KONFERENSEN

INFORMATIONSSÄKERHET FÖR OFFENTLIG SEKTOR

14–15 SEPTEMBER 2016

Myndigheten för samhällsskydd och beredskap

Informationssäkerheten i Sveriges kommuner

En fördjupad analys med rekommendationer

Robert Lundberg och Christina Goede, MSB

Bakgrund

- Regeringsuppdrag till MSB 2015; hur arbetar Sveriges kommuner med informationssäkerhet?
- 228 kommuner svarade på hela enkäten om systematiskt informationssäkerhetsarbete.
- Rapport lämnades till regeringen i december 2015. Publicerades på msb.se
- Nu finns en fördjupad analys med mål att ge relevanta rekommendationer till kommunerna
  - För närvarande i utkastform. Publiceras i oktober

Några resultat från analysen:

Kommunerna har påbörjat införandet av ramverk för informationssäkerhet och börjat utse ansvar, men…

- Över 40 % av kommunerna anger att de inte har någon utpekad funktion för informationssäkerhet.
  - *Av de som har funktion svarar nära 70 % att funktionen arbetar mindre än 10 % av sin arbetstid med informationssäkerhet*
- 3 av 4 kommuner uppger att det inte finns finansiella förutsättningar att bedriva systematiskt informationssäkerhetsarbete

Forts. resultat (riskanalys mm):

- Kommunerna har svag implementering av viktiga delar i systematiska informationsarbetet:
  - 40 % av kommunerna uppger att de inte har någon metod för riskanalys avseende informationssäkerhet
  - Nära 60 % uppger att de inte kontrollerar efterlevnaden av regelverk för informationssäkerhet.
  - Över hälften av kommunerna har ingen process för rapportering och hantering av incidenter med koppling till informationshanteringen

Forts. resultat (incidenthantering och kontinuitetshantering):

- Nära 60 % av kommunerna har inga kontinuitetsplaner för att hantera bortfall av information i kritiska verksamhetsprocesser i kommunen.

- Av de som har en kontinuitetsplan övar endast 20 % regelbundet

Positivt dock att 60 % av uppger att incident-rapporteringsprocessen innefattar kommunens externa leverantörer

Vad kan man se för skillnader utifrån några centrala frågor?

7 st. utvalda indikatorer :

- Finns det en utpekad funktion för informationssäkerhet inom kommunen?
- Kontrolleras efterlevnad rörande informationssäkerhet?
- Tillämpar kommunen ett systematiskt arbetssätt när det gäller informationssäkerhet?
- Har kommunen en metod för informationsklassning?
- Genomför kommunen riskanalys avseende informationssäkerhet?
- Finns kontinuitetsplaner för att hantera bortfall av information i kritiska verksamhetsprocesser inom kommunen?
- Finns det en process för rapportering och hantering av säkerhetsbrister/incidenter kopplade till informationshantering inom kommunen?

Indikatorer

- 15 kommuner svarade JA på samtliga 7 frågor.
- 21 kommuner svarade Nej på samtliga 7 frågor.

Urval av resultat

- De kommuner som svarat JA på frågorna hade i högre grad (93 %) än genomsnittet ett **samarbete med andra kommuner**, och de som svarat NEJ har på motsvarande sätt en lägre grad av samverkan (32 %).

- Av de kommuner som svarade JA på frågorna hade alla (100 %) en beslutad **informationssäkerhetspolicy**, och av de kommuner som svarade NEJ hade mindre än hälften en sådan policy (41 %).

- Av de kommuner som svarade JA på frågorna erbjöd 86 % **utbildning** i informationssäkerhet till de anställda. Motsvarande för de som svarade NEJ var 36 %.

Slutsats

Flera av resultaten är nära förknippade med resurser – de kommuner som har en företrädare för informationssäkerhetsfrågor med tillräcklig tid för uppdraget har generellt sett ett mer systematiskt informationssäkerhetsarbete.

Exempel på det är:

- rapporteringsvägar
- hur riskanalys och informationsklassning tillämpas
- hur informationssäkerhetsaspekter hanteras i samband med upphandlingar.

Rekommendationer

1. Utse en funktion för informationssäkerhet

- bör vara direkt underställd den högsta ledningen.
- behöver använda en majoritet av sin tid till uppdraget och få resurser.
- behöver kontinuerligt kompetensutvecklas och
- behöver etablera kontakter och hitta former för samverkan.

Rekommendationer

2. Ta fram en analys av nuläget i kommunen

- Ta fram en analys av nuläget i kommunen vilket handlar om att skapa en samlad bild om informationssäkerhetsnivån i kommunen.

Rekommendationer

3. Informera och skapa en handlingsplan utifrån nuläget:

- **Informera ledningen hur nuläget ser ut**. Visa exempel på reella hot och incidenter. Beskriv några centrala lagkrav, ex dataskyddsförordningen som får stor påverkan på hur kommunen hanterar personuppgifter.

- **Skapa handlingsplan** utifrån nuläget. Bör beslutas av ledningen.
  - I handlingsplanen bör det finnas en aktivitet som handlar om att Identifiera vilken kritisk information som hanteras inom kommunen för att sedan klassa den informationen. Fokusera på den mest kritiska informationen/känsliga informationen som är i behov av höga skyddskrav.

- Ta fram styrdokument som policy och riktlinjer samt åtgärda de viktigaste bristerna och sårbarheterna.

Rekommendationer

4. Höj säkerhetsmedvetandet:

- Se till att höja säkerhetsmedvetandet inom kommunen och stödja organisationens förmåga att efterleva kraven i riktlinjerna. Detta kan ske ex. genom utbildning, att ta fram vägledningar och annan information.

Rekommendationer

5. Utvärdera och uppdatera:

- Se över om kommunen efterlever det som står i de framtagna riktlinjerna. Planera in återkommande uppföljning/revison av verksamheten. Resultaten av uppföljning skall ingå som en del av den återkommande rapporteringen till ledningen.

Och glöm inte att övning ger färdighet!

Tack för att ni lyssnade!

Kontakt:

Robert.lundberg@msb.se

Christina.goede@msb.se

Mer information finns på:

www.informationssakerhet.se och www.msb.se