



Synkzone

En komplett guide till säker informationshantering.

Innehåll

- 1 Lagstiftning och användarvillkor
- 2 Kontroll
- 3 Riktig säkerhet
- 4 Stödja verksamheten
- 5 Skydd mot ransomware
- 6 Förenklat samarbete
- 7 Tillgänglighet vs. säkerhet
- 8 Inlåsnings effekter
- 9 Flexibilitet

9 saker att tänka på för säker informationshantering

Tjänster för molnlagring ger ett enkelt sätt för din organisation att snabbt komma åt, lagra och dela till exempel dokument och filer. Många av de tjänster som finns på marknaden kommer ursprungligen från konsumentmarknaden och har därefter anpassats för företagsmarknaden. Tyvärr har det fört med sig att dessa tjänster ofta har otillräcklig säkerhet och kontroll.

Att använda molnlagring har flera fördelar såsom exempelvis enkelhet och tillgänglighet men kan om det inte sker rätt skapa oreda och utsätta organisationen för onödiga typer av säkerhetshot. I värsta fall kan organisationens känsliga information bli tillgänglig för obehöriga.

Jämför gärna hur det fungerar/tidigare har fungerat i en organisation med egna filserverar. I en sådan struktur kan IT-personal ge sig själva access till hela organisationens information.

Med en osäker molntjänst riskerar du istället att molntjänstens personal nu har samma åtkomst till dina filer, även om du använder en molntjänst med kryptering då det ofta innebär att även leverantören har tillgång till krypteringsnycklar.

För att underlätta för er som står i valet att börja lagra information i molnet har vi tagit fram en kortguide med nio viktiga saker att tänka på, innan man bestämmer sig för en tjänst med molnlagring för professionellt bruk.

Christer Wik, Synkzone

#1

Lagstiftning och användarvillkor

Ha koll på:

- ✓ Vem står bakom molntjänsten?
- ✓ Vilket lands lagar vilar molntjänsten på?
- ✓ Lever molntjänsten upp till svensk/europeisk lagstiftning?

Förlora inte ägandet av din information, riskera att bryta mot gällande lagstiftning eller att information lämnas ut till utländska myndigheter.

Under vilken lagstiftning gäller tjänsten?

Många av de vanligaste tjänsterna som används inom företagsvärlden lyder under amerikansk lagstiftning – detta gäller även om informationen lagras i Sverige. Amerikanska leverantörer kan tvingas lämna ut dokument och filer till amerikanska myndigheter utan rättslig prövning i värdlandet eller kunders kännedom/medgivande.

Eftersom dokument och filer kan göras tillgängliga för leverantörer (oavsett kryptering) innebär det att amerikanska myndigheter kommer åt känslig information, personuppgifter och kommersiellt känsliga dokument.

Förutom lagstiftning gäller det också att vara säker på att ägarskapet till det som lagras inte ändras när det lagras i molnet. Det är också viktigt att ha koll på vilka rättigheter tjänsteleverantören tillskriver sig över dina lagrade data.

Exempelvis kanske tjänsteleverantören använder din information för att anpassa marknadsföringen av tredjepartsaktörer för dig.

#2

Kontroll

Ha koll på:

- ✓ Var lagras din information?
- ✓ Vem kan komma åt dina filer?

Förlora aldrig kontrollen över din information – välj lösningar som stärker din kontroll. Hur många får tillgång till din företagsinformation? Information är vår tids guld och en av de viktigaste tillgångarna för företag och organisationer.

Det är minst sagt ohållbart att förlora kontrollen över affärskritisk information – enbart för att man önskar lagra fler filer i molnet.

Den tjänst man väljer måste säkerställa att organisationen har full kontroll över sin information.

Det skall vara enkelt att administrera såväl information som användare/access, och det skall vara enkelt att begripa var filer lagras och vem som faktiskt kan komma åt dem.

Exempel på bristande kontroll kan vara dålig separation mellan olika kunders information, att tjänsteleverantören kan komma åt den lagrade informationen i klartext och att filer som tagits bort “permanent” faktiskt finns kvar.

Att enbart förlita sig på användarvillkor ger ett otillräckligt skydd.

#3

Riktig säkerhet

Ha koll på:

- ✓ Har tjänsteleverantörer möjlighet att komma åt din data?
- ✓ Har operatören tillgång till eventuella krypteringsnycklar?
- ✓ Information ska inte riskera att hamna i fel händer.

Har operatören av molntjänsten tillgång till dina data? De flesta molnlagringstjänster har sina rötter i konsumentmarknaden och har med rätta fått utstå mycket kritik för att säkerheten är otillräcklig och inte anpassad för företags och myndigheters användning.

En vanlig brist är att de filer som lagras faktiskt är fullt tillgängliga för operatören eller att operatören har tillgång till krypteringsnyckeln när materialet är krypterat.

Att enbart förlita sig på användarvillkor ger ett otillräckligt skydd.

Flera av vår tids stora dataläckor involverar personal på insidan (så kallade insiders) som haft tillgång till infrastrukturen och krypteringsnycklar.

Att organisationens information är exponerad och enkelt kan läsas eller kopieras av utomstående har gjort att många säkerhetsmedvetna organisationer och företag inte använder flertalet av de molntjänster som marknaden erbjuder.

#4

Stödja verksamheten

Ha koll på:

- ✓ Vilka risker finns om informationen försvinner
- ✓ Rätt information ger bättre beslut
- ✓ Skaffa en lösning som är smidig att komma i gång med - och enkel att växa i.

Blir du flexibel i din molntjänst? Undvik lösningar som enbart fokuserar på personlig effektivitet och delning/samarbete runt enstaka dokument.

Välj en lösning som gör det enkelt att skapa bra strukturer och organisera arbetet kring hur din organisation är uppbyggd och hur ni faktiskt arbetar. Rätt struktur underlättar effektivt arbete och samarbete såväl internt inom organisationen som exempelvis i projekt eller samarbeten som involverar flera parter och ofta även extern personal och partners.

Lösningen måste tåla att personal och konsulter börjar och slutar utan att man riskerar att dokumentation går förlorad eller sprids på grund av personliga konton.

Lösningen bör också vara byggd för att förenkla samarbete med underleverantörer, samarbetspartners och kunder. Att tillhandahålla en väl genomtänkt och säker lösning för samarbete mot kunder och partners hjälper dig att effektivisera verksamheten samtidigt som det skickar signalen om att ni tar IT-säkerhet på allvar och därmed behandlar gemensam information seriöst och säkert.

Detta skapar konkurrensfördelar såväl som bygger varumärke.

#5

Skydd mot ransomware

Ha koll på:

- ✓ Erbjuder molntjänsten isolering av infekterade datorer?
- ✓ Går det smidigt att återställa data efter attack?
- ✓ Lösningen bör ha skydd mot attacker och skador orsakade av ransomware inbyggt i tjänsten.

Hur fungerar molntjänsten vid yttre hot? Ransomware är ett slags virus som kan orsaka stora skador bland företagets information med låsta datorer som följd.

Flera lösningar som påstår att de ger skydd mot ransomware, är svåra att använda eller fungerar i praktiken inte tillfredsställande nog vid en attack.

Se till att din molnlagringstjänst kan isolera infekterade noder så som datorer, så att inte gemensamma filer skadas, samt att det enkelt eller automatiskt går att återställa alla filförändringar orsakade av en ransomwareattack.

#6

Förenklat samarbete

Ha koll på:

- ✓ Finns funktionalitet kopplat till filhanteringen?
- ✓ Finns det stöd för exempelvis konflikthantering?
- ✓ Skaffa en tjänst som kan ge stöd för effektivt samarbete – på riktigt.

Finns möjlighet att kommunicera kring informationen i molnet? Rätt verktyg kan underlätta gemensamt samarbete. Vi rekommenderar följande stödverktyg som verkligen kan underlätta gemensamt arbete.

Automatisk filloggning och chattfunktion – dessa gör det enkelt att se vem som gjort vad, ex. tagit bort, lagt till eller ändrat i en fil. En chattfunktion gör det också enkelt att skriva kommentarer som rör dokumenten eller verksamheten.

Distribuerat fillås gör det möjligt att säkerställa att enbart en person i taget kan ändra i ett dokument, varpå man kan undvika samtida ändringar och påföljande konflikter.

Automatisk hantering av lokal lagring – ett vanligt problem är att det är svårt att hantera när många filer skall synkroniseras till en enstaka dator.

Genom att se till att molntjänsten kan arkivera äldre filer automatiskt så undviker man att hårddisken svämmar över eller vanliga fel såsom att synkroniseringen stannar.

#7

Tillgänglighet vs. säkerhet

Ha koll på:

- ✓ Vilka anslutningar finns i molntjänsten?
- ✓ Erbjuds även en datorklient i molntjänsten?
- ✓ Undvik lösningar som enbart förlitar sig på webbaccess.

Vilken access finns till din information? Molnlagring kan ge stöd för att man ansluter olika datorer med olika operativsystem och även ger access via exempelvis webbsidor och appar.

Se till att du har kontroll över vilka typer av anslutningar din organisation accepterar vid olika scenarier och situationer.

Ibland kan till exempel anslutning från webbläsare eller appar vara direkt olämpligt då vissa typer av information skall hanteras. Se också till att det finns möjlighet att använda vanliga klienter då de ofta kan erbjuda en bättre upplevelse och högre säkerhet.

Att helt förlita sig på access via webb kan fungera för enstaka dokument. Vill man däremot arbeta med eller ha flera dokument åtkomliga lokalt är risken för dålig eller utebliven bandbredd stor, och stödet därmed sämre.

#8

Inlåsnings effekter

Ha koll på:

- ✓ Kan du få loss dina data?
- ✓ Hur går det till att lämna tjänsten du valt?
- ✓ Satsa på en molntjänst som du inte binder upp dig för hårt till.

Hur ser möjligheterna ut att få loss informationen som ligger i molntjänsten?

När man väljer leverantör av en molntjänst är det viktigt att ta eventuella inlåsnings effekter i beaktning. Med inlåsnings effekter menas eventuella försvårande hinder då det av någon anledning är dags att byta leverantör.

Viktigt är därför att säkerställa att vald leverantör kan säkerställa att du som kund får loss era data i ett format som gör det möjligt att enkelt migrera till annan leverantör.

#9

Flexibilitet

Ha koll på:

- ✓ Hur flexibel är tjänsten?
- ✓ Kan du bjuda in externa användare till tjänsten?
- ✓ Går det att integrera tjänsten mot andra system och applikationer?

Välj en molntjänst som går att växa i, ändra struktur i och bjuda in externa användare till.

Hur flexibel är molntjänsten? Ofta hittar man ett initialt behov av säker lagring/säker delning i organisationen för exempelvis ett begränsat projekt eller exempelvis styrelsearbetet. Det finns flera tjänster som löser det initiala behovet men det är också viktigt att tänka längre, i termer av skalbarhet, fler delar av organisationen och samarbeten utanför organisationen.

Att välja ett flexibelt system som är lätt att bygga ut utefter ett ökat behov, som också enkelt hanterar såväl externa som interna intressenter är viktigt.

Fundera också på huruvida det finns andra affärsprocesser och applikationer som hanterar och delar information med olika intressenter där det också kan finnas behov av att säkra information. Vilka möjligheter finns det att integrera det system jag väljer i andra applikationer och processer?