

# Risk- och sårbarhetsanalys



## Förord

Svenska kraftnät ska enligt förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap göra risk- och sårbarhetsanalyser i syfte att stärka krisberedskapen inom myndighetens ansvarsområde. Vart annat år ska analysen redovisas till regeringen och Myndigheten för samhällsskydd och beredskap (MSB).

I årets rapport görs fördjupningar inom tre områden, nämligen störningar i försörjning av drivmedel, exponering av skyddsvärda informationsresurser mot osäkra nätverk samt höga flöden i reglerade vattendrag.

Syftet med analysen är att bedöma faktorer som kan påverka förmågan att förebygga, motstå och hantera konsekvenser av ovan nämnda riskkällor för elförsörjningen. Fokus har legat på att identifiera eventuella brister och ta fram åtgärdsförslag.

Ett drygt tiotal elföretag inom distribution och produktion har lämnat viktiga bidrag till analysunderlaget.

I rapporten redovisas även en sammanfattning av den bedömning av myndighetens generella krisberedskap som gjorts utifrån de indikatorer som MSB har tagit fram.

Sundbyberg den 31 oktober 2016



Mikael Odenberg  
Generaldirektör

## Innehåll

Förord .....	3
1 Svenska kraftnäts ansvarsområde .....	7
2 Beskrivning av arbetsprocess och metod .....	9
2.1 Uppdraget .....	9
2.2 Förutsättningar .....	9
2.3 Mål och syfte .....	10
2.4 Mottagare .....	10
2.5 Sekretess .....	10
2.6 Metod och genomförande .....	10
2.6.1 Arbetet under 2016 .....	10
2.6.2 Bedömningsgrunder .....	13
2.6.3 Kommande arbete .....	14
3 Identifierad samhällsviktig verksamhet som är av nationell betydelse .....	15
4 Identifierade kritiska beroenden för identifierad samhällsviktig verksamhet ....	17
5 Identifierade och analyserade hot och risker .....	19
5.1 Hotbildsanalys .....	19
5.2 Störningar i försörjning av drivmedel .....	21
5.3 Exponering av skyddsvärda informationsresurser mot osäkra nätverk .....	23
5.4 Höga flöden i reglerade vattendrag .....	26
6 Bedömning av myndighetens generella krisberedskap enligt indikatorer i bilaga 1 .....	29

6.1	<i>Ledning och krishantering</i> .....	29
6.2	<i>Informationssäkerhet</i> .....	29
6.3	<i>Planering och övning</i> .....	29
6.4	<i>Samverkan och kommunikation</i> .....	29
6.5	<i>Resurser</i> .....	30
7	Beskrivning av identifierade sårbarheter och brister i krisberedskapen.....	31
7.1	<i>Sårbarheter och brister kopplade till störningar i försörjning av drivmedel</i> .....	31
7.2	<i>Sårbarheter och brister kopplade till exponering av skyddsvärda informationsresurser</i> .....	31
7.3	<i>Sårbarheter och brister kopplade till höga flöden i reglerande vattendrag</i> .....	32
8	Genomförda, pågående och planerade åtgärder sedan föregående rapportering.....	33
8.1	<i>Störningar i försörjning av drivmedel</i> .....	33
8.2	<i>Exponering av skyddsvärda informationsresurser mot osäkra nätverk</i> .....	34
8.3	<i>Höga flöden i reglerade vattendrag</i> .....	36
8.4	<i>Behov av ytterligare åtgärder med anledning av risk- och sårbarhetsanalysens resultat</i> .....	37
9	Bilaga 1.....	37



# 1 Svenska kraftnäts ansvarsområde

Affärsverket svenska kraftnät har till uppgift att på ett affärsmässigt sätt förvalta, driva och utveckla ett kostnadseffektivt, driftsäkert och miljöanpassat kraftöverföringssystem (stamnät), sälja överföringskapacitet och bedriva verksamheter i övrigt som är knutna till stamnätet.<sup>1</sup>

Utöver ansvaret för stamnätet har Svenska kraftnät också ett antal systemövergripande myndighetsuppgifter. Svenska kraftnät är systemansvarig myndighet för det nationella elsystemet<sup>2</sup>, elberedskapsmyndighet<sup>3</sup>, bevakningsansvarig myndighet<sup>4</sup>, säkerhetsskyddsmyndighet<sup>5</sup> för elförsörjningen samt främjande<sup>6</sup> och tillsynsvägläggande myndighet för dammsäkerhet<sup>7</sup>. Svenska kraftnät är även en av de myndigheter som är utpekad som särskilt ansvarig för krisberedskapen inom sin sektor.<sup>8</sup>

Vid en allvarlig händelse inom elförsörjningen ska Svenska kraftnät samverka med berörda aktörer och kunna lämna en samlad lägesbild för elförsörjningen till Regeringskansliet och Myndigheten för samhällsskydd och beredskap (MSB).

Vid krig ska Svenska kraftnät tillgodose samhällets behov av elkraft genom att planera, leda och samordna elförsörjningens resurser. Vid en fredstida allvarlig händelse krävs det ett regeringsbeslut för att Svenska kraftnät ska få motsvarande mandat.<sup>9</sup>

---

<sup>1</sup> Förordning (2007:1119) med instruktion för Affärsverket Svenska kraftnät

<sup>2</sup> Ellag (1997:857) och Förordning (1994:1806) om systemansvaret för el

<sup>3</sup> Elberedskapslag (1997:288) och Förordning (1997:294) om elberedskap

<sup>4</sup> Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap

<sup>5</sup> Säkerhetsskyddslag (1996:627) och Säkerhetsskyddsförordning (1996:633)

<sup>6</sup> Förordning (2007:1119) med instruktion för Affärsverket Svenska kraftnät

<sup>7</sup> Miljötillsynsförordningen (2011:13) Rapportering till regeringen om utvecklingen av dammsäkerheten i landet görs årligen. Se dammsäkerhetsutvecklingen i Sverige 2015, Dnr: 2015/2441

<sup>8</sup> Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap

<sup>9</sup> Förordning (2007:1119) med instruktion för Affärsverket Svenska kraftnät





## 2 Beskrivning av arbetsprocess och metod

### 2.1 Uppdraget

Svenska kraftnät ska, som särskilt ansvarig myndighet för krisberedskapen, analysera hot och risker inom myndighetens ansvarsområde som synnerligen allvarligt kan försämra förmågan till verksamhet inom området. I analysen ska särskilt beaktas

- > situationer som uppstår hastigt, oväntat och utan förvarning, eller en situation där det finns ett hot eller en risk att ett sådant läge kan uppstå,
- > situationer som kräver brådskande beslut och samverkan med andra aktörer,
- > att de mest nödvändiga funktionerna kan upprätthållas i samhällsviktig verksamhet, samt
- > förmågan att hantera mycket allvarliga situationer inom myndighetens ansvarsområde.

Analysen ska värderas och resultatet sammanställas i en risk- och sårbarhetsanalys.<sup>10</sup> Svenska kraftnät, förutom att analysera hot, risker och sårbarheter inom sin egen verksamhet, upprättar en nationell risk- och sårbarhetsanalys för elsektorn (produktion av, distribution av och handel med el) enligt elberedskapslagen.<sup>11</sup> Dessa båda aspekter sammanställs i en samlad risk- och sårbarhetsanalys.

### 2.2 Förutsättningar

Ändringar i elberedskapslagen (1997:288) som trädde i kraft den 1 juli 2012 innebär bland annat att elproducenter, nätföretag och elhandelsföretag har en skyldighet att genomföra risk- och sårbarhetsanalys avseende säkerheten i den egna verksamheten. Företagen har också en skyldighet att på begäran lämna in de uppgifter till Svenska kraftnät som krävs för upprättandet av den nationella risk- och sårbarhetsanalysen inom elsektorn.<sup>12</sup>

Företag inom elsektorn har eget ansvar för att vidta åtgärder för att undvika störningar som företaget rimligen kan förutse och som ligger inom ramen för vad det rimligen kan förebygga. Svenska kraftnät är elberedskapsmyndighet och ansvarar för fördelning av elberedskapsanslag för åtgärder som genomförs enligt elberedskapslagen.

<sup>10</sup> Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap, § 8

<sup>11</sup> Elberedskapslag (1997:288) 4 §

<sup>12</sup> Elberedskapslagen (1997:288) 4 §, Affärsverket svenska kraftnäts föreskrifter och allmänna råd om elberedskap SvKFS 2013:2, § 5-9

## 2.3 Mål och syfte

Målet med den samlade risk- och sårbarhetsanalysen är att Svenska kraftnät ska ha en god kännedom om hot, risker och sårbarheter som kan orsaka störningar av en sådan karaktär att de kan medföra svåra påfrestningar på samhället.<sup>13</sup>

Arbetet med risk- och sårbarhetsanalys syftar till att öka medvetenheten och kunskapen om vilka hot, risker och sårbarheter som föreligger. Analysen ska ligga till grund för åtgärder inom myndigheten och elsektorn med syfte att förebygga, motstå och hantera störningar som kan medföra svåra påfrestningar på samhället, både i fredstid och vid höjd beredskap och krig.<sup>14</sup>

## 2.4 Mottagare

Föreliggande rapport är en sammanställning av Svenska kraftnäts risk- och sårbarhetsanalys för elsektorn. Rapporten redovisas till Regeringskansliet och MSB. Även bedömning av myndighetens generella krisberedskap redovisas i samband med att rapporten redovisas.

Rapporten delges de myndigheter som ingår i Samverkansområde Teknisk infrastruktur, och görs tillgänglig för företag inom elsektorn. Rapporten publiceras på myndighetens hemsida.

## 2.5 Sekretess

Svenska kraftnät gör bedömningen att innehållet i denna rapport inte föranleder sekretess.

Uppgifter i myndigheters risk- och sårbarhetsanalyser kan under vissa omständigheter beläggas med sekretess enligt Offentlighets- och sekretesslagen.<sup>15</sup> Utgångspunkten i rapporten är dock att sammanställningen av arbetet med risk- och sårbarhetsanalys ska vara offentlig. Uppgifter som är av den karaktären att de bör omfattas av sekretess presenteras inte i rapporten.

## 2.6 Metod och genomförande

### 2.6.1 Arbetet under 2016

#### **Utveckling av processen för risk- och sårbarhetsanalys**

Under 2016 har processen för risk- och sårbarhetsanalys utvecklats så att den kan bedrivas i samverkan med säkerhetsanalysen samt utgöra ett mer systematiskt stöd till

---

<sup>13</sup> Händelser som kan medföra svåra påfrestningar på samhället är ofta extrema situationer som är svåra att förutse, som kräver samordning mellan flera aktörer i samhället för att klara konsekvenserna (till exempel elföretag, Svenska kraftnät, kommun och länsstyrelse, frivilligorganisationer) och som uppstår när en eller flera händelser utvecklar sig eller trappas upp. Jfr rapport Skyldigheter och befogenheter vid svåra påfrestningar på samhället i fred, Ds. 1998:32. Hur allvarligt samhället drabbas av störningar inom elförsörjningen beror på omfattning av händelsen eller en kombination av händelser.

<sup>14</sup> Jfr förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap, Förberedelser för och verksamhet under krissituationer § 8 och bevakningsansvariga myndigheters åtgärder inför och vid höjd beredskap, § 16 punkt 2.

<sup>15</sup> Offentlighets- och sekretesslag (2009:400) 15 kap. 2 §, 18 kap. 13 §

inriktning av elberedskapsmyndighetens verksamhet samt Svenska kraftnäts interna verksamhet. I detta arbete beaktas MSB:s nya föreskrifter för statliga myndigheters risk- och sårbarhetsanalyser<sup>16</sup> som trädde i kraft i augusti 2016.

### **Fortsatt arbete efter 2015 års särskilda regeringsuppdrag om informationssäkerhet**

Svenska kraftnät fick i 2015 års regleringsbrev ett särskilt uppdrag av regeringen att beakta och analysera informationssäkerheten i de delar av verksamheten och i de tekniska system som är nödvändiga för att affärsverket ska kunna utföra sitt arbete.<sup>17</sup>

Under 2016 har arbetet inom området fortsatt dels genom de åtgärder som vidtagits (se kapitel 8.2), dels genom fortsatt analys inom området (se kapitel 5.1.3).

### **Begäran om uppgifter till arbetet med nationell risk- och sårbarhetsanalys för elsektorn**

Som framkom i 2015 års risk- och sårbarhetsanalys är riskbilden kopplad mot elförsörjningen bred. I årets arbete har tre fördjupningsområden valts ut, delvis med utgångspunkt i föregående års analys.

Underlag till 2016 års analys har inhämtats både från berörda verksamhetsdelar hos myndigheten och från berörda elnäts- och produktionsföretag.<sup>18</sup>

### **Fördjupning: Störningar i försörjning av drivmedel**

Drivmedel och bränsle identifierades som kritisk materiel i Svenska kraftnäts risk- och sårbarhetsanalys för år 2015.<sup>19</sup> I 2015 års RSA identifierades också behovet av att se över bränsleförsörjningen under störda förhållanden och uthållighet vid krissituationer. Samhällsviktiga aktörers behov av att kunna samverka och leda under störda förhållanden i samhället, t.ex. vid osäker tillgång till drivmedel nämns i Försvarmaktens och MSB:s gemensamma grunder för en sammanhängande planering för totalförsvaret.<sup>20</sup>

Syftet med årets analys är att analysera faktorer som kan påverka förmågan att förebygga, motstå och hantera de negativa konsekvenserna av störningar i försörjning av drivmedel som i sin tur kan påverka förmågan till reparation, transporter, övervakning samt styrning av lokalt viktiga anläggningar inom elförsörjningen. Övergripande sammanfattning redovisas i kapitel 5.2 samt 7.1.

I årets arbete har vi tittat på hur beroendet till drivmedel ser ut i situationer inom elförsörjningen vid normala driftförhållanden samt vid omfattande störningar. I

<sup>16</sup> Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser MSBFS 2016:7

<sup>17</sup> Regleringsbrev för budgetåret 2015 avseende Affärsverket svenska kraftnät inom utgiftsområde 21 Energi

<sup>18</sup> Uppgiftsinhämtning från elföretag har genomförts med stöd i Svenska kraftnäts föreskrifter och allmänna råd om elberedskap (SvKFS 2013:2, § 9).

<sup>19</sup> Svenska kraftnät: Risk- och sårbarhetsanalys för år 2015, dnr. 2015/1763

<sup>20</sup> Försvarmakten och Myndighetens för samhällsskydd och beredskaps redovisning av regeringsuppdrag om gemensamma grunder för en sammanhängande planering för totalförsvaret, FM2016-13584:3, MSB 2016-25

arbetet omfattar begreppet drivmedel diesel till underhållsfordon, entreprenadmaskiner och bränsle i form av diesel till fast installerade eller mobila reservkraft verk som försörjer viktiga anläggningar inom elförsörjningen. Särskilda fokusområden är dieselförbrukning, uthållighet för reservkraft samt planer och avtal för att tillgodose behovet av drivmedel.

I framtida arbetet är det viktigt att tillsammans med berörda aktörer beakta utmaningar kopplade till drivmedelsförsörjning utifrån hela försörjningskedjan och hur dessa kan påverka elförsörjningen. Exempel på identifierade åtgärdsbehov redogörs i kapitel 8.1.

### **Fördjupning – Exponering av skyddsvärda informationsresurser mot osäkra nätverk**

Under 2015 analyserades informationssäkerheten inom myndigheten och dess ansvarsområde utifrån ett antal risker och hot av olika karaktär avseende tillgänglighet, riktighet, konfidentialitet och spårbarhet.<sup>21</sup> I analysen lyftes bland annat fram exponering av skyddsvärda resurser mot mindre säkra system/nät som en eventuell risk. Även minskad förmåga till egen kontroll över säkerheten i styr- och kontrollsystem i samband med utkontraktering och/eller användning av molntjänster identifierades i analysen. Årets analys fortsätter i dessa två spår och är avgränsad till att omfatta frågor kring säkerheten i IT-infrastruktur (inkl. IT-system, -tjänster och kommunikationsnät).

Syftet med årets analys är att analysera faktorer som kan påverka förmågan att förebygga, motstå och hantera de negativa konsekvenserna av omfattande störningar i/angrepp mot kritisk IT-infrastruktur. Övergripande sammanfattning redovisas i kapitel 5.3 samt 7.2. Exempel på identifierade åtgärdsbehov redogörs i kapitel 8.2.

### **Fördjupning – Höga flöden i reglerade vattendrag**

Svenska kraftnät genomförde år 2015 kartläggningar av objekt som kan översvämmas vid höga flöden och dammhaveri i de stora svenska kraftverksälvarna. Detta underlag har delgetts berörda dammägare, länsstyrelser m.fl. aktörer inom krisberedskapen. Med stöd av detta underlag vill vi nu även undersöka konsekvenserna för elförsörjningen vid olika översvämningsscenarier.

Majoriteten av vattendragen i Sverige är reglerade, vilket innebär att flödet i älvar till stor del kommit att styras av människan. Vattenstånd och vattenföring i kraftverksmagasinen och vattendragen varierar under året, och påverkas av faktorer som nederbörd, temperatur och snösmältning, samt driften av vattenkraftanläggningarna. I allmänhet innebär regleringen att höga flöden i älven (t.ex. vårfloden i Norrlandsälvarna) dämpas eftersom vatten kan magasineras. Men i vissa situationer, när magasinen är fyllda, behöver tillrinningen släppas förbi dammarna och flödena kan då till och med

---

<sup>21</sup> Svenska kraftnät: Risk- och sårbarhetsanalys för år 2015

bli högre än under naturliga förhållanden. Om man inte kan släppa fram vattnet så hotar dammhaverier.

Även om höga flöden i reglerade vattendrag inträffar sällan så kan konsekvenserna bli svåra när det väl händer. Omfattningen av skador och störningar beror i stor utsträckning på de geografiska förhållandena och samhällsplaneringen i det område som ligger i riskzonen för en översvämning. Vid mycket höga vattenflöden då den vanligtvis torr-lagda marken kring vattendragen översvämmas riskerar byggnationer och infrastruktur i området att påverkas, med skador, förstörelse och störningar som följd.

Syftet med årets analys är att analysera faktorer som kan påverka förmågan att förebygga, motstå och hantera de negativa konsekvenserna på elförsörjningen vid höga flöden och dammhaverier i reglerade vattendrag. Övergripande sammanfattning redovisas i kapitel 5.4 samt 7.3.

I årets arbete har vi avgränsat analysen till att omfatta ett begränsat antal kraftverksälvar i södra, mellersta respektive norra delen av Sverige, samt tre flödesscenarier: 100-årsflöde,<sup>22</sup> klass I-flöde<sup>23</sup> och dammhaveri<sup>24</sup>. Analysen omfattar påverkan på elnätet, med fokus på stationer, på regionnät- och stamnätsnivå.

Årets analys är översiktlig och har utgått från översvämningsskator som visar vattenutbredning vid de tre flödesscenarierna. Hänsyn har till exempel inte tagits till specifika vattennivåer, strömningsförhållanden eller tidsförlopp. I framtida arbete bör konsekvenser utredas och åtgärdsbehov konkretiseras ytterligare, med stöd av mer detaljerat underlag som nu finns tillgängligt. I årets analys ligger fokus på konsekvenser för elnätet, i framtida arbete bör påverkan på kraftstationer och konsekvenserna av detta inkluderas. Exempel på identifierade åtgärdsbehov görs i kapitel 8.3.

## 2.6.2 Bedömningsgrunder

### Skalan för bedömning av konsekvenser

I myndighetens interna riskanalys har en fyrgradig kvalitativ skala använts som utgångspunkt.

En liknande skala finns i vår vägledning för risk- och sårbarhetsanalyser för sektorn.<sup>25</sup>

Det förekommer osäkerhet i bedömningen av hur allvarliga konsekvenserna kan bli för olika riskkällor. Några gemensamma faktorer som kan påverka bedömningen är

<sup>22</sup> Flöde med återkomsttid på 100-år.

<sup>23</sup> Högsta möjliga flödet för vattendrag

<sup>24</sup> Scenariot beskriver ett värsta scenario och visar vilket område längs vattendraget som skulle kunna översvämmas som en följd av att någon av dammarna brister och uppdämt vatten strömmar ut okontrollerat.

<sup>25</sup> Svenska kraftnät och Svensk Energi: Vägledning för risk- och sårbarhetsanalyser för elsektorn. Finns tillgänglig online på <<http://www.svk.se/siteassets/gemensamt/dokument/vagledningar/vagledning-for-risk-och-sarbarhetsanalyser.pdf>>

- > händelsens omfattning, geografiska läge och varaktighet,
- > tiden innan reparations- och återställningsinsatser kan sättas in,
- > vilka och hur stora delar av verksamheten (t.ex. viktiga anläggningar som kan vara utspridda i ett stort geografiskt område) är drabbade,
- > huruvida överliggande nät/kraftsystemet är drabbat, samt
- > eventuella andra sammanfallande händelser/en upptrappning av händelsen.

För varje fördjupningsområde görs det sammanfattande konsekvensbedömningar. Sammanfattningarna är av övergripande karaktär och inkluderar svar från både myndigheten och av analysen berörda elföretag. Konsekvenser förekommer i varierande grad inom verksamheter inom elförsörjningen.

I arbetet ska ”situationer som uppstår hastigt, oväntat och utan förvarning”<sup>26</sup> beaktas. För de riskkällor där det sällan (eller inte alls) finns statistik över frekvensen görs det inga kvantitativa/kvalitativa sannolikhetsbedömningar i denna rapport.

### 2.6.3 Kommande arbete

#### **Framtida fokusområde – outsourcing av för elförsörjningen viktiga verksamheter**

Under året har även fokusområdet outsourcing framkommit som ett område där det finns behov av ytterligare utredning och analys. När aktörer inom elförsörjningen outsourcar delar av sin verksamhet medför det ändrade förutsättningar inom sektorn som är viktiga att studera närmare.

Outsourcing är det förhållande som uppstår när en organisation överlåter till en annan aktör att utföra en verksamhet som organisationen skulle kunna ha i egen regi. Outsourcing är på så sätt ett brett begrepp, och kan handla om allt från utläggning av enstaka tjänster eller resurser till hela affärsprocesser eller driftsmiljöer. För elförsörjningen kan detta innebära exempelvis utläggning av reparations- och underhållsarbete, IT-relaterade tjänster, kundsupport etc.

Anledningarna till att välja en outsourcinglösning kan vara flera, till exempel

- > ökat fokus på företagets kärnverksamhet,
- > möjlighet att tillgå expertkompetens,
- > effektiviserad resursanvändning,
- > möjlighet till ökad redundans genom större utbud av säkerhets- och kontinuitetslösningar, samt
- > ökad möjlighet till snabb utveckling av tjänster<sup>27</sup>

<sup>26</sup> Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap, § 8, punkt 1

Men outsourcing kan även medföra nya risker för verksamheten. Inom elförsörjningen innebär outsourcinglösningar till viss del bildandet av nya beroenden, där kritiska tjänster som tidigare hållits inom elföretagen läggs ut på externa leverantörer. Det blir i dessa fall viktigt att företagens kontinuitetshanteringsplaner och riskanalyser även omfattar externa leverantörer, och att det ställs krav på, och följs upp, att outsourcinglösningen inte har en negativ påverkan på verksamhetens förmåga att förebygga, motstå och hantera svåra påfrestningar.

Det kan även innebära att sådan verksamhet som tillhör elförsörjningen (underhåll/reparation/vissa IT-tjänster) utförs av aktörer som inte omfattas av den lagstiftning som gäller för elföretag (elberedskapslagen och säkerhetsskyddslagen<sup>28</sup>). Detta kan bland annat innebära

- > att möjligheten att bedriva tillsyn av för elförsörjningen viktig verksamhet minskar (då leverantörer till företag inom elsektorn inte omfattas av lagstiftning),
- > att beredskapsåtgärder inte kan utföras i verksamhet som bedrivs av aktörer som inte omfattas av elberedskapslagen, samt
- > att möjligheten att ställa adekvata säkerhetskrav minskar.

De säkerhetskrav som Svenska kraftnät kan ställa på verksamhet som bedrivs i Sverige är inte alltid möjliga att ställa för verksamhet som bedrivs utomlands. Det gäller t.ex. säkerhetsprövning av personal. Detta blir särskilt problematiskt om verksamheten finns utanför EU.

### 3 Identifierad samhällsviktig verksamhet som är av nationell betydelse

Med samhällsviktig verksamhet avses en verksamhet som uppfyller minst ett av följande villkor.

- > Ett bortfall av eller en svår störning i verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter kan leda till att en allvarlig kris inträffar i samhället.
- > 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.<sup>29</sup>

Elförsörjningen består av aktörer som producerar, distribuerar och handlar med el och är en av de samhällsviktiga verksamheter som är helt avgörande för samhällets funkt-

---

<sup>27</sup> Jfr FSPOS: Appendix G – kontinuitetshantering för outsourcad verksamhet, version 2.0

<sup>28</sup> Elberedskapslagen (1997:288), Säkerhetsskyddslagen (1996:627)

<sup>29</sup> Jfr Myndigheten för samhällsskydd och beredskaps föreskrifter<sup>1</sup> om statliga myndigheters risk- och sårbarhetsanalyser MSBFS 2016:7

ionalitet. Ett elavbrott påverkar bland annat elektroniska kommunikationer, transporter, kommunalteknisk försörjning, vård- och omsorg, energiförsörjning och finansiella tjänster. Flera samhällsviktiga verksamheter avstannar omedelbart vid ett elavbrott om de saknar reservkraft.

*Verksamhet inom elförsörjningen vars bortfall kan leda till att en allvarlig kris inträffar.*

### **Operativ driftverksamhet för elnät och storskalig elproduktion (vattenkraft och kärnkraft)**

Möjlighet till styrning och övervakning av stamnät och distributionsnät av el och elproduktion är grundläggande för ett fungerande elsystem. Inom detta faller till exempel att reglera elproduktion samt att styra elnätet.

### **Balanshållning i kraftsystemet**

Det måste finnas balans i elsystemet, det vill säga mellan den el som produceras och förbrukas i elsystemet. Om denna balansinte kan regleras, är risken att det blir stora störningar i elnätet med allvarliga konsekvenser som följd. Svenska kraftnät tillsammans med övriga nordiska systemoperatörer ansvarar för att balansen hålls.

*Verksamhet inom elförsörjningen som behövs för att hantera en redan inträffad kris.*

För att kunna hantera redan en inträffad kris, behövs en förmåga att minimera konsekvenser samt återställa verksamhet, genom exempelvis:

### **Reparationsberedskap**

Om en viktig del av den tekniska infrastrukturen inom elförsörjningen skadas måste det finnas en verksamhet med effektiva rutiner som möjliggör avhjälpning av fel, inom både distribution och produktion av el.

### **Verksamhet för att starta elsystemet**

För att minimera konsekvenserna för samhället och för att underlätta en driftåteruppbyggnad efter ett totalt elbortfall är det viktigt att det finns en strategi, utrustning och rutiner för att återstarta elsystemet. I dessa situationer kan det med vissa produktionsanläggningar finnas möjlighet att starta upp små delar av elsystemet. Ett sådant driftläge innebär att ett regional-, lokalnät eller en enskild anläggning försörjs med elkraft från en eller flera produktionsanläggningar inom ett avgränsat ödriftområde utan elektrisk förbindelse med omkringliggande nät.



## 4 Identifierade kritiska beroenden för identifierad samhällsviktig verksamhet

För den identifierade samhällsviktiga verksamheten på nationell nivå i kapitel 3 har följande kritiska beroenden identifierats<sup>30</sup>:

- > Elektroniska kommunikationer
- > Teknisk infrastruktur
- > Kritisk materiel
- > Framkomlighet
- > Personella resurser
- > Samverkan
- > Krisberedskapsorganisation
- > Information

---

<sup>30</sup> Se Svenska kraftnät: Risk- och sårbarhetsanalys för år 2015 för mer information



## 5 Identifierade och analyserade hot och risker

I detta kapitel redovisas de tre riskkällor som analyserats särskilt under 2016.

Kapitlet inleds med en hotbildsanalys med fokus på antagonistiska hot. Därefter följer övergripande konsekvensbeskrivningar inom årets tre fördjupningsområden.

### 5.1 Hotbildsanalys

Inom ramen för arbetet med myndighetens säkerhetsanalys har Svenska kraftnät tagit fram hotbildsanalyser, baserade till stor del på öppna källor i form av rapporter från Försvarsmakten och Säkerhetspolisen samt det senaste årets nyhetsflöde. Syftet med hotbildsanalyser är att tillhandahålla ett stöd i arbetet med att identifiera och värdera de risker och hot som elförsörjningen exponeras för. Nedan redovisas en aktuell bedömning för hot inom delområdena terrorism, kriminalitet, sabotage och spionage/underrättelseverksamhet.

Inom arbetet med hotbildsanalysen har även delområdet militärt angrepp beaktats. Den säkerhetspolitiska situationen i Europa har försämrats. Rysslands annektering av Krim och intervention i östra Ukraina 2014 visar, liksom invasionen av Georgien 2008, på Rysslands ökande benägenhet att med militära medel ta ensidiga strategiska initiativ på grannländers territoriella bekostnad. Den militära övnings- och underrättelseverksamheten i Östersjöområdet har ökat, och kränkningar av Östersjöländers territoriella integritet har skett.<sup>31</sup>

Återupptagen totalförvarsplanering utgår från ett väpnat angrepp mot Sverige,<sup>32</sup> inklusive angrepp mot civil infrastruktur av särskild betydelse (däribland elförsörjningen). Cyberattacker och informationskrigföring kan också vara en del i krigföringen. Detta innebär att inom arbete med hotbildsanalysen är det viktigt att även beakta delområdet militärt angrepp och följa den utveckling inom området som kan ha bäring på elförsörjningen.

#### **Terrorism**

Terrorhotet mot Sverige består främst av våldsbejakande islamistiska grupper. Hotet motiveras främst av upplevda kränkningar av islam men även av svensk och annan nordisk trupp utomlands. Hotet har minskat med tillbakadragandet från Afghanistan men kan med andra nya åtaganden öka igen.<sup>33</sup>

<sup>31</sup>Jfr Försvaret av Sverige – Starkare försvar för en osäker tid, Ds 2014:20 och Försvarspolitisk inriktning – Sveriges försvar 2016-2020, Prop. 2014/15:109, Regeringsbeslut 10 december 2015

<sup>32</sup>Försvarsmaktens och Myndigheten för samhällsskydd och beredskaps redovisning av regeringsuppdrag om gemensamma grunder för en sammanhängande planering för totalförsvaret, FM2016-13584:3. MSB 2016-25

<sup>33</sup>MUST Årsöversikt 2015

De terrorhandlingar som utförts av ovan nämnda grupper i västvärlden under senare tid bedöms rikta sig i första hand mot allmänheten, militära anläggningar, polis och rättsväsendet. Några allvarliga terrorhandlingar riktade mot kritiska infrastrukturer i västvärlden utförda av dessa grupper har inte förekommit. Med detta som grund bedöms risken för större organiserade terrorattacker mot elförsörjningen för närvarande som liten. Däremot kan risken för enskilda attacker från ensamagerande komma att öka. Dessa kan agera på uppdrag av en större organisation eller på egen hand. Sannolikheten bedöms dock som låg för att elförsörjningen ska drabbas av denna sorts antagonistiska hot med allvarliga konsekvenser.

***Bedömningen är att risken för denna sorts hot mot elförsörjningen är förhöjd men låg.***

#### **Kriminalitet/organiserad brottslighet**

Den grova organiserade brottsligheten bedöms sakna både avsikt och förmåga till att utgöra ett hot mot rikets säkerhet och den kritiska infrastrukturen i samhället. Hos denna typ av organisationer kan det finnas en latent avsikt och även en hög generell förmåga till att skada samhällsfunktioner eller demokratiska processer. Dessa processer är dock främst kopplade till rättsväsendet, varför hotet mot den svenska elförsörjningen bedöms som låg. Kopparstölder utgör dock ett problem som kan påverka person- och driftsäkerhet.

***Bedömningen är att risken för denna sorts hot mot elförsörjningen är oförändrat låg.***

#### **Sabotage**

Sabotage är ett antagonistiskt hot där aktörerna främst drivs av olika former av aktivism. Denna kan grupperas i olika inriktningar. Huvudsakligen i vitmakt rörelsen och autonoma grupperingar som till exempel djurrättsaktivister och/eller miljöaktivister. Grupperingarna skiljer sig ideologiskt och politiskt från varandra och sprider sig på hela höger-vänsterskalan.

***Bedömningen är att risken för denna sorts hot mot elförsörjningen är oförändrat låg men kan komma att öka de närmaste åren.***

#### **Spionage/underrättelseverksamhet**

Dagens teknikutveckling och teknikspridning talar för att framtida konflikter i högre grad kommer att utnyttja fjärrstridsmedel. Det innebär att risk och kostnad för väpnade attacker minskar, vilket i sin tur innebär att både statliga och icke-statliga aktörer kommer att använda sig av cyberkrigföring.

Då vårt moderna samhälle i hög utsträckning förlitar sig på IT-system, är cyberattacker en naturlig del av framtida konflikter. Cyberattackerna kommer att utföras enskilt eller i kombination med kinetiska attacker. Det finns redan exempel på hur SCADA-system har manipulerats för att orsaka skada.

Statsunderstödd underrättelseverksamhet har i detta scenario intresse av att tillskansa sig uppgifter om svenska elsystemet. Det bedöms även finnas ett intresse för att förbereda cyberattacker mot IT-system i allmänhet och SCADA-system i synnerhet.

Elsystemet är helt grundläggande för att upprätthålla samhällets funktionalitet. Försök till kartläggning och förberedelser för att kunna störa elförsörjningen vid en konflikt ter sig därför sannolika.

***Bedömningen är att resursstarka aktörer med stor förmågebredd utgör det dimensionerade hotet när ansvariga för viktiga elinfrastrukturer utformar och kravställer informations- och IT-säkerhetsfunktioner.***

## 5.2 Störningar i försörjning av drivmedel

På den nationella nivån fastställer Energimyndigheten årligen vilka aktörer (importörer, säljare och stora förbrukare av olja) i Sverige som är lagringskyldiga och vilka lagringsbränslen och mängder som respektive aktör måste hålla för att trygga tillgången av oljeprodukter såsom diesel under svåra försörjningskriser för olja i samhället.<sup>34</sup> Sverige ska under varje lagringsår ha ett beredskapslager som motsvarar minst 90 dagars genomsnittlig daglig nettoimport under referensåret.<sup>35</sup> Diesel utgör ungefär hälften av lagret.<sup>36</sup>

Inom elförsörjningen behövs drivmedel bland annat för att säkerställa reparationsarbeten och transporter av materiel, personal och utrustning. Drivmedel behövs också för fasta eller mobila reservverk till viktiga anläggningar inom elförsörjningen, t.ex. reservkraft till mottagningsstationer för att bibehålla skyddsfunktioner och styrningsmöjligheter. Tillgången till drivmedel är i sin tur beroende av fungerande logistik.

Utöver den ordinarie verksamheten kan det vid omfattande störningar i elförsörjningen tillkomma extra reparationsresurser i form av förstärkningsresurser som också behöver försörjas med drivmedel. Långvariga omfattande elavbrott kan i sig själva även störa den ordinarie logistiken för drivmedels- och bränsleförsörjning.<sup>37</sup>

Tillgång till reservkraft och försörjning av drivmedel under normala förhållanden (då det finns tillgång till drivmedel) ligger inom aktörernas eget ansvar. För särskilda förhållanden då det är störningar i försörjning av drivmedel (till exempel på grund av begränsad tillgång/höjd beredskap/krig etc.) kan det behövas särskild planering från aktörernas sida för att tillgose behoven inom elförsörjningen. Vid särskilda förhållan-

<sup>34</sup> Lag (2012:806) om beredskapslagring av olja där skyldigheter regleras för importörer, säljare och stora förbrukare av olja

<sup>35</sup> Referensåret är det kalenderår som varit närmast nästa lagringsår. Ex 2016 är referensåret för lagringsåret 2017/2018.

<sup>36</sup> Energimyndigheten: Ansvar och roller för en trygg energiförsörjning. ER2013:25. Sveriges lagringsskyldighet är knuten till EU-lagstiftning samt till åtaganden i enlighet med IEP-avtalet, som är en överenskommelse mellan 29 länder om ett gemensamt energiprogram. [www.energimyndigheten.se](http://www.energimyndigheten.se)

<sup>37</sup> Se även: MSB: Vägledning för hantering av Reservkraftprocessen, MSB784

den går det inte att räkna med att vanliga försörjningsled, som till exempel bensinstationer, fungerar.

Som referens för uthållighet har ”Vägledning för el-och teletekniskt utförande i stationsanläggningar i elnät<sup>38</sup>” använts där krav ställs på minst 96 timmars drift utan bränslepåfyllning för fast installerad reservkraft.

### **Övergripande sammanfattning**

Elförsörjningen har stor erfarenhet av störningar så omfattande att förstärkningsresurser har använts, att reservkraft använts för viktiga anläggningar och att stationer har bemannats och styrts lokalt. Några av aktörerna i analysen har vidtagit åtgärder eller har för avsikt att vidta åtgärder för att förbättra beredskapen inför eventuella störningar i försörjning av drivmedel.

Förbrukning av diesel under omfattande störningar i elförsörjningen där externa förstärkningsresurser används och reservkraft körs till viktiga anläggningar är högre än under vanliga driftförhållanden. Utifrån analysen bedöms de berörda aktörerna och verksamheterna ha en viss förmåga att hantera störningar men den egna förmågan räcker inte alltid i 96 timmar. Förutom att kunna uppfylla detta krav även under omfattande störningar i elförsörjningen bör aktörer inom elförsörjningen ha en plan<sup>39</sup> för hur de ska tillgodose behovet av drivmedel i en störningssituation med en längre varaktighet.

Analysen visar på svårigheten att i vissa fall teckna avtal med entreprenörer och underleverantörer som garanterar försörjning av drivmedel under bristsituationer/force majeure. Dessutom har inte alla verksamheter särskilda avtal med leverantörer av diesel, utan förlitar sig på att det finns diesel tillgänglig på marknaden. Därför är det viktigt att i verksamhetens kontinuitetsplanering beakta hantering av sådana situationer, och även omfatta eventuella beroendet av drivmedelsleverantör.

Tillgången till personella (t.ex. för reservdrift och reparationer samt underhåll) och materiella resurser (t.ex. reservdelar till reservkraftverk) är varierande, och i många fall är det leverantörer som försörjer med resurser vid längre avbrott och komplicerade fel.

Inom elförsörjningen bedrivs för närvarande samverkan kring försörjning av diesel vid störningar i drivmedelförsörjningen i låg grad. En bidragande faktor kan vara att det inte skett så omfattande störningar i drivmedelsförsörjning på nationell nivå som hade föranlett aktiv samverkan i frågan.

---

38 Svenska kraftnät och Svensk energi ”Vägledning för el-och teletekniskt utförande i stationsanläggningar i elnät” Dnr: 956/2008/BE40 <[39 Jfr SvKFS 2013:2 § 3](http://www.svk.se/siteassets/aktorsportalen/vagledningar/120327-vagledning-el-och-teletekniskt-utforande-stationsanlaggningar.pdf?_t_id=1B2M2Y8AsgTpgAmY7PhCf==&_t_q=teleteknisk&_t_tags=language:sv,siteid:40c776fe-7e5c-4838-841c-63d91e5a03c9&_t_ip=192.121.1.150&_t_hit.id=SVK_WebUI_Models_Media_OfficeDocument/_aea78a5a-7e82-4881-8daa-7f32051c350f&_t_hit.pos=1></a></p></div><div data-bbox=)

### **Konsekvenser för aktörers egen verksamhet**

Om störningar i elförsörjningen inträffar samtidigt som störningar i försörjning av drivmedel kan det bli allvarliga eller till och med oacceptabla konsekvenser för verksamheten om för kärnverksamheten viktiga anläggningar, funktioner och system påverkas. Planerade underhållsåtgärder och felavhjälpning kan påverkas och prioritering av vilka verksamheter som bör ha tillgång till reservkraft kan komma att bli aktuellt.

Nedan presenteras exempel på faktorer som kan påverka omfattningen av konsekvenser (utöver för verksamheten särskilda tekniska lösningar).

- > Tillgängliga drivmedelsreserver till reservkraftverk och fordon.
- > Möjlighet att fylla på bränsle (pumpar) vid störningar inom elförsörjningen.
- > Tillgång till reservdelar och reparationsresurser till reservkraftverk (även under kvällar och helger).

### **Konsekvenser för samhällets elförsörjning**

Konsekvenser för samhällets elförsörjning beror delvis på hur snabbt enskilda aktörer lyckas återställa sin verksamhet, om deras verksamhet har betydelse för elförsörjningen på den nationella nivån. Stopp i enskilda produktionsanläggningar medför inga konsekvenser för samhällets elförsörjning om tillgång till el är säkrad från andra håll och om den kan levereras (vilket förutsätter ett fungerande elnät).

Vid omfattande störningar i elförsörjningen som inte kan avhjälpas på grund av störningar i drivmedelsförsörjning kan även andra samhällsviktiga verksamheter, såsom värmeförsörjning, transporter, kommunikationer etc. påverkas i de drabbade områdena. Detta kan även innebära sekundära konsekvenser för infrastruktur och miljö i samhället, t.ex. genom skador på väg- och elnätet samt avloppssystemet.

## **5.3 Exponering av skyddsvärda informationsresurser mot osäkra nätverk<sup>40</sup>**

Det moderna elsystemet och det IT-stöd som används för att uppnå automation av produktion, transmission, distribution, handel och all därtill löpande förvaltning (arbetsordersystem, kartsystem, inventarie- eller planeringssystem, etc.) är förutsättningen för att skapa ett effektivt arbetsflöde hos de olika aktörerna inom elsystemet. På så vis skapas en intrikat sammankoppling mellan komponenter, system och processer. I praktiken kan detta innebära gemensamma system, delade kommunikationsflöden, likadan programvara/hårdvara då man vill uppnå effektiviseringsvinster och konsolidering.

---

<sup>40</sup> Med osäkra nätverk menas nätverk utanför den egna organisationens kontroll vars beroenden/relation till andra nätverk och system inte är kända. Detta innebär att organisationen inte har en direkt insyn, påverkan eller annan kontroll över tjänster eller resurser som tillhandahålls genom dessa nätverk. Det kan vara tjänster eller IT-resurser som tillhandahålls av en tredjepartsleverantör, till exempel tjänster som rör kommunikation, IT-drift, övervakning, installation, med mera. Exponering innebär i detta sammanhang att öka risken för att obehöriga får åtkomst till informationsresurser (system, filer, kommunikationsutrustning med mera), behöriga användare överträder sin normala behörighet och lyckas få åtkomst till sådant som de normalt sett inte haft behörighet till.

Verksamhetens egna känsliga data och system kan kopplas ihop med andra aktörer för utbyte för att tillgodose både driftoptimerande så väl som marknadsmässiga behov. Exempelvis så kan flera aktörer ha samma leverantör av driftövervakningssystem, alternativt kan en aktör sköta ett system som används av flera. Ett annat exempel är att en aktör skapar system utifrån behov av kommunikationsutbyte med en eller flera andra aktörer.

Denna typ av lösningar kan dock medföra vissa risker. Felaktigheter i såväl upphandling, projektering, utveckling eller löpande drift kan leda till exponering av skyddsvärda eller kritiska informationsresurser. Ett angrepp mot, eller en omfattande störning i, kritiska IT-system som har långtgående beroenden och utbyten med andra nätverk kan innebära att stora delar av IT-miljön drabbas om det inte vidtagits riskreducerande åtgärder.

### **Övergripande sammanfattning**

De av analysen berörda aktörerna och verksamheterna bedöms till stor del ha ett systematiskt arbetssätt gällande informations- och IT-säkerhet inom den egna verksamheten.

Majoriteten av aktörer har i enlighet med SvKFS 2013:1<sup>41</sup> samrått med Svenska kraftnät inför val av tekniska lösningar och IT-tjänster vid skapande, införande eller förändringar av kritiska IT-system.<sup>42</sup>

Majoriteten anger också att de gör risk- och sårbarhetsanalyser avseende de kritiska IT-systemens egenskaper, användning och underhåll/förvaltning, dock omfattar dessa i de flesta fallen inte tjänsteleverantörers interna risker som kan vara relevanta för säkerheten i och kring leverans av tjänsten. I de fallen där outsourcing av IT-drift och IT-relaterade tjänster kopplade till de kritiska IT-systemen är aktuellt, beaktas detta i varierande grad i risk- och sårbarhetsanalyser och säkerhetsanalyser. Enligt Svenska kraftnäs föreskrifter och allmänna råd om säkerhetsskydd (SvKFS 2013:1) ska säkerhetsrisker och sårbarheter som kan finnas i och kring vissa IT-system<sup>43</sup> analyseras, även i sådana fall där drift eller förvaltning av ett sådant IT-system upplåts till en annan part i utlandet.

Mer än hälften av de berörda aktörerna klassificerar information i sina kritiska system, helt eller delvis. Risker med bristfällig klassificering är att i vissa fall kan klassificerad information blandas med icke-klassificerad information i de viktiga systemen, vilket kan försvåra en korrekt hantering av information.

---

<sup>41</sup> § 15-16

<sup>42</sup> Aktuellt för system som införts efter juli 2013 då föreskrifterna trädde i kraft.

<sup>43</sup> Se § 15. Med sådana IT-system avses system som är avsedda för behandling av uppgifter som rör rikets säkerhet eller som särskilt behöver skyddas mot terrorism.



Kunskap om och en lägesbild kring tekniska sårbarheter, nya attacker, attacktrender mm. kan uppnås genom aktiv omvärldsbevakning inom området. Majoriteten av aktörer tar del av omvärldsbevakning, i många fall genom leverantörer och andra aktörer såsom MSB, och genom att delta i olika fora för informationsutbyte. Det är dock oklart om omvärldsanalys alltid bedrivs som ett dedikerat uppdrag eller om den drivs vid sidan av ordinarie arbetsuppgifter.

### **Konsekvenser för aktörers egen verksamhet**

Omfattande störningar i/angrepp mot kritisk IT-infrastruktur kan leda till upptill oacceptabla konsekvenser om för kärnverksamheten viktiga system drabbas och om sårbarhetsreducerande åtgärder inte vidtagits i förebyggande syfte.

Nedan presenteras exempel på faktorer som kan påverka graden av konsekvenser av en omfattande störning i/ett angrepp mot företagets kritiska IT-infrastruktur. (Utöver dessa faktorer påverkas konsekvenserna av hur viktiga IT-system som utsätts för störningar/angrepp är).

- > Hur väl segmenterade IT-miljöerna (kontors-IT och kritiska system) är för att begränsa otillbörlig åtkomst.
- > Tillgång till ev. reservdriftställe som är separerat från ordinarie driftställe vid händelse av otillgänglighet (t.ex. utslagen dc).
- > Hur säkert fjärraccessanslutningar är utformade (i de fall där fjärråtkomst bedöms nödvändig).
- > Att det finns backuper för de för verksamheten kritiska systemen där återläsningen är verifierad.
- > Hur väl och snabbt behov av personella resurser (för att t.ex. bemanna anläggningar/stationer för felavhjälpning och att kunna köra stationer lokalt) och reservdelar kan tillgodoses. Detta omfattar även beroendet av leverantörs- och entreprenörer som tillhandahåller tjänster och reservdelar. Även i återställning av system kan hjälp av konsulter och systemleverantörer behövas.
- > Aktuella driftläget och eventuella andra sammanfallande störningar som kräver personella resurser.
- > Fungerande talkommunikation för drift- och underhållspersonal på fältet att leda driften och för reparationsarbete samt kommunikation med Svenska kraftnät.

### **Konsekvenser för samhällets elförsörjning**

Samhällets elförsörjning kan på olika sätt drabbas av omfattande störningar i/angrepp mot kritisk IT-infrastruktur på grund av det direkta beroendet av IT som elförsörjning har.

Beroende av typ av störning och årstid kan det bli kännbara avbrott t.ex. i el- och värmeleveranser samt el- och värmeproduktion, vilket också kan påverka andra sam-

hällsviktiga verksamheter, särskilt om dessa inte har vidtagit robustgörande åtgärder såsom reservkraft.

Dock kan enskilda verksamheter i vissa fall vidta åtgärder som lokaldrift, ö-drift och genomföra andra omkopplingar i näten alternativt fortsätta styra anläggningar lokalt så att konsekvenserna på elförsörjningen och/eller samhället i stort reduceras något.

## 5.4 Höga flöden i reglerade vattendrag

Höga eller extrema flöden i reglerade vattendrag inträffar sällan, men konsekvenserna kan bli svåra när de väl inträffar. Vid mycket höga vattenflöden då den vanligtvis torr-lagda marken kring vattendragen översvämmas riskerar byggnationer och infrastruktur i översvämningsområdet att skadas eller förstöras helt.

För elförsörjningen kan höga flöden innebära att viktiga anläggningar ställs delvis under vatten, med skador och störningar som följd. Skador kan även uppkomma pga. det bråte som kan följa med flödet, detta kan även allvarligt försvåra återställnings- och reparationsarbete.

### Övergripande sammanfattning

Bedömningen av konsekvenser på elnät inkl. nätstationer vid höga flöden i reglerade vattendrag beror i hög grad på yttre faktorer såsom vattennivå och strömningsförhållanden, tid på året och hur övrig samhällsviktig verksamhet och infrastruktur påverkas.

Inom ramen för denna analys har framkommit att påverkan vid 100-årsflöden<sup>44</sup> generellt bedöms som liten för de aktörer som berördes av årets analys. Vissa mindre anläggningar kan komma att påverkas av översvämningen, men ingen uppger att denna typ av flöden i de berörda vattendragen skulle medföra stora negativa konsekvenser för verksamheten eller elförsörjningen i stort. Ett flertal aktörer gör bedömningen att anläggningarna i hög grad skulle klara av höga vattennivåer, men att vissa delar av systemet är mer känsliga, så som till exempel kontrollutrustning, stolpar och luftledningarna.

100-årsflödet är ett flöde som ofta beaktas i de berörda elföretagens risk- och sårbarhetsanalyser och vid projektering av nya anläggningar. Konsekvenserna vid denna nivå på flöden blir främst för mindre samhällen, och bedömningen är generellt att det finns en god beredskap inom organisationerna för att hantera detta.

Klass I-flöde<sup>45</sup> och dammhaveri<sup>46</sup> i större kraftverksdammar är de scenarier som bedöms ge allvarliga, upp till oacceptabla konsekvenser för verksamheterna och för sam-

<sup>44</sup> Flöde med återkomsttid på 100-år.

<sup>45</sup> Högsta möjliga flödet för vattendrag

<sup>46</sup> Scenariot beskriver ett värsta scenario och visar vilket område längs vattendraget som skulle kunna översvämmas som en följd av att någon av dammarna brister och uppdamt vatten strömmar ut okontrollerat.

hället. Erfarenheten av dessa typer av scenarier är av naturliga skäl mindre än för 100-års flöden, och analysen visar att dessa inte i lika hög grad omfattas av aktörernas planer och analyser.

Risk finns att ett stort antal större och mindre samhällen skulle drabbas hårt av elavbrott, och att reparationsarbetet skulle försvåras av brist på framkomlighet för personal och materiel, samt behovet av att låta vattnet sjunka undan och genomföra röjningsarbete innan arbetet kan genomföras. Vid denna typ av extrema fall är framkomlighet och möjligheten till kommunikation avgörande för hur snabbt elnätet kan återställas, och osäkerhet kring dessa faktorer bidrar till svårigheter i konsekvensbedömningarna. Vid omfattande störningar av detta slag kan även behovet av att prioritera resurser och att samverka med andra aktörer bli stort, då stora områden drabbas.

På grund av ovan nämnda osäkerheter är återställningstider svåra att ange, och kan variera mellan några dagar upp till flera veckor eller mer.

### **Konsekvenser för aktörers egen verksamhet**

Konsekvenserna av höga flöden kan, beroende på scenario och geografiskt läge, variera stort från obetydliga till oacceptabla. Nedan presenteras exempel på faktorer som kan påverka omfattningen av konsekvenser.

- > Förvarningstid och vattnets stighastighet – dvs. förutsättningar för att förutse vad som komma ska genom väderprognoser, vädervarningar, larmning vid dammhaveri etc. samt om vattnet stiger långsamt eller snabbt vid skadeobjektet. Ett förutsebart alternativt långsamt förlopp kan ge tid och möjlighet till att vidta skyddsåtgärder och t.ex. stänga av viss apparatur och göra eventuella omkopplingar.
- > Vattnets nivå – vilka delar av anläggningar som hamnar under vatten, och med vilket vattendjup.
- > Följdeffekter som ras och jordskred längs vattendraget, stora mängder träd och bråte mm. som följer med vattnet kan orsaka skador på anläggningar och försvåra återställningsarbetena.
- > Flödets/översvämningens påverkan på väg- och järnvägsnät samt broar som i sin tur påverkar framkomligheten i reparationsarbetet.
- > Flödets/översvämningens påverkan på kommunikationsnätet som är viktigt i hanterings- och återställningsarbetet.
- > Tillgänglighet till reparationsresurser och reservkraft, särskilt i situationer där ett större geografiskt område och flera samhällsviktiga verksamheter påverkas och det därmed finns behov av samverkan om resurser.

### **Konsekvenser för samhället**

Konsekvenser för samhällets elförsörjning blir vid lägre flöden lindriga, men kan vid klass I-flöden och dammahaverier i större kraftverksdammar bli oacceptabla. Sådana

scenarier kan i vissa älvar leda till att stationer och/eller stolpar och luftledningar skadas, eller måste sättas ur funktion, och att överföringskapaciteten mellan norra och södra Sverige därmed begränsas.

En omfattande översvämning av detta slag resulterar troligen även i störningar och skador på övrig infrastruktur och påverkar till exempel transporter och telekommunikation, som behövs i återställningsarbetet. I svåra fall kan infrastrukturen vara skadad längs en hel älvsträcka, och reparationsarbetet ta många veckor eller mer i anspråk.

Värt att notera är att denna analys fokuserar på påverkan på stationer i elnätet, vid till exempel dammhaveri skulle elproduktionen i en älv vara utslagen under mycket lång tid, vilket kan innebära påfrestningar på elförsörjningen.

## 6 Bedömning av myndighetens generella krisberedskap enligt indikatorer i bilaga 1

Bedömning av myndighetens generella krisberedskap redovisas i sin helhet i bilaga 1. Här redovisas enbart en sammanfattning utifrån ett urval indikatorer som MSB beslutar och som ligger till grund för bedömningen.

Den övergripande bedömningen är att myndighetens generella krisberedskap är god och där svagheter och brister har identifierats håller det på att vidtas åtgärder.

### 6.1 Ledning och krishantering

Det finns framtagna arbetssätt och rutiner för arbetet med risk- och sårbarhetsanalys.<sup>47</sup> Berörda verksamheter inom Svenska kraftnät involveras vid behov i arbetet. Risk- och sårbarhetsanalys används som underlag vid planering och beslut om åtgärder i syfte att stärka krisberedskapen inom myndigheten och dess ansvarsområde.

### 6.2 Informationssäkerhet

Systematiskt säkerhetsarbete bedrivs vid Svenska kraftnät i enlighet med MSB:s föreskrifter (MSBFS 2009:10) om statliga myndigheters informationssäkerhet. Det finns kunskap om beroenden mellan verksamhetens kritiska system. Myndigheten ställer krav på informationssäkerhet när informationshantering (nya IT-system och -tjänster) upphandlas av en extern leverantör.

### 6.3 Planering och övning

Delar av planeringen för att förebygga risker och sårbarheter samt plan för att hantera kriser är framtagen i samverkan med andra aktörer. För den operativa driften finns kontinuitetsplaner samt handlingsplaner för situationer där en kritisk resurs faller bort eller där uppbemanning krävs. För reparationsberedskapen inom Svenska kraftnät finns dokumenterade rutiner och arbetssätt.

Övnings- och utbildningsplan för krisledningsorganisationen ses över årligen och uppdateras vid behov. Enligt övnings- och utbildningsplanen ska organisationen övas minst en gång per år. Rutiner för att ta till vara erfarenheter från inträffade händelser och övningar finns dokumenterade i stabsinstruktion för krisledningsorganisationen.

### 6.4 Samverkan och kommunikation

Genom att stödja Elsamverkan (störningsberedskap för lokala och regionala störningar i elnät) samt utveckling och förvaltning av det webbaserade nationella verktyget SUSIE (som används för att underlätta samverkan mellan elnätsföretag under stör-

---

<sup>47</sup> Avseende risk- och sårbarhetsanalys som myndigheten årligen ska redovisa enligt förordningen (2006:942) om krisberedskap och höjd beredskap

ningar) har Svenska kraftnät tagit initiativ till att aktörer inom ansvarsområdet samverkar och uppnår samordning i planerings- och förberedelsearbetet inför hantering av kriser. Samverkan sker även med nordiska systemoperatörer på en operativ nivå och inom det nordiska samarbetet Nordic Asset Management Forum (NordAM) har de nordiska systemoperatörerna slutit ett avtal om ömsesidigt bistånd vid stora driftstörningar, som innebär att reparationsresurser kan avropas.

Inom ramen för arbetet med Svenska kraftnäts krisledningsorganisation och TiB-organisation pågår det ett arbete för att fastställa rutiner för att upprätta och förmedla en samlad lägesbild inom ansvarsområdet avseende kriser. I SUSIE visas en aggregerad lägesbild över störningar hos huvuddelen av elnätsverksamheten. Samverkan på den operativa nivån är dock mer utvecklad än på krisledningsnivå.

RAKEL används som en alternativ lösning för talkommunikation, både internt inom myndigheten och externt med aktörer inom elförsörjningen samt gentemot andra krisberedskapsaktörer. Svenska kraftnät har även ett drifttelefoninät som har en mycket god tillgänglighet.

För information till allmänheten finns det en särskild föreberedd webbplatsstartsida som kan aktiveras vid krissituationer. Det finns också en rutin för utökad bevakning av telefonväxelfunktionen i Svenska kraftnäts krisledningsorganisation.

## 6.5 Resurser

Svenska kraftnät har rollen bland annat som stamnätsförvaltare och elberedskapsmyndighet. För båda dessa verksamheter har det genomförts behovsanalyser av vilka materiella och personella resurser som krävs för att hantera kriser utifrån olika scenarier.

Avseende personella resurser finns det avtal med Försvarmakten, avtal med ett antal frivilligorganisationer (FRO, FFK, FAK och Bilkåren), frivilligavtal för f.d. civilpliktiga linjemontörer samt avtal med ett antal elnätsföretag och elentreprenörer

När det gäller materiella resurser finns det rutiner för att genomföra underhåll och kontrollera funktionalitet på fordon och utrustning som underhålls och besiktigas.

## 7 Beskrivning av identifierade sårbarheter och brister i krisberedskapen

Nedan redovisas de sårbarheter och brister i förmåga som framkommit vid analys av risker inom myndigheten och dess ansvarsområde (elsektorn). Bristerna är dock av övergripande karaktär och förekommer i varierande grad inom elförsörjningen.

### 7.1 Sårbarheter och brister kopplade till störningar i försörjning av drivmedel

#### **Hos enskilda aktörer/verksamheter**

- > Brister i kunskap om anläggningar har reservkraft och om uthålligheten
- > Bristande kontinuitetsplaner avseende hantering av bristsituationer av drivmedel.
- > Brister i avtal och överenskommelser med entreprenörer/underleverantörer. Avtalen är inte alltid reglerade så att det säkerställs att den egna verksamhetens behov av personella och materiella resurser tillgodoses.
- > Avsaknad av utvecklade samverkansformer inom/utom elförsörjningen kring försörjning av drivmedel

#### **På den nationella nivån**

- > Oklarhet i tillgång till drivmedel på den nationella nivån i bristsituationer – det är i dagsläget oklart om elförsörjningen kommer att prioriteras framför andra samhällsviktiga verksamheter.
- > Entreprenörers och underleverantörers skyldigheter regleras inte i elberedskapslagen, vilket innebär ett beroende av avtal och överenskommelser hos aktörer inom elförsörjningen.

### 7.2 Sårbarheter och brister kopplade till exponering av skyddsvärda informationsresurser

- > Brister i analyser av sådana risker och sårbarheter inom tjänsteleverantörers verksamheter och/eller outsourcade verksamheter som har bäring på den egna verksamheten.
- > Delvis bristfälliga kontinuitetshanteringsplaner i det avseendet att det saknas ett helhetsperspektiv för verksamhetens alla kritiska system (vilket innebär att eventuella kopplingar mellan de kritiska systemen kan vara okända utifrån ett kontinuitetshanteringsperspektiv).
- > Avsaknad eller bristfällig informationsklassning, vilket kan medföra att säkerhetsklassificerad information blandas med icke-klassificerad information i de viktiga systemen.
- > Brister i regelverk för och kontroll av åtkomst till viktiga system och tillträde till anläggningar.

### 7.3 Sårbarheter och brister kopplade till höga flöden i reglerande vattendrag

- > Risk- och sårbarhetsanalyser genomförs i olika hög grad, och tar ofta inte hänsyn till mer extrema scenarier. Det finns brister i kunskap om hur olika flöden påverkar den egna verksamheten, vilket kan bero delvis på bristande kännedom om tillgängliga översvämningskarteringar, delvis på den osäkerhet i konsekvensbedömning som nämnts tidigare.
- > Tidigare analyser som inte hänsyn till höga flöden har lett till placering av viktiga anläggningar i översvämningsområden.
- > Det framkommer bitvis eftersatt kunskap om vattnets skadeverkan på anläggningsdelar, vilket kan vara viktigt för att kunna upprätta ev. relevanta reservdelslager.



## 8 Genomförda, pågående och planerade åtgärder sedan föregående rapportering

I detta kapitel redogörs för åtgärder kopplade till årets fördjupningsområden.

Dels redovisas specifika åtgärder som har eller ska genomföras, dels redovisas exempel på åtgärder av mer generell karaktär, som kan komma att ligga till grund för eventuella elberedskapsåtgärder och åtgärder inom myndigheten framöver. Dessa kan också komma att utgöra rekommendationer till aktörer inom elförsörjningen.

De sårbarheter och brister, kopplade till informationssäkerhet, som redovisades i 2015 års risk- och sårbarhetsanalys har legat till grund för arbetet med åtgärder inom området. Dessa redovisas i delkapitel 8.2 under ”Genomförda och pågående elberedskapsåtgärder”.

### 8.1 Störningar i försörjning av drivmedel

#### **Genomförda och pågående elberedskapsåtgärder**

I tidigare genomförda förmågebedömningar har ett behov av att öka kompetensen för att underhålla och köra reservkraft inom branschen identifierats. Med anledning av detta har en komplett utbildningsmiljö för reservkraft anskaffats. Svenska kraftnät har också tecknat avtal med frivilliga organisationer och står för utbildning för att de ska tillhandahålla 30 reservkraftsoperatörer.

Även personal från elförsörjningen utbildas till reservkraftsoperatörer.

#### **Exempel på åtgärder för att kunna förebygga och hantera störningar i försörjning av drivmedel**

- > Tillgång till mobila tankstationer som är dimensionerade för att klara av eventuella störningar i drivmedelsförsörjning
- > Regelbunden provkörning av reservkraftaggregaten och service av utrustning
- > Upprättade rutiner och störningsplaner för hur hantera en bristsituation inklusive prioritering av anläggningar och plan för bemanning av anläggningar
- > Övningar för hur hantera störningar i försörjning av drivmedel i den egna verksamheten
- > Se över hållbarheten för lagrat drivmedel
- > Möjlighet att pumpa drivmedel från tankställe utan tillgång till ordinarie elförsörjning.
- > Hybridbilar (el/diesel) som kan användas som montörsbilar (minskar bränsleförbrukning, kräver tillgång till el.)
- > Utredda behovet av mobil reservkraft till elförsörjningens egna anläggningar

### **Exempel på åtgärder för att kunna återställa verksamheten efter störningar i försörjning av drivmedel**

- > Regelbunden tillsyn och lagerhållning av förbrukningsmateriel för reservkraften samt tillgång till snabb påfyllning av både drivmedel och reservdelar
- > Säkrad lokal produktion av alternativa bränslen med reservkraft så att bränsle kan produceras även under störningar i elförsörjningen.

### **Identifierade behov för Svenska kraftnät att arbeta med framöver tillsammans med berörda aktörer**

I framtida arbetet är det viktigt att tillsammans med berörda aktörer beakta utmaningar kopplade till drivmedelsförsörjning utifrån hela försörjningskedjan på en nationell nivå och hur dessa kan påverka elförsörjningen. Arbetet bör bland annat behandla olika alternativ för hur tillgodose behovet av drivmedel inom elförsörjningen i bristsituationer, inklusive logistiken kring distribution av drivmedel.

## **8.2 Exponering av skyddsvärda informationsresurser mot osäkra nätverk**

### **Genomförda och pågående elberedskapsåtgärder**

#### ***Uppdateringar och utökningar av befintliga vägledningar***

Arbete med att utöka och uppdatera Svenska kraftnäts befintliga vägledningar inom säkerhetsområdet avseende rutiner och funktioner för säkerhetskopiering och återställning av system som är kritiska för elförsörjningen (inklusive exempel på logg- och larmhantering i system) har påbörjats under året. Inom ramen för det arbetet kommer det utredas hur ytterligare förtydliga och exemplifiera hur Svenska kraftnäts föreskrifter kan uppfyllas av elföretagen.

En vägledning för drift- och styrcentraler som adresserar hela säkerhetsproblematiken omfattande säkerhet, beredskap och säkerhetsskydd håller på att tas fram.

En bilaga till "Vägledning för IT-säkerhetsarkitektur för elsektorn"<sup>48</sup> (som ger exempel på hur en IT-arkitektur kan utformas för att uppnå en god säkerhetsnivå) som kommer att innehålla ett antal krav som kan användas vid upphandlingar håller på att tas fram.

---

<sup>48</sup> Svenska kraftnät: IT-säkerhetsarkitektur. En vägledning för elbranschen med typexempel på referenslösningar. 2015.

### **Genomförande av säkerhetshöjande åtgärder**

Under året har ett antal elföretag fått utbildning/information om risker kopplade till brister i säkerhetsprövning av personal som tar del av skyddsvärd information eller kan påverka skyddsvärda resurser.

### **Exempel på åtgärder för att kunna förebygga och hantera omfattande störningar i/angrepp mot kritisk IT-infrastruktur<sup>49</sup>**

- > Risker inom tjänsteleverantörers verksamhet och/eller outsourcad verksamhet som har bäring på den egna verksamheten inkluderas i organisationens egen risk- och sårbarhetsanalys/säkerhetsanalys.
- > Krav på säkerhetsanalys, säkerhetsorganisation och kontinuitetsplanering i entreprenörsavtal
- > Helhetsperspektiv på kontinuitetshantering för att säkerställa att eventuella kopplingar/beroenden mellan olika system omhändertas i analysen.
- > Krav från ledningen på ett systematiskt säkerhetsarbete (inkl. incidentrapportering och – hantering) som omfattar alla för kärnverksamheten viktiga system och tjänster.
- > Regelbundna utbildningar i IT-säkerhet samt övningar inklusive manuella rutiner.
- > Ändamålsenliga rutiner som reglerar åtkomsten till viktig utrustning på anläggningar.
- > Ändamålsenlig IT-säkerhetsarkitektur som svarar mot aktuella risker, omfattande bland annat åtkomststyrning med möjligheter till spårbarhet av systemanvändare, segmentering av kritiska resurser från kontorsmiljön, adekvata lösningar för fjärraccessanslutningar och reservdriftställe (i de fall de bedöms nödvändiga)

### **Exempel på åtgärder för att kunna återställa de kritiska systemen efter en omfattande störning i/ett angrepp mot kritisk IT-infrastruktur**

- > Rutiner för redundanstester och regelbunden kontroll av att backupen för de kritiska systemen (inklusive reservsystem och dess uppdateringar) körs. Rutiner för regelbunden återskapning/återläsning av data i backupen
- > Rutiner för att bemanna stationer lokalt. Kartlägg personalresurser inom IT i fall av storstörning. Personalen ska vara säkerhetsprövad och skyddsklassad.
- > Reservkapacitet avseende viktig IT-utrustning.

<sup>49</sup> Se även: IT-säkerhetsarkitektur – en vägledning för elbranschen med typfall och referenslösningar. 2015. <[http://www.svk.se/siteassets/aktorsportalen/sakerhetsskydd/dokument/vagledning-it-sakerhetsarkitektur-final.pdf?\\_t\\_id=1B2M2Y8AsgTpgAmY7PhCf%3d%3d&\\_t\\_q=V%3%a4gledning+IT-S%3%a4kerhetsarkitektur&\\_t\\_tags=language%3asv&\\_t\\_ip=192.121.1.150&\\_t\\_hit.id=SVK\\_WebUI\\_Models\\_Media\\_OfficeDokument/\\_93732dd1-1c90-40e3-9908-68e1b7403bc0&\\_t\\_hit.pos=1](http://www.svk.se/siteassets/aktorsportalen/sakerhetsskydd/dokument/vagledning-it-sakerhetsarkitektur-final.pdf?_t_id=1B2M2Y8AsgTpgAmY7PhCf%3d%3d&_t_q=V%3%a4gledning+IT-S%3%a4kerhetsarkitektur&_t_tags=language%3asv&_t_ip=192.121.1.150&_t_hit.id=SVK_WebUI_Models_Media_OfficeDokument/_93732dd1-1c90-40e3-9908-68e1b7403bc0&_t_hit.pos=1)>

### **Identifierade behov för Svenska kraftnät att arbeta med framöver tillsammans med berörda aktörer**

- > I det framtida arbetet är det viktigt att fortsätta ställa krav på aktörers säkerhetsarbete och följa upp att elsektorns aktörer efterlever de regler som följer av säkerhetsskyddslagen med tillhörande förordning och föreskrifter.
- > Det finns ett behov av information om ”best practices”- lösningar/metodstöd inom området informationssäkerhet, t.ex. avseende stöd för tydlig kravställning vid upphandlingar och outsourcing av tjänster knutna till kritisk infrastruktur inom elförsörjningen.
- > Det finns också ett behov av samverkansforum för säkerhetsfrågor och för att tydliggöra roller och ansvar mellan företagen och myndigheten.

## **8.3 Höga flöden i reglerade vattendrag**

### **Exempel på åtgärder för att kunna förebygga och hantera konsekvenser till följd av höga flöden**

- > Vid projektering (inkl. placering) av nya anläggningar ta hänsyn till tillgängliga kunskapsunderlag om höga flöden/översvämningsområden
- > Genomföra konsekvensanalyser för befintliga anläggningar och öka kännedomen/medvetenheten om risker kopplade till höga flöden
- > Utveckling av planer för hantering av höga flöden
- > Storstörningsorganisation som är övad för att hantera krissituationer
- > Regelbunden kontroll av kritisk materiel, personella resurser och entreprenöravtal
- > Redundanta kommunikationssystem

### **Exempel på åtgärder för att kunna återställa verksamheten efter störningar på grund av höga flöden**

- > Tillgång till kritisk materiel och maskiner, så som stolpar, pumpar och reservelverk.
- > Tillgång till personella resurser (inom företagen och/eller reglerat genom avtal med entreprenörer).

### **Identifierade behov för Svenska kraftnät att arbeta med framöver tillsammans med berörda aktörer:**

- > I framtida arbete finns behov av fortsatta fördjupning av konsekvenser, brister och åtgärdsbehov av höga flödens påverkan på elförsörjningen. Det behövs ett helhetsperspektiv för elförsörjningen, omfattande både produktion och nät, för att öka förståelsen för risker kopplade till höga flöden, framförallt sådana mer extrema än 100-årsflöden. Ett sådant arbete kan till exempel ligga till grund för bättre planer för att hantera denna typ av störningar, och fortsatta utredningar om till exempel materiella resursbehov kopplade till scenarierna.

## 8.4 Behov av ytterligare åtgärder med anledning av risk- och sårbarhetsanalysens resultat

Enligt MSB ska i detta kapitel redovisas ytterligare identifierade åtgärdsbehov som ligger utanför myndighetens mandat eller uppdrag.

Svenska kraftnät har i årets arbete inte identifierat sådana åtgärder som ligger utanför myndighetens ansvar, utan har fokuserat på att identifiera och redovisa åtgärder som ligger inom myndighetens ansvarsområde.

## 9 Bilaga 1

Formulär för bedömning av myndighetens generella krisberedskap (bifogas separat)