Dialogunderlag – Informations- och IT-säkerhet – 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:

Säkerhet 1: https://samverka.sambruk.se/s/LmSgXEpTMxNGeBK
Säkerhet 2: https://samverka.sambruk.se/s/bBtQroXS9ySBBDW
Säkerhet 3: https://samverka.sambruk.se/s/N52aFBfE3oLdXRA
Säkerhet 4: https://samverka.sambruk.se/s/EjHjf7k6HCnmWtH

Introduktionstext (Läs gärna denna innan workshopen)

I en tid med ökande cyberhot och en alltmer komplex digital miljö ställs krav på att både informations- och IT-säkerhet ska vara integrerade och proaktiva delar av verksamhetens strategi. Offentliga organisationer möter utmaningar som alltmer sofistikerade attacker, interna risker samt behov av att skydda både känslig information och kritisk infrastruktur. Detta leder till frågan: Hur kan vi implementera en helhetsstrategi för säkerhet som både omfattar det tekniska och det organisatoriska perspektivet, och som samtidigt skapar en balans mellan skydd, tillgänglighet och användarvänlighet? För att möta dessa utmaningar krävs en öppen dialog om riskbedömningar, incidenthantering och kontinuerlig förbättring av säkerhetspraxis.

Konversationsstartare

1. Borde vi prata digital beredskap eller borde vi prata om digital suveränitet?
2. Borde offentlig sektor koppla sin egen **verksamhetskontinuitetsplan** till PlanB arbetet?
3. **Vad är lämpliga alternativa** molntjänster och IT-lösningar att migrera till ur ett informationssäkerhetsperspektiv. Argumentera för varför ett alternativ förespråkas.
4. Hur ska offentlig sektor fundera över digital suveränitet kopplat till PlanB?
5. **Vilka konkreta säkerhetsincidenter eller hot har ni observerat, och hur har dessa påverkat er syn på behovet av en integrerad säkerhetsstrategi?**
   Diskutera både tekniska och organisatoriska aspekter samt erfarenheter av incidenthantering.

6. **Vilka verktyg och metoder kan ni tänka er att implementera för att både förebygga och snabbt åtgärda säkerhetshot, med hänsyn till den snabba tekniska utvecklingen?**
   Utforska möjligheter med automatisering, kontinuerlig övervakning och utbildning, samt hur dessa insatser kan mätas och förbättras över tid.
7. **Vilka konkreta säkerhetsincidenter eller hot har ni observerat, och hur har dessa påverkat er syn på behovet av en integrerad säkerhetsstrategi?**
   Diskutera både tekniska och organisatoriska aspekter samt erfarenheter av incidenthantering.
8. **Vilka verktyg och metoder kan ni tänka er att implementera för att både förebygga och snabbt åtgärda säkerhetshot, med hänsyn till den snabba tekniska utvecklingen?**
   Utforska möjligheter med automatisering, kontinuerlig övervakning och utbildning, samt hur dessa insatser kan mätas och förbättras över tid.
9. Hur skulle man kunna genomföra en **migrering** på ett säkert sätt?
10. **Vilka förändringar behöver göras i IT-säkerhetsarbetet för att tidigt identifiera och hantera de juridiska och säkerhetsmässiga konsekvenserna av att vara beroende av utländska molntjänster?**
    Utforska metoder och verktyg som möjliggör en kontinuerlig riskbedömning samt integrering av säkerhet och regelefterlevnad redan i kodnings- och testfasen.
11. Vad skulle hända om de Amerikanska IT-säkerhetsverktyg som nyttjas plötsligt stängdes av?