Bedömning av Customer Lockbox

Intraservice, Staffan Wikström

1 Bakgrund

Stadsledningskontoret gjorde under hösten 2017 en bedömning att information som överlämnas till en extern part kan om den, enligt offentlighets- och sekretesslagen, omfattas av sekretess och ej anses ha ett fullgott skydd betraktas som röjd. Detta röjande sker oavsett om leverantören tar del av den sekretessbelagda informationen eller ej. För att omhänderta detta röjande inom ramen för införande av Office 365 köptes en tilläggstjänst som heter Customer Lockbox. Denna tjänst gjordes en preliminär bedömning av vilken pekade på att det teoretiska röjandet inte längre ägde rum.

Den preliminära bedömningen gjordes dock utifrån de förutsättningar som fanns vid det givna tillfället och det ålades projektet för Office 365 att vidare göra de verifieringar som behövdes för att tillse att inget röjande vidare skedde.

2 Tjänstebeskrivning

Någon detaljerad tjänstebeskrivning har inte kunnat erhållas från leverantör, men i stort går tjänsten ut på att ett extra processteg införs i supportprocessen där Göteborgs Stad ges ett attestflöde i de supportärenden där Microsoft behöver åtkomst till kunddata för att kunna lösa supportärendet i fråga. Om inte Göteborgs Stad godkänner denna åtkomst kommer ärendet att stängas utan lösning.

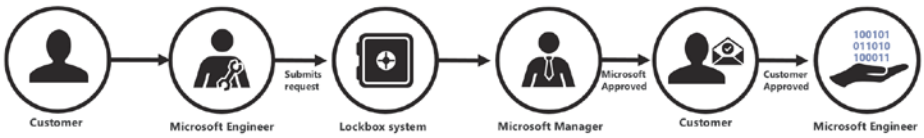

Bild – Process för åtkomst med Customer Lockbox

I ett tilläggsavtal (Amendment) till Göteborgs Stads huvudavtal med Microsoft gällande Office 365 utfästs löftet att innan Microsoft eller deras underleverantörer får ”Natural person access” behövs ett godkännande från Göteborgs Stad. Detta gäller för tjänsterna Exchange Online, Sharepoint Online och OneDrive for Business. Med ”Natural person access” avses mänsklig interaktion med information som lagras inom tjänster, dvs sådant som går utanför begreppet maskinell bearbetning.

3 Analys

Tilläggstjänsten Customer Lockbox är inte produkt som höjer den tekniska säkerhetsnivån utan är tänkt som ett kontrollverktyg. De säkerhetsåtgärder som krävs för att erhålla en adekvat skyddsnivå av information kan således inte tillgodoses alls av denna produkt vars enda syfte är att omhänderta problematiken med ett juridiskt röjande. Exempelvis kommer Microsoft behöva

åtkomst till de krypteringsnycklar som krävs för att konsumera den lagrade informationen oavsett om Customer Lockbox används eller ej.

Tjänsten har, utifrån den tänkta nyttan att omhänderta ett eventuellt röjande, analyserats. Det som framkommit har dock inte varit till tjänstens favör, utan bedömningen i stort är att om ett röjande sker utan denna tjänst kommer sannolikt samma röjande vara tillämpligt även med tjänsten i fråga.

Bakgrunden till denna bedömning är flera.

1. Enligt beskrivning i kapitel 2 påverkas supportprocessen för felavhjälpning av Customer Lockbox så att staden får möjlighet att godkänna åtkomst till kunddata innan denna sker. Samma möjlighet finns redan då det är på stadens initiativ som supportprocessen initieras. Således är det på stadens initiativ som denna åtkomst medges redan från början. Customer Lockbox innebär bara att staden får ett extra steg för godkännande i de ärenden som staden själv begär. Customer Lockbox kan vara relevant i en organisation där många är behöriga att skapa supportärenden men organisationen vill ha central kontroll över när åtkomst sker. I Göteborgs Stads fall är det samma personer som begär supportärenden som också attesterar åtkomst till kunddata om sådan behövs.
2. Omfattningen för tjänsten Customer Lockbox är åtkomst till kunddata som finns lagrat i tjänsterna Exchange Online, Sharepoint Online och OneDrive for Business. Detta är förvisso de primära lagringsytorna inom ramen för tjänsten Office 365. Dock finns det andra informationsbärare som inte täcks av Customer Lockbox. Exempel på sådana kan vara Teams eller Yammer. Ytterligare ett exempel är den katalogtjänst (Azure Active Directory) som hanterar alla konton och behörigheter till information som lagras i Office 365 och Microsofts andra onlinebaserade tjänster. Customer Lockbox har således inte full teckning över alla ingående delar som är relevanta för Office 365 utifrån ett systemperspektiv.
3. Precis som i alla IT-leveranser finns det alltid ett fåtal personer som har sådana tekniska behörigheter att de kan åsidosätta alla säkerhetsfunktioner. Så är även fallet med Office 365. Denna kategori av personer kommer kunna göra detta oavsett om tjänsten Customer Lockbox används eller ej. Customer Lockbox skyddar alltså inte mot denna angreppsvektor.
4. Om Microsoft enligt lag är tvungna att lämna ut kundägd infoformation kommer de också under vissa förutsättningar vara skyldiga att göra så. Denna typ av utlämnande av information kommer inte hindras av en tilläggstjänst som Customer Lockbox.
5. Vid tecknande av tilläggsavtalet gällande Customer Lockbox under hösten 2017 genererades det en uppfattning om att Göteborgs Stad fått en specialanpassad version av tjänsten Customer Lockbox. Uppfattningen var att denna anpassade version har en större omfattning i sin innebörd. Detta har under våren 2018 Microsoft bekräftat att så

inte är fallet utan staden har samma implementation av tjänsten som övriga kunder. Detta innebär också att verifiering av tjänstens förmåga inte kunnat genomföras då förväntningarna inte kunnat infriats.

Utöver ovan redovisade punkter finns det en inneboende problematik i att klass 2-information finns idag i flertalet olika leveransmodeller hos eller åt Intraservice. Office 365 är bara en av dessa leveransmodeller. Någon liknande tilläggstjänst som Customer Lockbox finns inte att komplettera övriga leveransmodeller med. Detta är således inte en återanvändningsbar lösning på ett större problem.

4 Sammanfattning

Intraservice sammanvägda bedömning är att Customer Lockbox inte löser den problematik kring röjande av information som beskrivs i Stadsledningskontorets promemoria avseende Office 365 daterad 2017-10-20.