SAMMANFATTNING

RISK- OCH SÅRBARHETSANALYS FÖR ÅR 2018

Affärsverket svenska kraftnät

SVENSKA KRAFTNÄT

SVENSKA KRAFTNÄT

Svenska kraftnät är ett statligt affärsverk med uppgift att förvalta Sveriges stamnät för el, som omfattar ledningar för 400 kV och 220 kV med stationer och utlandsförbindelser. Vi har också systemansvaret för el. Vi utvecklar stamnätet och elmarknaden för att möta samhällets behov av en säker, hållbar och ekonomisk elförsörjning. Därmed har Svenska kraftnät också en viktig roll i klimatpolitiken.

Foto
Tomas Ärlemo

Org. Nr 202100-4284

SVENSKA KRAFTNÄT
Box 1200
172 24 Sundbyberg
Sturegatan 1

Tel 010-475 80 00
Fax 010-475 89 50

www.svk.se

Denna rapport är en sammanfattning av Svenska kraftnäts rapport ”Risk- och sårbarhetsanalys för år 2018”, Svk 2017/3349, som har redovisats till Regeringskansliet och Myndigheten för samhällsskydd och beredskap (MSB) enligt förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

1. För en robust elförsörjning

Elförsörjningen är en av våra viktigaste samhällsfunktioner och en förutsättning för ett fungerande samhälle. Arbetet med risk- och sårbarhetsanalys syftar till att öka medvetenheten och kunskapen om vilka hot, risker och sårbarheter som föreligger och är ett viktigt verktyg för systematiskt säkerhetsarbete. Risk- och sårbarhetsanalysen ska ligga till grund för åtgärder inom elförsörjningen med syfte att förebygga, motstå och hantera störningar som kan medföra svåra påfrestningar på samhället.[1]

I arbetet med risk- och sårbarhetsanalys ska även höjd beredskap och krig beaktas. Den återupptagna planeringen för totalförsvaret innebär utökade krav på uthållighet och robusthet för att kunna upprätthålla nödvändiga samhällsviktiga funktioner även under särskilda förhållanden. Förmågan vid svåra påfrestningar inom elförsörjningen är avhängig av infrastrukturens robusthet, adekvat säkerhetsskydd och förmågan till reparationsberedskap. Att ha den kunskap och beredskap som behövs för att möta kommande utmaningar är av central betydelse.

[1] Jfr Elberedskapslagen (1997:288) och Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap

2. Nationell risk- och sårbarhetsanalys för elförsörjningen

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. Svenska kraftnät, förutom att analysera hot, risker och sårbarheter inom sitt eget ansvarsområde, upprättar en nationell risk- och sårbarhetsanalys för elsektorn (produktion av, distribution av och handel med el) enligt elberedskapslagen. Dessa båda aspekter sammanställs i en samlad risk- och sårbarhetsanalys.

3. Samhällsviktig verksamhet inom elförsörjningen som är av nationell betydelse

En viktig utgångspunkt för riskanalysen är att identifiera den samhällsviktiga verksamheten inom elförsörjningen och dess kritiska beroenden. 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 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.[2]

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

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 balans inte 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.

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, både inom distribution och produktion av el.

[2] Jfr Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser MSBFS 2016:7

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. Kritiska beroenden för identifierad samhällsviktig verksamhet

För den identifierade samhällsviktiga verksamheten på nationell nivå har följande kritiska beroenden identifierats:

- Elektroniska kommunikationer
- Teknisk infrastruktur
- Kritisk materiel
- Framkomlighet
- Personella resurser
- Beredskapsorganisation
- Information

5. Hot, risker och sårbarheter inom elförsörjningen

Analysen beskriver den aktuella antagonistiska hotbilden[3] och ett axplock av icke-antagonistiska hot och framtida utmaningar inom elförsörjningen.

5.1. Hotbildsanalys

Hotbildsanalysen är indelad på delområdena underrättelseverksamhet, sabotage (bl.a. inom ramen för hybridkrigföring), terrorism och brottslighet.

Underrättelseverksamhet

Ett antal länder bedriver olovlig underrättelseverksamhet i Sverige och energiförsörjningen är ett område som bedöms vara av särskilt intresse för främmande makt. Spionage och underrättelseinhämtning utgör det enskilt största hotet mot Sveriges elförsörjning. Till skillnad från övriga hot är underrättelseinhämtning mot elförsörjningen en pågående realitet av omfattande karaktär och bedrivs på ett systematiskt och långsiktigt vis.

Spionage och underrättelseinhämtning bedrivs bland annat genom cyberangrepp, värvning av insiders, signal-, flyg- och satellitspaning samt genom granskning av öppna källor. Syftet är att kartlägga sårbarheter i elförsörjningen och förbereda för framtida angrepp. Det förekommer även industrispionage mot elförsörjningen som kan innebära att främmande makt kommer över uppgifter som rör rikets säkerhet, även om spionaget huvudsakligen är ekonomiskt motiverat.

Den huvudsakliga metoden för spionage och underrättelseinhämtning mot elförsörjningen är teknisk inhämtning genom främst avancerade cyberangrepp, men det förekommer även traditionell inhämtning genom värvning av insiders, samt inhämtning via öppna källor där information som aggregeras uppnår en skyddsvärd nivå.

Cyberhotet inbegriper bland annat riktad e-post som innehåller skadlig kod. Sådana e-postmeddelanden utformas på ett mycket trovärdigt vis där angriparen simulerar tidigare kommunikationsmönster. Andra former av angrepp kan exempelvis vara att förse USB-stickor med skadlig kod, och sedan på något sätt se till att de används i den skyddsvärda verksamheten.

Insiderhotet utgörs av utländska underrättelseofficerare som värvar insiders på de elföretag som utgör mål för angrepp. Insiders kan efter påtryckning eller på frivillig grund

[3] Med ett antagonistiskt hot avses en aktör som har avsikt och förmåga att skada elförsörjningen på en nivå som får konsekvenser för rikets säkerhet.

lämna ut skyddsvärd information eller bistå i angrepp mot företaget. Om elföretag utkontrakterar skyddsvärda verksamheter till tredje part kan även dessa bli attraktiva mål för underrättelseinhämtning.

Sabotage

Sabotage mot elförsörjningen bör betraktas inom ramen för gråzonsproblematiken, där attacker mot elnätet ämnar destabilisera samhällets funktionalitet. I förlängningen kan allvarliga angrepp mot elförsörjningen utgöra ett påtryckningsmedel i syfte att utöva inflytande på Sveriges handlingsförmåga och utrikes- och säkerhetspolitiska agerande. Sabotage kan även genomföras i syfte att testa elförsörjningens förmåga att förebygga och hantera angrepp.

I händelse av att Sverige blir utsatt för väpnad konflikt bedöms sabotage mot elförsörjningen utgöra ett led i hybridkrigsföring. Sabotage kan ske både genom cyberangrepp och genom fysiskt sabotage.

Det har skett en markant ökning av cyberangrepp mot svenska myndigheter och företag i form av avancerad skadlig kod. Statliga och statsunderstödda aktörer har även i högre utsträckning börjat genomföra enklare former av överbelastningsattacker i syfte att lamslå system och informationskanaler.

Det går heller inte att utesluta att kvalificerade angripare placerar avancerad skadlig kod i hårdvara hos leverantörer som sedan köps in och används i samhällskritiska IT-system, som exempelvis SCADA-system.

Även fysiskt sabotage kan få allvarliga konsekvenser för elförsörjningen. Resursstarka antagonister kan genomföra avancerade former av fysiska angrepp genom större sprängladdningar, elektromagnetiska hot eller beskjutning med vapen som är avsedda att förstöra material. Mindre kvalificerade angripare kan med relativt enkla medel angripa ledningsstolpar.

Terrorism

Terrorhotet mot Sverige utgörs företrädesvis av den våldsbejakande islamistiska miljön. Hoten motiveras av upplevda kränkningar av islam, samt svensk militär närvaro i länder med stark anknytning till islam.

Terrorhotet riktar sig främst mot allmänheten, polis och andra symboliska mål, i syfte att sprida skräck och skapa motsättningar i samhället. Det har inte förekommit några terrorattentat mot elförsörjningen i Västeuropa, men däremot attentat mot dammar och annan kritisk infrastruktur i Syrien och Irak.

Vidare bedöms terrorhotet främst komma från ensamagerande aktörer som genomför småskaliga attentat med enkla medel, vilket är ett tillvägagångssätt som inte bedöms vara effektivt för terrorattentat mot elförsörjningen.

Brottslighet

Den traditionella organiserade brottsligheten bedöms sakna avsikt att utgöra ett hot mot elförsörjningen. Däremot föreligger det en förhöjd risk att elföretag utsätts för utpressningsvirus, så kallad ransom ware. Även om den typen av angrepp är ekonomiskt motiverade kan det få negativa konsekvenser för delar av elförsörjningen.

5.2 Omvärldsanalys av icke-antagonistiska hot

Att utveckla elsystemet innebär långa ledtider vilket ytterligare stärker behovet av att analysera möjliga framtidsutvecklingar. Det finns flera tänkbara händelseutvecklingar som kan komma att påverka elförsörjningens robusthet negativt, med konsekvenser som exempelvis kapacitets- eller energibrist, olyckor och tekniska fel.[4]

Analysen innehåller inte värderingar av hur troliga händelseutvecklingarna är, utan fokus ligger på att finna händelseutvecklingar som skulle kunna påverka robustheten i elförsörjningen nu och i framtiden.

Människor och arbetsmarknad
Åldrande befolkning kan medföra en förlust av upparbetad kompetens och expertis genom omfattande pensionsavgångar, som inte kan kompenseras genom nyrekryteringar, vilket ökar risken för bristande djup kompetens inom traditionell elkraftskunskap. Parallellt med detta ställer teknikutvecklingen krav på ny kompetens. Automatisering av arbetsuppgifter innebär att behovet av kompetens inom de digitala processer som understödjer robotiken och den artificiella intelligensen ökar.[5]

Ökande urbanisering kommer att leda till större befolkningscentra, vilket innebär en koncentration av förbrukningen till vissa punkter. Detta kan komma att ställa nya krav på hur elsystemet byggs ut. Konsekvenserna av avbrott riskerar att bli allvarligare i städer genom att fler människor drabbas.

Dagens elproduktion sker till stor del i glesbygden och en utflyttning därifrån skulle därför kunna medföra en brist på arbetskraft i produktionsorterna. Även möjligheten till underhåll av lokal- och regionnät skulle kunna påverkas då avstånden mellan arbetskraften och behoven växer.

[4] Delkapitlet baseras mestadels på Totalförsvaret forskningsinstitutets (FOI) Litteraturstudie om framtidens elförsörjning och elberedskap (2018). Beskrivningar i rapporten är baserade på strategiska framtidsanalyser och bedömningar genomförda av flertal myndigheter, forskningsinstitut mm. Vad gäller utmaningar kopplade till naturhändelser hänvisas till vårt svar på regeringsuppdrag om klimatförändringars påverkan på elsystemet.
[5] Å andra sidan kan säkerheten tänkas öka, särskilt hos mindre aktörer med färre personella resurser som istället kan använda sig av automatiseringslösningar. På samma sätt kan automatiseringen tänkas hålla medelgamla anläggningar lönsamma eftersom färre personer behövs på plats. Automatisering kan dock leda till nya risker och beroenden, t.ex. risk för cyberincidenter av skilda slag, antagonistiska såväl som icke-antagonistiska, i och med ett ökat beroende av it. Automatiseringen skulle också kunna skapa nya typer av beroenden, bland annat genom ett förändrat behov av reservdelar. Se ”Litteraturstudie om framtidens elförsörjning och elberedskap…”

Energitillgång och elproduktion
Parallellt med att användningen av fossila bränslen minskar så ökar andelen förnybar energi i elförsörjningen. Till exempel ökar produktion genom vindkraft, vattenkraft, solenergi och elproduktion baserat på förnybara bränslen. Flera av dessa kännetecknas av variabel produktion som är väderberoende och därmed inte kan planeras, vilket kräver balansering från andra kraftkällor eller på användarsidan.

Vid omfattande skador på stamnätet är förmågan till ö-drift (regional försörjning utan elektrisk förbindelse med stamnätet) av yttersta vikt. För ö-drift har lokala kraftvärmeverk en viktig roll att spela då dess produktion ligger i närheten av områden där förbrukningen är som mest behövd. Nedläggning och minskad nybyggnation av kraftvärmeverk samt omvandlande av kraftvärmeverk till fjärrvärmeverk begränsar möjligheten till ö-drift, särskilt i närheten av större städer. Elproducenterna har allt svårare med lönsamheten när det gäller elproduktion i kraftvärmeverk på grund av lägre elpriser och höga reinvesteringskostnader. Dessutom har flera företag som strategi att bli fossilfria. Detta medför att äldre oljeeldade anläggningar läggs ned då de inte uppnår lönsamhets- eller miljökrav.

Det finns begränsade möjligheter att använda förnybar energi såsom vindkraft i ö-driftverksamhet, då vindkraften är väderberoende och inte bidrar med den svängmassa i systemet som behövs för att driften ska förbli stabil även under ansträngda förhållanden. Dessutom är vindkraftverken ofta placerade allt för långt bort från ö-driftområden för att vara brukbara i ö-driften.

Teknik och infrastruktur
Elsystemet sammankopplas allt mer med infrastrukturen för telekommunikation - ett modernt, intelligent nät är inte möjligt utan internet. Så kallade smarta elnät, artificiell intelligens och digitala stationer medför stora möjligheter för framtidens elsystem, men för också med sig sårbarheter som behöver beaktas. Sårbarheten hos kraftsystemet för cyberincidenter ökar i och med att det finns fler kontaktytor som exponeras.

Digitaliseringen, parallellt med utvecklingen mot ett mer decentraliserat elsystem genom mer distribuerad produktion och lagerhållning, gör kunderna till mer aktiva komponenter i systemet. Fler system och enheter ska kunna fjärrstyras eller fjärravläsas, vilket gör att de exponeras för intrång då de kopplas upp mot internet. Fler utplacerade mätenheter innebär också ökad fysisk sårbarhet.

I samband med ny- och ombyggnationer av anläggningar avlägsnas ofta funktioner för lokal styrförmåga av aggregat. I allt högre utsträckning förlitar sig produktionsbolagen istället på att kunna styra anläggningar från en driftcentral. Det innebär att produktionen blir sårbar för störningar i den centrala styrningen, som exempelvis fel i IT-nätet.

Utvecklingen under de senaste årtiondena har dessutom inneburit en generell minskning av driftgrupper inom den egna organisationen, vilket medför svårigheter kring

kompetensförsörjning och långvarig bemanning av kraftstationer i händelse av kris. Vid en svår påfrestning på elförsörjningen medför detta begränsade möjligheter att klara upprätthållande av drift.

Tillgång till reservdelar är ett kritiskt beroende inom elförsörjningen. Det finns redan i dag ett omfattande beroende av leverantörer för bland annat reservdelshållning och underhållsarbete,[6] vilket innebär att brister i leverantörskedjan kan medföra stora konsekvenser för systemkritiska funktioner och verksamheter.

[6] Se även Svenska kraftnät: Risk- och sårbarhetsanalys för år 2016, SvK 2015/1294

6. Tematiska analyser

Den nationella risk- och sårbarhetsanalysen för elförsörjningen omfattar även fördjupade riskanalyser inom olika tematiska områden, med fokus på konsekvenser och vad som kan påverka förmågan att hantera händelser.

6.1 Uppdrag i årets regleringsbrev: Klimat- och sårbarhetsanalys

Regeringen har i regleringsbrevet för 2018 uppdragit åt Svenska kraftnät att redovisa en analys av klimatförändringarnas negativa påverkan på elsystemet i Sverige.

Analysen har sammanställt hur följdverkningar av klimateffekter, t.ex. stormar, nedisning, höga flöden och erosion, förväntas påverka produktion och distribution av el i Sverige fram till år 2100. En översiktlig uppföljning har gjorts av slutsatserna om elförsörjningen som redovisades i klimatutredningen[7] och Energimyndighetens rapport[8] som är grunden för föreliggande uppdrag.

De effekter av klimatförändringarna som kan beröra elförsörjningen kommer att ske gradvis över lång tid. Befintliga anläggningar bedöms generellt klarar sig fram till sin tekniska livslängd. Svenska kraftnäts erfarenheter som elberedskapsmyndighet är att åtgärder för att höja robustheten i allmänhet är verkningsfulla oavsett vilken typ av händelse som orsakar störningen.

En stor utmaning för elförsörjningen i framtiden på grund av klimatförändringarna är översvämningar och höga flöden. Även extremvärme kan innebära utmaningar för elsystemet. Överföringskapaciteten på luftledningar kan minska på grund av säkerhetsskäl då ledningstemperaturen ökar. Även andra komponenter i elsystemet, som behövs kylas vid generering och distribuering av el, t.ex. transformatorer och jordkablar, kan påverkas av värme. Elförsörjningens anpassning till ett klimat i förändring kommer att utvecklas när klimatscenarier tillämpas i fler analyser och bedömningar.

6.2 Fortsatt fokusområde: outsourcing

Utkontraktering av delar av elförsörjningsverksamhet sker i en större omfattning under senare tid. Okontrollerad utkontraktering kan resultera i att säkerhetsskyddsklassificerade uppgifter eller i övrigt säkerhetskänslig verksamhet utsätts för risker i samband med utkontraktering, upplåtelse och överlåtelse av sådan verksamhet. Konsekvenserna kan slå mot förmågan att effektivt och samordnat förebygga och möta omedelbara hot mot och utmaningar för Sveriges säkerhet.

[7] Sverige inför klimatförändringarna – hot och möjligheter SOU 2007:60

[8] Statens Energimyndighet: Extrema väderhändelser och klimatförändringens effekter på energisystemet (ER 2009:33)

Den nya säkerhetsskyddslagen[9] kommer att innebära en skärpning av kraven på statliga myndigheter när de utkontrakterar säkerhetskänslig verksamhet.[10] Enligt regeringens förslag ska den nya lagen gälla i alla verksamheter som är av betydelse för Sveriges säkerhet, vilket skulle bland annat innebära att kravet på säkerhetsskyddsavtal vid upphandling utvidgas även till privata aktörer som ansvarar för säkerhetskänslig verksamhet.

En fortsatt analys av konsekvenser av utkontraktering av samhällsviktiga verksamheter inom elförsörjningen pågår inom ramen för arbetet med den nationella risk- och sårbarhetsanalysen.

[9] Lagen kommer att träda i kraft i april 2019

[10] Justitieutskottets betänkande 2017/18:JuU21 , se s.6-7

6.3 Fördjupning: höga flöden och dammhaveri

En vattenkraftdamm som dämmer upp en stor vattenvolym högt upp i en älv, kan vid ett haveri förorsaka stora översvämningar som sträcker sig längs hela vattendraget ned till havet. Högt upp i de stora kraftverksälvarna[11] finns totalt ca 25 dammanläggningar som skulle kunna förorsaka särskilt stora konsekvenser, med dominobrott och förstörelse längs en stor del av en älvdal. Ett dammhaveri i en sådan damm skulle förorsaka omfattande översvämningar och skador på bebyggelse, vattenkraftstationer, vägar, kraftledningar, ställverk, telenät m.m. längs hela älvsträckan ned till kusten. Det skulle kunna medföra allvarliga störningar bl.a. i stamnätets funktion och i annan samhällsviktig verksamhet.

Högsta beräknade flöde[12] och dammhaveri[13] i större kraftverksdammar är scenarier som bedöms ge allvarliga, upp till katastrofala konsekvenser för verksamheterna och för samhället.

Konsekvenser för samhällets elförsörjning

Konsekvenserna av dammhaveri kan variera starkt och beror främst på volymen uppdämt vatten, dammens höjd och längd samt vad som finns i området som kan översvämmas till följd av haveriet. För elförsörjningen skulle det innebära ett storstörningsscenario, och nätstationer med tillhörande ledningar i direkt anslutning till större vattenkraftstationer, ledningar längs älvdalen och korsande ledningar är exempel på stamnätsobjekt som kan skadas vid översvämning.

I händelse av höga flöden eller dammhaveri kan förutsättningarna för driften av stamnätet förändras, på grund av eventuella skador på stationer, stolpar och utrustning, eller på grund av att ledningar behöver kopplas ur.

Behovet av att prioritera resurser och att samverka med andra aktörer kan bli stort om 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. I svåra fall kan infrastrukturen vara skadad längs en hel älvsträcka.

Reparationsarbetet skulle försvåras av brist på framkomlighet för personal och materiel, samt behovet av att låta vattnet sjunka undan och genomföra röjning före reparation. 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.

[11] Luleälven, Skellefteälven, Umeälven, Ångermanälven, Indalsälven, Ljungan, Ljusnan, Dalälven, Klarälven, Göta älv
[12] Återkomsttiden för högsta beräknade flöde för ett vattendrag kan i medeltal uppskattas till i storleksordningen 10.000 år.
[13] Scenariot dammhaveri 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.

Förmågan att hantera händelser är generellt sett god på den nationella nivån. Förmågan att kunna förebygga och återställa är av särskilt stor vikt vid extraordinära händelser (såsom dammhaverier) som kan orsaka omedelbara och omfattande skador.

I detta fall är förmågan att kunna hantera och återställa beroende av expertis och befintlig kunskapsunderlag samt en reparationsberedskap som är dimensionerad utifrån scenariot ”storskaliga översvämningshändelser”.

Den förebyggande förmågan kan förstärkas genom dimensionering av den tekniska infrastrukturen utifrån storstörningsscenariot.

6.4 Fördjupning: informationssäkerhet för samhällsviktig verksamhet inom elförsörjningen

Den samhällsviktiga verksamheten inom elförsörjningen är beroende av information som kännetecknas av konfidentialitet, riktighet och tillgänglighet. Av antagonistiska hot bedöms spionage och underrättelseinhämtning samt cyberspionage och cyberattacker vara de största aktuella hoten mot elförsörjningen. I detta sammanhang är informationssäkerheten kopplat till kritiska IT-miljöer och – system inom elförsörjningen samt information som rör skyddsvärda delar i det svenska elsystemet av särskilt vikt att analysera.

Icke-antagonistiska hot mot informationssäkerheten omfattar i första hand tekniska fel och handhavandefel som berör skyddsvärd information eller IT-system. Sådana fel kan handla om tekniska fel i datautrustning, utrustning för datakommunikation, operativsystem och andra stödsystem, tillämpningsprogram, kablage m.m. Tekniska fel är relativt vanliga och kan i värsta fall resultera i informationsläckage och avbrott i IT-system som är vitala för det svenska elsystemet.

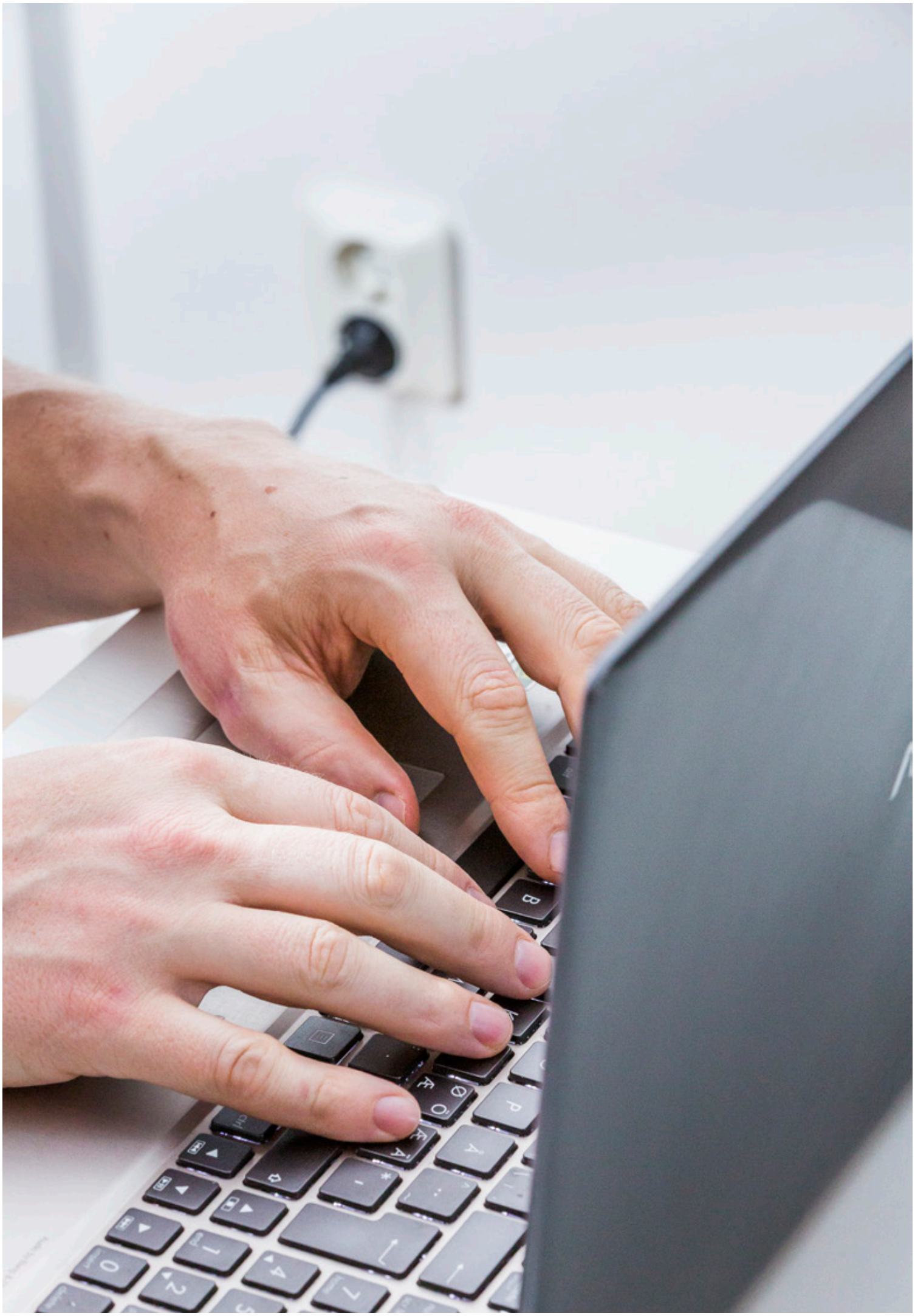
Bristande rutiner för uppdateringar av IT-system kan öka risken och öppna för att sårbarheter i IT- och kommunikationsutrustning samt programvara utnyttjas. Det kan i första hand härledas till leverantörers oförmåga att snabbt leverera uppdateringar som svarar mot sårbarheter i sina IT- system och -tjänster. Det krävs även effektiva interna rutiner för att uppdateringar ska ske snarast möjligt efter att en leverantör publicerar nya uppdateringar.

Utkontraktering av IT eller användning av molntjänster innebär ofta att leverantören placerar olika kunders system och information i samma fysiska datorsystem. Detta medför en ökad risk eftersom en störning i en kunds system kan orsaka störningar eller avbrott hos flera andra kunders system. Hamnar en stor mängd skyddsvärd information hos en enskild leverantör riskerar denne dessutom att bli ett attraktivt mål för bland annat andra länders underrättelseinhämtning. Begränsade möjligheter till uppföljning och kontroll av säkerheten hos leverantörer och leverantörers underleverantörer är ett annat problem. Det kan bidra till att säkerhetsbrister och sårbarheter hos leverantörer inte identifieras/upptäcks och åtgärdas.

Utkontraktering eller användning av molntjänster innebär också en sårbarhet som ökar riskerna med cyberspionage. Till exempel ökar antalet möjliga mål för en attack samtidigt som möjligheterna att säkerställa fullgod informationssäkerhet i alla led minskar.

Konsekvenser för den egna verksamheten/samhällets elförsörjning

Cyberattack mot en organisations IT-miljö kan leda till att skyddsvärd information röjs eller att system som innehåller sådan information eller system som är viktiga för drift och övervakning av elförsörjningen påverkas negativt.



En cyberattack kan göra information och IT-system otillgängliga vilket i sin tur kan ha negativ påverkan för effektiviteten i de samhällsviktiga verksamheterna och tjänsterna. Vilken verksamhet som drabbas av en störning och hur omfattande konsekvenserna blir beror på vilken information eller vilket IT-system som drabbas samt hur lång tid återställningsarbetet tar. Konsekvenserna för en organisations egen verksamhet och samhället kan således variera från försumbara till allvarliga.

Svenska kraftnät bedömer att förmågan att förebygga och motstå ett cyberangrepp hos de större elaktörer i Sverige överlag är god. Dessa aktörer arbetar systematiskt och riskbaserat med informations- och IT-säkerhet.

För att hantera konsekvenserna efter ett cyberangrepp är elföretag dock delvis beroende av samhällets tillgängliga expertresurser. De statliga aktörer som kan stödja ett drabbat elföretag är i första hand MSB, Säkerhetspolisen och FRA.

7. Genomförda, pågående och planerade åtgärder

De identifierade och analyserade hoten, riskerna och sårbarheterna är ett viktigt underlag för fortsatt arbete med åtgärder. Förmågehöjande åtgärder vidtas inom elförsörjningen för att hantera olika slags händelser och dess konsekvenser.

Nedan redovisas åtgärder kopplade till rapportens två fördjupningsområden.

7.1 Höga flöden och dammhaveri

Förebyggande åtgärder är inriktade dels på att förebygga dammhaverier, dels att förebygga att infrastrukturen påverkas vid en översvämningshändelse. Åtgärdernas effekt på bristerna kan förstärkas genom intern kommunikation, utbildning och övning.

Svenska kraftnät genomför aktiviteter i sin egen verksamhet som handlar om att planera för att kunna motstå och hantera översvämningar. Inom ramen för arbetet med beredskapsplanering för dammhaveri genomförs aktiviteter under perioden 2017-2020 som handlar om att stärka samhällsaktörers och dammägares förmåga att hantera ett dammhaveri och dess konsekvenser.

7.2 Informationssäkerhet inom samhällsviktig verksamhet

Informations- och IT-säkerhetsarbetet har som inriktning att skapa en förmåga inom elförsörjningen att förutse, motstå, begränsa och snabbt återhämta sig från en informations- och eller cyberattack.

Under 2017-2018 har Svenska kraftnät hållit ett antal utbildningar rörande säkerhetsskydd och cybersäkerhet för aktörer inom elförsörjningen. Det finns fortsatt behov av att tydliggöra företagens roller och ansvar inom säkerhetsskydd, t.ex. genom utbildning.

”Energisäkerhetsportalen” används som plattform för att informera om aktuella hot samt ge stöd till aktörer inom säkerhetsarbetet.

Svenska kraftnät är ett statligt affärsverk med uppgift att förvalta Sveriges stamnät för el, som omfattar ledningar för 400 kV och 220 kV med stationer och utlandsförbindelser. Vi har också systemansvaret för el. Vi utvecklar stamnätet och elmarknaden för att möta samhällets behov av en säker, hållbar och ekonomisk elförsörjning. Därmed har Svenska kraftnät också en viktig roll i klimatpolitiken.

SVENSKA KRAFTNÄT
Box 1200
172 24 Sundbyberg
Sturegatan 1

Tel 010-475 80 00
Fax 010-475 89 50

www.svk.se

SVENSKA KRAFTNÄT