2025

Scenario:

Det upptrappade läget - El

Del av övningspaket för att stärka energisektorna förmåga inför kriser och krig

Februari, 2025

Energimyndigheten

Bakgrund

Övningsbestämmelser

Scenario: Det upptrappade läget

Moment

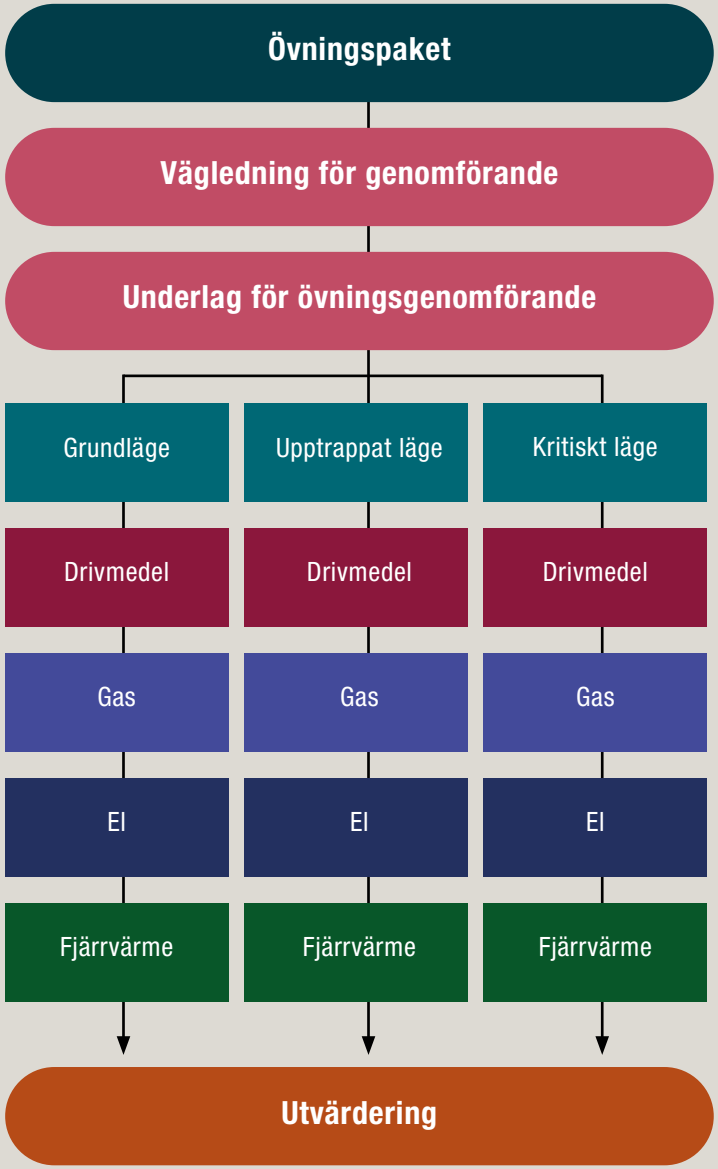
Reflektion och utvärdering

Varför övar vi?

Energiförsörjningen har en avgörande betydelse för samhällets funktionalitet och för att skydda liv, hälsa och samhällets motståndskraft vid olika typer av samhällskriser. Energiförsörjningen måste fungera både i vardagen, under fredstida samhällskriser och krig.

Alla energibolag har en viktig roll. Övning är ett effektivt sätt att stärka den mentala förberedelsen inför olika typer av störningar och underlätta identifiering av förebyggande åtgärder som gör det möjligt att upprätthålla verksamheten även under störda förhållanden.

I takt med den ökade digitaliseringen skapas nya sårbarheter och nya hot. Samtidigt medför klimatförändringarna att tidigare kända hot kan få mer omfattande konsekvenser och bli mer frekventa.
De senaste åren har även det säkerhetspolitiska läget försämrats i Sveriges närområde. Sammantaget innebär det att vikten av att stärka motståndskraften för olika typer av störningar i energiförsörjningen får ökad betydelse.



Syfte och mål med dagen

Varför övar vi?

Det här vill vi uppnå med dagens övning

Förmågor med särskilt fokus

Innan vi samlar in, aggregerar, diskuterar eller dokumenterar underlag som rör känsliga delar av verksamheten - analysera behovet av skydds-åtgärder!

Energimyndigheten

Gemensamma övningsbestämmelser

Vilka förhållningsregler vill vi ha under övningen?

Exempelvis att alla får komma till tals och där scenariot har brister är vi kreativa och finner en väg framåt.

Informationssäkerhet

- Säkerställ att ni använder ändamålsenliga lokaler och hjälpmedel utifrån hur skyddsvärd information som ska avhandlas.
- Bevaka löpande under övningen om det finns risk för att skyddsvärd information röjs till obehörig och pausa i så fall den diskussionen.
- På Energimyndighetens, Säkerhetspolisens och Försvarshögskolans hemsidor finner du mer information om säkerhetsskydd och informationssäkerhet.

Detta har hänt tidigare och är grundläget för övningen.

Scenario A:
Grundläget

Det är februari och mycket kalla vintertemperaturer i Europa. Den gångna hösten har varit mildare och det har förekommit flera kraftiga skyfall som lett till översvämningar.

Det råder invasionskrig i Europas närområde sedan två år tillbaka. Detta inkluderar bland annat fortsatta attacker mot civilsamhälle och energiinfrastruktur.

Gasledningen av större vikt är tagen ur drift.

De växande spänningarna i mellanöstern har ökat risken för fullskaligt krig i regionen samt påverkade transportflöden.

Sveriges inträde i NATO medför anpassning och utveckling av Sveriges försvarsförmåga.

Andra länder samlar in information om kritisk energiinfrastruktur i Sverige.

Försök till överbelastning och intrång i kritiska IT-system bland samhällsviktiga verksamheter, däribland energibolag, sker dagligen.

Sanktioner påverkar europeiska och svenska energimarknader, med ökad konkurrens om energiresurser och högre energipriser som följd.

Det är svårt att få tag på vissa komponenter till kritisk energiinfrastruktur via ordinarie internationella försörjningskedjor.

Energimyndigheten

Fundera på innan ni går vidare:

Vad innebär scenariot för oss på ett övergripande plan?

Energimyndigheten

Scenario B:
Det upptrappade läget

Det är februari och mycket kalla vintertemperaturer i Europa. Den gångna hösten har varit mildare och det har förekommit flera kraftiga skyfall som lett till översvämningar.

Det råder invasionskrig i Europas närområde sedan två tillbaka. Detta inkluderar bland annat fortsatta attacker mot civilsamhälle och energiinfrastruktur.

Gasledningen av större vikt är tagen ur drift.

De växande spänningarna i mellanöstern har ökat risken för fullskaligt krig i regionen samt påverkade transportflöden.

Sveriges inträde i NATO medför anpassning och utveckling av Sveriges försvarsförmåga.

Andra länder samlar in information om kritisk energiinfrastruktur i Sverige.

Försök till överbelastning och intrång i kritiska IT-system bland samhällsviktiga verksamheter, däribland energibolag, sker dagligen.

Sanktioner påverkar europeiska och svenska energimarknader, med ökad konkurrens om energiresurser och högre energipriser som följd.

Det är svårt att få tag på vissa komponenter till kritisk energiinfrastruktur via ordinarie internationella försörjningskedjor.

Moment 1:
Hot mot personal

Den senaste tiden har flera samhällsviktiga verksamheter inom energisektorn vittnat om ökade hot mot den egna personalen. Av den information som framkommit verkar hoten framförallt gått ut på att pressa nyckelpersoner på känslig information eller att hjälpa till att släppa in obehörig personal på känsliga anläggningar. Enligt Säkerhetspolisen antas det finnas ett mörkertal. Även andra samhällsviktiga verksamheter kan vara utsatta för liknande kampanjer.

Exempel på diskussionsfrågor:

Har vi tidigare erfarenhet av att hantera liknande hot?

Kan känslig information om vår verksamhet röjas om detta inträffar?

Har vi personalgrupper som kan vara särskilt utsatt för detta typ av hot?

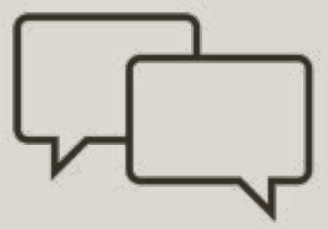
Hur kan vi ta reda på om vi är drabbade? Genomför vi exempelvis några kontroller?

Vilka åtgärder vidtar vi?

Vilka förebyggande åtgärder kan vi vidta för att minska risken för den här typen av hot?

Moment 2:
Störningar i IT-systemen

En medarbetare använder ett USB-minne för att avsiktligt distribuera skadlig kod som börjar kryptera den information som lagras i IT-systemen. Detta medför att kritisk information i IT-systemen blir otillgänglig.



Exempel på diskussionsfrågor:

Hur skiljer sig konsekvenserna och hanteringen åt beroende på om det är OT- eller IT-systemen som påverkas?

Har vi tillgång till något system som gör det möjligt att tidigt upptäcka om det specifika hotet inträffar?

Har vi identifierat viktiga processer i verksamheten som är prioriterade att fortsätta bedrivas?

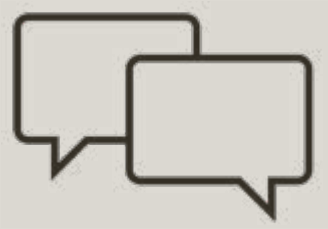
Har vi analyserat acceptabla avbrottstider?

Har vi reservrutiner för att kunna fortsätta bedriva vår verksamhet?

Vilka förebyggande åtgärder kan vi vidta för att minska risken för den här typen av hot?

Moment 3:
Skytt på arbetsplatsen

Vid lunchtid börjar en beväpnad medarbetare att skjuta slumpvis mot andra anställda i lunchrummet. Skytten tar sedan en högt uppsatt chef som gisslan och barrikaderar sig själv i ett rum utan fönster.



Exempel på diskussionsfrågor:

Hur säkerhetskontrollerar vi vår personal?

Finns detta hot med i våra beredskapsplaner?

Finns detta hot med i våra utbildningar?

Hur skulle vår larmkedja och uppstart av krisledning kunna se ut i den här situationen?

Vad kommunicerar vi internt och externt? Omedelbart och senare?

Vilka förebyggande åtgärder kan vi vidta för att minska risken för den här typen av hot? Vilka förebyggande åtgärder kan vi vidta för att minska risken för den här typen av hot?

Vad kommunicerar vi internt och externt?

Hur kan vi säkerställa att vi har tillräckliga resurser och kompetenser på plats i den givna situationen?

Har vi planer för att säkerställa tillgång till personal?

Finns det tillräckligt lagstöd för det vi vill göra?

Vilka förebyggande åtgärder kan vi vidta för att minska risken för smittspridning?

Moment 4:
Parallella skador på nätinfrastruktur

Under veckan har flera stolpar inom ert regionnät förstörts med hjälp av bland annat sprängämnen. Detta har medfört skador och avbrott på flera platser. Eftersom det inte finns tillräckligt med reservdelar och personal för att reparera alla skador samtidigt behöver reparationsinsatserna nu prioriteras. Ytterligare nätinfrastruktur kan komma att drabbas.

Exempel på diskussionsfrågor:

Vad är vårt ansvar och roll kopplat till händelsen?

Hur agerar ni på händelse? Vad behöver ni göra?

Hur ser er kontinuitetsplanering ut för händelse?

Hur ser vår reparationsberedskap ut för att snabbt kunna få fungerande infrastruktur igen? Hur sker prioritering?

Vilka andra aktörer behöver vi samverka med och hur sker den samverkan?

Hur snabbt kan vi mobilisera resurser för att hantera detta hot?

Vilka förebyggande åtgärder kan vi vidta för att minska risken för den här typen av hot?

Moment 5:
Kapade elkablar

Larm inkommer om avbrott på utlandskablarna X och Y. Detta innebär reducerad kapacitet för import och export av el. Berörda myndigheter utreder om det varit flera parallella olyckor eller medvetet sabotage

Exempel på diskussionsfrågor:

Vad är vårt ansvar och roll kopplat till händelsen?

Vilken information har vi behov av och vem har den?

Vilka konsekvenser får detta för elleveranser till kund?

Vilka åtgärder vidtar vi?

Hur skiljer sig vår hantering åt om det skulle vara resultatet av en olycka eller en medveten handling?

Vilka förebyggande åtgärder kan vi vidta för att minska risken för den här typen av hot?

Moment 6:
Avbrott i betalsystemen

Betydande leverantörer av finansiella tjänster drabbas av cyber-angrepp vilket medför avbrott i betalsystemen. Det finns ingen prognos för när de kan fungera igen, men det antas bli långvarigt.

Exempel på diskussionsfrågor:

Hur väl förberedda är vi för att hantera situationen?

Vilken information har vi behov av och vem har den?

Vilka konsekvenser får detta för vår verksamhet?

Vilka andra aktörer behöver vi samverka med och hur sker den samverkan?

Har vi alternativ till ordinarie betalsystem? Hur länge kan vi använda dessa?

Vilka förebyggande åtgärder kan vi vidta för att minska risken för den här typen av hot?

Reflektion och utvärdering

Tips!

Se och inspireras av det framtagna underlaget för utvärderingen.

Hur känns det nu?

Vilka är våra styrkor?

Vilka är våra förbättringsområden?

Vad tar vi med oss i vår organisation framåt?

Ser vi behov av några åtgärder som kräver en sektorsgemensam hantering/strategi och bör lyftas till Energimyndigheten?

Energimyndigheten


Energimyndigheten