmiljö, programkod och själva molnstjänsten? Var och hur sker autentisering? Kan man använda ADFS och SAML mot den egna AD katalogen?
- **Behörigheter** - behörigheter som skapas för utvecklarna under integration är oftast större än efter produktionssättning. Man får inte glömma bort att strypa eller ta bort onödiga behörigheter som utvecklarna har i den nya molntjänsten.

Avtal

Alla relevanta krav bör vara med i avtalet såsom:

- Parternas åtaganden.
- Betalningsvillkor.
- Tidplan för leverans.
- Äganderätt och när går risken/ansvaret över till slutkund.
- Immateriella rättigheter, t ex varumärken, äganderätten till utveckling.
- Sekretess.
- Ansvarsbegränsning.
- Informationshantering, t.ex. personuppgiftshantering enligt PuL.
- Avtalets löptid och uppsägning.
- Force Majeure.
- Ändringar och tillägg.
- Tolkningsordning.

- Lagval.
- Tvisteforum.
- SLA (Service Level Agreement).
- Exit-bilaga.

I övrigt, för att undvika oälkomna överraskningar, är det viktigt att avtala villkor gällande även:

- **Uppgraderingar** - ny funktionalitet, när/var/hur får detta göras?
- **Byte av underleverantör** – när/var/hur får detta göras?

Uppföljning (Audit)

Vad gäller uppföljning av en molntjänst och dess säkerhet finns ett antal frågor att beakta:

- Hur skall man kunna följa upp det som avtalats?
- Går det genomföra audit (står det med i avtalet)?
- Extern revision eller kunden själv?
- Regelbundna pen-tester.
- Får vi som kund, eller kan vi kräva, rapporter från tester eller hantering av upptäckta sårbarheter?

Avslut/exit

Som kund kan man efter en tid önska att helt enkelt avsluta användningen av en molntjänst för att inte använda den mera. I ett sådant fall är det viktigt att ta till vara på det man önskar ha kvar i form av t.ex. data för att ev. kunna använda i andra sammanhang. Då är det av vikt att de data som fås går att använda i andra sammanhang samt att molntjänsten städas ur ordentligt så att inga data, användaruppgifter och meta-data mm finns kvar och ligger i gamla back-uper etc.

- Har vi en strategi för avslut?
- Garanterar leverantören att all information som tillhör kunden ska tas bort och förstöras?
- Har det reglerats redan i avtalet hur en exit skall gå till (i form av en Exit-bilaga)?

Ett kanske vanligare scenario är att man som kund önskar byta molntjänstleverantör för att fortsätta med samma eller en liknande molntjänst på annat håll. Då behövs en s.k. exitstrategi för att göra bytet så smidigt, kostnadseffektivt och säkert som möjligt. Att ha det som behövs för en välplanerad exit med i avtalstexterna från början underlättar betydligt.

- Finns det stöd i avtalet att informationen kan exporteras till en annan tjänst eller kunden själv?
- Gäller ovan all information? Även behörigheter och användarinformation?
- Vilket format kan data hämtas med?
- Finns det färdiga skript för export av data?
- Krävs det support från leverantör av molntjänst vid export?
- Krävs det speciella avtal för att få support vid återtagande av data?
- Kan export ske dygnet runt?
- Kan kund få support på svensk kontorstid av leverantören?
- Ingår support för exit i tjänstens kostnad?
- Kan en exit testas enbart genom att kopiera data?
- Är det möjligt att återfå metadata?
- Är det möjligt att återfå användardatabas?
- Kan loggar exporteras?
- Kan egenutvecklade tillägg till molntjänsten exporteras?
- Vilken bandbredd kan leverantören av molntjänsten garantera?
- Sker all export krypterad? Krypteringsnivå?
- Mellanlagras data under export? Var mellanlagras data?
- Kan kunden själv ta bort data efter export?
- Garanterar leverantören att data tas bort efter exit.

Stöd i certifieringar

Kravställning och utvärderingsprocessen kan förkortas om leverantören innehar certifieringar. Dock är det viktigt att validera för vilket område certifieringen gäller (SOA – statement of applicability) och för vilken nivå av molntjänster (om en tjänst är byggt ovanpå en annan). Exempel på relevanta säkerhetscertifieringar finns nedan (och snart tillkommer även ISO/IEC 27017):

- ISAE 3402/SSAE 16 (tidigare SAS70) - certifiering för operativa drift krav.
- Cloud Security Alliance Security, Trust & Assurance Registry (CSA STAR) self-assessment[14] – leverantörens egna svar på ett antal säkerhetsfrågor (som är mappade mot många säkerhetskrav och standarder).
- Cloud Security Alliance STAR certifiering[15]
- CSA STAR registry[16]

4. Sammanfattning

Nedan sammanfattas denna förenklade checklista i några relevanta punkter, vilka påvisar på en hög nivå viktiga områden, som behöver ses över innan införskaffande av molntjänst, under användning av molntjänster samt när det blir dags att byta till en annan eller avsluta användningen:

- Ingen tillfällig ”hype” - molntjänster är här för att stanna!
- Många molntjänstleverantörer är bra, men det finns både små och stora spelare med bristande rutiner och lösningar.
- Utvärdera kvalitet och säkerhet på alla nivåer. Blir säkerheten bättre eller sämre jämfört med idag?
- Beräkna en totalkostnad inklusive integration – blir det mer ekonomiskt och bättre?
- Genomför laglighetskontroll och en risk- och sårbarhetsanalys för att se vilka krav som inte uppfylls. Vad blir konsekvensen för dig och din information?
- Samarbetet ska regleras i avtal med samtliga parter.
- Molntjänstanvändningen bör utvärderas kontinuerligt - förändras säkerheten om en organisation börjar använda molntjänster? Är det skillnad om molntjänsterna används i kritiska affärs- eller verksamhetsprocesser där hög tillgänglighet krävs jämfört med de processer som klarar en eller ett par dagars avbrott?
- Lägg till säkerhet och molnsäkerhet till de ev. ramverk för riskbedömning din organisation har.

Förhoppningsvis kan nu en säker resa till, inom, och slutligen från eller mellan molntjänster företas!

5. Källhänvisning

[1] CSA Swedish Chapter (2014). Aspects to consider within information security during procurement and use of cloud services, v2.00. https://chapters.cloudsecurityalliance.org/sweden/research/

[2] NIST (2011). ‘The NIST Definition of Cloud Computing (draft), NIST Special Publication 800-145 (draft)’. National Institute of Standards and Technology, US Dept of Commerce, January 2011.

[3] CSA (2015). Privacy Level Agreement Guidelines to Address Personal Data Protection Compliance, v2, https://cloudsecurityalliance.org/media/news/cloud-security-alliance-releases-new-privacy-level-agreement-guidelines-to-address-personal-data-protection-compliance/

[4] Cloud Security Alliance (2014). Cloud Control Matrix (CCM), https://cloudsecurityalliance.org/research/ccm/

[5] Cloud Security Alliance (2014). Consensus Assessments Initiative Questionnaire (CAIQ) - https://cloudsecurityalliance.org/research/cai/

[14] https://cloudsecurityalliance.org/star/self-assessment/
[15] https://cloudsecurityalliance.org/star/certification/
[16] https://cloudsecurityalliance.org/star/?r=8588#_registry

Nedan finns ytterligare källor som kan vara av intresse:

[i]. Microsoft (2010). Cloud Computing Security Considerations. http://www.microsoft.com

[ii]. CSA – Cloud Security Alliance (2010). Top Threats to cloud computing v1.0. http://www.cloudsecurityalliance.org

[iii]. ENISA (2009). Cloud Computing: Benefits, risks and recommendation for information security. http://www.enisa.eu

[iv]. CSA – Cloud Security Alliance (2009). Security Guidance for critical areas of focus in cloud computing v2.1. http://www.cloudsecurityalliance.org

[v]. OWASP (2015). OWASP top ten project, http://www.owasp.org

[vi]. Microsoft (2010). Information Security Management System for Microsoft Cloud Infrastructure, http://www.globalfoundationservices.com/security/documents/InformationSecurityMangSysforMSCloudInfrastructure.pdf

[vii]. CSA – Cloud Security Alliance (2013). Cloud Controls Matrix v1.4, https://cloudsecurityalliance.org/research/ccm/

[viii]. Cloud Sweden (2011). Areas and problems to consider within information security and digital preservation during procurement and use of cloud services, v1.1.1, http://natverk.dfs.se/node/21531#attachments

[ix]. Cloud Sweden (2011). Legal issues when moving to the cloud – a checklist. https://natverk.dfs.se/engelsk-oversattning-legal-issues-when-moving-cloud-checklist

[x]. Cloud Sweden (2013). Molnet i publik sektor, http://cloudsweden.files.wordpress.com/2013/06/molnet-i-offentlig-sektor.pdf

[xi]. Edvardsson and Frydlinger (2013). Legal – Molntjänster, Norstedts förlag.

[xii]. IT&Telekomföretagen (2010). Cloud Computing, kommentar till IT&Telekomföretagens standardavtal Cloud Computing version 2010, http://www.itotelekomforetagen.se/standardavtal/boken-om-cloud-computing

[xiii]. IT&Telekomföretagen (2010). IT&Telekomföretagens standardavtal Cloud Computing version 2010, http://www.itotelekomforetagen.se/standardavtal/boken-om-cloud-computing

Personal information – Swedish Personal Data Act and the Personal Data Ordinance, and the Data Protection Directive (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data)., as indicated above cf. www.Datainspektionen.se which comprises useful information on personal data legislation and related security issues also in English.

Fler säkerhetsdokument kan hittas på CSAs globala hemsida: https://cloudsecurityalliance.org/