Myndigheten för samhällsskydd och beredskap

Datum	Diarienr	Utgåva
2018-10-01	MSB2017-07165-76	

Bevakningsansvariga myndigheters informations- och cybersäkerhet

Ett utdrag från en sammanvägd rapport utifrån redovisningar enligt Ju2017/05787/SSK

Innehållsförteckning

1. Inledning

Regeringen gav den 29 juni 2017 Myndigheten för samhällsskydd och beredskap (MSB) i uppdrag att, i samverkan med Försvarsmakten och Säkerhetspolisen, redovisa en sammanvägd rapport utifrån samtliga bevakningsansvariga myndigheters redovisningar av analyser och bedömningar av sin informationssäkerhet i de delar av den egna verksamheten som är nödvändiga för att myndigheten ska kunna utföra sitt arbete. Krisberedskapsperspektivet samt planering för det civila försvaret skulle beaktas i redovisningarna.

Säkerhetspolisen och Försvarsmakten har i samverkan bidragit med sina respektive perspektiv på den bild och den analys som MSB sammanställt baserat på redovisningarna.

Det finns en betydande variation gällande både kvalitet och omfattning i de bevakningsansvariga myndigheternas redovisningar. Av denna anledning har MSB gjort bedömningen att det inte är lämpligt att dra precisa statistiska slutsatser utifrån redovisningarna. MSB:s fokus ligger på att identifiera omständigheter i redovisningarna vilka enligt MSB:s bedömning behöver uppmärksammas.

2. Analys och slutsatser

MSB bedömer att redovisningarnas varierande kvalitet och omfattning beror på myndigheternas varierande mognad i informationssäkerhetsarbetet. En mogen organisation identifierar många risker som är relevanta och organisationen har ett systematiskt arbetssätt för att åtgärda bristerna. En mindre mogen organisation identifierar färre brister och inte nödvändigtvis de som är mest kritiska för verksamheten. Därutöver tenderar en mindre mogen organisation att inte heller precisera vilka åtgärder som ska genomföras för att minska de identifierade riskerna.

Det är av största vikt att alla myndigheter uppnår en nivå av informations- och cybersäkerhet där de har förmåga att arbeta systematiskt så att de kan identifiera sina risker och åtgärda brister på ett adekvat sätt.

Ansvaret för informations- och cybersäkerhetsarbetet bör vara en naturlig del i verksamhetsansvaret, även för myndighetsledningar. Det är ytterst ledningen som måste göra en riskbedömning och avgöra vilka sårbarheter som ska åtgärdas och vilka risker som en verksamhet ska acceptera.

Vidare är det MSB:s uppfattning att myndigheter behöver utbyta erfarenheter kring sitt praktiska informations- och cybersäkerhetsarbete för att tillsammans kunna utveckla skyddet av samhällets informationstillgångar.

MSB drar bland annat följande övergripande slutsatser av redovisningarna.

- Det finns brister i koppling mellan verksamhetsansvar och informations- och cybersäkerhetsansvar.
- Få myndigheter följer MSB:s föreskrifter i sin helhet.
- Underlaget från bevakningsansvariga myndigheter kan förbättras gällande både omfattning och kvalitet.
- Arbetet med informations- och cybersäkerhet och säkerhetsskydd är inte tillräckligt integrerat.

3. Återkoppling till bevakningsansvariga myndigheter

I samverkan mellan Säkerhetspolisen, MSB och Försvarsmakten har följande identifierats som särskilt viktiga att återkoppla till myndigheterna.

- Det systematiska informationssäkerhetsarbetet kräver kunskap och resurser. Ledningen ska säkerställa att detta finns för att genomföra informations- och cybersäkerhetsarbetet i den omfattning som behövs.
- Effektiva arbetssätt för informations- och cybersäkerhet ska ta sin grund i bland annat verksamhetsanalys, informationsklassning och riskanalys.
- Det ska finnas en tydlig ansvarsfördelning för informations- och cybersäkerhetsarbetet, som följer ansvaret för övriga verksamheten.
- Det ska finnas interna regler för informations- och cybersäkerheten som är anpassade till den verksamhet som bedrivs och de medarbetare som ska förstå och följa reglerna.
- Det ska ske en tydlig kravställning av både funktion och säkerhet vid upphandling av produkter och tjänster, vilket ska kopplas till en aktiv uppföljning av efterlevnad.
- Skyddsåtgärder ska utformas utifrån arbetssätt. Nya metoder kan kräva nya eller anpassade skyddsåtgärder, i vissa fall kan arbetssätt behöva anpassas efter vilka skyddsåtgärder som är möjliga.
- Myndigheterna ska ha ett systematiskt och riskbaserat arbetssätt för att ges förutsättningar att skydda sina informationstillgångar även vid kriser och vid höjd beredskap.

- Myndigheterna bör höja skyddsnivån i sina it-system genom att använda vedertagna it-säkerhetsåtgärder.

Analys, slutsatser och de områden som identifierats avseende återkoppling i rapporten kommer omhändertas i det fortsatta arbetet med en samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022 (Ju2018/03737/SSK).