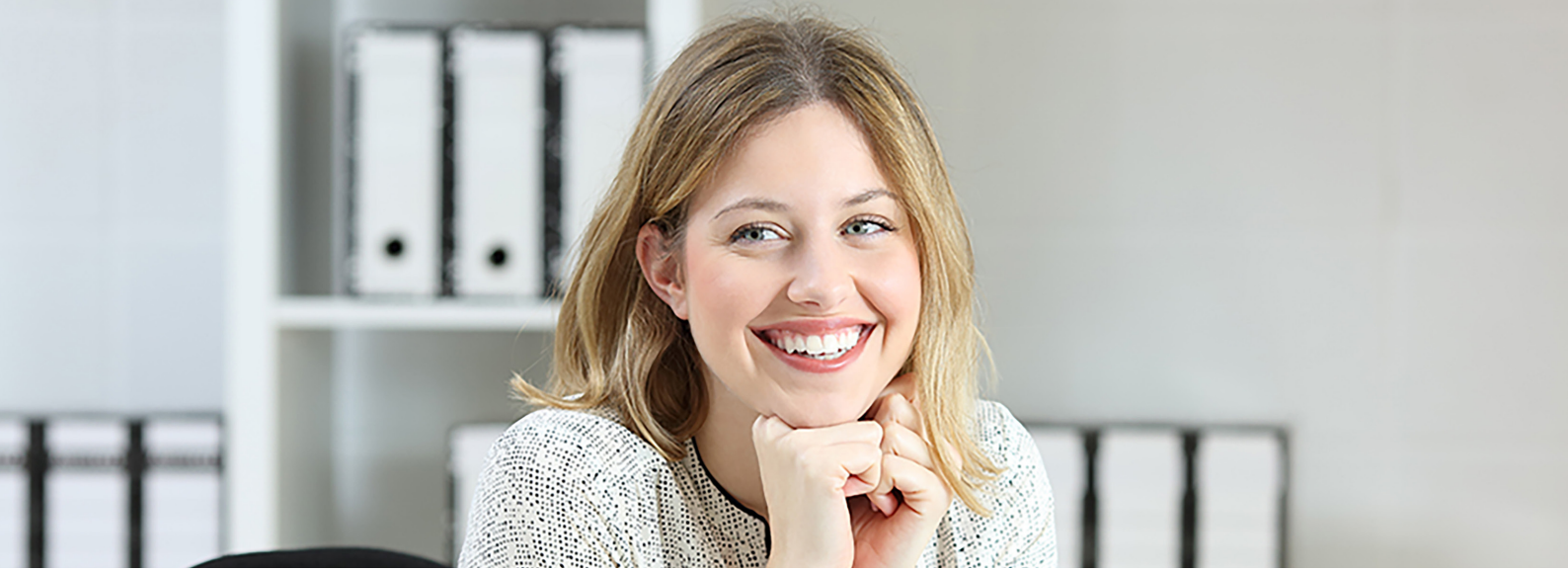


5 säkerhetsaspekter att tänka på vid skapandet av din digitala assistent

Digitala assistenter börjar bli vardag för många människor. Fler och fler styr sina mobiltelefoner, bilar, smarta hem, datorer och sajter med olika typer av digitala assistenter. En del organisationer stressar därför igenom besluten för att tidigt ligga i framkant. Resultatet blir ofta en enkel chatbot som i bästa fall svarar rätt och i värsta fall röjer företagshemligheter eller bryter mot lagar.

Den digitala assistentens styrka är att samla stora mängder information och presentera den på ett enkelt sätt för användaren. Detta ställer krav på att informationsmängden som presenteras har klassificerats och analyserats. Exempelvis är det viktigt att patientjournaler och andra känsliga personuppgifter bara hanteras av de personer som har rätt att ta del av dem.

Riskerna med en digital assistent

En digital assistent öppnar upp för nya möjligheter att få ett dataintrång. Det är därför viktigt att arbeta med säkerhet ur flera aspekter när en digital assistent tas i bruk. Informationen som görs tillgänglig kan vara känslig, vilket medför att det måste finnas flera nivåer av säkerhetslösningar beroende på vilken typ av information som delges.

En uppenbar risk med traditionella digitala assistenter är sårbarheten för intrång. Ett intrång skulle exempelvis kunna vara riktat för att lyssna av trafiken eller i värsta fall svara på frågor i din organisations namn för att vilseleda frågeställaren.

En assistent som matas med stora mängder oklassificerade data riskerar också att lämna ut fel information till fel personer. Det kan till exempel vara patientjournaler och känsliga personuppgifter alternativt avtal eller andra företagshemligheter.

En konsekvens av att informationen blir digital är att nya arbetssätt krävs för hur den hanteras. Digital information kan enklare flyttas, raderas och spridas av misstag än motsvarande information som finns i fysisk form. Det är viktigare än någonsin att upprätthålla tilltro till det data ni har i form av att säkerställa tillgänglighet, konfidentialitet, riktighet och spårbarhet.

Därför ska du implementera en assistent i din organisation

Dagens organisationer samlar stora mängder information, ofta finns data i silos som inte är tillgängliga utanför datasystemet som informationen är lagrad i. Man har inom en relativt begränsad tidsperiod gått över från fysisk lagring av de flesta av informationstillgångarna till digital lagring.

Den digitala assistenten samlar samtliga dessa datakällor och använder artificiell intelligens för att värdera resultaten. Genombrott i tekniken gör att de resultat som den digitala assistenten levererar har bättre kvalitet än vid manuell hantering.

Den digitala assistentens användningsområden finns inom alla organisationer. Ofta är det fantasin och tillgängliga data som sätter begränsningar för vilka tjänster som kan skapas med teknologin. En digital assistent kopplat med AI ger exempelvis en kommunal verksamhet möjlighet att ge högre service till medborgarna genom att tillhandahålla stora mängder av kommunens information och processer på ett lättillgängligt sätt. Det är viktigt att komma ihåg att också hantera andra aspekter av detta såsom juridik, informationssäkerhet och IT-säkerhet.

För att hjälpa dig igång i skapandet av din egna digitala assistent har vi listat fem punkter vi anser som avgörande för att upprätthålla säkerheten i implementationen.

1. Gedigen riskanalys

Tidigt i projektet måste du göra en gedigen riskanalys utifrån det data som hanteras. De allvarligaste riskerna som identifieras ska hanteras med tekniska, administrativa och organisatoriska åtgärder. Om detta utförs tidigt i införandeprojektet, minskas risken för obehagliga överraskningar under resans gång.

2. Informationsklassning

Med en korrekt utförd informationsklassning blir det enklare för den artificiella intelligensen att avgöra vilken information som ska presenteras för vilken användare och kan också tydligt kopplas till möjligheten att efterleva kraven i GDPR. Ett strukturerat informationssäkerhetsarbete bör genomsyra organisationen, exempelvis genom att arbeta enligt ISO 27 000, där informationsklassning är en fundamental del.

3. Personuppgiftsbiträdesavtal

En konsekvens av att den digitala assistenten kräver avancerad teknik och komplicerad drift är att tjänsten uteslutande levereras i form av molntjänster. Enligt GDPR (och även PUL) måste man då teckna ett personuppgiftsbiträdesavtal som tydliggör rättigheter och ansvar för molnleverantören så personuppgifter skyddas och individers rättigheter bibehålls.

4. Kryptering

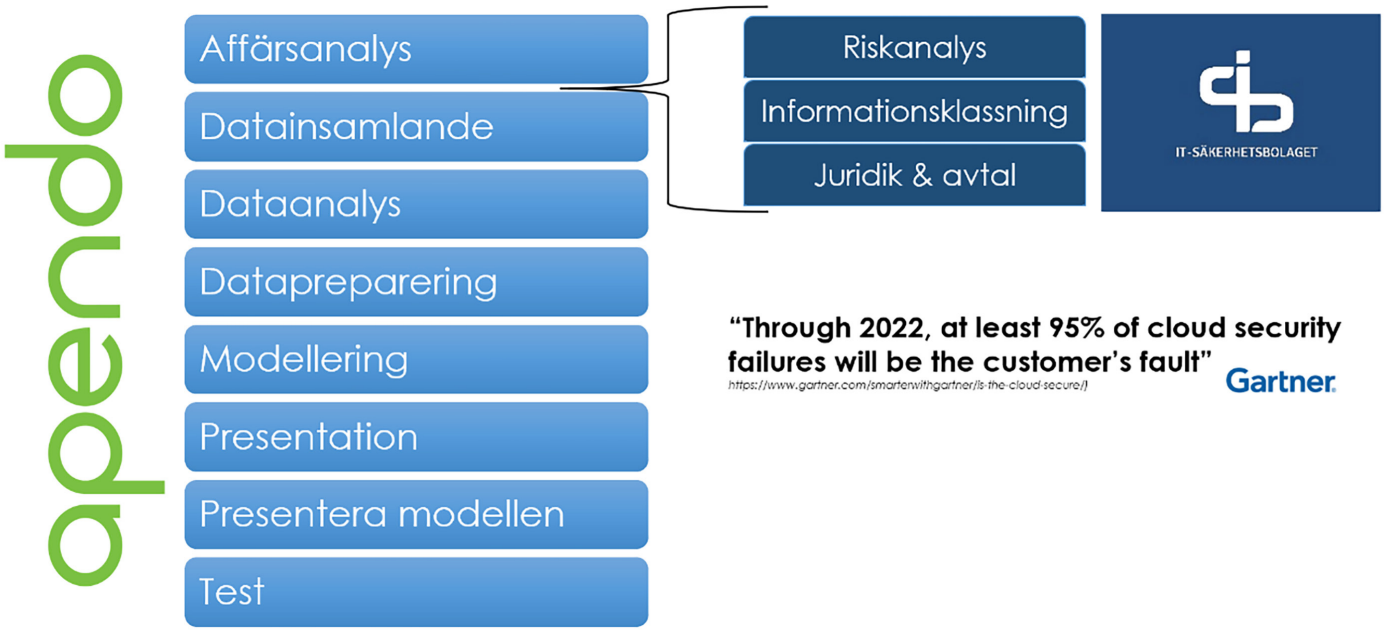
Alla känslig information ska skyddas med kryptering ska skyddas med kryptering, både i transport och vila. Säkerställ att leverantören kontinuerligt uppdaterar algoritmer och nyckellängder.

5. Tvåfaktors-autentisering

Har du känslig information måste det finnas tvåfaktors-autentisering, t ex Mobilt BankID, om assistenten ska kunna hantera känslig information. Det är viktigt att stöd för detta byggs in tidigt i lösningen, då det ofta kan vara både kostsamt och tidsödande att lägga till sådan funktionalitet efteråt.

Nästa steg

Tiden för att skapa en digital assistent driven av artificiell intelligens som möter alla säkerhetskrav är nu. Apendo har tillsammans med IT-Säkerhetsbolaget kompletterat erbjudandet kring den digitala assistenten att hantera informationens hela livscykel.



Apendo är IBM:s ledande partner inom ECM och BPM och är en av IBM certifierad World Wide Support Provider. Vår mjukvara bygger på en unik svensk version av IBMs AI Watson. Vi har ett standardiserat arbetssätt för att tillhandahålla digitala assistenter som hanterar hela införandet från idé till färdig tjänst.

Tillsammans med **IT-Säkerhetsbolaget**, som har en bakgrund i ledande säkerhetspositioner inom offentlig verksamhet, levererat GDPR-tjänster sedan 2016 och mångårig erfarenhet som informationssäkerhetskonsulter, finns möjligheten att komplettera utvecklingsprocessen med analyser av data, klassning av informationen samt den GDPR-analys som lagen kräver för att få en riskminimerad lösning.

Patrik Jonasson, vd IT-Säkerhetsbolaget
Tel 070-924 92 50 | patrik@itsakerhetsbolaget.se

Marcus Norberg, Regional Manager, ansvarig Digital Assistent, Apendo
Tel: 070-664 11 29 | marcus.norberg@apendo.se

apendo