Datum
2015-12-08

Dnr
2015:7252
KONFIDENTIELL

GD-sekretariatet
Mats Löwenberg
016-542 06 13
mats.lowenberg@energimyndigheten.se

Sammanställning av uppdrag i regleringsbrevet 2015 avseende informationssäkerhet

1. Uppdragets bakgrund

Enligt regleringsbrevet för budgetåret 2015 har energimyndigheten fått följande uppgift:

”Statens energimyndighet ska i arbetet med 2015 års risk- och sårbarhetsanalyser särskilt beakta och analysera informationssäkerheten i de delar av verksamheten och i de tekniska system som är nödvändiga för att myndigheten ska kunna utföra sitt arbete. I detta arbete ska även informationssäkerheten inom myndigheten ansvarsområde beaktas och analyseras. Myndigheten ska redovisa en bedömning av informationssäkerheten samt vidtagna åtgärder. Redovisningen ska vara en del av den sammanställning som görs i arbetet med risk- och sårbarhetsanalyser enligt 9 § förordningen (2006:942) om krisberedskap och höjd beredskap”

Denna bilaga beaktar dock inte informationssäkerheten i myndighetens ansvarsområde utan endast egen intern organisation och verksamhet.

1.1 Syfte

Syftet med arbetet är att genomföra en informationssäkerhetsanalys utifrån kraven i regleringsbrevet för 2015 och MSB:s tillhörande vägledning. Den övergripande ambitionen med arbetet är att studien kan utgöra underlag för vidare utveckling av informationssäkerhetsarbetet inom myndigheten.

1.2 Metod

Arbetsprocessen har genomförts genom följande aktiviteter:

1. *Identifikation och klassificering*
   a) Identifiering av samhällsviktig verksamhet.
   b) Identifiering av informationstillgångar för de samhällsviktiga och kritiska verksamheterna.

Box 310 • 631 04 Eskilstuna • Besöksadress Kungsgatan 43
Telefon 016-544 20 00 • Telefax 016-544 20 99
registrator@energimyndigheten.se
www.energimyndigheten.se
Org.nr 202100-5000

KONFIDENTIELL

2. *Analys*
   a) Identifiering och analys av risker och sårbarheter mot identifierade verksamheter och dess informationstillgångar.
   b) Identifiering av förbättringsförslag.
   c) Identifiering och analys av rättsliga krav, utifrån ett informationssäkerhetsperspektiv.
3. *Bedömning*
   a) Sammanställning av analyserade risker, sårbarheter och rättsliga krav.
   b) Slutsatser och rekommendationer.

1.3 Definitioner

Termer och begrepp som används i denna rapport är:

Term eller begrepp	Definition och källa
Samhällsviktig verksamhet	En verksamhet som uppfyller minst ett av följande villkor: 1. Ett bortfall av, eller en svår störning i verksamheten som ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid kan leda till att en allvarlig kris inträffar i samhället. 2. Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt. Källa: MSB
Kritiskt beroende	En verksamhet kan vara kritiskt beroende av en viss resurs, och om denna resurs försvinner eller drabbas av störningar får den beroende verksamheten snart mycket svårt att fungera och uppfylla sina prioriterade åtaganden. Ett beroende är kritiskt om det är svårt att ersätta resursen med en annan. Källa: FOI

KONFIDENTIELL

Krisberedskap	Med krisberedskap avses förmågan att förebygga, motstå och hantera krissituationer, genom utbildning, övning och andra åtgärder samt genom den organisation och de strukturer som skapas före, under och efter en kris. Källa: FOI
Informationstillgång	En organisations informationsrelaterade tillgångar. Exempel på informationstillgångar är: − information (kunddatabas, metodik, dokument) − program (applikation, operativsystem) – tjänster (kommunikationstjänst, abonnemang) − fysiska tillgångar (dator, datamedia, lokala nätverk) Informationstillgångar kan vara av fysisk eller logisk karaktär, eller bådadera. Källa: SIS. Terminologi för Informationssäkerhet Utgåva 3
Informationssäkerhet	Bevarande av konfidentialitet, riktighet och tillgänglighet hos information; vidare kan andra egenskaper såsom autenticitet, spårbarhet, oavvislighet och tillförlitlighet också inbegripas. Källa: I SS-ISO/IEC 27002
Tillgänglighet	Att behöriga användare har tillgång till de resurser de är behöriga till i rätt tid och omfattning. Källa: Standarden SS-ISO/IEC 17799
Riktighet	Att information inte obehörigt ändras eller modifieras. Källa: Standarden SS-ISO/IEC 17799
Konfidentialitet	Att endast behöriga användare kommer åt informationen. Källa: Standarden SS-ISO/IEC 17799
Spårbarhet	Att kunna se vem som gjort vad och vid vilken tidpunkt. Källa: Standarden SS-ISO/IEC 17799

2. Resultat

2.1 Samhällsviktig verksamhet

Nedan presenteras en lista över den identifierade samhällsviktiga verksamheten inom Energimyndigheten.

Enheten för trygg energiförsörjning
Enheten ansvarar till stor del för det energikrisförebyggande arbetet och skapar därigenom förutsättningar för myndighetens operativa roll vid energikriser.

Ledning av myndigheten
Myndighetens ledningsgrupp utgörs av sju personer, inklusive generaldirektören. Ledningsgruppen kan ge mandat till krisledningsgruppen, vilken består av en krisledare med berörda stödfunktioner.

Tjänsteman i beredskap (TiB)
TiB har till uppgift att initiera och samordna det inledande arbetet för att uppräcka, verifiera, larma och informera vid allvarliga olyckor och kriser som berör Energimyndigheten.

Kommunikationsenheten
Enheten kan involveras i ett brett spektra av olika händelser och har beredskap för att hantera händelser som innebär kriskommunikation.

2.2 Kritiska verksamheter

Nedan presenteras verksamheter inom myndigheten som identifierats som nödvändiga eller mycket väsentliga för att upprätthålla myndighetens samhällsviktiga verksamheter.

Registratur
Utifrån ett krisberedskapsperspektiv utgör registraturen en av kanalerna in till myndigheten och är viktig för att externa intressenter ska kunna komma i kontakt med myndigheten.

Växel och telefoni
Växeln är viktig för att intressenter ska komma i kontakt med myndigheten på ett effektivt sätt. Intressenter kan fortfarande komma i kontakt med myndigheten om växeln ligger nere genom direkt- mobil- eller kortnummer.

IT-drift och support
IT-enheten och IT-drift bedöms utgöra kritiska verksamheter, då de är centrala för att upprätthålla myndighetens IT-miljö.

KONFIDENTIELL

2.3 Rättsliga regler

I detta avsnitt beskrivs de lagar, förordningar och föreskrifter som bedöms påverka Energimyndighetens informationssäkerhetsarbete. Vidare ges en kort kommentar om huruvida myndigheten har beaktat kravet eller inte.

Personuppgiftslagen
Syftet med denna lag är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Personuppgifter definieras som all slags information som direkt eller indirekt kan hänföras till en fysisk person i livet.

Personuppgiftslag(1998:204)
Datainspektionens allmänna råd om säkerhet för personuppgifter

Kommentar: Myndigheten har utsett en personuppgiftsansvarig. Lämpliga tekniska och organisatoriska åtgärder bedöms ha vidtagits. Vidare har myndigheten diskuterar lagen och dess omfattning och utbildat chefer i hantering av personuppgifter. Sammantaget bedöms Energimyndigheten beakta och efterleva Personuppgiftslagen.

Offentlighets- och sekretesslagen
Offentlighetsprincipen, reglerar vilken typ av information hos myndigheterna som ska betraktas som allmänna handlingar och då enligt huvudregeln vara tillgängliga, offentliga. Vissa allmänna handlingar innehåller dock känsliga uppgifter, exempelvis rörande rikets säkerhet eller den enskildes personliga förhållanden. Offentlighets- och sekretesslagen specificerar därför vilka av de allmänna handlingarna som ska beläggas med sekretess.

Tryckfrihetsförordning (1949:105)
Offentlighets- och sekretesslag (2009:400)

Kommentar: Energimyndigheten bedömer att flertalet medarbetare känner en osäkerhet vid utlämning och skydd av handlingar, i enlighet med Offentlighets- och sekretesslagen. Medarbetarna har möjlighet att begära hjälp från myndighetens jurister, men medarbetarna har en bristande kompetens och förståelse för hur lagen och tillhörande förordning ska följas.

MSB:s föreskrifter om statliga myndigheters informationssäkerhet, (MSBFS 2009:10)
Informationssäkerhet i verksamheter byggs i stor utsträckning upp genom systematiskt arbete som involverar ledningen, grundas på risk- och sårbarhetsanalyser och rätt vidtagna åtgärder, såväl administrativt som tekniskt. Myndigheten för samhällsskydd och beredskap anvisar att myndigheterna ska

införa ett ledningssystem för informationssäkerhet som baseras på de internationella standarderna ISO/IEC 27001 och ISO/IEC 27002.

MSB:s föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet, MSBFS 2009:10

Kommentar: Sammantaget uppfyller Energimyndigheten flertalet av de krav som åligger myndigheten, i enlighet med föreskriften. Myndigheten har dock ett behov av att se över och förbättra ett antal områden. En av de allvarligaste bristerna är bristen på systematik i informationssäkerhetsarbetet.

Arkivera information
Att arkivera information har många kopplingar till informationssäkerhet, då arkivering säkrar riktigheten hos och skapar tillgänglighet till allmänna handlingar. Arkivering ställer särskilda krav, särskilt när det gäller elektronisk information. Riksarkivet utfärdar föreskrifter på området.

Arkivlag (1990:782)
Arkivförordning (1991:446)
Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar, RA-FS 2009:1
Riksarkivets föreskrifter om och allmänna råd om tekniska krav på elektroniska handlingar, RA-FS 2009:2

Kommentar: Myndigheten har under en längre tid arbetat med att förbättra arkivverksamheten både gällande arbetsmetoder och informationssäkerhet. Ett steg mot bättre skydd har tagits då tillgängligheten till arkiven har begränsats. Förbättringsarbetet pågår och en ny chefsarkivarie har anställts.

Sekretessbelagd information rörande rikets säkerhet
Information som är sekretessbelagd med hänsyn till rikets säkerhet ges ett särskilt skydd genom säkerhetsskyddslagen. Säkerhetsskyddet ska bland annat förebygga att sådana uppgifter på ett obehörigt sätt röjs, ändras eller förstörs samt hindra obehöriga att få tillträde till platser där de kan få tillgång till den typen av uppgifter.

Säkerhetsskyddslag (1996:627)
Säkerhetsskyddsförordning (1996:633)
Säkerhetspolisens föreskrifter och allmänna råd om säkerhetsskydd (PMFS 2015:3)
En ny säkerhetsskyddslag (SOU 2015:25)

Kommentar: Myndigheten genomför säkerhetsprövning och registerkontroll i samband med nyanställningar. Myndigheten anser att det finns ett behov av att ta

fram och genomföra egna personutredningar, för att själv bilda sig en uppfattning om personen är lämplig ur säkerhetssynpunkt. Myndigheten har även ett behov av att genomföra en säkerhetsskyddsanalys och se över organisationens säkerhetsskyddsarbete. Här är den pågående informationsklassningen ett grundläggande ingångsvärde.

Civila myndigheters kryptoberedskap
Myndigheten för samhällsskydd och beredskap föreskriver att civila myndigheter ska säkerställa kryptoberedskap under ordinarie kontorstid.

Myndigheten för samhällsskydd och beredskaps
föreskrifter om civila myndigheters kryptoberedskap (2009:11)

Kommentar: Energimyndigheten bedöms följa gällande föreskrifter. Myndigheten arbetar även med kompetensutveckling för att anställda ska kunna använda signalskyddsutrustningen.

3. Analys

De informationstillgångar som Energimyndigheten behöver för att upprätthålla identifierad samhällsviktig verksamhet eller kritiska beroenden, varierar beroende på vilken verksamhet som avses. De informationstillgångar som är signifikanta och gemensamma för flera av verksamheterna berör elektroniska kommunikationssystem och dataöverföring, information och medarbetare.

De rättsliga kraven visar att myndigheten efterlever merparten av de krav som åligger myndigheten. Energimyndigheten har dock ett behov av se över och vidta förbättringsåtgärder. De största bristerna grundar sig i en bristande systemetik i informationssäkerhetsarbetet och avsaknad av ett antal skyddsåtgärder.

De risker som identifierades spänner över ett stort område och varierar i karaktär och omfattning. Flertalet av riskerna kan medföra allvarliga konsekvenser för myndighetens förmåga att upprätthålla den samhällsviktiga verksamheten. De risker som identifierats mot kategorierna Information och Medarbetare, indikerar att det finns en avsaknad av bland annat styrande dokument, kontinuitetsplaner och rutiner. Vidare har de anställda bristande kompetens i exempelvis informationsklassning, sekretessprövning och hur de ska skydda sig mot diverse risker i rollen som användare. Många av riskerna inom dessa kategorier kan åtgärdas genom administrativa skyddsåtgärder, exempelvis utbildning och ett tydligt regelverk. Vidare har myndigheten ett behov av att se över hur leverantörer upphandlas och vilka krav som kan ställas på leverantörer av exempelvis IT-system.

De risker som identifierats mot kategorierna Programvarutillgångar och Tjänster har ett behov av mer tekniskt orienterade åtgärder. Många av dessa tekniska åtgärder förutsätter dock att verksamheterna klassificerar informationstillgångar

och kommunicerar dessa krav till IT-enheten. Informationsklassificering bidrar till att identifiera vad som är skyddsvärt och vilka krav som finns på skyddet.

Sammantaget visar analysen att det finns ett antal risker som kan medföra allvarliga konsekvenser för myndigheten och dess åtaganden. Det finns däremot flera åtgärder som är enkla och relativt kostnadseffektiva att genomföra för att stärka informationssäkerheten. Myndigheten behöver dock ta ett helhetsgrepp på informationssäkerhetsarbetet och kombinera tekniska och administrativa skyddsåtgärder till en väl fungerande helhet.

4. Slutsats och rekommendationer

4.2 Slutsats

Analysen har visat att det finns brister i informationssäkerhet i förhållande till de krav och risker som finns gentemot myndigheten. En stor del av den information som skapas och lagras hos myndigheten är både viktig och känslig. Det kan få allvarliga följder om informationen stjäls, manipuleras, förloras eller sprids till obehöriga. Brister i informationssäkerheten skulle även kunna medföra att energimyndigheten inte uppfyller sina prioriterade åtaganden.

Informationssäkerhet omfattar både administrativa rutiner med policys och riktlinjer samt tekniskt skydd med bland annat brandväggar och kryptering. Energimyndigheten har ett behov av att ta ett helhetsgrepp och skapa en fungerande långsiktig process för att ge organisationens tillgångar ett adekvat skydd. Att åstadkomma en god informationssäkerhet är en komplex process som inbegriper hela verksamheten och som kräver engagemang och reglering från myndighetens ledning.

4.3 Rekommendationer

För att Energimyndighetens informationssäkerhet ska bli ändamålsenlig utifrån de risker och krav som ställs ges följande rekommendationer:

- Grundläggande förutsättningar i form av ett ändamålsenligt regelverk, som tydligt anger inriktningen för myndighetens informationssäkerhet. Myndigheten har visserligen ett regelverk, men det finns ett behov av att revidera dess struktur.
- En fortsatt inventering och klassificering av skyddsvärda tillgångar, för att identifiera vad som ska skyddas och vilka krav det ska finnas på skyddet.
- Förtydligande av ansvar och roller för hur informationssäkerhetsarbetet ska bedrivas, samt ett systematiskt och processinriktat arbetssätt, vilket med fördel kan utformas utifrån ISO/IEC 27000-serien.

KONFIDENTIELL

- Medarbetare är en av organisationens viktigaste tillgångar, men bristande medvetenhet kan utsätta myndigheten för onödiga risker. Myndigheten bör kontinuerligt utbilda personalen i informationssäkerhet. Utbildningen bör åtminstone omfatta organisationens regelverk, aktuella risker och grundläggande skyddsåtgärder, såväl tekniska som administrativa.
- Systematiska och kontinuerliga analyser av hot, risker och krav som påverkar informationssäkerhetsarbetet bör genomföras. Dessa analyser kan med fördel kombineras med en säkerhetsskyddsanalys.