Handläggare
Peter Wengrud

Redovisning av regeringsuppdrag om informationssäkerhet

Inledning

SGU fick i sitt regleringsbrev för 2024 uppdraget att övergripande redogöra för hur myndigheten arbetat för att stärka sin informationssäkerhet och för hur den planerar för att möta framtida behov. SGU hade ett liknande uppdrag i regleringsbrevet för 2022 och 2023. Denna redovisning utgör därför till stora delar en uppföljning av tidigare rapporteringar.

SGU har fortsatt att genomföra insatser för att stärka informationssäkerhetsarbetet.

Under 2022 och 2023 genomfördes särskilt satsningar på säkrad it-infrastruktur på SGU:s undersökningsfartyg Ocean Surveyor.

Under 2024 har stort fokus legat på förstärkningar i nätverk och servermiljö samt förstärkning av den säkerhetsskyddsklassade it-miljön. Flera förstärkningar planeras även inom ramen för nya lokaler.

Enligt uppdraget ska SGU särskilt redogöra för sju mer detaljerade områden vilka redovisas nedan.

Styrning och uppföljning av informationssäkerhetsarbetet.

Uppdrag: Åtgärder för att utveckla den interna styrningen och uppföljningen av informationssäkerhetsarbetet inkl. myndighetsledningens roll i detta.

Säkerhetschefen har regelbunden rapportering/dialog med GD och även dragningar i myndighetens ledningsgrupp, för att informera och diskutera olika aspekter av myndighetens säkerhetsarbete.

Infosäkkollen

Uppdrag: Huruvida myndigheten gjort en utvärdering av det egna informationssäkerhetsarbetet genom Myndigheten för samhällsskydd och beredskaps verktyg Infosäkkollen, samt huruvida åtgärder vidtagits med anledning av resultatet.

SGU har genomfört utvärderingen Cybersäkkollen 2024 som redovisats 2024-09-06. Resultatet visade att SGU även fortsättningsvis har ett stort behov av förbättring av säkerhetsarbetet. Det återstår en hel del arbete med styrdokument och systematik.

Resultatet av Cybersäkkollen 2024 kommer att ligga till grund för planeringen av fortsatta insatser.

En del insatser har genomförts för att förbättra informationssäkerhetsarbetet. Den relativt stora satsningen på it-infrastruktur samtidigt med en viss personalomsättning har dock gjort att myndigheten inte nått så långt som planerat.

SGU har under hösten beslutat rekrytering av informationssäkerhetsansvarig, CISO.

Beroenden av externa parter

Uppdrag: Huruvida en analys gjorts av kopplingar till och beroenden av externa parter, exempelvis it-tjänsteleverantörer och andra myndigheter, samt om åtgärder vidtagits eller planerats för att minska ev. identifierade risker med anledning av detta.

Den tidigare planerade riskanalysen kommer att genomföras under Q4. I arbetet kommer erfarenheter från incidenten med Primula att tas om hand.

Analys av distansarbete

Uppdrag: Huruvida en analys gjorts av hur arbete på distans påverkar informationssäkerheten.

SGU har under alla år bedrivit en stor del av sin verksamhet i fält. Det har inneburit att den it-infrastruktur som byggts upp genom åren, har varit anpassad även för distans- och fältarbete. I samband med pandemin ökade arbetet på distans i vissa verksamheter men minskade i andra.

SGU har kontinuerligt arbetat med att förbättra informations- och it-säkerheten, framför allt med beaktande av försämrat omvärldsläge och ökad hotbild de senaste åren. SGU har för avsikt att fortsätta med detta framöver.

Utifrån en sammantagen bedömning anser SGU att ingen förändrad riskbild föreligger med anledning av arbetet på distans.

Hantering av it-incidenter

Uppdrag: Huruvida åtgärder vidtagits för att öka förmågan att identifiera och rapportera it-incidenter, samt för att skyndsamt kunna vidta nödvändiga åtgärder.

SGU har fortsatt det arbete som initierades 2022 och har en övergripande rutin för incidenthantering. I dagsläget finns information på SGU:s intranät om hur man påtalar och dokumenterar en händelse eller incident. SGU:s har skapat en kontaktpunkt för att ta emot anmälningar av incidenter och besluta om hantering. Kontaktpunkten är dock enbart aktiv för anmälan under kontorstid.

I december 2023 genomfördes en skrivbordsövning rörande en it-incident. Ett antal förbättringsåtgärder identifierades.

Det är en utmaning för en medelstor myndighet att rekrytera och behålla den typ av resurser som krävs. Generellt är det en stor brist på denna specifika kompetens.

Analys av hot och sårbarheter

Uppdrag: Huruvida en analys gjorts av om hot och sårbarheter för myndigheten förändrats i och med det rådande omvärldsläget, samt om åtgärder vidtagits eller planerats för att minska eventuella identifierade risker med anledning av detta.

SGU kommer genomföra säkerhetsskyddsanalys under 2024 och även rapportera risk- och sårbarhetsbedömning, RSB, till MSB 2024-09-30.

Åtgärder för att hantera identifierade risker och sårbarheter planeras och genomförs successivt.

Ett antal förbättringsåtgärder genomförs även inom ramen för SGU:s flytt till nya lokaler våren 2025.

Analys av risker för informationsläckage från applikationer

Uppdrag: Huruvida en analys har gjorts i förhållande till applikationer och dess förmåga att samla in data och information från myndighetens telefoner och it-system, och om det finns särskilda rutiner för att säkerställa att lämpliga åtgärder vidtas och efterlevs.

En sådan särskild analys har inte genomförts.

SGU har en central styrning av appar för mobiltelefoner. Dock finns brister i säkerhetsgranskningen av nya appar.

SGU har en central vitlista med godkända programvaror. SGU:s licensråd bedömer varje önskemål om ny programvara. Vår it-säkerhetsfunktion kontrollerar varje installation av nya system och programvaror.