Google Sweden AB
Kungsbron 2
111 22 Stockholm
www.google.se

Main Phone +46 8 505 103 00
Main Fax +46 8 505 103 85
Org. No. 556656-6880
Registered Office: Stockholm

Remissvar från Google Sweden AB rörande I2021/00342

Introduktion

Den svenska regeringen har satt upp målet att skapa ett ramverk för att stödja trygg och säker användning av molnteknik i den offentliga sektorn. Google Cloud är tacksamma för att kunna bidra till denna värdefulla insats. Vi hoppas att utredningen klargör att publika molntjänster kan vara ett säkert och lagenligt alternativ för statliga myndigheter. Det nya ramverket bör stödja ett ekosystem där lokala lösningar (så kallade ”on-prem-lösningar”), lokala aktörer och globala leverantörer kan samexistera och samarbeta. Det skulle möjliggöra för offentliga organisationer att bygga de IT-lösningar som passar deras behov och samtidigt säkerställer lämpliga nivåer av kontroll och tillsyn. Vi har strukturerat våra kommentarer utifrån utredningens eget huvudtema – **säker och kostnadseffektiv IT-drift.**

Molntjänster ökar säkerheten

Det säkerhetsskydd som erbjuds av publika molntjänstleverantörer kan vara mer robust, skalbart och kostnadseffektivt än det som är tillgängligt vid drift i egen datormiljö. Det här bekräftas av oberoende forskning, inklusive "Cloud Computing Risk Assessment" som genomförs av Europeiska unionens Cybersäkerhetsbyrå (ENISA).

- Det är viktigt att framhålla att organisationer inom samhällets mest reglerade branscher - såsom finansiella tjänster - redan använder molntjänster och fortsätter att flytta fler processer till molnet.
- Google Cloud har en global infrastruktur som är utformad för att tillhandahålla säkerhet genom hela livscykeln för informationsbehandling. Säkerheten för infrastrukturen är utformad i progressiva lager med utgångspunkt i den fysiska säkerheten för datacenter, och fortsätter till säkerheten för hårdvaran och programvaran som ligger till grund för infrastrukturen, och slutligen, de tekniska begränsningar och processer som finns på plats för att stödja operativ säkerhet.
- Kommitténs fokus ligger på att skydda känslig information. Utredningen är dock mycket fokuserad på juridiska frågor kring sekretess och ägnar mindre uppmärksamhet åt informationssäkerhet. Vi föreslår att säkerhetshänsyn tas med i diskussionen om det framtida politiska scenariot. Ett beslut att lagra känslig information i en myndighets egen infrastruktur gör inte uppgifterna säkrare om den infrastrukturen är lättare att bryta sig in i eller manipulera med. De olika riskerna behöver vägas mot varandra tills en balans kan uppnås.
- En av de frågor som vi anser förtjänar mer uppmärksamhet vid riskbedömningen är den roll som kryptering spelar för att skydda kunddata. Kryptering av informationen under transport och i vila säkerställer att data endast kan nås av behöriga roller och tjänster med granskad åtkomst till krypteringsnycklarna. Om data av misstag hamnar i en angripares händer, kan de inte komma åt datan utan att också ha tillgång till krypteringsnycklarna. Även om en angripare får tag i lagringsenheter som innehåller kunddata kan de inte förstå eller dekryptera den. Kryptering är en viktig komponent i hur molntjänstleverantörer säkerställer integriteten för kunddata. Det gör att våra system kan behandla data, till exempel för säkerhetskopiering, och våra ingenjörer kan supportera infrastrukturen, utan att ges tillgång till datans innehåll. Google använder flera lager av kryptering för att skydda kunddata i vila. Vi krypterar all kundinformation som lagras i vila, utan att någon aktivitet krävs av kunden, med hjälp av en eller flera krypteringsmekanismer. Data

Google Sweden AB
Kungsbron 2
111 22 Stockholm
www.google.se

Main Phone +46 8 505 103 00
Main Fax +46 8 505 103 85
Org. No. 556656-6880
Registered Office: Stockholm

för lagring delas upp i bitar och varje bit krypteras med en unik datakrypteringsnyckel. Dessa krypteringsnycklar lagras tillsammans med datan, krypteras med (”inslagna” av) nyckelkrypteringsnycklar som exklusivt lagras och används i Googles centrala nyckelhanteringstjänst. Googles nyckelhanteringstjänst är redundant och globalt distribuerad.

- Ytterligare verktyg kan bidra till säkerheten för känslig information, såsom funktionalitet som begränsar vad leverantörer kan göra när de administrerar tjänster. Google Cloud har exempelvis utvecklat verktyg som gör det möjligt för kunder att se och kontrollera när och hur man når åtkomst till kunddata – såsom konfidentiell databehandling, extern nyckelhanterare och åtkomsttransparens och godkännande.
- Molntjänstleverantörer måste verka på den globala marknaden och uppfylla många globala cybersäkerhetskrav. Denna exponering höjer ribban för både förväntningar och verktyg och ger tillgång till denna förbättrade globaliserade standard för varje molntjänstkund.
- Det är viktigt att betona att kunder och tjänsteleverantörer behöver verka på basis av ett delat ansvar. Kunderna bär ansvaret för sitt innehåll, applikationer byggda ovanpå infrastrukturen, vissa konfigurationer för kryptering och säkerhetsfunktioner där det är tillämpligt samt för åtkomstkontroller. Molntjänstleverantörer förblir ansvariga för infrastrukturen, den övergripande miljön med många olika kunder och tjänster som erbjuds till deras kunder.

Innovation kräver flexibilitet

Google anser att multi- och hybridmolnstrategier är vägen framåt för att möjliggöra innovation. De publika molntjänsterna erbjuder många fördelar när det gäller kostnad och produktivitet, men dessa fördelar bör inte betraktas som ett val mellan ”allt eller inget”. För de flesta organisationer är flytten till molnet en gradvis process. De kan ha investerat i äldre IT-system, tillsammans med kunskaperna för att hantera dem. I den offentliga sektorn kan vissa processer behöva behandlas i egen miljö på obestämd tid. Detta gör hybrid-IT till den bästa långsiktiga strategin. Organisationer borde kunna använda flera moln, byta leverantörer över tiden och bevara viss självständighet från sina leverantörer. Vi anser att utredningen bör ta större hänsyn till multi- och hybrid-molndimensionen när de arbetar för att forma framtiden för IT för offentlig sektor i Sverige. Andra europeiska länder har ett liknande tillvägagångssätt. Till exempel inkluderar den italienska regeringens vision för den offentliga sektorn ett ”nationellt moln” för en delmängd av känsliga data och funktioner. Resten av myndigheterna i den offentliga sektorn uppmuntras att använda publika molntjänster.

Korrekt datakategorisering är en nödvändig komponent i detta synsätt. Varje organisation borde veta vilken typ av data den behandlar - det är helt enkelt god praxis. Det här kommer att bli ännu viktigare i samband med tillämpningen av den nya lagen, som förlitar sig på graden av känslighet hos de aktuella uppgifterna. Offentliga myndigheter måste ha system på plats för att identifiera vilken information de behandlar och om något av det är känsligt. Det här gör det möjligt för myndigheterna att bygga sin IT-infrastruktur på ett sätt som möjliggör att de kan dra nytta av molntjänster samtidigt som de följer lagen fullt ut. Regeringen borde stödja detta arbete med tydliga riktlinjer.

Molntjänsternas fördelar är fler än kostnadsminskning

Traditionellt har organisationer tittat på publika molntjänster för att spara pengar. Fördelarna med att använda molntjänstteknik är dock fler än de ekonomiska aspekterna. Dessa inkluderar:

Google Sweden AB
Kungsbron 2
111 22 Stockholm
www.google.se

Main Phone +46 8 505 103 00
Main Fax +46 8 505 103 85
Org. No. 556656-6880
Registered Office: Stockholm

- Cybersäkerhet - konkurrenskraftiga molntjänstmarknader kräver att molntjänstleverantörer erbjuder alltmer förbättrade säkerhetsfunktioner och tekniska framsteg för att bäst lagra, underhålla och skydda data.
- Skalbarhet - molntjänstteknik säkerställer kapacitet när aktivitetstoppar inträffar, vilket varit fallet under pågående pandemi. Vid sådana tillfällen är tillgängligheten och funktionaliteten hos offentliga tjänster ännu viktigare.
- Tillgång till teknik som AI - tack vare molnets förmåga att leverera datorkraft till relativt låg kostnad blir artificiell intelligens mer lättanvänt och utbrett. För att bli verkligen tillgängliga behöver molnbaserade maskininlärningsverktyg vara tillräckligt enkla för att icke-experter ska kunna använda dem - och molntjänstleverantörer arbetar hårt på lösningar. Verktyg som Google Cloud AutoML och maskininlärnings-API:er erbjuder organisationerna en utgångspunkt för en mycket större förståelse av deras data.
- Hållbarhet och energieffektivitet - molntjänsterna möjliggör en mer effektiv resursanvändning. Våra datacenter är dubbelt så energieffektiva som ett typiskt företagsdatacenter, också tack vare maskininlärning. Redan idag är verksamheten koldioxidneutral, och vi har nu satt det ambitiösa målet att ha en koldioxidfri verksamhet senast år 2030.

Det är viktigt att varje policy som adresserar digitalisering av den offentliga sektorn tar hänsyn till dessa fördelar. Ett för snävt fokus på risker - snarare än möjligheter - kan bromsa upptagningen av teknik.

Förslagen till ändring av offentlighets- och sekretesslagen

Vi stöder fullt ut målet att klargöra den aktuella situationen och ge rättslig klarhet om tillämpningen av offentlighets- och sekretesslagen i en miljö för molntjänstupphandling. Vi tror dock att den nuvarande formuleringen kanske inte uppnår det önskade resultatet. ”Teknisk bearbetning” och ”teknisk lagring” är inte klart definierade och är inte termer som marknaden skulle känna igen. Vi föreslår användning av mer allmänt använda termer som leverantörer och kunder använder i sina kontrakt. En alternativ version av meningen skulle kunna lyda: Sekretess hindrar inte att en uppgift lämnas ut till *en IT-leverantör i samband med tillhandahållandet av en tjänst på uppdrag av den utlämnande myndigheten*.

Man kan också hänvisa till leverantörer som behandlar uppgifterna "enligt kundinstruktioner", i enlighet med den allmänna dataskyddsförordningen (GDPR) och leverantörernas roll som personuppgiftsbiträde för kunddata.

Vi tror att ytterligare klarhet kan uppnås när det gäller följande stycke - "*En uppgift ska inte lämnas ut om det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut.*" Vi anser särskilt att lagstiftaren bör:

- bättre definiera vad som utgör övervägande skäl som ger företräde. Det här kan göras i lagen eller i form av riktlinjer. Utan ytterligare klarhet förväntar vi oss en situation där myndigheter åter är osäkra på tillämpningen av lagen. Utan vägledning från regeringen kommer tolkningen återigen att överlåtas på varje myndighet. Det här kommer de facto att återskapa den aktuella situationen med t ex eSam-uttalandet.
- introducera en ny dimension utöver vilken typ av information som avslöjas - nämligen vilka typer av verktyg och funktionalitet som finns tillgängliga för att skydda informationen. Även de mest känsliga uppgifterna kan skyddas med verktyg som end-to-end-kryptering, åtkomstkontroll och transparens och avancerade cybersäkerhetskonfigurationer. Dessa verktyg utgör en effektiv åtgärd för att minska risken för att känslig information kan nås och manipuleras. Offentliga

Google Sweden AB
Kungsbron 2
111 22 Stockholm
www.google.se

Main Phone +46 8 505 103 00
Main Fax +46 8 505 103 85
Org. No. 556656-6880
Registered Office: Stockholm

myndigheter bör tillåtas utkontraktera även när behandlingen involverar känsliga uppgifter, så länge de kan förlita sig på leverantörer som erbjuder höga skyddsnivåer. Dessa skyddsnivåer skulle kunna bedömas genom överensstämmelse med t ex internationella säkerhetsstandarder eller andra certifieringar.

Dessa förslag härrör från en önskan om att ge offentliga myndigheter val och tydlighet att röra sig framåt i sin digitala omvandling. En alltför strikt metod för t ex dataklassificering skulle hindra hela statliga funktioner från att använda de mest avancerade digitala verktygen.

Genom att överväga verktyg och parametrar snarare än datatyper som ska skyddas kan lagstiftaren förbättra datasäkerheten på flera sätt.

Först och främst, skulle detta förbättra ovan nämnda verktyg och funktionalitet. Att kräva vissa typer av funktionalitet för vissa typer av skyddsvärd information skulle stimulera branschen att bygga verktyg som är utformade för att förbättra cybersäkerheten. Att tillåta alla typer av data så länge de är skyddade skulle uppmuntra till ett kreativt tillvägagångssätt för dataskydd och därmed främja ett långsiktigt tillvägagångssätt för säkerhetsverktyg.

För det andra skulle detta höja ribban för industristandarden avseende säkerhet för alla typer av data, snarare än att främja vissa typer över andra. Skydd som är gemensamma för banksektorn kan till exempel också skydda sjukvårdsdata.

Slutligen, att tillåta alla typer av data skulle säkerställa att alla datatyper skyddas. Att utesluta vissa kategorier av data kan skada inte bara cybersäkerhetsprinciper utan också individer. Om till exempel all hälso- och sjukvårdsdata skulle vara utesluten kan det göra sjukvårdsdata sårbar för attacker. Det här skulle kunna påverka individers personuppgifter utöver att exponera cybersäkerhetsproblemen mer allmänt och därigenom förvärra det ursprungliga problem som den nya lagen avser lösa.

***