



Dialogunderlag – IT-arkitektur (server, klient och nätverk) – PlanB

Arbetsordning

1. Gör en kort presentation i gruppen. Vilken organisation representerar ni? Vilken är er roll?
2. Utse en person som tar anteckningar som sammanfattar det gruppen vill belysa.
3. Läs igenom introduktionstexten nedan, såvida inte alla anser sig ha gjort det redan.
4. Utgå från Kom-igång-frågorna nedan, men begränsa er inte till dem utan ta också upp egna frågeställningar.

Observera – Notera löpande via denna länk, passord delas ut på plats:

<https://samverka.sambruk.se/s/twJTsrpb53B8esC>

Introduktionstext (Läs gärna denna innan workshopen)

I dagens digitala miljö blir offentliga verksamheter alltmer beroende av molnlösningar för att driva kritiska applikationer och system. Många av dessa tjänster tillhandahålls dock huvudsakligen av amerikanska aktörer, vilket medför en rad sårbarheter. Detta beroende innebär inte bara tekniska och driftsmässiga utmaningar utan medför även juridiska och geopolitiska risker. Frågor om datalagring, nationell säkerhet, rättsliga jurisdiktioner och potentiella sanktioner kan snabbt omvandla en välfungerande lösning till en källa av osäkerhet.

Utmaningen för dagens IT-arkitektur blir därför att inte bara skapa system som fungerar optimalt under normala förhållanden, utan även att designa robusta och flexibla lösningar som kan hantera störningar orsakade av externa faktorer. Detta inkluderar att noggrant utvärdera riskerna med att vara beroende av utländska molntjänster och att ta fram strategier som möjliggör diversifiering och redundans. En effektiv arkitektur måste kunna växla över till alternativa system eller leverantörer vid behov, och därigenom minimera risken för att kritiska tjänster ska drabbas av beslut eller åtgärder utanför den egna kontrollen.

Genom att integrera en holistisk och framtidssäker strategi i IT-arkitekturen, där beroendet av molntjänster granskas kontinuerligt, kan vi bygga en mer resilient infrastruktur. Detta skapar förutsättningar för en "Plan B" som inte bara är en nödåtgärd utan en integrerad del av den övergripande arkitekturen – en lösning som stärker den digitala suveräniteten och minimerar sårbarheterna inför en alltmer osäker global kontext.

Konversationsstartare

1. Vad innebär digital beredskap för offentlig sektor?

2. Hur borde en **IT-arkitektur** se ut där digital beredskap är en viktig förutsättning?
Krav på öppen källkod? Modulär arkitektur?
3. **Vilka utmaningar har ni mött när det gäller att integrera server-, klient- och nätverkskomponenter i en sammanhängande och säker IT-arkitektur?**
Diskutera konkreta exempel på hur fragmenterade system eller bristande redundans har påverkat er verksamhet och vilka lärdomar ni dragit.
4. **Hur kan vi modernisera våra IT-arkitekturer för att bättre möta de ökade säkerhetskraven och de snabba förändringarna i teknologilandskapet?**
Utforska möjligheter med nya tekniska lösningar, såsom virtualisering, containerisering eller software-defined networking, och hur dessa kan integreras med befintliga system.
5. **Vilka strategier och metoder kan implementeras för att säkerställa hög tillgänglighet och snabb återhämtning vid störningar, med beaktande av både fysiska och digitala säkerhetsåtgärder?**
Fundera på hur redundans, backup-lösningar och proaktiv övervakning kan bidra till att skapa en robust IT-arkitektur som står emot både interna fel och externa attacker.