Ny molntjänst: Doodle

Beskrivning av behovet

Vi behöver kunna samordna mötesbokningar på ett sådant sätt att deltagarna själva markerar vilka tider som passar och kanske passar, så man kan välja en bra tid. Det måste gå att ha externa deltagare med, och det måste gå att hantera fall där man inte vet vilka alla deltagare är. Det behöver gå att begränsa antalet val av alternativ som en deltagare gör, och det måste gå att begränsa hur många deltagare som får välja respektive alternativ. Systemet måste vara enkelt att använda.

Beskrivning av tjänsten

Doodle är en mötesbokningstjänst som uppfyller behovet. Man kan skapa en aktivitet och koppla ett antal alternativa tider till den. Personer som får en länk via e-post kan fylla i vilka tider som passar dem. Det går också att hantera t.ex. medarbetarsamtal genom att begränsa hur många alternativ man får välja, och hur många deltagare som kan välja ett visst alternativ. Tjänsten är mycket enkel att använda och används av massor av människor.

Alternativa lösningar

Vi har undersökt alla alternativa lösningar vi kan hitta. Den enda andra lösning som har möjlighet att begränsa antalet val per deltagare och antalet deltagare per val är foodle, men utvecklingen av foodle är nedlagd. Vid LiU finns meet-o-matic och Outlook som system för mötesbokning. Inget av dem hanterar begränsning av val, meet-o-matic underhålls inte och är krångligt att använda, och Outlook låter inte deltagarna själva välja tider. Microsoft har haft andra lösningar, t.ex. FindTime, men de är nedlagda eller har väldigt begränsad funktionalitet.

Information som lagras i tjänsten

Namn och e-postadresser till deltagarna som oftast uppges av deltagarna själva. Information om mötet som ska bokas som uppges av mötesbokaren.

Risk- och sårbarhetsanalys

Information som behandlas i tjänsten

Följande information lagras i tjänsten.

Information	Konfidentialitet	Riktighet	Tillgänglighet	Personuppgifter
Namn på deltagare	Normal	Normal	Normal	Normal
E-post till deltagare	Normal	Normal	Normal	Normal
Val av mötestider	Normal	Normal	Normal	Normal
Beskrivning av möte	Normal	Normal	Normal	Inga

Motivering

Bristande tillgänglighet eller riktighet kommer inte att påverka LiU:s verksamhet i nämnvärd omfattning. Bristande konfidentialitet kan leda till en personuppgiftsincident men informationen som lagras i systemet har väldigt lågt skyddsvärde. Större delen kommer att vara uppgiven av deltagarna själva. Systemet har inte inloggning med LiU-konto, utan kommer oftast att användas utan inloggning. Informationen som lagras utgör inte en allmän handling förrän bokningen är fastställd, och då lagras normalt bokningen i Exchange. Därför bör inte LiU behöva åtkomst till enskilda medarbetares Doodle-möten.

Det finns möjlighet att koppla sin Exchange-kalender till Doodle, och en del personer väljer att göra så. Det finns därmed en risk att information i kalendern är tillgänglig för Doodle men vi kan inte bedöma hur mycket det handlar om.

Fördjupad risk- och sårbarhetsanalys

Notera att en fördjupad analys bara behöver göras på begäran av IT-säkerhetsgruppen eller informationssäkerhetssamordnaren. För Doodle skulle en fördjupad analys troligen inte krävas, utan den finns med här enbart för att visa hur den kunde se ut.

Konsekvenser

Bristande konfidentialitet kan leda till att information om när möten hålls och vilka som deltar kommer i orätta händer. Under förutsättning att känslig information inte läggs in i tjänsten bedöms konsekvensen som försumbar. Bristande riktighet kan leda till att mötesbokningar blir fel. Detta är en typ av händelse som måste hanteras även med dagens lösningar. Konsekvensen bedöms som försumbar. Bristande

tillgänglighet innebär att mötesbokningar inte kan göras vid tänkt tillfälle. Skulle detta inträffa kan deltagarna och mötesbokaren hantera bokningen på annat sätt. Konsekvensen bedöms som försumbar.

Riktlinjer för informationssäkerhet

Kapitel 2

Kapitel 2 är relevant i den utsträckning tjänsten kan förhindra medarbetare att följa riktlinjerna. Doodle bedöms inte äventyra medarbetares möjligheter att följa regelverket. Det bör noteras att tjänsten inte ska användas för känsliga möten, t.ex. bokning av rehabmöten eller annat som utgör känsliga personuppgifter. Doodle har möjlighet att skicka e-post, men den möjligheten behöver inte användas, och om den används är det för den specifika tillämpningen att skicka information om inbjudningar och bokningar.

Kapitel 3

Kapitel 3 är inte tillämpbart.

Kapitel 4

Kapitel 4 är inte tillämpbart.

Kapitel 5

Under förutsättning att en informationsägare utses, så att inventering och klassificering kan genomföras enligt riktlinjerna, finns inga hinder för att riktlinjerna uppfylls. IT-direktören föreslås vara informationsägare.

Baskrav för IT-system

Kapitel 2

Kraven är uppfyllda. Systemet är helt webbaserat.

Kapitel 3

Systemet använder inte federerad inloggning. De flesta användare kommer dock inte att logga in alls, och de som loggar in gör det med ett konto som inte ser ut som LiU-ID. Det är tydligt att det inte är en LiU-tjänst. Hanteringen av lokala konton är så långt vi kan avgöra tillräckligt säker.

Det saknas stöd för tvåfaktorautentisering, men informationen som behandlas bedöms inte ha sådant skyddsvärde att det behövs.

Auktorisering sker internt i systemet utan koppling till LiU:s AD. LiU kan inte begära en rapport över användare eller behörigheter. Informationen i systemet bedöms inte ha sådant skyddsvärde att det behövs.

LiU kan inte radera konton i systemet, men vi ser inte att ett sådant behov egentligen finns i den här tjänsten.

Kapitel 4

Vi bedömer att leverantören uppfyller dessa krav.

Kapitel 5

Det går inte att avgöra om kraven är uppfyllda, men informationen har så lågt skyddsvärde att det inte torde behövas. LiU kan inte ta del av loggdata, men bör aldrig behöva det.

Kapitel 6

Vi bedömer att inte är relevanta.

Kapitel 7

Vi bedömer att kraven är uppfyllda.

Kapitel 8

Vi bedömer att användbarheten i systemet är tillräckligt god. Doodle är känt just för sin användbarhet.

Kapitel 9

Vi bedömer att kraven är uppfyllda.

Kapitel 10

Inga integrationer förekommer.

Kapitel 11

Vi bedömer att kraven inte är tillämpbara.

Kapitel 12

Systemet är inte anpassat till LiU:s grafiska profil, men det bedöms inte vara nödvändigt eftersom det inte ska presenteras som ett LiU-system och inte använder LiU-konton. Kraven är i övrigt inte tillämpbara eller uppfyllda.