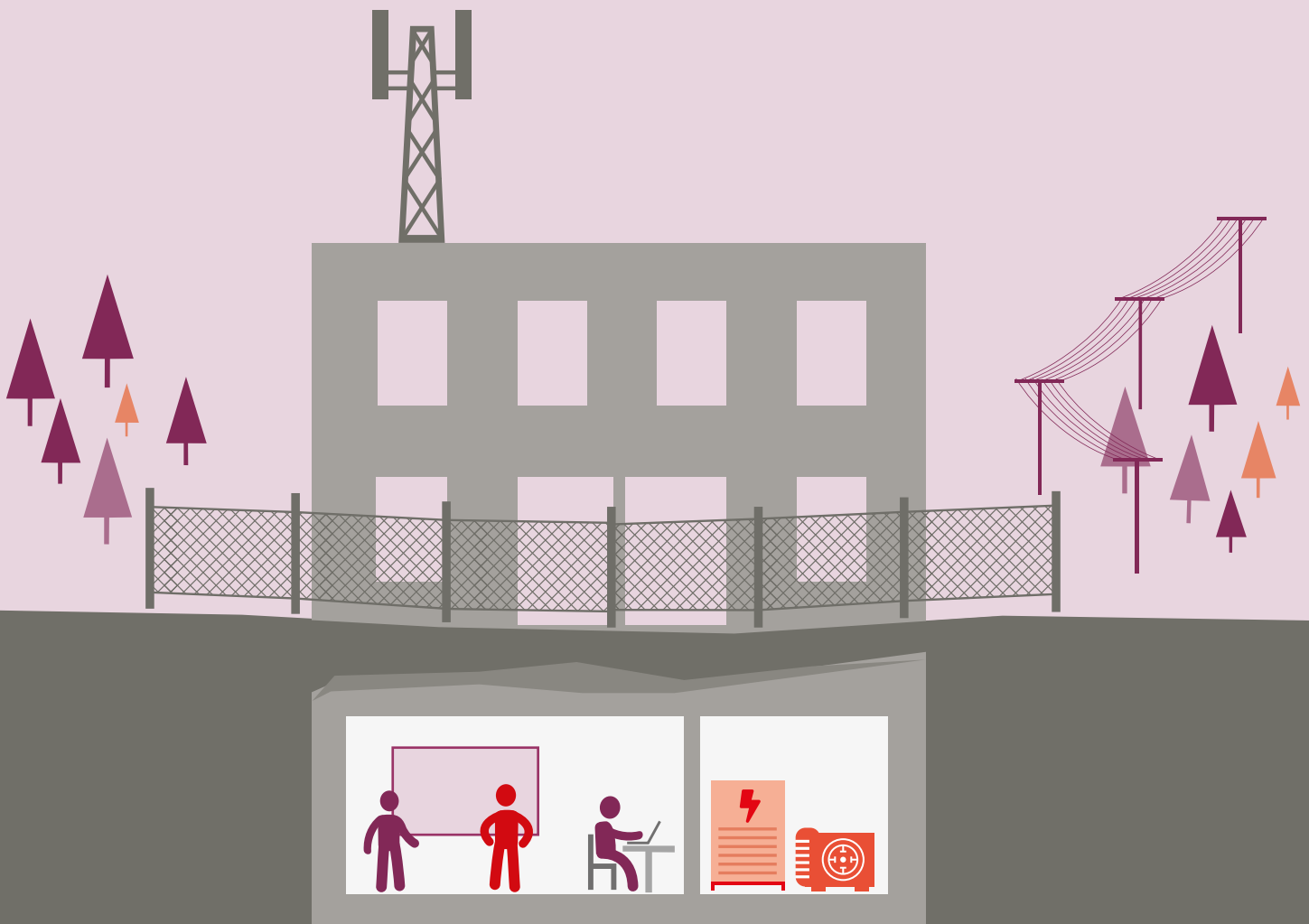




Myndigheten för
samhällsskydd
och beredskap

Vägledning för ledningsplatser



Vägledning för ledningsplatser

© Myndigheten för samhällsskydd och beredskap (MSB)

Produktion: Advant

Publikationsnummer: MSB1815 - september 2021

ISBN: 978-91-7927-178-7



Innehåll

Inledning	6
Allmänt	6
Det sårbara samhället	8
Naturhot och oavsiktliga hot	9
Antagonistiska hot	10
Utvecklingen i samhället	11
Digitalisering	11
Cyberfysiska system och fastighetsautomation	11
Beroendet av externa leverantörer	12
Försörjningsberedskap	13
Ledningsplatsen – en del av kontinuitetshandlingen	14
Att skapa en robust, säker och uthållig ledningsplats	14
Ingångsvärden	15
Hot, sårbarheter och risker	15
Styrning av verksamheten	16
Hantera hot, sårbarheter och risker	17
Kontinuitetshandling	17
Risk- och sårbarhetsanalys enligt förordningen	19
Systematiskt informationssäkerhetsarbete	19
Säkerhetsskyddsanalys	21
Framgångsfaktorer för ledningsplatsverksamhet	25
Säkerställ ledningens engagemang	25
Säkerställ en lärande organisation	25
Låt robusthet genomsyra verksamheten	25
Beakta robusthet vid upphandling	26
Proaktivitet och engagemang vid ny- och ombyggnation	27
Arbeta systematiskt med kontinuitetshandling	28
Ta hänsyn till existerande robusthet vid verksamhetsflytt	28
Säkerställ långa hyresavtal	28
Ledningsplatsstruktur	29
Behov på olika ledningsnivåer	29
Lokal nivå	29
Kommunal räddningstjänst	29
Regional nivå	29
Nationell nivå	29
Ordinarie ledningsplatser	30
Ordinarie ledningsplats	30
Aktörsgemensam ledningscentral	30
Alternativa ledningsplatser	30
Mobil ledningsplats	31
Skyddad ledningsplats	31
Sekundär ledningsplats	33

Ledningsplatsens utformning	34
Byggnadsrelaterade åtgärder	34
Skyddsnivåer	34
Platsval	36
Utanför fastigheten	36
I fastigheten	36
Byggnadstekniska specifikationer	38
Skydd kontra design	39
Tillträdesskydd – lås, larm och passersystem	39
Kamerabevakning	39
Rumsbildningar	40
Lokalval	40
Verksamhetsutrymmen	40
Lokaler för hantering av skyddsvärd information	40
Lokaler för sambands- och kommunikationsystem	41
Lokaler för fastighetstekniska installationer	42
Arbetsmiljörelaterade åtgärder	42
Tekniska försörjningssystem	43
Elförsörjning	43
Värme och ventilation	44
Vatten och avlopp	44
Fastighetstekniska styr- och övervakningssystem	44
Skydd mot elektromagnetiska störningar och hot	45
Tekniska system för samverkan och ledning	46
Robusta system	46
Redundanta system	46
Nätanslutningsutredning	46
Fastighetsnät	47
System för tal, video och datakommunikation	47
It-system	48
SGSI – Swedish Government Secure Intranet	48
Radiosystem	48
Raket	48
Visualiserings- och videokonferenssystem	49
Omvärldsbevakning	49
System för internkommunikation	49
Drift och förvaltning av ledningsplatsen	50
Engagerad verksamhetsutövare	50
Tydligt utpekade roller och ansvarsområden	51
Prova tekniska system regelbundet	52
Driftlarm	52
Utbildad och övad personal	52
Personal i beredskap	53
God krisledningsförmåga	53
Krigsorganisation	53
Säkerställ tillgång på kritiska varor och tjänster	53
Samverka med viktiga leverantörer	54
Korrekt och lättanvänd dokumentation	54

Inledning

Allmänt

Den här vägledningen vänder sig till aktörer som bedriver samhällsviktig verksamhet och som ska kunna leda den egna verksamheten och samverka med andra aktörer i vardagen, under samhällsstörningar och ytterst vid höjd beredskap och krig. Begreppen att leda verksamhet och därtill hörande ledningsförmåga innefattar aktörens behov av att kunna samla in omvärldsinformation som ingångsvärden till sin beslutsprocess, fatta beslut och därefter kommunicera tagna beslut. För att säkerställa kontinuerlig och uthållig förmåga att samverka och leda behöver aktören ett antal resurser, personella och materiella som tillsammans med metoder och rutiner skapar förutsättningar för ledningsförmågan. I vägledningen beskrivs en delmängd i detta, ledningsplatsen, med fysiskt anpassade lokaler, uthålliga försörjningssystem, robusta system för informationsdelning och en utbildad och övad organisation för drift och förvaltning.

Syftet med vägledningen är att ge konkreta råd för nybyggnation och utveckling samt drift och förvaltning av ledningsplatser med målsättningen att aktörer med samhällsviktig verksamhet ska få ökad förmåga att samverka och leda över hela hotskalan. Sådan verksamhet behöver teknik och lokaler som är robusta och fungerar utan avbrott även i en störd miljö och där hanterad information skyddas utifrån behov av sekretess. Vägledningen grundar sig i MSB:s uppdrag att stödja offentliga aktörers arbete med att stärka sin förmåga att verka från ordinarie och alternativ ledningsplats.

För att arbetet med ledningsplatser ska bli effektivt är det av stor vikt att vägledningen och dess innehåll är känt i verksamheten. Ett flertal befattningar behöver vara engagerade i arbetet förutom den "ledningsplatsansvarige". Exempel på kompetensområden som kan beröras är verksamhetsledning, ledningsorganisation (stab), kontinuitetshantering, civilt försvar, säkerhets-skydd, informationssäkerhet, it-drift, signalskydd, samband, arbetsmiljö, miljö, upphandling, logistik samt drift, förvaltning och utveckling av fastigheter och tekniska fastighetssystem.

Vägledningen är generellt skriven för att kunna användas på alla nivåer i ledningsstrukturen. Den ska också kunna användas både vid utveckling av befintliga som vid planering och anskaffning av nya ledningsplatser.

Inledningsvis beskrivs ett antal analysmetoder som verksamheten kan använda för att identifiera åtgärder som behöver vidtas för att säkerställa en kontinuerlig och uthållig ledningsförmåga. Analyserna tar sin utgångspunkt i verksamheten och den omvärld verksamheten ska kunna verka i där hot, sårbarheter och risker måste identifieras och hanteras.

Därefter beskrivs ett antal framgångsfaktorer för ledningsplatsverksamhet. Det handlar ytterst om att låta ledningsplatsen få status som en viktig och integrerad del i verksamhetens ledningsförmåga och att den behöver förvaltas och utvecklas över tid för att vara funktionsduglig. Allt arbete behöver präglas av en helhetssyn där förståelse för ledningsplatsens tekniska uppbyggnad med krav på robusthet är grundläggande men också av ett arbetssätt där övriga kravställningar på ledningsplatsen drivs av samtliga inblandade intressenter, inte minst den organisation som ska använda ledningsplatsen.

Vägledningens sista del beskriver övergripande strukturen för ledningsplatser på olika ledningsnivåer i samhället och definierar begrepp som ordinarie och alternativ ledningsplats. Här återfinns också information om hur ledningsplatsen kan utformas ur olika aspekter – byggnadstekniskt, tekniska försörjningssystem och tekniska system för samverkan och ledning. Vidare redovisas framgångsfaktorer för driften och förvaltningen av ledningsplatsen.

Vägledningen fokuserar på kontinuitetshöjande åtgärder i ledningsplatser som ska resultera i en höjd ledningsförmåga hos aktörerna. I vissa verksamheter kommer en analys att påvisa liknande kontinuitetshöjande behov inte bara för verksamhetens ledning utan också för organisationens kärnverksamhet. Även i dessa fall kan vägledningen användas i tillämpliga delar.

Utformningen av en ledningsplats styrs till del av tvingande kravställningar, exempelvis genom Boverkets byggregler, Arbetsmiljöverkets författningar eller Säkerhetspolisens föreskrifter om säkerhetsskydd. Vidare kan det förekomma ledningsplatsrelaterade åtgärder som verksamheten har krav på sig att uppfylla genom regleringsbrev eller för att kunna äska statliga bidrag inom området. Därutöver finns ett antal åtgärder som erfarenhetsmässigt behöver genomföras för att säkerställa robusthet, säkerhet och uthållighet. Löpande återfinns i vägledningen checklistor där ledningsplatsrelaterade kravställningar och behov lyfts fram. Checklistorna kan användas som ett stöd vid de krav- och behovsanalyser som verksamheten måste genomföra för att kunna ta hänsyn till lokala förutsättningar. Därutöver finns ett antal ”Läs mer-rutor” där hänvisningar finns till referensmaterial, publikationer och hemsidor där det går att hitta ytterligare information i ämnet.

Vägledningen innehåller inga kompletta och detaljerade tekniska projekteringsanvisningar utan informationen hålls på en övergripande nivå.

Då vägledningen är generellt skriven och ses som ett övergripande dokument kommer den vid behov att kompletteras med specifika dokument för olika aktörer och målgrupper. De återfinns på MSB:s hemsida tillsammans med annan ledningsplatsrelaterad information.



Läs mer

- www.msb.se sök Ledningsplatser

Det sårbara samhället

Vid planering av all verksamhet finns en mängd beroenden och påverkansfaktorer som måste identifieras och tas hänsyn till. Det samma gäller när samverkan och ledning ska möjliggöras från en ledningsplats. Nedanstående områden är exempel på ingångsvärden som regelbundet behöver beaktas och analyseras i samband med ledningsplatsverksamhet.





Naturhot och oavsiktliga hot

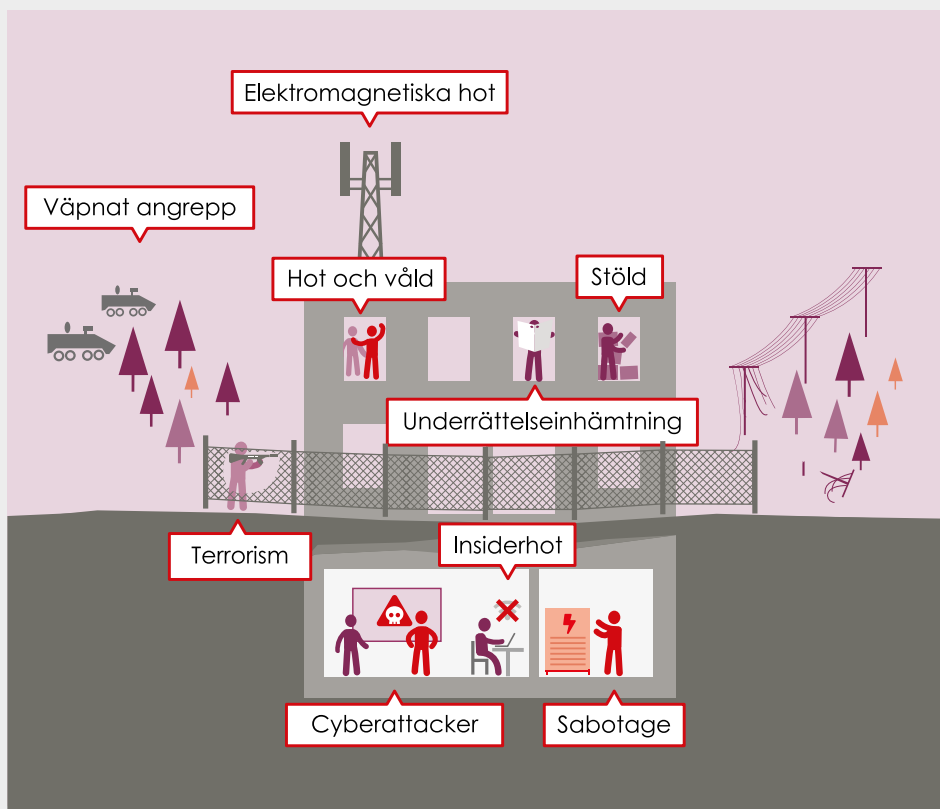
Exempel på frågeställningar

Naturhot

- Åska, statisk elektricitet – hur skyddas byggnad, elektrisk och elektronisk utrustning?
- Storm, skogsbränder, stora snömängder, jordskred – kan detta påverka verksamheten?
- Närliggande vattendrag, kraftiga regn – finns risk för inträngande vatten?
- Biologiska hot
- Pandemier, epidemier, influensa och epizootier – hur säkerställs personalförsörjningen?

Olyckor

- Brand – finns brandsektionering, brandlarm och brandsläckanläggning?
- Trasigt vätskesystem – kan innehållet skada tekniska system? Finns fuktalarm?
- Gasutsläpp utanför lokalerna – finns gasdetektering? Kan ventilationen snabbt stängas av eller kan inkommande luft filtreras?
- Industriverksamhet eller transport av farligt gods i närheten – kan en olycka påverka verksamheten?
- Oavsiktliga avbrott i teknisk infrastruktur och försörjningssystem
- Avbrott i infrastruktur för vatten, avlopp, fjärrvärme, el, tele och datakommunikation – finns redundanta system eller andra kontinuitetsåtgärder för att klara av uppkomna avbrott?
- Utebliven bränsleförsörjning – vilken egen lagringsvolym finns? Finns alternativ leverantör?



Antagonistiska hot

Exempel på frågeställningar

- Kriminella hot – exempelvis inbrott, stöld, dataintrång, överfall, skadegörelse och sprängningar.
- Främmande underrättelseverksamhet – består av främmande stater, organisationer och personer som är beredda att använda våld, spionera eller begå andra brott för att orsaka skador på det skyddsvärda i samhället och komma över känsliga uppgifter.
- Gråzonsproblematik – antagonistisk gråzonsstrategi används i syfte att försöka vinna något utan att provocera försvararen till att reagera kraftfullt och eskalera konflikten. Det handlar om aktiviteter som riktas mot hela samhället och utnyttjar olika medel för att uppnå politiska målsättningar eller för att skapa gynnsamma förutsättningar för ett framtida militärt agerande. Medel för att möta gråzonsaktiviteter kan vara cyberförsvar, robust infrastruktur, redundanta samhällsfunktioner, fysiskt skydd och psykologisk försvar.
- Höjd beredskap och krig – För närvarande präglas det globala säkerhetspolitiska läget av instabilitet och oförutsägbarhet. Utvecklingen är svårbedömd och stundtals snabb. Det kan inte uteslutas att militära maktmedel eller hot om sådana kan komma att användas mot Sverige. Målbilden för totalförsvaret är att Sverige ska, under minst tre månader, kunna möta och hantera en säkerhetspolitisk kris i Europa och närområdet som leder till allvarliga konsekvenser för samhällets funktionalitet.



Läs mer

- Säkerhetspolisen: Introduktion till säkerhetsskydd
- Säkerhetspolisen: Årsböcker
- MUST: Årsöversikter
- FRA: Årsrapporter
- FOI-rapport 6338 Typfall 5: Gråzonsproblematik
- FOI-rapport 4769 Civilt försvar i gråzon
- FOI-rapport 4959 Samverkan och ledning i gråzon
- FOI-rapport 5089 Hotbildsunderlag i utvecklingen av civilt försvar
- Sverige kommer att möta utmaningarna, en gemensam grundsyn
- www.msb.se sök Civilt försvar

Utvecklingen i samhället

Digitalisering

Den digitala utvecklingen går fort framåt. Den skapar nya och förändrade informationsflöden vilket bland annat leder till behov av nya arbetsmetoder och säkerhetsåtgärder. Med utvecklingen följer stora möjligheter men också utmaningar. It-system och infrastrukturer blir alltmer avancerade, komplicerade och integrerade vilket skapar sårbarheter och beroenden. I och med specialisering och globalisering utförs och tillhandahålls it-relaterade tjänster ofta av upphandlade entreprenörer på olika håll i världen. Det kan röra sig om till exempel utveckling av it-system, outsourcing av drift, molntjänster eller konsulttjänster för drift och förvaltning av it-tjänster i organisationens egna lokaler. Digitaliseringen påverkar både möjligheterna och förutsättningarna för bedrivandet av ordinarie verksamhet och för den verksamhet som behöver upprätthållas under kris och krig. Detta ställer särskilda krav på det egna informationssäkerhetsarbetet särskilt med avseende på informationsklassning och riskanalys. Det ställer också särskilda krav på upprätthållande av egen beställarkompetens gentemot olika leverantörer av it-tjänster och mjuk- och hårdvarukomponenter. Vid utformningen av ledningsplatser behöver krav ställas på infrastruktur vad gäller data och it-försörjning såsom flera olika kommunikationsvägar in (redundanta med geografisk diversitet) med tillgång till robusta och säkra nätverk för elektroniska kommunikationer. Dessa krav behöver följas upp och utvärderas kontinuerligt.



Läs mer

- www.informationssakerhet.se
- MSB: Årsrapporter om it-incidentrapportering

Cyberfysiska system och fastighetsautomation

I takt med ökad digitalisering ökar också uppkoppling och automatisering av maskiner, fordon och fastighetsinstallationer. Cyberfysiska system är ett samlat begrepp för dessa olika typer av uppkopplade system som på olika sätt känner

av, mäter eller interagerar med den fysiska verkligheten. Det kan röra sig om utrustning i form av exempelvis olika mätinstrument, sensorer och styrdon. Idag blir informations- och styrsystem mer automatiserade och är ibland sammankopplade med internet och andra publika nätverk för att uppnå ökad flexibilitet. Det blir även vanligare att koppla system för fastighetsautomation till andra egna nätverk och system för att ha tillgång till olika slags data för t.ex. värme, kyla och ventilation, samt att göra styrningen mer centraliserad, automatiserad och tillgänglig på distans.

Sensorer som ansluts till exempelvis fastighetsinstallationer har ibland begränsad förmåga att hantera bortfall av ordinarie strömförsörjning. Erfarenhetsmässigt har också smarta internetuppkopplade enheter ibland visat sig ha en relativt låg säkerhet i sina grundinställningar och konstruktion. Haverier i byggnaders styr- och övervakningssystem beroende på komponentfel, bristfällig implementation eller cyberattacker kan få omedelbar påverkan på möjligheten att bedriva verksamhet eller på olika sätt hota informationssäkerheten. Ledningsplatsen behöver därför vara utrustad med robust utrustning samt utformad för att kunna motstå externa störningar i exempelvis sensorerna som sådana, men även i de el- och kommunikationsnätverk som antingen upprätthåller eller upprätthålls av uppkopplade sensorer och styrdon. Som alternativ ska förmåga finnas att styra systemen manuellt vilket kräver tydlig dokumentation och instruktioner för handhavande.



Läs mer

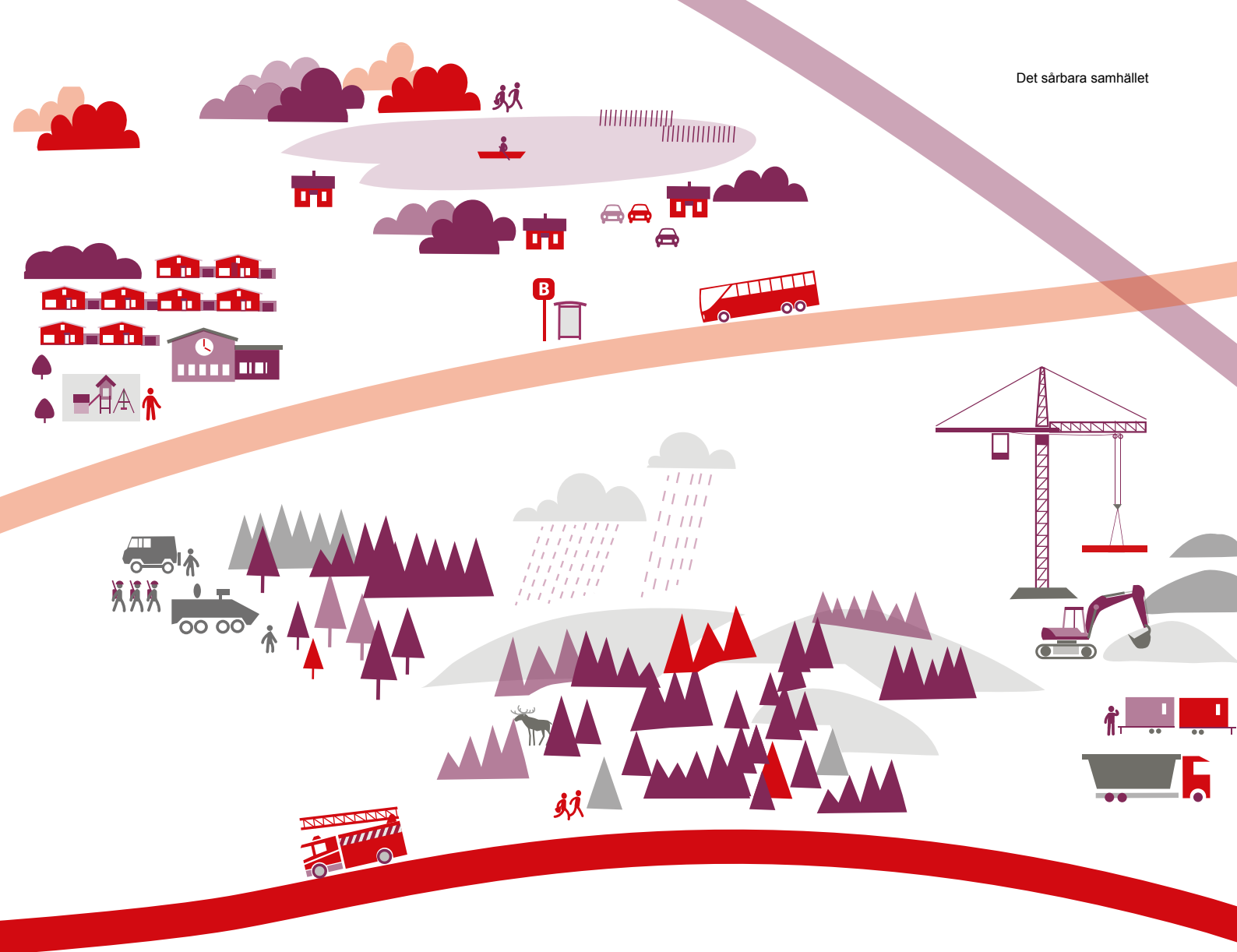
- MSB718 Vägledning till ökad säkerhet i industriella informations- och styrsystem

Beroendet av externa leverantörer

Samhällsviktiga verksamheter är idag beroende av många olika leverantörer för varor, tjänster, drift och felavhjälpning. Dessa beroenden kan medföra risker som är relaterade till leverantörernas förmåga att leverera varor eller tjänster i vardag, i kris och i krig om inte behovet av robusthet särskilt beaktas i upphandlingen. Dessutom ökar antalet gränssytor mellan beställare och utförare, vilket ökar komplexiteten som i sin tur kan påverka funktionssäkerheten.

Beroendet till olika digitala leveranskedjor (de leverantörer och infrastrukturer som levererar mjuk- och hårdvarukomponenter, tjänster och information vilka används för att upprätthålla en verksamhets informationshantering och informationssystem) är idag särskilt påtagligt och riskerna kring dessa måste identifieras och hanteras. Incidenter i digitala leveranskedjor kan få direkt påverkan på den egna verksamhetens förmåga. Det kan också uppstå svårigheter kring att få information om och förhålla sig till incidenter om rapporteringen mellan leverantörer och beställare brister till följd av oklara avtal eller att rapporteringen inte är inövad.

Dessa risker gör att ett antal krav behöver ställas vid upphandling och på ledningsplatsens funktioner, t.ex. standardisering av tekniska system, it-försörjning, uthållighet, fysiskt skydd samt drift och underhåll.



Läs mer

- MSB1275 Upphandling till samhällsviktig verksamhet
- MSB: Årsrapport 2020 över NIS-leverantörers it-incidentrapportering

Försörjningsberedskap

Försörjningen med varor är idag uppbyggd bland annat med just-in-time-principen, som bland annat lett till färre varor i produktions- och återförsäljarleden, och att en stor del av dessa varor finns ute på vägarna eller till sjöss. Ett annat exempel är globaliseringen med komplexa varuflöden och komponentberoenden. Dessutom är logistikflödena beroende av fungerade digitala kommunikationslösningar samt drivmedels- och elförsörjning. Med denna bakgrund behöver bland annat drivmedels- och reservdelsförsörjningen samt försörjning av digitala resurser som mjukvara, uppdateringar och data till ledningsplatserna säkerställas.

Ledningsplatsen – en del av kontinuitetshanteringen

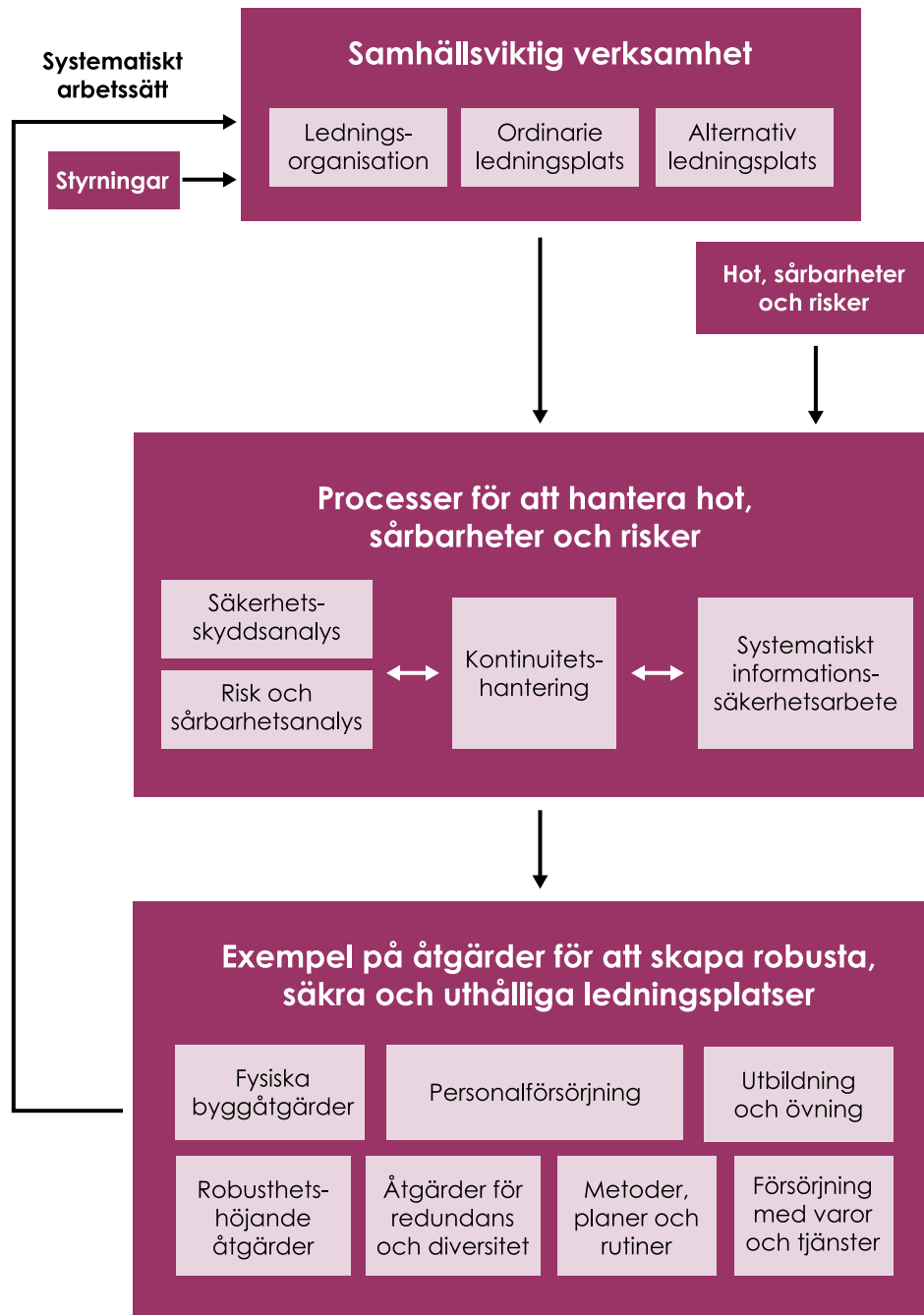
En verksamhet påverkas alltid av den omvärld som den verkar i. För att kunna hantera denna påverkan behöver hot, sårbarheter och risker regelbundet analyseras och resultaten användas för att utveckla verksamheten. Med detta arbetsätt finns förutsättningar att skapa kontinuitet i verksamheten – även om den utsätts för påverkan utöver det vanliga.

Att skapa en robust, säker och uthållig ledningsplats

Bilden nedan är ett exempel på hur en verksamhet kan arbeta med sina ledningsplatser. Verksamheten med dess organisation, uppdrag och processer är samhällsviktig och ska kunna samverka med andra aktörer och leda sin egen verksamhet över hela hotskalan. Kompetens finns bland annat för att handlägga frågor kring riskhantering, civilt försvar, säkerhetsskydd, it-säkerhet, signal-skydd, ledningsplatser och fastigheter. För att lösa uppgiften att kontinuerligt kunna samverka och leda över hela hotskalan finns en utbildad och övad ledningsorganisation (stab) med stödfunktioner (betjäningsorganisation) och med arbetsmetoder, rutiner och planer. Ledningen ska kunna utövas från en ordinarie och minst en alternativ ledningsplats.

Verksamheten bedriver ett systematiskt arbete för att identifiera hot, sårbarheter och risker för att på så sätt säkerställa kontinuitet. Kontinuitetshanteringsarbetet genomförs med målsättningen att ordinarie och alternativ ledningsplats är;

- Robust – d.v.s. att ledningsplatsens personal, lokaler och tekniska system tål de störningar som kan förväntas. Några exempel på robusthetshöjande åtgärder är fysiskt skydd av lokaler, filtrering av inkommande luft, geografiskt divergerande anslutningar till externa el- och kommunikationsnät, säkerställd personalförsörjning samt rutiner och utbildning för driftsättning av redundanta tekniska system.
- Säker – d.v.s. att det som är skyddsvärt i ledningsplatsen såsom personal, information och utrustning förblir opåverkade av de störningar som kan förväntas. Denna säkerhet kan exempelvis nås genom tillträdesskydd, inbrottslarm, brandsläckutrustning, it-säkerhetsåtgärder, upphandling av entreprenörer med SUA samt utbildning i säkerhetsskydd.
- Uthållig – d.v.s. att ledningsplatsens personal och tekniska system kan verka kontinuerligt under planerad tid. Uthållighet kan exempelvis nås genom en anpassad arbetsmiljö, säkerställd försörjning av dricksvatten, livsmedel, drivmedel och reservdelar samt planer för personalomsättning.



Figur 1. Att skapa robusta, säkra och uthålliga ledningsplatser

Ingångsvärden

Hot, sårbarheter och risker

I kapitel 2 – Det sårbara samhället, finns en samställning över hot som kan påverka en aktörs förmåga att samverka och leda. Utöver hotet från antagonister och främmande makter finns en mängd hot av biologisk art, hot av naturkrafter samt olyckor skapade av människan. Vidare skapar företeelser i det moderna samhället såsom privatisering, teknikutveckling och ökad internationalisering nya möjligheter och utmaningar.

Styrning av verksamheten

Verksamheten styrs av externa författningar såsom lagar, förordning och föreskrifter, de grundläggande principerna ansvars-, närhets- och likhetsprinciperna samt andra styrande dokument. Offentliga aktörer styrs exempelvis av lagar och förordningar om totalförvar och höjd beredskap, föreskrifter för risk- och sårbarhetsanalyser samt informationssäkerhet.

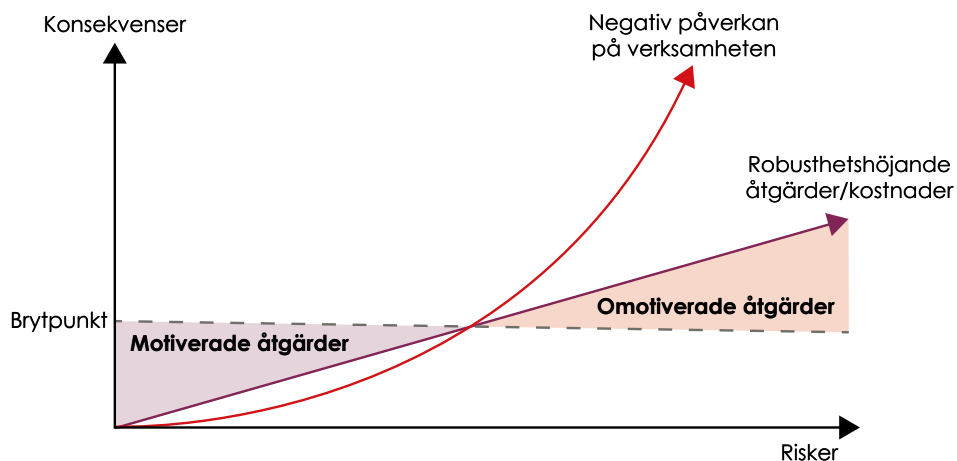
För samhällets styrning av utvecklingen av civilt försvar tar MSB i samarbete med Försvarsmakten fram en sammanhängande planering för området som tar sin utgångspunkt i och koordineras på nationell nivå med den militära försvarsplaneringen.



Läs mer

- www.msb.se sök Civilt försvar

En avgörande faktor i styrningen av verksamhetens arbete med att hantera risker är omfattningen av de ekonomiska medel som avsätts för arbetet. Diagrammet nedan beskriver förhållandet mellan risker, nytta och kostnader i ny- och ombyggnadsprojekt där olika typer av risker ska hanteras. Det kan användas som ett diskussionsunderlag inför projekt när omfattningen, och därmed kostnaden, för de robusthetshöjande åtgärderna ska bestämmas. Diagrammet beskriver hur risker kommer att, om de realiserats, leda till konsekvenser för verksamheten. Det beskriver också effekten av att vidta robusthetshöjande åtgärder. För ett antal risker kommer de åtgärder som vidtas att ha effekt och konsekvenserna för verksamheten minskar eller uteblir (motiverade åtgärder). För ytterligare ett antal risker kommer vidtagna åtgärder inte att kunna hantera den negativa påverkan och dess konsekvenser (omotiverade åtgärder). Att identifiera brytpunkten där det trots vidtagna åtgärder kan bli stora konsekvenser för verksamheten blir alltså ett sätt att fastställa omfattningen av motiverade åtgärder. De risker som inte kan hanteras kan utgöra underlag för att identifiera behov av ytterligare åtgärder, exempelvis behov av alternativ ledningsplats.



Figur 2. Risker, nytta och kostnader i ny- och ombyggnadsprojekt

Aktörer som har till uppgift att samverka och leda gör detta i ett större sammanhang, tillsammans med andra och aktörsgemensamt. I syfte att skapa ett gemensamt förhållningssätt för samverkan och ledning vid kriser som berör flera aktörer och verksamheter finns publikationen *Gemensamma grunder för samverkan och ledning vid samhällsstörningar*. Grunderna ska bidra till att aktörer över hela landet och på alla nivåer i ledningsstrukturen har ett gemensamt arbetsätt vid samhällsstörningar. Att organisera arbetet att samverka och leda sin verksamhet vid samhällsstörningar på ett likartat sätt underlättar för aktörerna att förstå varandra, samordna sig och ta fram en gemensam inriktning för hur störningen ska lösas.



Läs mer

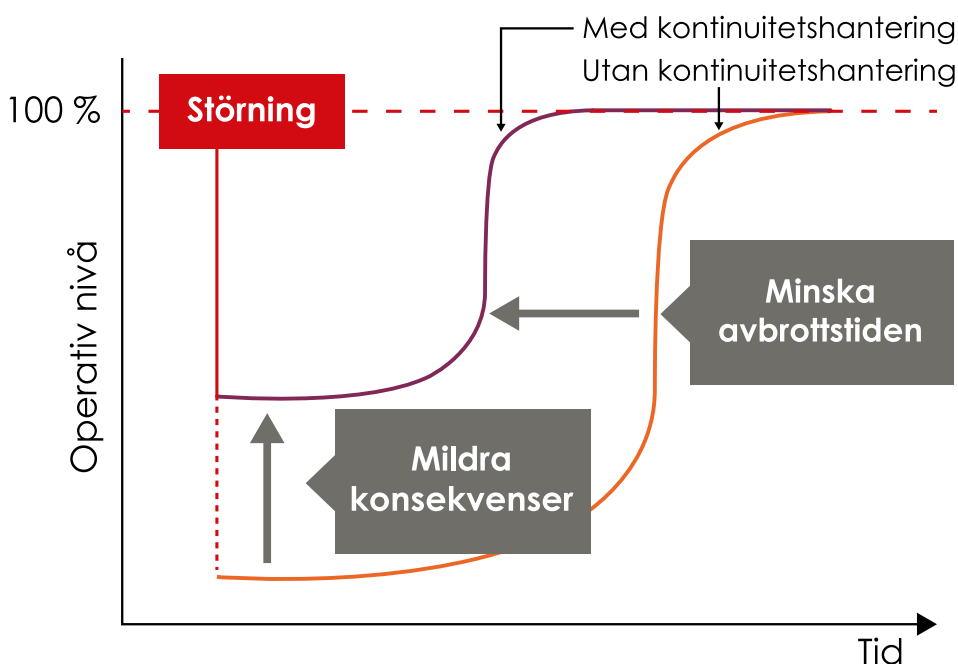
- MSB777 Gemensamma grunder för samverkan och ledning vid samhällsstörningar

Hantera hot, sårbarheter och risker

Kontinuitetshantering

En robust, säker och uthållig ledningsplats är en viktig del i en verksamhets ledningsförmåga. Kontinuitetshantering är en metod som bidrar till att säkerställa ledningsplatsens funktionalitet. Arbetet med kontinuitetshantering behöver kompletteras och kombineras med andra metoder och verktyg såsom risk- och sårbarhetsanalys, säkerhetsskyddsanalys och systematiskt informationssäkerhetsarbete.

Kontinuitetshantering handlar om att planera för att upprätthålla sin verksamhet och ledningsförmåga på en tillräcklig nivå, oavsett vilken störning den utsätts för. Med rätt förutsättningar kan ledningsförmågan upprätthållas eller konsekvenserna av en inträffad händelse mildras vilket innebär kortare störningsperioder i verksamheten.



Figur 3. Kontinuitetshantering

Genom att analysera vilka krav som ställs på verksamheten kan brister och sårbarheter som behöver åtgärdas identifieras och prioriteringar göras. Sårbarheter kan vara både organisatoriska och tekniska. I sin enklaste form utgår kontinuitetshandling från en kartläggning av verksamhetens kritiska aktiviteter där konsekvenserna av ett bortfall av dessa analyseras samt dess beroenden av olika resurser som t.ex. personal, el, värme, vatten, informationssystem samt olika former av fastighetstekniska installationer och förbrukningsvaror. Därefter införs åtgärder som minskar risken för störningar och planer upprättas för hur de störningar som ändå kan uppstå ska hanteras.

För att bäst identifiera behov av prioriteringar måste kontinuitetshandling av ledningsplatser genomföras i dialog med olika intressenter. Exempel på intressenter förutom representanter för verksamheten är ansvariga för beredskap, säkerhet, fastighet, upphandling, tekniskt sakkunniga, representanter för drift- och underhållsorganisationer samt leverantörer. Det är viktigt att alla inblandade får klart för sig ledningsplatsens betydelse och att robusthet, säkerhet och uthållighet utgör grunden för verksamheten. Utöver befintlig redundans (t.ex. reservlösningar) för de identifierade resurserna behöver åtgärdsförslag tas fram som syftar till att

- minska sannolikheten för störningar
- minska tiden för störningar
- mildra konsekvenserna av störningar.

Checklistan nedan är en sammanställning av exempel på ledningsplatsrelaterade åtgärdsbehov från ett arbete med kontinuitetshandling;

Checklista

- ✓ Behov av åtgärder för att höja ledningsplatsens fysiska robusthet.
- ✓ Behov av robusta sambands- och försörjningssystem.
- ✓ Behov av åtgärder för att säkerställa verksamhetens uthållighet.
- ✓ Plan för utbildning och övning i driftsättning av ledningsplatsen.
- ✓ Rutiner för verksamheten vid arbete i ledningsplatsen.
- ✓ Redundant tillgång till nyckelpersonal för drift och underhåll.
- ✓ Robusta avtal med leverantörer av varor såsom mat, drivmedel, reservdelar och it-komponenter samt tjänster såsom driftentreprenörer för att säkerställa leveranser över tid. Vid behov har alternativa leverantörer upphandlats.
- ✓ Behov av förrådshållning av kritisk förbrukningsmateriel och reservdelar.
- ✓ Behov av tillsyn, funktionsprov och underhåll av ledningsplatsen.
- ✓ Tillgång till alternativ ledningsplats.

MSB har samlat en verktygslåda med metodstöd inklusive en webbkurs för kontinuitetshandling. Metodstödet kan med fördel användas såväl för aktörens övergripande arbete med kontinuitetshandling som för mer detaljerade behovsanalyser inför utveckling och förvaltning av ledningsplatser.

**Läs mer**

- www.msb.se sök Kontinuitetshantering

Risk- och sårbarhetsanalys enligt förordningen

Som en del av riskidentifieringen för ledningsplatsverksamheten genomför aktörer en risk- och sårbarhetsanalys (RSA) där bland annat samhällsviktig verksamhet identifieras och kritiska beroenden kartläggs. I RSA-arbetet ingår att identifiera vilka oönskade händelser som kan påverka ledningsplatsen och dess verksamhet samt en bedömning görs hur troligt det är att händelserna inträffar. Därefter bedöms omedelbara negativa konsekvenser och slutligen analyseras verksamhetens sårbarheter liksom dess förmåga att hantera olika påfrestningar.

**Läs mer**

- MSB245 Vägledning för risk- och sårbarhetsanalyser
- MSB1178 Vägledning för risk- och sårbarhetsanalys avseende antagonistiska elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur

Systematiskt informationssäkerhetsarbete

Arbetet med informationssäkerhet handlar om att ta ett helhetsgrepp och skapa ett fungerande långsiktigt arbetssätt för att ge verksamhetens information det skydd den behöver. Arbetet omfattar att införa och förvalta administrativa regelverk såsom policys och riktlinjer, tekniskt skydd med bland annat brandväggar och kryptering samt fysiskt skydd med till exempel skal- och brandskydd. Vilka säkerhetsåtgärder som ska skydda information utifrån dess behov av skydd för konfidentialitet, riktighet och tillgänglighet behöver analyseras för varje verksamhet, också för den verksamhet som kommer att bedrivas på ledningsplatsen.

Information som hanteras på en ledningsplats kan vara både fysisk och digital. Det är viktigt att identifiera den information som kommer att hanteras, klassa informationen och bedöma risker med informationshanteringen, helst innan ledningsplatsen tas i bruk.

Information som till exempel lägesbilder, organisation och kontaktvägar visas ofta överskådligt i lokalerna och ska då kunna släckas ner eller döljas vid eventuella besök. Även muntlig information innefattas av informationssäkerhet och det kan finnas behov av att kunna dela information med endast ett begränsat antal deltagare.

För att kunna arbeta effektivt behöver verksamheten också kunna hantera information digitalt och via elektronisk kommunikation. Hanteringen behöver skyddas av it-säkerhetsåtgärder men också av rutiner som användarna behöver för att kunna hantera information och it-system rätt.

It-säkerhet är en del av informationssäkerheten där man fokuserar på olika tekniska säkerhetsåtgärder. Exempelvis kan data som behöver skyddas placeras på lokala servrar i ett slutet nät. Dessa servrar behöver skyddas med fysiska och logiska tillträdesbegränsningar och placeringen av serverutrymmet tas i

beaktning (fysisk säkerhet). Tillträdesbegränsningar till nätverksutrustning och serverutrymme ses över (informations- och personalsäkerhet). Ett annat exempel är hur behörigheten till olika nätverk och informationssystem styrs för olika personalgrupper, såväl i egen organisation som för besökare och samverkande personal.

Infosäkkollen, ett verktyg för systematiskt informationssäkerhetsarbete framtaget av MSB, kan nyttjas för att utvärdera och följa upp de arbetssätt som används för att skapa en god informationssäkerhet.

Denna sammanställning ger exempel på ledningsplatsrelaterade åtgärdsbehov från analyser ut ett informationssäkerhetsperspektiv;

Checklista

Teknisk infrastruktur

- ✓ Viktiga verksamhetssystem har redundans.
- ✓ Externa och interna förbindelsevägar samt kopplingspunkter skyddas mot sabotage och annan åverkan.
- ✓ Redundant el- och kylförsörjning finns till teknikutrymmen.
- ✓ Styrsystem för den tekniska infrastrukturen i ledningsplatsen är motståndskraftiga mot it-attacker.
- ✓ Åtgärder för skydd mot elektromagnetiska hot är genomförda.
- ✓ Åtgärder för brandskydd är genomförda.
- ✓ Åtgärder för att förhindra skador av inträngande vatten i teknikutrymmen är genomförda.
- ✓ Driftlarm finns på den tekniska infrastrukturen.

Förvaltning/organisation

- ✓ Ansvar för informationssäkerhetsarbetet samt drift och underhåll av ledningsplatsens funktioner inklusive it-utrustningen är fördelat.
- ✓ Personal med rätt kompetens finns i tillräcklig omfattning.
- ✓ Information som hanteras i ledningsplatsen är identifierad och klassad utifrån behov av skydd (konfidentialitet, riktighet, tillgänglighet).
- ✓ Information som är nödvändig för att kunna samverka och leda under störda förhållanden är identifierad.
- ✓ Åtgärder för att kunna upprätta och dela känslig information är genomförda.
- ✓ Tillgång till kritiska reservdelar är tillgodosedd.
- ✓ Rutiner finns för hantering av driftlarm, underhåll och funktionskontroller.
- ✓ Rutiner för att hantera incidenter finns på plats.

Säkerhetsskydd och höjd beredskap

- ✓ Informationsmängder som omfattas av säkerhetsskyddslagstiftningen är identifierade med stöd av informationsklassning.
- ✓ Åtgärder att kunna upprätta och dela säkerhetsskyddsklassificerade uppgifter är genomförda.
- ✓ Åtgärder för att försvåra RÖS-spaning är genomförda.
- ✓ Åtgärder för att försvåra överhörning av samtal innehållande säkerhetsskyddsklassificerad information är genomförda.
- ✓ Förvaringsmöjligheter finns för skyddsvärd information och utrustning.

MSB har samlat metodstöd för informationssäkerhetsarbetet på webbplatsen informationssakerhet.se. Metodstödet baseras på de internationella standarder för informationssäkerhet SS-EN ISO/IEC 27000-serien vilket också gäller för Infosakkollen. Båda kan med fördel även användas som stöd i informations-säkerhetsarbetet, utöver den analys som behöver göras för ledningsplatsens funktion och säkerhet.



Läs mer

- www.informationssakerhet.se
- www.msb.se sök infosakkollen
- MSB629 Vägledning för fysisk informationssäkerhet i it-utrymmen

Säkerhetsskyddsanalys

En säkerhetsskyddsanalys genomförs för att klarlägga om det bedrivs verksamhet som är säkerhetskänslig med anknytning till ledningsplatsen. I samband med detta arbete kommer krav och förutsättningar att identifieras som krävs för att säkerhetsskyddet ska kunna upprätthållas på ledningsplatsen.

Det är verksamhetsutövaren i ledningsplatsen som ansvarar för säkerhetsskyddet och därmed säkerhetsskyddsanalysen som genomförs i syfte att besvara följande frågor;

- Bedrivs skyddsvärd och/eller säkerhetskänslig verksamhet?
- Mot vad ska den skyddas?
- Hur ska den skyddas?

I säkerhetsskyddsanalysen ska beaktas antagonistiska hot som spioneri, sabotage och terroristbrott samt andra brott som kan hota verksamheten och skada Sveriges säkerhet. Analysen ska identifiera och bedöma skyddsvärden utifrån ett konsekvensperspektiv, det vill säga utifrån hur allvarlig konsekvensen av en eventuell skada blir, istället för att fokusera på sannolikheten för att ett säkerhetshot realiseras. Identifieras säkerhetskänslig verksamhet omfattas denna av säkerhetsskyddslagen, vilket medför ytterligare ett antal krav. Exempelvis ska nödvändiga säkerhetsskyddsåtgärder planeras och genomföras med utgångspunkt i säkerhetsskyddsanalysen.

Därutöver kan annan skyddsvärd verksamhet och information identifieras som inte omfattas av säkerhetsskyddslagen men som måste hanteras på ett säkert sätt.

I säkerhetsskyddsanalysen ska särskilt tillträdeskontrollen till ledningsplatsen beaktas. Vilken personal ska ha tillträde till lokalerna? Vilken personal ska kunna tilldela behörighet? Behöver behörighet utökas eller tas bort utifrån enskilda händelsers behov? Särskilt beaktas eventuellt tillträdesbehov för personer utanför den egna organisationen såsom samverkande aktörer och förstärkningsresurser.



Läs mer

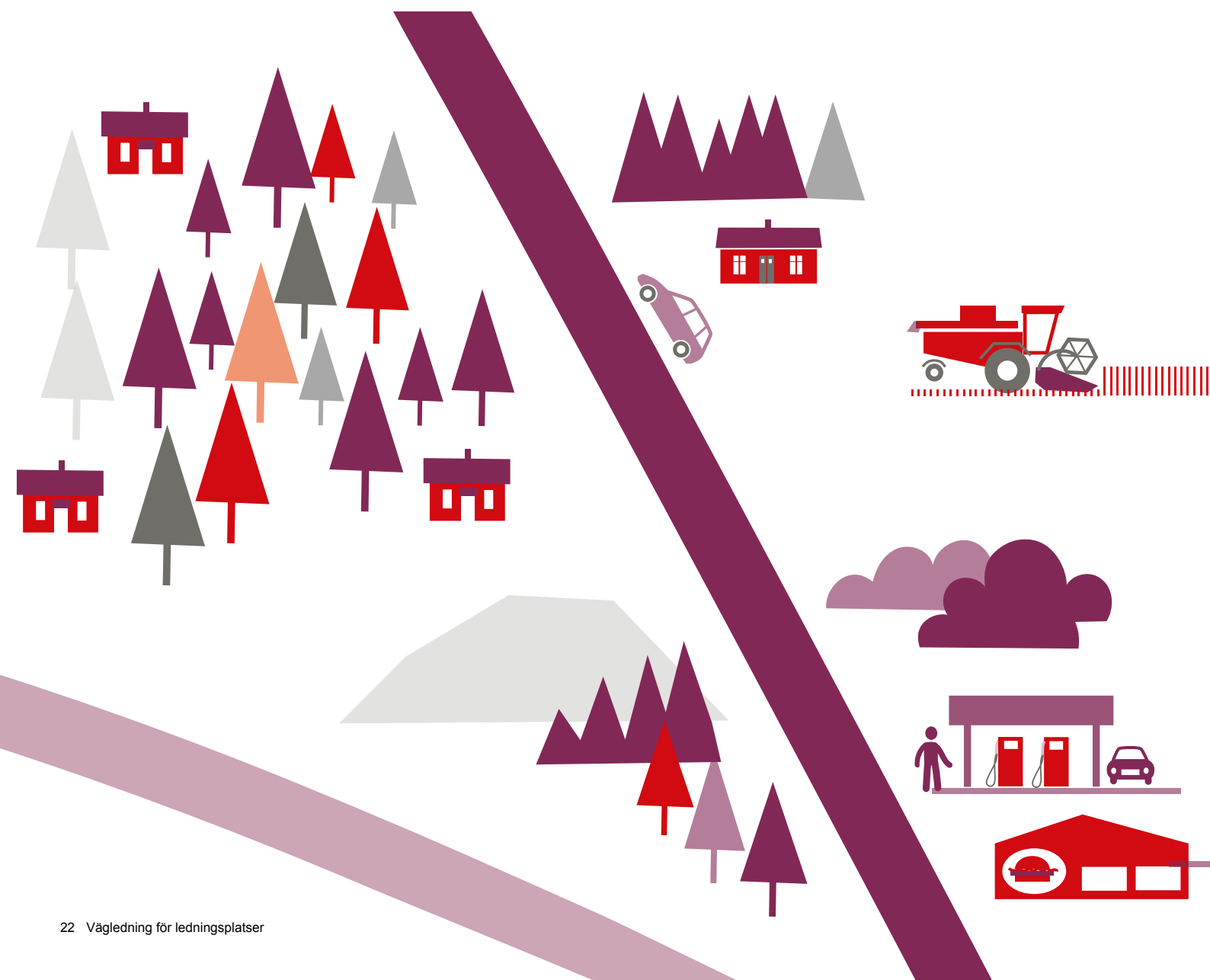
- Säkerhetspolisen: Vägledning i säkerhetsskydd – Säkerhetsskyddsanalys

När säkerhetsanalysen är genomförd krävs en översyn av klassning av den information som är knuten till ledningsplatsen. Offentlighets- och sekretesslagen (OSL 2009:400, vanligtvis 15 kap. 2 § ”försvarssekretess”, 18 kap. 8 § ”säkerhets- och bevakningsåtgärder” eller 18 kap. 13 § ”RSA-sekretess”) och Säkerhetsskyddslagen (2018:585) ligger till grund för bedömningen hur informationen ska klassificeras och hanteras. Resultatet av klassningen styr vilka regler och rutiner som ska gälla för informationshanteringen. Klassningen kan variera utifrån vilken händelse som ska hanteras i ledningsplatsen och behöver regelbundet ses över.



Läs mer

- Säkerhetspolisen: Vägledning i säkerhetsskydd – Informationssäkerhet
- Säkerhetspolisen: Vägledning i säkerhetsskydd – Introduktion till säkerhetsskydd
- Säkerhetspolisen: PMFS 2019:2



Med säkerhetsskyddsanalysens samtliga komponenter som grund skapas sen en så kallad säkerhetsskyddsplan som beskriver hur de identifierade skyddsvärdena ska skyddas mot specifika säkerhetshot. Säkerhetsskyddsplanen kan beskrivas som ett organiserat system bestående av defensiva åtgärder med syfte att skydda verksamhet och information som är av betydelse för Sveriges säkerhet.

Säkerhetsskyddsplanen kommer att kunna ställa krav på fysisk säkerhet som ska förebygga att obehöriga får tillträde till ledningsplatsen där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter samt att förebygga skadlig inverkan på ledningsplatsen.

Denna sammanställning som är hämtad ur Säpos vägledning för fysiskt skydd ger exempel på åtgärdsbehov som går att applicera på en ledningsplats;

Checklista

Utformning av den fysiska säkerheten

- ✓ Det finns en tydlig koppling mellan utformningen och vad den fysiska säkerheten ska skydda samt ur vilken aspekt det som ska skyddas är skyddsvärt.
- ✓ Utformningen är baserad på ifall den fysiska säkerheten ska skydda mot obehörigt tillträde och/eller mot skadlig inverkan.
- ✓ Den fysiska säkerheten har utformats utifrån vilka antagonistiska förmågor den ska klara av att skydda mot.

Principer för den fysiska säkerheten

- ✓ Lökrprincipen med flera lager av skydd har använts vid utformning av den fysiska säkerheten.
- ✓ Verksamheten har delats upp i olika fysiska sektioner enligt principen för sektionering.
- ✓ Det finns variation i den fysiska säkerheten som försvårar för en antagonist att med samma metod tränga igenom flera lager i skyddslöken.
- ✓ Information om säkerhetskänsliga delar av verksamheten och sårbarheter som kan hämtas via öppna källor eller fysisk/teknisk inhämtning har minimerats.
- ✓ Bebyggelseinriktad brottsprevention har använts vid utformning av byggnader och omgivning.
- ✓ Kritiska delar av den fysiska säkerheten har redundans.
- ✓ Behovet av skydd mot insiders har beaktats.

Upptäckande säkerhetsskyddsåtgärder

- ✓ Det finns personell bevakning och/eller teknisk övervakning för att så tidigt som möjligt upptäcka obehörigt tillträde och skadlig inverkan.
- ✓ Principer för upptäckande funktion har beaktats vid val av tekniska övervakningssystem.

Försvårande säkerhetsskyddsåtgärder

- ✓ Säkerhetsskyddsåtgärder för att fördröja obehörigt tillträde ger tillräcklig tid för att hinna vidta hanterande säkerhetsskyddsåtgärder.
- ✓ Det finns säkerhetsskyddsåtgärder för att reducera skadan av angrepp som inte går att fördröja.

Säkerhetsskyddsanalysen kan också påvisa om ledningsplatsen ska klassas som skyddsobjekt. Enligt Skyddslagen (2010:305) och Skyddsförordningen (2010:523) får länsstyrelse besluta att vissa typer av byggnader, anläggningar och områden ska vara skyddsobjekt. Bestämmelserna syftar framför allt till att ge ett ökat juridiskt skydd mot sabotage, terroristbrott, spioneri och grovt rån. Ett beslut om skyddsobjekt innebär vanligtvis att obehöriga inte har tillträde till objektet. Tillträdesförbudet kan också förenas med ett förbud att fotografera eller göra andra avbildningar av eller inom objektet.



Läs mer

- Säkerhetspolisen: Vägledning i säkerhetsskydd – Fysisk säkerhet

Förutom den fysiska säkerheten kommer säkerhetsskyddsplanen att ställa krav på säkerhetsaspekter inom;

- Informationssäkerhet – här beskrivs de åtgärder som identifierats i de systematiska analyser ur ett informationssäkerhetsperspektiv som beskrivs ovan. Det är genom den analysen en aktör identifierar om den hanterar säkerhetskänslig verksamhet/information och behöver beakta säkerhetsskyddslagen och dess förordningar. Åtgärderna ska förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, och förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet.
- Personalsäkerhet som ska förebygga att personer som inte är pålitliga ur säkerhetssynpunkt deltar i en verksamhet där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller i en verksamhet som av någon annan anledning är säkerhetskänslig, och säkerställa att de som deltar i säkerhetskänslig verksamhet har tillräcklig kunskap om säkerhetsskydd. Fysisk säkerhet kan nyttjas som en del av skyddet mot insiderhot, exempelvis genom sektionering och behörighetsstyrning. Men för ett fullgott skydd gentemot alla typer av antagonister, såväl externa som interna, behöver personalsäkerhet vara en integrerad del av säkerhetsarbetet.



Läs mer

- Säkerhetspolisen: Vägledning i säkerhetsskydd – Informationssäkerhet
- Säkerhetspolisen: Vägledning i säkerhetsskydd – Personalsäkerhet

Framgångsfaktorer för ledningsplatsverksamhet

En fungerande ledningsplats är avgörande för verksamhetens ledningsförmåga över hela hotskalan. I det här kapitlet redovisas ett antal framgångsfaktorer för att säkerställa att ledningsplatsen fyller sin funktion – när det behövs.

Säkerställ ledningens engagemang

Drift och förvaltning samt utveckling av en ledningsplats kräver att omfattande resurser avsätts för ändamålen. Det är därför viktigt att verksamhetens ledning har en hög medvetenhet kring de krav som ställs på ledningsförmågan och därmed på ledningsplatsen. Ledningen behöver säkerställa att nödvändiga finansiella och personella resurser finns för att kunna vidmakthålla och utveckla ledningsplatsen.

Ledningens ansvar för ledningsplatsverksamheten omfattar bl.a. att tillse att det finns förutsättningar att följa lagar och förordningar inom området, säkerställa personal- och kompetensförsörjningen, fastställa interna regler som beskriver ansvar och roller, säkerställa att kontinuitets- och riskarbetet fortlöper, fastställa beslutsunderlag för vidmakthållande och utveckling, samt att bidra till en god förmåga att hantera oönskade händelser genom övnings- och utbildningsverksamhet.

Säkerställ en lärande organisation

Inträffade oönskade händelser och incidenter är viktiga källor till utveckling och förbättring av såväl organisation, metodik och teknik. Organisatoriskt lärande där rapportering och att utreda orsaken till problem uppmuntras och att lärdomar från inträffade händelser tas till vara och omsätts till åtgärder för att förbättra verksamheten är viktigt. Det ska finnas enkla och tydliga processer och rutiner för utvärdering och erfarenhetsåterföring från inträffade incidenter och oönskade händelser när ledningsplatsen använts.

Låt robusthet genomsyra verksamheten

Vid ny- och ombyggnation av ledningsplatser och vid upphandling av leverantörer av varor och tjänster är behovsanalyser avseende robusthet centrala. Behovsanalyserna är också ett viktigt ingångsvärde till kontinuitetshanteringen som beskrivs tidigare i vägledningen. I behovsanalyserna behöver verksamheten ta

höjd för att den kan påverkas av störningar i olika grad. Behovet av robusthet ser olika ut i vardagen, vid en samhällsstörning och under krig och det är alltid scenariot med störst påverkan, normalt krig, som ska vara dimensionerande.

I behovsanalyserna är det viktigt att beakta krav, behov och önskemål från alla intressenter i ledningsplatsen. Involvering av drift- och underhållsorganisationen i behovsanalys och design av lösningar bidrar till att en optimal lösning väljs, allas kompetens ökar och att driftstarten förenklas.

Beakta robusthet vid upphandling

Inför en upphandling behöver en analys göras där lämpligheten i upphandlingen prövas. I analysen bör principer såsom leveranskrav och avbrottstider specificeras och utifrån detta kan en lämplighetsbedömning av upphandlingen göras. Om upphandlingen fortfarande anses vara lämplig finns då också en kravbild till avtalet framtagen.

I samband med upphandlingar av varor och tjänster behöver även robusthetsperspektivet beaktas. Avtalen behöver så långt det är möjligt säkerställa att leverantörerna har förmåga att upprätthålla leveranser av varor och tjänster över hela hotskalan och för 24/7-verksamhet. Exempelvis vid upphandling av entreprenör för drift- och underhåll av fastighetstekniska system bör avtalet innehålla tydliga krav på faktorer som ökar robustheten som exempelvis krav på kompetens, inställelsetider och felavhjälpningstider. Vid bedömning av leveransförmågan behöver flera aspekter beaktas som koncentration av produktion till enskilda geografiska områden, risk för störningar i leveranskedjor samt leverantörens åtaganden gentemot andra beställare. Krav kan ställas på att leverantörerna själva genomför egna riskanalyser och kontinuitetshantering.

Ett område där tillgänglighet och driftsäkerhet särskilt måste analyseras och kravställas vid upphandling är området it och telefoni där ofta flera olika leverantörer bidrar med fysisk infrastruktur och tjänster. Avseende den fysiska infrastrukturen är flervägsanslutningar, dvs. anslutning av kommunikationsförbindelser till flera externa tekniknoder anslutna med geografisk skilda och fysiskt säkra kabelvägar en viktigt robusthetshöjande åtgärd. I detta sammanhang måste överlämningspunkter definieras och ansvarsförhållanden klargöras. SLA:er (service level agreements) kan användas för att definiera tillgänglighet och kvalitet på tjänster.

Om upphandling av en tjänst innebär att leverantören kommer att få åtkomst till verksamhet eller informationstillgångar som omfattas av Säkerhetsskyddslagen ska upphandlingen genomföras med så kallat säkerhetsskyddsavtal (SUA).



Läs mer

- MSB1275 Upphandling till samhällsviktig verksamhet
- MSB1693 Den robusta sjukhusbyggnaden – kap 18 It, telefoni och Rakel
- Säkerhetspolisen: Vägledning i säkerhetsskydd – säkerhetsskyddad upphandling

Proaktivitet och engagemang vid ny- och ombyggnation

Ny- och ombyggnationer av ledningsplatser drivs normalt i projektform. Arbetet är ofta omfattande och resurskrävande och ställer stora krav på beställande aktör. Nedan beskrivs ett antal faktorer som bidrar till att ledningsplatsprojekt kan genomföras framgångsrikt.

Gör tidigt en informationsklassning och säkerhetsskyddsanalys för att identifiera vad som hanteras i projektet som är skyddsvärt och på vilket sätt. Visar resultatet att verksamheten berörs av Säkerhetsskyddslagen tas en säkerhetsskyddsplan fram som redovisar vilka åtgärder som behöver vidtas för att säkerställa att inga skyddsvärden röjs eller går förlorade. Exempel på åtgärder är att entreprenader ska upphandlas med säkerhetsskyddsavtal (SUA) samt att rutiner skapas för projektets informationshantering.

Säkerställ tillgång till personella resurser som ska representera beställande verksamhet vid behovsanalys samt vid planering och genomförande av projektet. För att minimera avvikelser under genomförandet och uppnå önskad funktionalitet på ledningsplatsen krävs en engagerad beställare.

Vid genomförande av behovsanalysen är det viktigt att samla personer med olika kompetens och erfarenheter för att få en så heltäckande analys som möjligt. Nedan ges exempel på perspektiv som bör vara representerade i en analysgrupp.

- Verksamhetsperspektivet som handlar om att upprätthålla samhällsviktig verksamhet. Ledningsplatsen betraktas här som en av flera kritiska komponenter i verksamhetens ledningsförmåga och blir därmed en del i kontinuitetshanteringen.
- Hotperspektivet som tar utgångspunkt i det skyddsvärda. Fokus ligger här på åtgärder som exempelvis skydd mot inbrott, tillträdesbegränsning, teknisk övervakning och åtgärder för att skydda informationstillgångar.
- Teknikperspektivet som tar utgångspunkt i fastighetens konstruktion, tekniska systems robusthet samt förutsättningar för drift och förvaltning.

I projektgruppen finns vanligen ansvariga med fokus på särskilda sakområden som arbetsmiljö, säkerhetsskydd, informationssäkerhet och miljöfrågor. En framgångsfaktor är att på samma sätt tillsätta en person som ansvarig för att bevaka robusthetsfrågor under hela projektet.

Nybyggnations- och utvecklingsprojekt innebär många beslut och det kan uppstå målkonflikter. En vanlig målkonflikt är den mellan projektkostnad och förvaltningskostnad. Besparingar i projektet blir inte sällan fördyrande i förvaltningsskedet, särskilt då ändringar kan komma att behöva göras i en färdig installation. Målkonflikter kan även uppstå mellan å ena sidan robusthet och å andra sidan arkitektoniska krav, miljö- och arbetsmiljökrav samt krav på logistiska flöden. Här gäller det att balansera kraven så att byggnader som innehåller samhällsviktig verksamhet kan erhålla den robusthet som behövs när byggnaden är i drift. Grunden är att alla kritiska resurser och funktioner minst ska dubleras och i största möjliga utsträckning ska de dubblerade systemen finnas i olika brandceller.

Vid en samhällsstörning kan olika verksamheter och därmed olika lokaler i en byggnad behöva prioriteras före andra. Dessa lokaler bör vara mer motståndskraftiga och ska kunna prioriteras i händelse av brist på exempelvis värme, kyla, vatten och el. Det kan innebära att lokaler utanför ledningsplatsen, som kontor och konferensrum behöver ha en högre fysisk skyddsnivå, tillgång till reservkraft, specifika datanätverk etc. Det är vidare viktigt att kunna hantera säkerheten i lokaler med dubbel funktion när de inte används, exempelvis genom styrd behörighet för tillträde.

Som regel är enkla tekniska lösningar mer robusta än mer komplicerade lösningar. Detta gäller både för den tekniska lösningens driftsäkerhet som för möjligheten att med enkla medel åtgärda fel. Enkelhet vid utformning av teknisk utrustning, styrsystem och andra fastighetstekniska installationer bör därför eftersträvas så långt det är möjligt. Ett exempel är att ventiler enkelt ska kunna manövreras manuellt om styrsystemet inte fungerar.

Vidare ökar robustheten om tekniska lösningar är utformade på så lika sätt som möjligt. Likhet underlättar för driftpersonalen och minskar sannolikheten för handhavandefel. Likhet underlättar också om systemen behöver kommunicera med varandra samt minskar behovet av reservdelshållning.

Arbeta systematiskt med kontinuitetshantering

För att undvika att förändringar i t.ex. byggnaders utformningar eller i dess fastighetstekniska system påverkar ledningsplatsens funktions säkerhet negativt behöver kontinuitetshantering och risk- och sårbarhetsanalyser genomföras inför förändringar. Arbetsättet gör att man på ett systematiskt sätt kan vidta åtgärder vid behov. Detta gäller såväl inför mindre som större förändringar i byggnadens funktion eller konstruktion, som vid byten av leverantörer som är knutna till ledningsplatsen.

Ta hänsyn till existerande robusthet vid verksamhetsflytt

Vid verksamhetsflyttar ska hänsyn tas till utformningen av robustethöjande åtgärder i de nya lokalerna. I förberedelseskedet kan kostnadsbesparingar uppnås genom att existerande robusthet inkluderas i beslutsunderlaget samtidigt som fördyrande och ofta komplicerade ändringar kan undvikas i förvaltningsskedet.

Planering och etablering av ledningsplatser bör samordnas med planer på övriga ny- och ombyggnationer då det är en fördel ur både förmåge- och kostnads-perspektiv. Vid nybyggnation finns de bästa förutsättningarna att integrera krav på skydd, uthållighet och tillförlitlighet. Detta gäller både vid etablering av ordinarie och olika former av alternativa ledningsplatser.

Säkerställ långa hyresavtal

I samband med verksamhetsflyttar eller omförhandling av befintligt hyresavtal behöver statliga aktörer särskilt beakta hyresavtalens längd. Statens krav på korta (normalt 6-åriga) hyresavtal begränsar möjligheten att bygga upp förmåga och robusthet för de bevakningsansvariga myndigheterna.

Ledningsplatsstruktur

Behov på olika ledningsnivåer

Lokal nivå

På lokal nivå behöver kommuner utöva övergripande ledning, samordning och prioritering av resurser utifrån det geografiska områdesansvaret. Ledningsplatser behövs här som en knutpunkt för det samordnade stödet på lokal nivå och varifrån en effektiv samordning med regionala aktörer kan bedrivas.

Kommunal räddningstjänst

Ledning av kommunal räddningstjänstverksamhet bedrivs på lokal nivå men också i räddningstjänstförbund och större regionala räddningsledningssystem. Räddningstjänsten utövar ledning med möjlighet att upprätta både skadeområdesnära ledning och ledning vid en ordinarie ledningscentral. Räddningstjänstens övergripande ledning är ofta knuten till en ledningscentral. Om ledningscentralen bedriver både larmhantering och ledning brukar den ofta benämnas räddningscentral.

Regional nivå

Länsstyrelser och regioner kännetecknas av att de har ett samordnande ansvar gentemot lokal och nationell nivå över hela hotskalan. Under höjd beredskap stärks därtill länsstyrelsernas roll som högsta civila totalförsvarsmyndighet i länet med ytterligare krav på att kunna upprätthålla samverkan och ledning med olika aktörer inom och utom länet.

Regionernas ansvar för bl.a. hälso- och sjukvård ställer krav på förmåga till aktörsgemensam samverkan och ledning. Regionernas behov av väl fungerande ledningsplatser ökar också under samhällsstörningar eller höjd beredskap då samhällets sjukvårdsbehov kan öka kraftigt.

Nationell nivå

För bevakningsansvariga myndigheter på nationell nivå finns en stor variation av verksamhetsspecifika behov. I likhet med den regionala nivån utgår behovet från aktörsgemensam samverkan, företrädesvis med andra centrala myndigheter och med regional nivå inom ett samverkansområde eller ett avgränsat geografiskt område. En behovsanalys måste utgå från myndighetens egna samhällsviktiga verksamhet liksom de tekniska system för samverkan och ledning som behövs för att bedriva den samhällsviktiga verksamheten.

Ordinarie ledningsplatser

Ordinarie ledningsplats

Alla aktörer som bedriver samhällsviktig verksamhet och som har ett behov av att kunna samverka med andra aktörer och leda egen verksamhet har normalt en ordinarie ledningsplats för att säkerställa kontinuerlig ledningsförmåga såväl i vardagen som under störda förhållanden. Planeringen och utförandet av ledningsplatsen ska ske med utgångspunkt bl.a. i de krav på förmågor som ställs på aktören under samhällsstörningar, höjd beredskap och krig, ledningsorganisationens storlek och arbetsformer samt utfallet av genomförda hot-, risk- och sårbarhetsanalyser. Med denna information som underlag utformas därefter ledningsplatsen så att den ger tillräcklig robusthet, säkerhet och uthållighet för att kunna motstå de bedömda störningar som kan uppstå.

En ordinarie ledningsplats är ett särskilt utformat utrymme oftast inom eller i direkt närhet till verksamhetens ordinarie lokaler vilket ger fördelen att den är lättillgänglig och kan nyttjas till vardags. Ledningsplatsen kan på så sätt vara en integrerad del av aktörens ordinarie verksamhet vilket underlättar övergången till arbete i lokalerna under en samhällsstörning. Därutöver kommer ledningsplatsens funktioner att testas regelbundet.

Aktörsgemensam ledningscentral

En aktörsgemensam ledningscentral är en form av ordinarie ledningsplats där flera aktörer delar lokaler eller sitter i samma byggnad. Aktörsgemensamma ledningscentraler förekommer dels som lokala etableringar där exempelvis räddningstjänst och polis eller ambulansverksamhet delar sin stationering i samma fastighet, dels regionala lösningar där en större räddningstjänstorganisation har sin verksamhet i anslutning och integrerat med exempelvis SOS Alarms verksamhet. I dessa anläggningar finns även lokaler för samverkande aktörer. Fördelen med aktörsgemensamma ledningscentraler är snabb informationsdelning mellan olika aktörer samt goda förutsättningar att arbeta med en gemensam samlad lägesbild.

Alternativa ledningsplatser

Den ordinarie ledningsplatsen behöver kompletteras med en eller flera alternativa ledningsplatser för att säkerställa verksamhetens förmåga till kontinuerlig ledning främst under höjd beredskap och krig. En alternativ ledningsplats syftar till att kunna ersätta eller komplettera den ordinarie ledningsplatsen om situationen så kräver. Skäl till detta kan vara att lokalerna för den ordinarie ledningsplatsen inte längre kan brukas, att en främre ledningsplats behövs eller att verksamheten behöver bedrivas från en skyddad plats.

Alternativ ledningsplats är ett samlingsbegrepp för ledningsplatstyperna mobil, skyddad och i vissa fall sekundär ledningsplats. Den alternativa ledningsplatsen ska normalt erbjuda samma funktionalitet som den ordinarie ledningsplatsen.



Mobil ledningsplats

Med mobil ledningsplats avses ett koncept med en flyttbar teknikplattform som tillsammans med tillfälliga arbetslokaler skapar förutsättningar för en aktör att samverka och utöva ledning. Den kan också fungera som ett komplement till den ordinarie ledningsplatsen, exempelvis då ett stort samverkansbehov föreligger eller en främre ledningsplats behöver upprättas.



Skyddad ledningsplats

Med en skyddad ledningsplats avses en alternativ ledningsplats med hög fysisk skyddsnivå (fortifikatoriskt skydd), robusta försörjningssystem och anpassad uthållighet. Skyddade ledningsplatser utformas i vissa fall specifikt för en aktör eller i andra fall liknande en aktörs gemensam ledningscentral.

Skyddade ledningsplatser kan delas in i tre kategorier beroende på nivån på det fysiska eller fortifikatoriska skyddet;

- Betonganläggningar ovan jord erbjuder en nivå av fortifikatoriskt och fysiskt skydd. Anläggningar av typen RC90 som många kommunala räddningstjänster förfogar över idag är konstruerade för daglig verksamhet men är relativt oskyddade i fredsdraft. Igensättningselement som exempelvis ställuckor i kombination med betongblock för fönsteröppningar och dörrar kompletterar det fysiska skyddet vid skyddsdrift.
- Betonganläggningar under jord har en högre fortifikatorisk skyddsklass. Betonganläggningar under jord har kapacitet för ledning och samverkan under störda förhållanden och höjd beredskap men kräver förberedelser för att uppnå den beskrivna skyddsnivån.
- Berganläggningar erbjuder en hög skyddsklass och skyddar mot merparten av antagonistiska attacker. Anläggningar av den här typen är dimensionerade för att bedriva ledning och samverkan under störda förhållanden och höjd beredskap men kräver på motsvarande sätt som betonganläggningar under jord förberedelser för omställning till skyddsdrift.

Utformning av fortifikatoriskt skyddade anläggningar utförs enligt principen med zonindelning med tillägget att de konstrueras för att skydda mot stötvåg och annan vapenverkan. Anläggningarna skyddas även mot verkan av farliga ämnen (CBRNE) genom en byggnadskonstruktion med fastställd "gasgräns", luftrening och anpassad slussfunktion med sanering. För att indikera farliga ämnen och strålning kan sensorer och mätinstrument användas. Därutöver förekommer även skydd mot elektromagnetiska hot.



Fortifikatoriskt skyddade anläggningar ställer höga krav på brandsäkerhet med noga förberedda utrymningsvägar. Brandkonsult bör involveras tidigt i arbetet med översikts- och detaljplaner för att de regelverk som finns för brandskydd och personsäkerhet ska kunna efterlevas.

Fortifikatoriskt skyddade anläggningar är komplexa anläggningstyper som erfordrar särskild kompetens vid konstruktion och utformning varför de inte beskrivs ytterligare i denna vägledning.



Läs mer

- www.msb.se sök CBRNE
- MSB1693 Den robusta sjukhusbyggnaden – kap 10 Skydd mot farliga ämnen

Sekundär ledningsplats

Med sekundär ledningsplats avses här en dedikerad och förberedd ledningsplats på en annan geografisk plats än verksamhetens ordinarie. Exempel på sekundära ledningsplatser är när en aktör flyttar delar av sin verksamhet till ett eget verksamhetsställe på annan ort eller till en aktör som har liknande verksamhet.

En sekundär ledningsplats ska erbjuda samma funktionalitet som den ordinarie ledningsplatsen men uppfyller inte alltid den alternativa ledningsplatsens krav på skydd av verksamheten. Av den anledningen ses ofta en sekundär ledningsplats som ett komplement till den ordinarie och den alternativa ledningsplatsen. Ett komplement som utifrån ett kontinuitetsperspektiv stärker verksamhetens möjligheter att utöva ledning i första hand i den nedre delen av hotskalan.

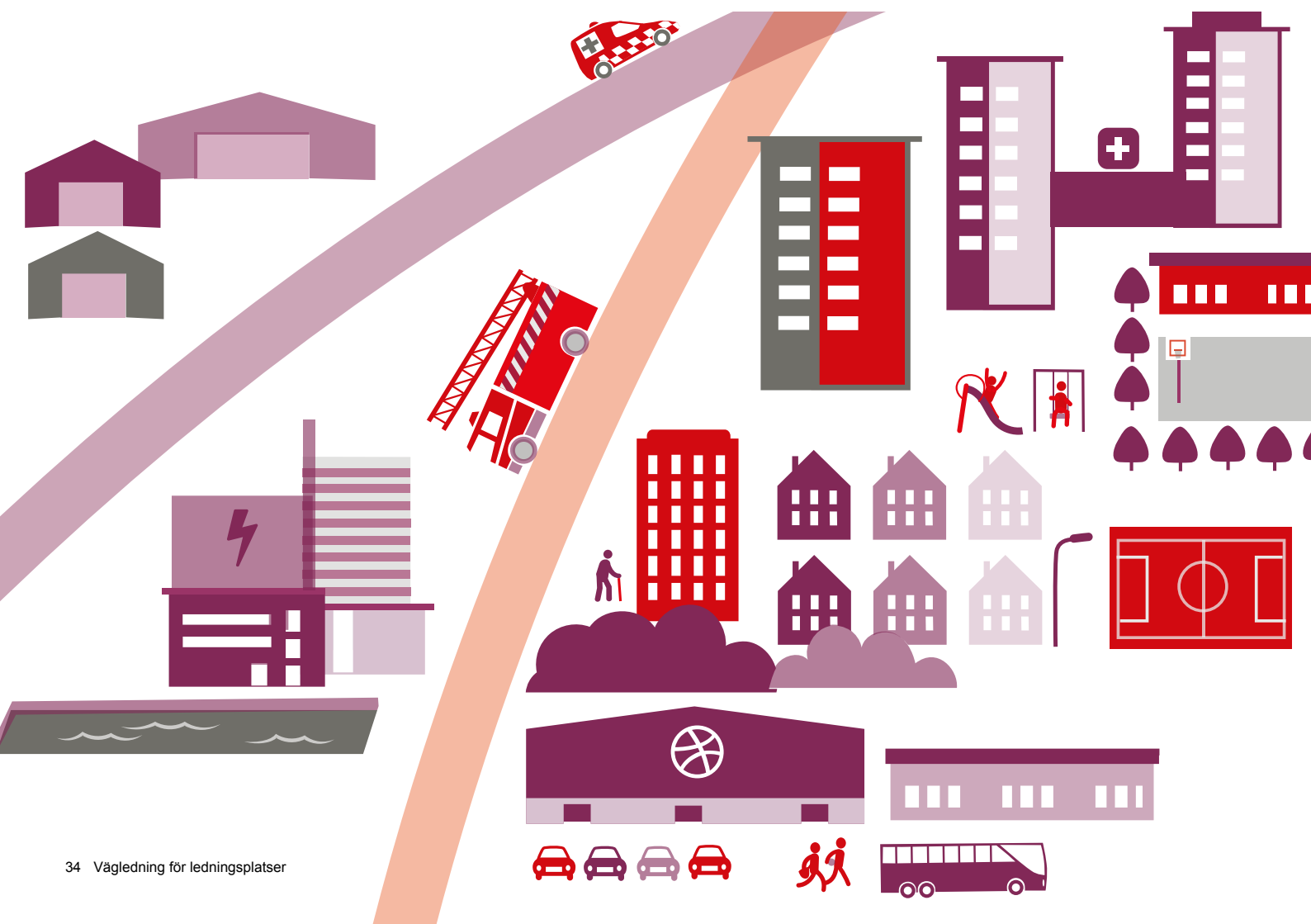


Ledningsplatsens utformning

Byggnadsrelaterade åtgärder

Skyddsnivåer

Fortifikationsverket har systematiserat skyddsåtgärder i sju nivåer som kan användas för att minimera verkan av ett angrepp genom att avskräcka, upptäcka, försvåra och hantera antagonistiska angrepp. Indelningen är gjord utifrån en angriparens perspektiv och kan användas som en checklista vid behovsanalysen.



Skyddsnivå	Beskrivning	Exempel
Begränsa kunskapen om ledningsplatsen	Skyddsnivån kan delas in i två delar, att minimera kunskapen om själva byggnaden och att begränsa kunskapen om att ledningsplatsen finns i byggnaden.	Uppgifter om ledningsplatsens belägenhet omfattas av sekretess. Läget är endast känt av behörig personal inom organisationen.
Minska viljan att angripa byggnaden	Skyddsnivån handlar om att etablera tydliga skydd som angriparen upplever för svåra. Ett annat sätt är att skapa ovisshet kring byggnaden och ledningsplatsen.	För att ta sig in i byggnaden finns tydliga yttre skydd som försvårar ett angrepp. Det finns inga anvisningar om hur man kommer till ledningsplatsen.
Försvåra initiering av ett angrepp	Skyddsnivån handlar om att försvåra eller förhindra ett angrepp genom t.ex. övervakning av byggnaden och perimeterområdet, behörighetskontroll, säkerhetskontroll, begränsad insyn m.m.	Ledningsplatsen är övervakad och kontrollerad med kameror och behörighetskontroller som gör det lättare att upptäcka ett angrepp.
Mildra skador genom aktiva åtgärder	Skyddsnivån handlar om att skydda det som ännu inte har påverkats av angreppet. Detta kan göras genom att informera människor i byggnaden, utrymma byggnaden, agera på misstänkta föremål samt förbereda platser med särskilt skydd.	Personalen är övad i att hantera ett angrepp och kan snabbt agera för att skydda det som ännu inte påverkats samt agera mot angreppet. Det finns brandlarm och brandsläcksystem.
Minska verkan från ett angrepp	Skyddsnivån handlar om att minska verkan från ett angrepp t.ex. genom att skapa avstånd till byggnaden eller fysiska skydd som murar för att förhindra en stötvåg.	Ledningsplatsen har fortifikatoriskt skalskydd. Det finns inga fönster. Alla dörrar är kontrollerade med sluss. Ledningsplatsens byggnadsstomme är konstruerad så den inte tar upp energier från explosioner. Brott på enskilda komponenter utlöser inte fortskridande ras.
Skydda byggnadens innehåll	Skyddsnivån handlar om att byggnaden ska verka som skydd för ledningsplatsen genom att t.ex. stärka byggnadens omslutningsyta, begränsa spridning av brand, hindra insyn, dämpa spridning av ljud.	Dörrar är inbrottsklassade. Det går inte utifrån att avlyssna samtal. Lokalerna har brandsektionering.
Mildra skador genom passiva åtgärder	Skyddsnivån handlar om att mildra skador genom passiva åtgärder i byggnaden, t.ex. genom att placera ledningsplatsen med omgivande rum samt stärka skyddet för troliga angreppspunkter som entré och godsmottagning.	Teknikrum har förstärkt skydd enligt lökprincipen. Receptionen är försedd med slussfunktion för allmänheten.



Läs mer

- Fortifikationsverket, Handbok Skydd av byggnader, 2017.

Platsval

Vid nybyggnation av en ledningsplats är det viktigt med ett tidigt samråd med kommun, länsstyrelse och fastighetsägare för att stämma av möjliga lokaler samt förutsättningar för nybyggnation med hänsyn taget till exempelvis gällande översikts- och detaljplaner samt planer för totalförsvaret. Tidigt i processen behöver behov av antenninstallationer utredas då höjder på dessa kan påverkas av detaljplaner. Ett klokt platsval utgör grunden för utformning av en väl fungerande ledningsfunktion över hela hotskalan.

Utanför fastigheten

Ett viktigt ingångsvärde vid val av lokalisering för en ledningsplats är möjligheten att kunna skapa ett tillräckligt stort område utanför ledningsplatsen där åtgärder kan vidtas för att skapa ett bra skydd. Området kallas perimeterområde och påverkas av aktuella skyddskrav där syftet bland annat är att minska viljan att angripa byggnaden, försvåra initieringen av ett angrepp och minska verkan från ett angrepp.

Perimeterområdet kan användas för att skapa ett tillräckligt stort avstånd mellan byggnaden och obehöriga. Avståndet kallas skyddsavstånd och syftar till att hindra eller försvåra för en angripare att komma nära byggnaden. Det minskar även verkan av olika angrepp som utförs i närheten av byggnaden. Olika typer av hinder krävs för att stoppa eller störa en angripare till fots eller en fordonsburen angripare. Skyddsavstånd kan därför skapas genom olika metoder t.ex. genom att anpassa placeringen av byggnader, begränsa framkomligheten med hjälp av yttre fordonsbarriärer såsom pollare på trottoarer, stängsel runt fastighetsgränsen samt utformning av infartsvägar. Placering av parkeringsplatser bör ses över då exempelvis parkeringsgarage under byggnader skapar en särskild sårbarhet.



Läs mer

- MSB1448 Säkerhet i offentlig miljö: skydd mot antagonistiska hot och terrorism

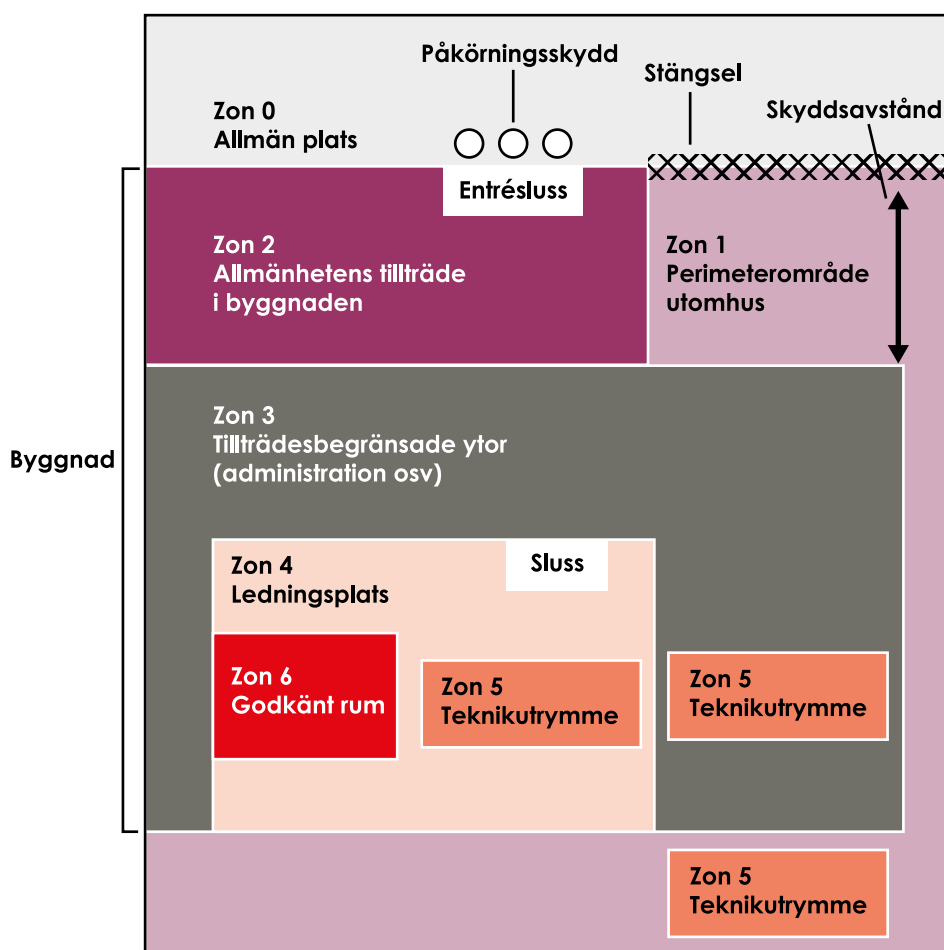
I fastigheten

Åtgärder som vidtas för att öka det fysiska skyddet blir ofta mest effektiva om de planeras in i ett tidigt skede av byggprocessen. Genom att tidigt tänka på hur utrymmen bör utformas utifrån möjliga antagonistiska angrepp kan entréer, godsmottagningar och andra angreppsvägar erhålla ett bra fysiskt skydd.

För att öka skyddet inne i byggnaden och i ledningsplatsen kan s.k. sektionering användas. Syftet med sektionering är att dela upp byggnaden som inrymmer ledningsplatsen i mindre zoner för att mer specifikt kunna styra tillträdet. Sektioneringen gör det lättare att skydda ledningsplatsen från angripare och skydda besökare och personal. En genomtänkt sektionering kan vidare minska risken för bland annat brand, spridning av farliga ämnen och underrättelseinhämtning. Sektioneringen bidrar även till att tid kan vinnas i händelse av ett fysiskt angrepp.

Ytterligare åtgärder som används som skyddsbarriärer är lås, larm- och passerkontrollsystem kompletterade med kamerabevakning och system för internkommunikation. För att uppnå ett fullgott skydd behöver barriärerna vara samspela och jämnstarka så att inga svaga punkter kan utnyttjas av antagonister. För vissa typer av anläggningar tillkommer även att definiera en så kallad ”stötvägsgräns” för explosioner samt en ”gasgräns” för farliga ämnen (CBRNE). I vissa fall kan även en zonindelning för skydd mot elmiljöhot erfordras. Nedan illustreras hur sektionering kan utföras i och utanför en byggnad med ledningsplats.

Figur 4. Exempel på sektionering i och utanför byggnad med ledningsplats



Exempel på sektionering i och utanför byggnad

Zon 0	Allmän plats utanför byggnad och områdesskydd
Zon 1	Perimeterområde – områdesskyddad yta utomhus
Zon 2	Områdesskyddad yta, allmänna ytor inomhus
Zon 3	Tillträdesbegränsade verksamhetsytor med lägre krav
Zon 4	Ledningsplats
Zon 5	Teknikutrymmen med koppling till ledningsplatsen
Zon 6	Godkänt rum för hantering av säkerhetsskyddsklassificerad information

Byggnadstekniska specifikationer

Vid nybyggnation av en ledningsplats ska den skyddsnivå eftersträvas som uppfyller kraven utifrån gällande hotbild. Vid ombyggnation av en ledningsplats görs en samlad bedömning av befintliga förhållanden och möjliga kompletteringar för att erhålla en så hög skyddsnivå som möjligt utifrån aktuell hotbild. Nedan redovisas exempel på byggnadstekniska kravställningar vid utformningen av en ledningsplats.

Exempel på byggnadstekniska kravställningar

Tak och väggar	Tak- och golvbjälklag samt väggar utförs i betong. Omslutande byggnadsstomme ska vara så tät att ett övertryck upprätthålls.
Armeringsnät	Inre och yttre armeringsnät skall utföras väl sammanlänkat i omslutande, obrutna slingor i flera dimensioner i ledningsplatsens betongstomme för skydd mot elmiljöhot. Intagsplåt, karmar och genomföringar i yttervägg ska anslutas till armeringen
Entrésluss	In- och utpassage till ledningsplatsen ska vid krissituationer ske kontrollerat exempelvis genom entrésluss via en yttre och en inre slussdörr. Slussen ska då endast medge passage genom en dörr i taget och bestyckas med larm, passagesystem, porttelefon och kamerabevakning. Entréslussens alla omgivande ytor ska uppfylla kraven för specificerad skyddsklass.
Täthet för övertrycksventilation	Ledningsplatsens krav på övertrycksventilation utförs i definierade zongränser med sådan täthet att ett övertryck kan upprätthållas vid exempelvis utvändig brand och kemikalieutsläpp. Fönster ska inte vara öppningsbara. Ventilationsanläggning ska kunna stoppas. Övertrycksventilation över skyddsfilter ska kunna startas manuellt via omkopplare. Vid driftfall med övertrycksventilation ska passage alltid ske via slussdörrarna. Övriga dörrar i övertrycksgränsen stängs och låses vid driftfallet och ska inte kunna öppnas från utsidan. Dörrar i övertrycksgräns och slusspassage ska helst vara inåtgående för att minimera luftläckage vid övertryck. Täthetskrav avseende lufttäthet ska uppfyllas för fönster och dörrar.
Öppningar	För att upprätthålla kraven på fysiskt skydd, skydd mot överhörning, övertrycksventilation m.m. ska hål och genomföringar genom ledningsplatsens interna begränsningsväggar och omslutande ytor utföras med stor noggrannhet och med typgodkända brandtätningar och inkrypsskydd.
Fönster och dörrar	Fönster och dörrar i omslutande ytor ska motstå antagonistiska hot och utföras enligt specificerad skyddsklass. Passersystem installeras som medger dörröppning med kort/tag och kod samt ev. öppn knapp/fjärröppning. Lås för dörrar i zongränser ska harmonisera med dörrens säkerhetsnivå.
Utrymningsvägar	Ledningsplatsens brandskyddsdocumentation bestämmer behovet av utrymningsvägar. Krävs en utrymningsväg genom zongräns ska öppningen uppfylla specificerade krav.
Brandsektionering	Utöver krav på brand- och brandgasspridning enligt BBR kan det finnas ytterligare krav från ingående verksamheter. Dessa måste definieras och styra utformningen av byggnadens brandskydd. Brandlarm- och släcksystem ska installeras enligt krav i brandskyddsdocumentation. Lägsta nivå är att ledningsplatsen förses med brandlarm som uppfyller "Regler för automatisk brandlarmläggning (SBF 110)".

Skydd kontra design

Det förekommer att robusthetshöjande åtgärder vad gäller form och omslutningsyta ställs mot arkitektonisk utformning och miljökrav. Till exempel kan fasader av glas vara mindre motståndskraftiga mot sprängverkan än fasader av andra materialval. Även indragningar av fasader så det skapas olika grad av inneslutningar är negativt ur robusthetssynpunkt. En avvägning måste göras mellan olika värden utan att göra avkall på säkerheten. Det går att bygga robust och samtidigt estetiskt tilltalande och tillgängliga byggnader. Vid användande av glas i fasader kan säkerhetsglas minska risken för skadligt glassplitter vid en explosion i närheten. Fönster kan även beläggas med skyddsfilm. Vid en tryckvåg riskerar dock hela fönstret att tryckas in med stor kraft och det kan behövas en mekanism för att fånga upp glaset. Vid val av bärande stomme är det viktigt att den kan motstå olika typer av olyckor eller antagonistiska angrepp. För att stommen ska vara motståndskraftig krävs mer än att beakta enskilda byggkomponenters motståndsförmåga. Knutpunkter och infästningar måste kunna tåla stor deformation utan att helt förlora bärförmågan. Särskilt sårbara punkter som vid deformation kan leda till stora raskonsekvenser måste elimineras eller skyddas.

Tillträdesskydd – lås, larm och passersystem

Användandet av lås, larm och passersystem är en del av det yttre och inre skal-skyddet med låsning, larmövervakning och behörighetskontroll av olika zoner.

Stöldskyddsföreningen har olika normer och kravspecifikationer för användning och installation av inbrottslarm (SSF regelverk 130 och 140). Systemet för inbrottslarm ska utformas utifrån genomförd hot-, sårbarhets- och riskanalys. Det ska också integreras med passerkontrollsystemet vad gäller tidsstyrd förbikoppling av larmområden för passage till manöverpanel samt larm vid upp-brytning eller öppethållande av passerkontrollförsedd dörr för länge. Inbrottslarmssystemet ska anslutas till godkänd larmsändare.

Passer- och larmsystem bör ha back-up-system samt vara kopplade till avbrottsfri kraft. Det behövs också manuella rutiner för de fall då passersystemet är ur funktion.

System för internkommunikation ska finnas för att kunna uppmärksamma personal vid larm.

Det är viktigt att arbetet med tillträdesskydd tidigt synkroniseras med brandskydds- och utrymningsstrategin för lokalerna då dessa kan stå i motsats till varandra.

Kamerabevakning

Att installera kamerabevakning där det enligt lagstiftning om kamerabevakning är tillåtet är ett sätt att öka säkerheten. Förekomst av kameror och en realtidsövervakning av viktiga utrymmen ökar förmågan att snabbt reagera på ett angrepp. Kamerabevakning kan även verka i avskräckande syfte. Verksamheten bör ha full rådgighet över den här typen av tekniska system och de bör heller inte anslutas till internet med hänsyn till cyberhot.

Rumsbildningar

Lokalval

Utformning och placering av ledningsplatsens lokaler har stor påverkan på hur väl arbetsutrymmena kommer att fungera för avsedd verksamhet. Generellt är det en fördel om lokalerna är lättillgängliga och finns i nära anslutning till ordinarie verksamhet. För att kunna nyttja lokalens kapacitet bör ett mer flexibelt användande av lokalerna övervägas. Att nyttja en ledningsplats till verksamhet även till vardags, utan att frångå säkerhetskrav, ger både praktiska och ekonomiska fördelar. Brukarna kommer då att lära sig använda lokalen och dess funktioner samtidigt som den tekniska utrustningen blir funktionskontrollerad.

Kan ledningsplatsen samutnyttjas med andra aktörer bidrar det till att lokalerna används mer kontinuerligt vilket i sin tur leder till en mer effektiv hantering av samhällsstörningar. Att arbeta tillsammans med andra aktörer bidrar till en snabb informationsdelning och till bättre möjligheter till att skapa en samlad lägesbild.

Viss verksamhet är lämplig att hantera utanför ledningsplatsen såsom större samverkansaktiviteter, upplysningscentral och utrymmen för massmedia.

Verksamhetsutrymmen

Vid planering av en ledningsplats behöver verksamhetens behov och önskemål beskrivas. I beskrivningen ska det framgå vilken verksamhet som ska bedrivas, hur den organiseras i funktioner, hur den utförs och vilka samverkans- och stödfunktioner som behövs. Behovsbeskrivningen används sedan som underlag för hur lokalerna på bästa möjliga sätt kan utformas och användas av verksamheten. Finns möjlighet så skapas egna utrymmen i ledningsplatsen för verksamhetens olika funktioner. Om det inte är möjligt så måste funktionerna samordnas och utrymmena prioriteras. Vidare kan utrymmen behövas för exempelvis stödfunktioner och samverkande aktörer.

Lokaler för hantering av skyddsvärd information

Normalt kommer känslig information och ibland även säkerhetsskyddsklassificerade uppgifter att hanteras i ledningsplatsen. Resultat från säkerhetsskyddsanalys och informationsklassning samt tekniska föreskrifter styr vilka krav som ska ställas på lokalerna för att kunna hantera information på ett säkert sätt.

Beroende på hur informationen hanteras – muntligt, synligt i pappers- eller elektroniskt format och/eller i elektroniska kommunikationssystem samt lokalens placering bestämmer vilka säkerhetshöjande åtgärder som behöver vidtas. Normalt behöver nedanstående ingångsvärden beaktas vilket innebär att lokalen kan komma att utformas utifrån en kombination av åtgärder.

- Risk för att obehöriga tar del av synlig information. Åtgärdas med passersystem och behörighetskontroll. Fönster ska gå att täcka för. Rutin för att täcka över/släcka ner känslig information vid besök ska finnas.
- Risk för överhörning av talad information. Akustisk överhörning ställer särskilda krav på bland annat lokalen där sådana uppgifter ska delges. Förutom att den som delger uppgifter alltid ska säkerställa att mottagarna av uppgifterna är behöriga, så ska delgivningen ske i en lokal som är anpassad och av verksamheten godkänd ur säkerhetssynpunkt. Det ska till exempel inte gå att avlyssna ett möte utifrån eller från en angränsande lokal. Samma krav måste också uppfyllas vid användning av exempelvis telefoni och videokonferens.
- Risk för att obehöriga får tillgång till lokalen. Lokaler ska vara försedda med inbrottslarm och passersystem för behörighetskontroll. Det ska inte finnas möjlighet att installera avlyssningsutrustning.
- Risk för RÖS-spaning. Med RÖS – röjande signaler menas inte önskvärda elektromagnetiska och eller akustiska signaler som alstras i informationsbehandlade utrustningar och som, om de kan tydas av obehörig, kan bidra till att känsliga eller säkerhetsskyddsklassificerade uppgifter röjs. För att reducera risken att bli avlyssnad så finns det skyddsmetoder som kan vidtas. Ett sätt är att använda s.k. RÖS-klassad utrustning som är konstruerad för att inte avge RÖS. Andra exempel är att nyttja lokaler belägna i den inre delen av en större byggnad, lokaler under mark samt lokaler med tjockare väggar av armerad betong och utan fönster då dessa alternativ dämpar signalen kraftigt ur ett RÖS-perspektiv. Om detta inte är möjligt kan s.k. RÖS-rum byggas där rummet omsluts av elektriskt skärmande material och där det elektriska kablagen förses med anpassade filter som reducerar risken för ledningsbunden RÖS (röjande signaler som överlagras på en elektrisk ledare).

Informationshanteringen i sin helhet behöver därutöver analyseras i det systematiska informationssäkerhetsarbetet.

Behov av säkerhetsskåp (antal och placering) behöver tidigt kravställas med hänsyn till krav på golvens hållfasthet.



Läs mer

- Säkerhetspolisen – Avlyssningsskyddade utrymmen
- MSB1310 Riskreducerande åtgärder för lokal

Lokaler för sambands- och kommunikationsystem

I ledningsplatsen behövs lokaler för sambandsutrustning, kommunikationsnoder och olika it-system. Vid utformning av lokalprogrammet är det viktigt att granska hur dessa utrymmen är placerade och hur de kan skyddas mot skador eller olaga intrång exempelvis genom använda zonindelning i lokalerna. Hur kabelvägar för yttre nätanslutningar, fastighetsnät och antennkablar ska skyddas behöver också hanteras.

Lokalerna för sambands- och kommunikationssystem ska utformas utifrån högt ställda krav på säkerhets och driftmiljö med avseende på tillträdesbegränsning,

elförsörjning, teknikkyla, brandskydd, skydd mot vattenskador och säker förläggning av kabelanslutningar. Exempelvis ska lokalerna förses med avbrottsfri kraft, kylinstallationer, erforderlig brandsektionering och brandlarm samt kan kompletteras med fast släcksystem. Där vatteninträngning inte kan uteslutas ska fuktalarm installeras. Tillträdet till lokalerna ska regleras och de bör vara övervakade med inbrottslarm.

Resultatet av den informationssäkerhetsanalys som beskrivs i kapitel 3 styr bland annat de fysiska åtgärder som krävs för it-systemens tekniska infrastruktur. Åtgärderna beaktas vid planering av ledningsplatsens lokaler för installationer av it-system.



Läs mer

- MSB629 Vägledning för fysisk informationssäkerhet i it-utrymmen

Lokaler för fastighetstekniska installationer

Lokaler som innehåller fastighetstekniska system utformas i stort på samma sätt som de för sambands- och kommunikationssystemen.

Reservkraftutrustningen placeras i en eller flera lokaler med brandsektionering i minst klass EI 60. Bränsletankar vallas in enligt gällande regler. Dörr till reservkrafttrum ska vara utåtgående, läsbar och vara försedd med panikregel. Reservkraftaggregatens utvändiga öppningar för till- och frånluft kompletteras med mekaniskt inbrottskydd anpassade för att klara ställda skyddskrav. Bullerabsorbenter monteras på tak och väggar i största möjliga omfattning och bör vara heltäckande. Rör för avgasutblås ljudisoleras och placeras så att verksamheter i egen fastighet eller närliggande fastigheter inte påverkas.

Arbetsmiljörelaterade åtgärder

En genomtänkt arbetsmiljö krävs för att förbättra uthålligheten hos den personal som arbetar i ledningsplatsen. De samhällsstörningar som uppstår kan vara långvariga och påverka personalens fysiska uthållighet vilket ställer höga krav på ergonomi, belysning, akustik och luftkvalitet. Ledningsplatsen ska även i största möjliga omfattning kunna erbjuda de faciliteter som behövs för kontinuerligt arbete i form av vilrum, toaletter, kök och mötesplatser.

Vid de tillfällen det är många människor närvarande i ledningsplatsen kan det uppstå en hög ljudvolym. Det är då viktigt att ha lokaler som är konstruerade och utformade för att dämpa ljudvolymen i en bullrig ljudmiljö.

Belysningen ska vara anpassad för det arbete som bedrivs på ledningsplatsen. Vid arbetsplatser och i gemensamma utrymmen ska belysningen utformas som reglerbar direkt- och indirekt belysning.

I ledningsplatsen ställs höga krav på inomhusklimatet avseende värme, kyla och ventilation. Det är därför viktigt att utifrån ett verksamhetsperspektiv tidigt beskriva hur många personer som maximalt ska vistas i respektive utrymme för att på så sätt kunna dimensionera ventilationssystemet.



Tekniska försörjningssystem

Elförsörjning

Ledningsplatsens elförsörjning måste uppfylla höga krav på tillförlitlighet och redundans. Bortfall av det allmänna elnätet får inte påverka ledningsplatsens prioriterade funktioner varför dessa förses med avbrottsfri kraftförsörjning med reservkraftaggregat i kombination med UPS-system. I vissa fall kan ledningsplatsen därutöver förses med dubbla serviser från olika fördelningsstationer i nätleverantörens nät. Om möjligt bör huvudställverk etc. vara utformade så att enskilt fel inte slår ut all försörjning. Vidare bör anslutning av extern reservkraft förberedas, i första hand med färdig inkopplingspunkt alternativt att instruktion finns för inkoppling.

Reservkraftsystemet ska bestå av ett eller flera stationära automatstartande reservkraftaggregat som dimensioneras utifrån de prioriterade systemens effektbehov och krav på tillförlitlighet. Reservkraftsystem utförs enligt kategori 3 (reservkraftsanläggning som in- och urkopplas automatiskt utan avbrott, så kallad blinkfri övergång) eller kategori 4 (reservkraftsanläggning som in- och urkopplas automatiskt utan avbrott, så kallad blinkfri övergång samt att den även kan drivas parallellt med nätet).

UPS-system är ett elektriskt system byggt på bl.a. batterier som tillhandahåller en hög kvalitet på elförsörjning även vid strömavbrott eller andra störningar. UPS-systemet dimensioneras och utformas utifrån krav på uthållighet och tillgänglighet för ledningsplatsen. Utrustningen bör utgöras av dubbelkonverterande on-line växelströms-UPS med inbyggd automatisk och yttre manuell förbi-kopplingsfunktion. Vid höga tillförlitlighetskrav utformas systemet som två parallella redundanta system s.k. A- och B-system. I det utförandet kan som exempel båda systemen anslutas till servermiljöer med dubbla nätaggregat. Som alternativ kan ett så kallat N+1 system installeras. Ett sådant system består av ett antal parallella UPS-er (N) som strömförsörjer den prioriterade utrustningen. Utöver det finns ytterligare en UPS i reserv (+1) om någon av de ordinarie UPS-utrustningarna slutar fungera. Varje UPS har sina egna batterier och batterierna dimensioneras för anpassad batteridrifttid.



Läs mer

- www.msb.se sök Reservkraft

Värme och ventilation

Ledningsplatsen behöver ett ventilations- och värmesystem dels för att förse verksamhetsutrymmen med ett bra inomhusklimat, dels för att kunna kyla teknikutrymmen.

För ledningsplatser med högre skyddsnivåer används luftbehandlingsaggregat med till- och frånluftsfläktar, värmeåtervinning och värmebatteri/kylbatteri. Dessutom tillkommer möjlighet till skydd mot farliga ämnen (CBRNE). Ett sätt att lösa detta är att luftbehandlingsaggregat förses med spjällfunktioner så att aggregatet kan vara i drift med stängda luftvägar för till- och frånluft. Finns hälsofarliga ämnen i uteluften kan då drift med enbart cirkulationsluft användas i ledningsplatsen. Denna funktion medför att klimatregleringen fungerar och att en förlängd uthållighet erhålls för ledningsplatsen. Krävs ytterligare uthållighet kan ventilationsanläggningen ställas i ett driftläge som medför att intagsluften renas från farliga ämnen och partiklar via anpassade filterlösningar. Reservfilter behöver finnas att tillgå i anläggningen samt skyddsdräkter för att kunna genomföra filterbyten. Funktionen ska förutom antagonistiska hot även kunna hantera motsvarande störningar som kan uppkomma genom exempelvis olyckor med farligt gods. För att indikera farliga ämnen i uteluften kan sensorer användas.

Utrymmen med kritisk värmealstrande utrustning som exempelvis serverrum bör ha redundanta kylsystem.

Vid placering av utvändigt utrustning som ventilationsöppningar och kondensorbatterier beaktas sabotagerisk. Vid placering av intag för uteluft ska hänsyn tas till avgaser från bl.a. reservkraftaggregat.



Läs mer

- www.msb.se sök CBRNE

Vatten och avlopp

För att kunna upprätthålla verksamheten behöver försörjningen av dricksvatten och omhändertagande av spillvatten säkerställas när samhällets funktioner för vatten och avlopp inte fungerar. Vid driftstörning eller avbrott på kommunal vattenförsörjning behöver dricksvattentank eller djupborrad brunn finnas alternativt en planering för hur personalen förses med dricksvatten. Råvatten för exempelvis hygienbruk och toaletter behöver inte hanteras på samma sätt som dricksvatten och kan exempelvis lagras i vattentank med andra krav på renhet och omsättning.

Fastighetstekniska styr- och övervakningssystem

Med hjälp av styr- och övervakningssystem kan fastighetstekniska funktioner i ledningsplatsen kontinuerligt styras och övervakas. Eftersom avbrott i styrningen och övervakningen kan få stora konsekvenser ställs höga krav på robusthet. Inledningsvis genomförs en inventering och en säkerhetsgranskning av de system i den aktuella fastigheten som kan påverka ledningsplatsen. Därefter genomförs eventuella säkerhetshöjande åtgärder samt åtgärder för att höja

systemens robusthet såsom att strömförsörja vitala delar med UPS- och reservkraft samt att reglera vilken personal som har behörighet att koppla in sig i systemet och göra ändringar.

Verksamheten bör ha full rådighet över den här typen av tekniska system och de bör heller inte anslutas till internet med hänsyn till cyberhot. Om system ändå går ner bör det finns rutiner, utrustning och utbildad driftpersonal för att lokalt och manuellt ta över styrning och övervakning.

Samtliga drift- och övervakningslarm, även från tekniska system för samverkan och ledning, bör anslutas till dataundercentraler (DUC). Larmen bör sedan överföras till bemannad larmmottagare. Viktiga larm (A-larm) ska resultera i omedelbar åtgärd.



Läs mer

- MSB718 Vägledning till ökad säkerhet i industriella informations- och styrsystem
- MSB1468 Tillägg till Vägledning till ökad säkerhet i industriella informations- och styrsystem
- MSBF 2020:7 Föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter
- www.informationssakerhet.se Vägledning till MSBFS 2020:7

Skydd mot elektromagnetiska störningar och hot

Ledningsplatsen bör ges skydd mot elektromagnetiska störningar och hot som exempelvis åska, statisk elektricitet, störsändare, elektromagnetisk puls från kärnvapen (EMP) och mikrovågsvapen (HPM). Nedan redovisas ett antal åtgärder som kan vidtas.

- Informationsbegränsning: Begränsa öppen tillgång till information som kan användas för ett EM-angrepp.
- Identifiera sårbara verksamhetskritiska system genom regelbundna riskanalyser avseende EM-hot.
- Trådburet för viktiga förbindelser: Använd inte trådlös kommunikation i verksamhetskritiska system.
- Skyddsavstånd: Ju längre bort från det skyddsvärda systemet en avspärrning eller staket finns desto mindre blir verkan av EM-hotet.
- Utför en indelning i elmiljözoner. Installera anpassade skärmade skal i kombination med transientskydd och filterkomponenter på elektriska kablar i respektive zongräns. Bygg bort sårbarheter där så är lämpligt och genomför regelbunden tillsyn av skyddsutrustning.
- Utbilda personal i incidenthantering.



Läs mer

- www.msb.se sök Elektromagnetiska hot
- MSB 0174-10 Elmiljö i anläggningar för räddningstjänst
- Fortifikationsverket: Handbok EMC, 2020
- Fortifikationsverket: Vägledning för skydd mot avsiktliga EM-hot, 2021
- MSB1178 Vägledning för risk- och sårbarhetsanalys avseende antagonistiska elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur.
- FOI Memo 7507 Incidenthantering av elektromagnetiska hot mot samhällsviktiga tjänster

Tekniska system för samverkan och ledning

Robusta system

Det är viktigt att beakta den exponering gentemot internet som sker till följd av att nätansluta olika tekniska system i ledningsplatsen. Exponeringen av system och informationstillgångar innebär en förhöjd risk för olika fjärrangrepp – både mot de direkt anslutna systemen men också för andra system som exempelvis är sammankopplade via ett lokalt nätverk. För att skapa ett skydd mot cyberangrepp eller minska konsekvenserna av ett cyberangrepp som lyckas behöver verksamheten särskilt beakta behovet av olika robusthetshöjande åtgärder. Det kan exempelvis röra sig om segmentering av olika system och nätverk inom ledningsplatsen, ha backuper samt rutiner för hur dessa ska hanteras eller begränsa olika behörigheter till system och lagringsytor.

Redundanta system

Verksamheten är beroende av att interna och externa system för tal, video och datakommunikation fungerar. För detta behövs flera av varandra oberoende kommunikationssystem samt att, där så är möjligt, de externa anslutningarna utförs med geografisk diversitet d.v.s. systemen ska externt anslutas till två geografiskt åtskilda noder. Används kabelförbindelser ska även de förläggas geografiskt åtskilda fram till ledningsplatsen. Även tillgång till flera leverantörer av infrastruktur och IP-tjänster innebär en redundans. Om ledningsplatsen är integrerad med verksamhetsställe bör ledningsplatsen vara huvudnod ur kommunikationshänseende och ordinarie verksamhetslokaler utgöra en undernod.

Nätanslutningsutredning

En viktig aspekt för funktionaliteten hos olika nätverk i ledningsplatsen är att kunna säkra yttre nätanslutningar. För att kunna optimera anslutningar av teknisknoder med avseende på nätoperatörernas ledningsnät, kanaliseringar och noder för kommunikationsnät är det lämpligt att utföra en nätanslutningsutredning. Nätanslutningsutredningen ska visa geografiska data för ledningsnät och framföringsvägar som har betydelse för ledningsplatsens tillgänglighet samt vilka förbättringsåtgärder som kan genomföras.

Fastighetsnät

Fastighetsnät är de kabelnät för informationsöverföring som finns i och mellan lokalerna och som det finns egen rådighet över. Normalt består näten av en blandning av fiber- och kopparkablar. Vid projektering av fastighetsnät är det viktigt att använda etablerade tekniska standarder vid kravställning av nätverkens olika delar. Den fysiska dragningen av näten måste ske genomtänkt för att skyddas mot olika typer av hot såsom antagonistiska handlingar, oavsiktlig fysisk påverkan och brand. Fastighetsnät och elkablar förläggs separerade från varandra.



Läs mer

- www.robustfiber.se

System för tal, video och datakommunikation

Tekniska system för tal, video och datakommunikation är en viktig funktion i en ledningsplats. Att digitalt och på ett säkert sätt kunna dela och bearbeta information är avgörande för att effektivt kunna leda verksamhet och samverka med andra aktörer. För att identifiera krav på tekniska stödsystem för tal, video och datakommunikation behöver verksamheten göra en analys över sitt eget ansvar, sina samverkansbehov samt vilken typ av information som ska utbytas, med vem och hur ofta.

Systemen för informationsöverföring bygger idag ofta på IP-teknik. Hur de tekniska lösningarna är uppbyggda skiljer sig sedan åt. Olika typer av växel-lösningar för telefoni förekommer, ofta kompletterade med mobiltelefoni och med anslutningar till ett eller flera trådlösa accessnät med inomhustäckning. Även visualiseringssystem använder IP-teknik vilket gör att information enkelt kan delas i och utanför ledningsplatsen.

För att uppnå en säker och robust informationsdelning är det viktigt att analysera alla ingående delar. Att använda ett fungerande kommunikationssystem är inte tillräckligt för att säkerställa att informationsdelningen kan ske säkert och robust utan verksamheten måste se över alla ingående aktiviteter i informationsdelningen för att säkerställa att de tillsammans uppfyller ställda krav. Det handlar till exempel om att införa och förvalta administrativa regelverk som beskriver hur kommunikationssystemet och informationen i det får användas. Kommunikationssystemet behöver också uppfylla krav utifrån it-säkerhetsperspektiv såsom brandväggar och kryptering och lokalen där kommunikationssystemet är installerat behöver förses med fysiska skydd såsom inbrotts- och brandskydd. Vidare ska den personal som hanterar kommunikationssystemet ha rätt utbildning.

Möjligheten att kommunicera bör säkerställas med så många olika tekniska system och olika operatörer som möjligt.



Läs mer

- MSB1285 Vägledning för säker och robust samverkan

It-system

Verksamheten behöver säkerhetsställa att de it-resurser exempelvis i form av nätverk, servrar, persondatorer, skrivare och programvaror som behövs finns i ledningsplatsen med rätt kapacitet och tillgänglighet. Personal för it-support måste finnas i tillräcklig omfattning.

It-resurserna ska fungera över hela hotskalan vilket gör att en analys behöver genomföras av behovet av tillgänglighet för varje del som bidrar till en fungerande ledningsplats. Analysen behöver bland annat ta hänsyn till kravställningar utifrån olika hotscenarion, verksamhetskrav för sekretess, riktighet och tillgänglighet med avseende på verksamhetens information, tillgänglighetskrav för olika system samt placering av centrala kommunikationsutrustningar, kopplingspunkter och externa och interna förbindelsevägar.

Det bör finnas ett trådlöst nätverk inom ledningsplatsen som är dimensionerat för beräknat antal bärbara datorer och smarta telefoner. Det bör även finnas ett gästnätverk avsett för samverkande aktörer.

SGSI – Swedish Government Secure Intranet

SGSI är ett intranät skiljt från internet för säker och krypterad kommunikation mellan samhällsviktiga aktörer. Nätet är utformat för att klara höga krav på tillgänglighet och driftsäkerhet. Med SGSI kan åtkomst fås till andra anslutna aktörers databaser, möjlighet att skicka skyddad e-post och att använda förbindelsen till att genomföra skyddade videokonferenser.



Läs mer

- www.msb.se sök SGSI

Radiosystem

Ett antal system på ledningsplatsen har behov av radiotäckning såsom Rakel och mobiltelefoni. I de fall byggnadens utformning avskärmar systemens radiotäckning i området används repeater eller en mindre basstation inom anläggningen.

Rakel

Rakelsystemet är Sveriges nationella kommunikationssystem för samverkan och ledning och används av aktörer inom allmän ordning, säkerhet, hälsa och försvar. Via systemet kan aktörer med samhällsviktiga uppdrag kommunicera driftsäkert och effektivt, internt eller genom samverkan med andra, i vardag, kris och krig. Rakel är byggt för att klara höga krav på robusthet, såsom att exempelvis klara långvariga elavbrott, och har en utökad robusthet jämfört med mobiltelefoni. Rakel kan, förutom att vara ett samverkanssystem, även överföra larmsignaler från verksamhetskritiska larpunkter.

**Läs mer**

- www.msb.se sök Rakel

Visualiserings- och videokonferenssystem

För att kunna förmedla aktuell lägesinformation som lägesbilder, kartor och arbetsplanering behövs ett övergripande visualiseringssystem inom ledningsplatsen. Omfattning och uppbyggnad av teknikstödet ska anpassas till verksamhetens behov och arbetsätt.

Visualiseringssystemet bör vara lättanvänt eftersom många olika personer ska kunna använda det både i vardagen och vid en samhällsstörning. Systemets funktioner ska finnas tillgängliga, lätt åtkomliga och vara användarvänliga. Placering av bildvisningsytor anpassas så att arbetet i ledningsplatsens lokaler får ett naturligt flöde. Det bör även finnas funktionalitet för att kunna dela och samarbeta i applikationer och att utföra presentationer i valfritt rum. Visualiseringssystemet kompletteras med whiteboards.

Videokonferenssystem användas i ledningsplatsen för samverkan med andra aktörer. Systemet bör integreras med visualiseringssystemet.

Omvärldsbevakning

System för mottagning och distribution av markbunden och satellitdistribuerad TV samt FM-radio bör finnas.

System för internkommunikation

Interna kommunikationssätt såsom intranät eller en applikation för mobiltelefoner kan komplettera den bredare informationsspridningen i ledningsplatsen. Därutöver kan tekniska system med exempelvis högtalare i lokalerna användas för att informera personal i verksamheten och i ledningsplatsen om pågående angrepp och för att leda utrymning. Även ordinarie brandlarmsystem kan användas för att initiera en utrymning vid angrepp. Här är det dock viktigt att göra en bedömning om samma larm ska användas för utrymning vid olika typer av händelser.

Drift och förvaltning av ledningsplatsen

Efter det att en ledningsplats utvecklats och färdigstälts behöver den vidmakthållas så att dess funktionalitet bibehålls. Även i detta skede är kontinuitetshanteringen central för att säkerställa att ledningsplatsen är robust, säker och uthållig över tid. Det gäller särskilt lokaler som inte används i vardagen. Nedan följer ett antal framgångsfaktorer för drift- och förvaltningskedet.

Engagerad verksamhetsutövare

Verksamhetens ledning har uppgiften att ge inriktning för arbetet, avsätta tillräckliga resurser och följa upp verksamheten för att ledningsplatsen ska kunna nyttjas på avsett sätt och med kort varsel. Det är av stor vikt att verksamhetens ledning är engagerad i ledningsplatsens drift- och förvaltning över tid.



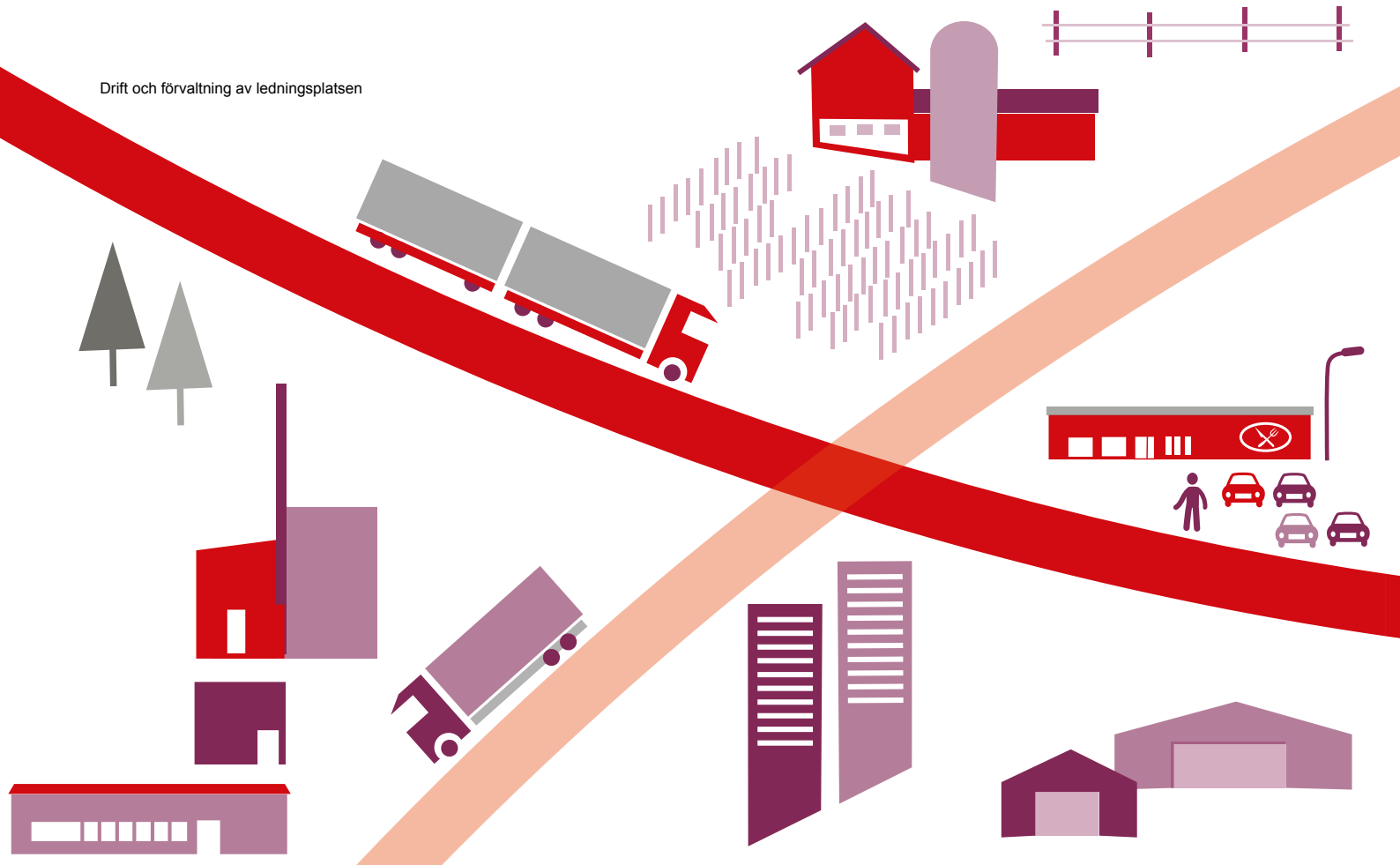
Tydligt utpekade roller och ansvarsområden

Det bör alltid vara tydligt utpekad vilken roll eller funktion som är ansvarig för ledningsplatsen, dess drift, förvaltning, försörjning och underhåll samt de olika situationer som kan uppstå. Följande är ett exempel på förekommande intressenter och ansvarsområden;

- Verksamhetens ledning ansvarar för övergripande styrningar för ledningsplatsverksamheten.
- Verksamhetens ledningsorganisation ansvarar för kravställning för ledningsplatsens utformning, funktion och uthållighet samt säkerställer att de rutiner som behövs för att ledningsorganisationen och dess stödfunktioner (betjäningorganisation) ska kunna verka i ledningsplatsen över hela hotskalan finns framtagna och att de implementeras med utbildning och övning. Rutinerna omfattar exempelvis säkerhetsskydd, yttre skydd och bevakning, sanering, sjukvård samt utrymning.
- Verksamhetens funktion som ansvarar för ledningsplatsens drift och förvaltning tillser att ledningsplatsen uppfyller ledningsorganisationens kravställningar, tekniska funktionskrav samt tillämpliga lagar och förordningar. Vidare säkerställer funktionen kompetens för driftsättning, drifthållning och underhåll samt försörjning med varor och tjänster.
- Drift- och underhållsorganisation för fastighetsförvaltning och underhåll av tekniska system kan vara verksamhetens egen eller en upphandlad extern leverantör.
- Drift- och förvaltningsorganisation för verksamhetens it-system.
- Externa leverantörer av varor och tjänster.

Ett särskilt förhållande uppstår när verksamheten hyr lokalerna. Det är då av stor vikt att säkerställa fastighetsägarens möjlighet att tillhandahålla en drift- och förvaltningsorganisation över hela hotskalan.





Prova tekniska system regelbundet

Alla byggnadens tekniska installationer – ordinarie och reserv ska provas regelbundet enligt dokumenterade rutiner. Detta kan med fördel inkluderas i övningsrutiner för driftorganisationen då även arbetssätt och rutiner testas tillsammans med tekniska system.

Driftlarm

Kritiska tekniska system i ledningsplatsen ska förses med driftlarm och larmövervakning för att minimera den tid som systemen inte fungerar enligt ställda krav.

Utbildad och övad personal

Utbildad och övad personal med kompetens i sitt ansvarsområde i ledningsplatsen är en förutsättning för att säkerställa dess funktion.

Drift- och underhållsorganisationen ska, även ur ett kontinuitetsperspektiv, ha tillräcklig kompetens för att driftsätta, handha och underhålla ledningsplatsen inklusive dess tekniska system. Här är också möjligheter till kompetensöverföring viktiga. Eftersom reserv- och nödanordningar inte används lika ofta som ordinarie funktioner behöver kompetensen upprätthållas även för dessa genom utbildning och övning.

Ledningsorganisationen och dess stödfunktioner (betjäningsorganisationen) har som verksamhetsutövare behov att utbilda och öva sig i de arbetssätt, rutiner, uppgifter och förhållanden som arbete i ledningsplatsen medför.

Personal i beredskap

Drift- och underhållsorganisationen ska ha personal i beredskap med inställetider utifrån identifierade behov. Personalen ska ha kompetens att felsöka tekniska system och kunna hantera oförutsedda händelser. Anlitas extern leverantör ska avtal finnas med inställetider för felavhjälpning av akuta störningar.

God krisledningsförmåga

Verksamheten bör utöver drift- och underhållspersonal ha en krisledning för ledningsplatsens drift och förvaltning som kan leda organisationens arbete vid större störningar i ledningsplatsen eller i dess tekniska installationer. Krisledningen bör regelbundet öva på att hantera störningar och oönskade händelser. Bland annat behöver drift- och underhållspersonalen kunna nå även då telenäten är utslagna.

Krigsorganisation

Personalstyrkan som behövs för att betjäna, drifhålla och underhålla ledningsplatsen i händelse av höjd beredskap och krig behöver krigsplaceras. Det innebär att verksamheten behöver identifiera vilka befattningar och roller som krävs i händelse av höjd beredskap och krig.



Läs mer

- MSB1183 Rätt person på rätt plats: Vägledning för myndigheters arbete med krigsorganisation och krigsplacering
- MSB1400 Rätt person på rätt plats – kommuner: Vägledning för krigsorganisation och krigsplacering
- MSB1401 Rätt person på rätt plats – regioner: Vägledning för krigsorganisation och krigsplacering

Säkerställ tillgång på kritiska varor och tjänster

Vid större händelser i vardagen och under höjd beredskap och krig behöver leveranser av kritiska varor och tjänster som exempelvis mat, drivmedel, reservdelar och serviceentreprenörer för kvalificerade tekniska installationer säkerställas. Vissa varor som mat och reservdelar kan lagerhållas. En analys bör göras av reservdelshållningen för att identifiera reservdelar som används ofta, är särskilt kritiska eller är svåra att få tag på.

För olika digitala leveranser, exempelvis av tjänster, mjukvara eller olika data, behöver redundans skapas. Det är också viktigt att kravställa om säkerhet och robusthet gentemot leverantörer och deras underleverantörer avseende deras it-miljöer och infrastrukturer som används för att möjliggöra leveransen. Misstag, olyckor eller angrepp mot sådana leveranskedjor kan få stor påverkan på verksamheten.

Samverka med viktiga leverantörer

I verksamhetens arbete med kontinuitetsshantering inkluderas behovet av samverkan och upparbetad kontakt med leverantörer som verksamheten och ledningsplatsen är beroende av. Detta kan inkludera huvudmän för fjärrvärme, fjärrkyla, el, vatten, avlopp, IP-trafik och olika it- och kommunikationstjänster. Om etablerade kontakter finns och organisationerna har förståelse för varandras förmåga och behov ökar förmågan att hantera oönskade händelser. Nedan återges exempel på krav och frågor som kan ställas till leverantör som levererar en kritisk tjänst eller produkt:

Checklista:

- ✓ Krav på kapacitet, nu och i framtiden.
- ✓ Krav på alternativa matningsvägar.
- ✓ Krav på prioritering av aktuell fastighet.
- ✓ Krav på säkerhet och robusthet i it-system och infrastrukturer som möjliggör olika digitala leveranser.
- ✓ Krav på reservlösningar och beredskap för elavbrott.
- ✓ Information om matningsnätets uppbyggnad.
- ✓ Kontaktpersoner.
- ✓ Plan för regelbundna avstämningar.

Korrekt och lättanvänd dokumentation

En korrekt och lättanvänd teknisk dokumentation utgör en förutsättning för att över tid hålla en hög kompetensnivå hos personal för driftsättning, drift och underhåll. Vidare behövs enkla handhavandebeskrivningar avsedda för användarna av de olika tekniska stödsystemen.



Myndigheten för
samhällsskydd
och beredskap