Myndigheten för samhällsskydd och beredskap

Sveriges Kommuner och Regioner

HANDBOK I KOMMUNAL KRISBEREDSKAP

2. Kommunala verksamheter

It

Handbok i kommunal krisberedskap – 2. Kommunala verksamheter – It

Det här kapitlet är en del av publikationsserien *Handbok i kommunal krisberedskap* där fler kapitel finns.

Produktion: Advant

Publikationsnummer: MSB1682 - mars 2021
ISBN: 978-91-7927-097-1

Innehåll

Övergripande beskrivning

Dagens samhälle och inte minst samhällsviktig verksamhet är i hög grad beroende av fungerande it-infrastruktur- och tjänster. Kommunal verksamhet är inget undantag. Utifrån ett krisberedskapsperspektiv är it en mycket viktig förutsättning för verksamhetens möjlighet att utföra sitt uppdrag.

Detta kapitel har två olika syften:

1. Informera om hur störningar i it-stöd kan leda till samhällsstörningar.
2. Informera om it-stödets roll vid hantering av samhällsstörningar.

Avsnittet ”Risker och sårbarheter” handlar framförallt om det första syftet medan ”planering” och ”utbildning och övning” tar upp båda syftena. Först av allt kommer dock en övergripande beskrivning av området samt vilka de främsta offentliga aktörerna på området är.

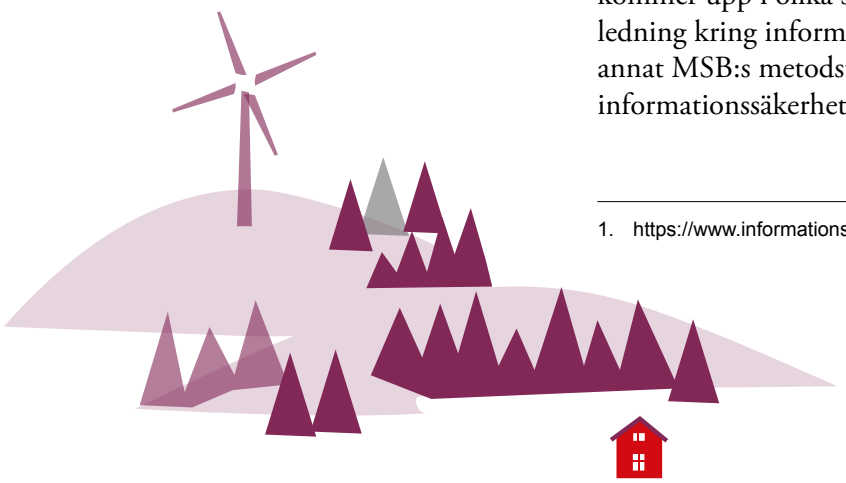
Övergripande om it-drift och -tjänster

Idag finns en stor variation i kommunernas it-miljöer. Det gäller bland annat drift av både enskilda system och it-miljö/-infrastruktur. Vissa kommuner driftar sin egen it-miljö, vissa driftar delar av den medan andra helt har utkontrakterat sin it-drift. Även för de som i hög grad svarar för egen drift sker ett skifte mot fler och fler molntjänster för enskilda verksamhetssystem. It-miljön kan därför bli mer komplex. Oavsett driftform är det viktigt att organisationen har klassat alla sina informationstillgångar utifrån behovet av konfidentialitet, spårbarhet, robusthet/tillgänglighet och riktighet.

Informationen som ges här syftar till att vara relevant oavsett hur kommunens it-stöd driftas.

Avgränsning

Syftet med detta kapitel är inte att gå in på djupet kring informationssäkerhet (inklusive it-säkerhet), även om det av naturliga skäl kommer upp i olika sammanhang. För vägledning kring informationssäkerhet, se bland annat MSB:s metodstöd för systematiskt informationssäkerhetsarbete.[1]



1. https://www.informationssakerhet.se/metodstodet/

Ansvar och roller

Här beskrivs de myndigheter, offentliga organisationer och samarbeten som är mest relevanta på området. Utöver dessa är kommunens leverantörer av hård- och mjukvara samt drift eller andra tjänster givetvis helt centrala för it-stödet.

Kommunens ansvar för it-stöd

Kommunens ansvar är att upprätthålla samhällsviktiga verksamheter – inklusive att kunna hantera samhällsstörningar. It-stöd av olika slag är ofta en förutsättning för att detta ska vara möjligt. I förlängningen är ansvaret därför att säkerställa en acceptabel nivå på leverans av it-stöd. Det finns sällan explicita krav från till exempel staten på hur it-stödet ska vara utformat eller exakt vad det ska leverera. I huvudsak är det upp till kommunen att bestämma över it-drift och det skydd som ska ges för den information som hanteras utifrån gällande lagstiftning[2].

Det finns ett fåtal lagstiftningar som innehåller konkreta säkerhetskrav gällande informationshanteringen i it-stöd och som är relevanta ur ett krisberedskapsperspektiv. En av dem är NIS-regleringen som innebär krav för de samhällsviktiga tjänster som berörs (exempelvis dricksvatten- och elförsörjning). Lagstiftningen syftar till att minska riskerna för störningar i de samhällsviktiga tjänsterna genom ett systematiskt och riskbaserat arbete med informationssäkerhet.

Författningar inom säkerhetsskyddsområdet innehåller krav på utformning och hantering av informationssystem som hanterar säkerhetsskyddsklassificerade uppgifter eller som är av betydelse för säkerhetskänslig verksamhet. I Säkerhetspolisens vägledningar ges mer information samt råd och stöd. Även MSB har visst stöd – exempelvis om så kallad fristående dator.

Läs mer

NIS-direktivet (msb.se)

Det nya totalförsvaret – En hjälp på vägen! : hantering av hemliga uppgifter i en fristående dator (msb.se)

Vägledning i säkerhetsskydd. Informationssäkerhet (sakerhetspolisen.se), säkerhetsskyddsförordningen (2018:658) och säkerhetsskyddslagen (2018:585) samt Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd (sakerhetspolisen.se).

Länsstyrelsens roll

Länsstyrelsen har inget utpekat ansvar i förhållande till en kommuns informationssäkerhet eller it-stöd. Däremot kan länsstyrelsen vara ett stöd på olika sätt. De har bland annat ett tydligt uppdrag vad gäller signalskydd- och säkerhetsskyddsfrågor.

MSB:s uppgifter

MSB:s uppgifter inom området informationssäkerhet, cybersäkerhet och säkra kommunikationer är bland annat att ansvara för utveckling och förvaltning av system för säkra kommunikationer, vara råd- och stödgivande i informationssäkerhetsarbetet och hantera samt förebygga it-incidenter.

2. Till exempel GDPR, arkivlagen och Socialstyrelsens föreskrifter om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40). Typiskt sett är dock dessa mindre relevanta ur ett krisberedskapsperspektiv.

Inom området säkra kommunikationer ansvarar MSB för utveckling och förvaltning av Rakel, SGSI (Swedish Government Secure Intranet) och WIS (webbaserat informationssystem). Detta beskrivs i handbokens kapitel om elektroniska kommunikationer.

MSB:s uppdrag inom området cyber- och informationssäkerhet är att analysera utvecklingen i omvärlden, vara regelgivande inom området samt lämna råd och stöd i det förebyggande arbetet till andra statliga myndigheter, kommuner, regioner, företag och organisationer.[3]

MSB stödjer också åtgärder som stärker kommunal ledningsförmåga. Stöd ges genom analys och rådgivning samt genom ekonomiska bidrag till tekniska åtgärder för att stärka ledningsförmåga och säkerställa robusta ledningsfunktioner. Stöd kan exempelvis lämnas för reservkraftsförsörjning av ledningsplatser och it-infrastruktur samt tekniskt skydd sett till släckutrustning, skalskydd med mera.

MSB har mandat att ge ut föreskrifter gällande informationssäkerhet, säkerhetsåtgärder för informationssystem och incidentrapportering för statliga myndigheter. Det material som finns framtaget för statliga myndigheter kan med fördel även läsas och följas av till exempel kommuner.

Läs mer

Kommunens ledningsplats (msb.se)

3. MSB:s bemyndigande att utfärda föreskrifter på området är baserade på Förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

MSB/CERT-SE

Computer Emergency Response Team, CERT-SE, är en funktion inom MSB som stödjer samhället i arbetet med att hantera och förebygga it-incidenter. Till uppgifterna hör bland annat att

- agera skyndsamt vid inträffade it-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och medverka i arbete som krävs för att avhjälpa eller lindra effekter av det inträffade. Exempelvis har CERT-SE lämnat stöd till kommuner som drabbats av allvarliga konsekvenser på grund av skadlig kod.
- samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet.
- vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder samt utveckla samarbetet och informationsutbytet med dessa.

CERT-SE publicerar information om sårbarheter och säkerhetsbrister samt förslag på åtgärder. Vid särskilt akuta eller allvarliga sårbarheter eller incidenter skickas också information direkt till berörda parter eller via en prenumerationstjänst.

CERT-SE är Sveriges nationella CSIRT (Computer Security Incident Response Team). I övriga EU:s länder finns också nationella CSIRT.

Läs mer

Hantering och förebyggande av it-incidenter – CERT-SE (msb.se)

Andra statliga myndigheter

Förutom MSB har ett antal andra myndigheter särskilt ansvar för informationssäkerhet i Sverige. Det är Post- och telestyrelsen (PTS), Försvarets radioanstalt, Försvarets materielverk/Sveriges Certifieringsorgan för it-säkerhet (FMV/CSEC), Försvarsmakten, Polismyndigheten och Säkerhetspolisen.

Dessa myndigheter samarbetar inom ramen för Samverkansgruppen för informationssäkerhet (SAMFI). Gruppen arbetar huvudsakligen inom följande aktivitetsområden:

- Strategi, handlingsplan och regelverk
- Tekniska frågor och standardiseringsfrågor
- Nationell och internationell utveckling inom informationssäkerhetsområdet
- Informationsaktiviteter
- Övningar och utbildning
- Hantering och förebyggande av it-incidenter.

Respektive myndighet har sitt ansvarsområde, men det kan för en utomstående verka komplicerat hur arbetet är uppdelat.

Nationella cybersäkerhetscentret

Regeringen aviserade under 2019 att ett nationellt cybersäkerhetscenter ska inrättas och har i budgetproposition för 2021 avsatt finansiering för centret. Försvarsmakten, Försvarets radioanstalt, MSB och Säkerhetspolisen har i ett förslag till regeringen uttryckt att syftet med centret är att det ska öka dessa myndigheters förmåga att förebygga, upptäcka och hantera cyberangrepp och andra it-incidenter.

Informationssäkerhetsnätverket Sveriges kommuner

Informationssäkerhetsnätverket Sveriges Kommuner, KIS, är ett nätverk för de som arbetar med eller har ett ansvar för arbetet med informationssäkerhet i kommuner och kommunala bolag. Nätverket bildades hösten 2010 utifrån ett behov av stärkt samverkan. Nätverkets syfte är att stärka informationssäkerhetsarbetet genom omvärldsbevakning samt erfarenhets- och kunskapsutbyte. Nätverket träffas två gånger per år samt har en digital samverkansyta för löpande erfarenhetsutbyte och liknande.

Läs mer

Nätverket KIS (skr.se)

Nätverk för offentliganställda (informationssäkerhet.se)

Forum för informationsdelning (FIDI)

FIDI är privat-offentliga samverkansforum som syftar till att genom informationsutbyte, omvärldsanalys och produktion av gemensamt informationsmaterial öka informationssäkerheten hos alla deltagande aktörer. I dagsläget administrerar MSB fem nätverk inom områdena: SCADA, hälso- och sjukvård, it-drift, telekom och finans.[4]

Externa samarbetsparter

Kommunens leverantörer av produkter och tjänster är naturligtvis avgörande för att it-stödet ska kunna upprätthållas. Som nämnts ovan ser situationen olika ut för olika kommuner. Vissa har valt att själva drifta it-miljön medan andra har valt att utkontraktera hela eller delar av den. Oavsett lösning finns det ett stort beroende av leverantörer – inte minst för informationsdelning och möjlighet att få säkerhetsuppdateringar och support.

I fortsättningen av kapitlet beskrivs relationen till leverantörer bland annat kring upphandling och inköp.

4. Mer information hittas här: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/samverkan-inom-informationssakerhet/ Hämtad 2020-08-18.

Planering

Avsnittet innehåller information om hur en kommun genom planering kan öka robustheten i de it-stöd som används. Det beskriver förebyggande arbete, upphandling och avslutas med hantering av inträffade incidenter.

Planeringen genomförs av olika delar av kommunen. Vissa delar utförs av en it-avdelning eller motsvarande funktion, vissa utförs av den verksamhet som använder it-stöd och vissa delar utförs inom krisberedskapsområdet. I många fall är det lämpligt att planera tillsammans.

Upphandling av it-stöd

Leverantörsrelationer är mycket viktiga för en kommuns it-stöd. Det främsta sättet på vilka dessa kan styras är genom upphandlings-/inköpskrav samt överenskomna avtalsförhållanden. Det finns olika stöd för att göra en lyckad upphandling. MSB:s vägledning ”Upphandling till samhällsviktig verksamhet” fokuserar på hur behov av krisberedskap i samhällsviktig verksamhet kan inkluderas i inköpsprocesser. Vägledningen ger stöd i hela upphandlingsprocessen från planering av den till förvaltning av ett ingånget avtal.

Stöd för upphandling av tjänster och produkter ur ett informationssäkerhetsperspektiv finns i MSB:s vägledning ”Upphandla informationssäkert – en vägledning”. Där finns bland annat ett kapitel som handlar om kravställning vid upphandling av it-system. e-SAM har också tagit fram en vägledning kring it-avtal.

Finansiella sektorns privat-offentliga samverkan (FSPOS) har tagit fram en vägledning kring kontinuitetshantering. I den finns stöd för hela upphandlingsprocessen, från att analysera verksamhetens krav på kontinuitet och hur dessa sedan kan omsättas i upphandlings- och avtalskrav till uppföljning och avslut av ett avtal. Till skillnad från ovan nämnda vägledningar har denna just ett fokus på kontinuitetshantering.

Figur 1. Inköpsprocessens steg.
Källa: Upphandlingsmyndigheten

Läs mer

Upphandling till samhällsviktig verksamhet – en vägledning (msb.se)

Upphandla informationssäkert – en vägledning (msb.se)

It-avtal – en vägledning om it-tjänsternas avtal (pdf, esamverka.se)

FSPOS Vägledning för Kontinuitetshantering (pdf, fspos.se)

Utkontraktering inklusive molntjänster

Inom krisberedskapsområdet samt civilt försvar måste särskild hänsyn tas till utkontraktering till externa leverantörer. I begreppet utkontraktering ingår även det som vardagligt kallas molntjänster. Utkontraktering kräver överväganden både vad gäller juridiska förutsättningar och lämplighet ur andra aspekter. Ett grundläggande moment är att inför en utkontraktering genomföra en informationsklassning.

Den juridiska situationen kring molntjänster är i vissa avseenden oklar. Det råder olika uppfattningar om sekretessbelagd information är att betrakta som röjd om den kan bli tillgänglig för rättsvårdande myndigheter i andra länder utan en föregående rättsprövning av svenska myndigheter. Inom krisberedskapsområdet förekommer många informationsmängder[5] som kan vara bedömda som sekretessbelagda i enlighet med offentlighets- och sekretesslagen. Dessa uppgifter kräver alltså särskilda överväganden vid eventuell utkontraktering.

En statlig utredning har i uppdrag att bland annat analysera de rättsliga förutsättningarna för statliga myndigheter, kommuner och regioner att med bibehållen säkerhet utkontraktera it-drift till privata leverantörer (dir 2019:64).

Det finns också andra överväganden att göra än sådana som är rent juridiska. Kan en utkontraktering, inklusive användning av molntjänster, leda till högre driftsäkerhet även i en samhällsstörning? Hur påverkas sådana lösningar vid en samhällsstörning – kommer leverantören kunna upprätthålla sina åtaganden? Finns risk att leverantörens åtaganden upphör genom hänvisning till force majeure?

Försäkringskassan utkom under hösten 2019 med rapporten ”Vitbok – Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt”. Enligt Försäkringskassan måste det göras en bedömning om det är lämpligt att svenska myndigheter, genom användning av framförallt publika molntjänster, lämnar ifrån sig kontrollen över uppgifter i samhällsbärande verksamhet till privata företag eller till andra länder.

Läs mer

Säker och kostnadseffektiv it-drift för den offentliga förvaltningen (regeringen.se)

Vitbok – Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt (pdf, forsakringskassan.se)

Säkerhetsskyddade upphandlingar/inköp

Om det i en upphandling förekommer säkerhetsskyddsklassificerade uppgifter (säkerhetsskyddsklass konfidentiell eller högre) eller ges åtkomst till i övrigt säkerhetskänslig verksamhet av motsvarande betydelse är den upphandlande myndigheten skyldig att ingå ett säkerhetsskyddsavtal. Därför måste myndigheten analysera vilka skyddsvärden som finns i upphandlingen. Säkerhetspolisen har föreskrifter och vägledning om förfarandet vid upphandlingar som omfattas av säkerhetsskyddslagen.

Vid användning av externa leverantörer kopplat till it-stöd för säkerhetskänslig verksamhet kan det behöva tecknas säkerhetsskyddsavtal. Det kan exempelvis röra sig om VA-verksamhet, el- eller värmeförsörjning. Säkerhetsskyddsklassificerade uppgifter kan vara information om säkerhetskänslig verksamhet i egen eller annans regi men kan också innefatta uppgifter om till exempel totalförsvarsplanering.

Läs mer

Säkerhetsskydd vid upphandlingar och affärsavtal (sakerhetspolisen.se)

5. Även informationstillgångar som hanterar uppgifter som rör själva it-miljön kan komma att bedömas omfattas av sekretess enligt offentlighets- och sekretesslagen 15:2, 18:8 eller 18:13.

SKR:s verktyg KLASSA

Ett stöd i upphandlingsarbetet är att använda sig av SKR:s verktyg KLASSA. Genom att först informationsklassa molntjänsten kan man sedan få förslag på upphandlingskrav. Kraven är i mångt och mycket baserade på de säkerhetskontroller som finns i ISO 27001. Det finns även exempel på kontroller i standarden.

Det pågår ett arbete att uppdatera KLASSA. En ny version kommer under 2021.

Läs mer

KLASSA, informationsklassning (skr.se)

Force majeure

Kravställningen kring force majeure blir viktig när it-stöd som upphandlas/köps in är centralt för att bedriva samhällsviktig verksamhet. Givetvis är det särskilt viktigt ju större beroende man har till en extern part. Force majeure beskriver under vilka onormala eller oförutsedda händelser som en avtalspart inte är bunden av sina förpliktelser enligt avtalet. Naturkatastrofer, statliga ingripanden, krig och arbetskonflikt är exempel på sådana händelser.

För att säkerställa att samhällsviktig verksamhet fungerar även under denna typ av förhållanden måste en force majeure-klausul utformas noggrant. Den får inte ges en vidare möjlighet till befrielse än vad som är motiverat med hänsyn till verksamhetens speciella art. Klausulen bör formuleras så att uppräknade händelser är uttömmande, det vill säga att inga andra händelser kan åberopas som force majeure. Det ger förutsägbarhet och begränsar möjligheten att åberopa force majeure.

Mer detaljerad vägledning finns i MSB:s vägledning ”Upphandling till samhällsviktig verksamhet”.

Kontinuitetshantering

Med kontinuitetshantering kan organisationer snabbare återhämta sig från och mildra konsekvenserna av en inträffad händelse. Det handlar om att planera för att upprätthålla sin verksamhet på en tolerabel nivå oavsett vilken störning den utsätts för. Till exempel när personalen inte kommer till jobbet, lokalerna inte går att använda, leveranser av viktiga varor och tjänster inte når fram eller organisationen drabbas av strömavbrott.

Kontinuitetshantering innebär framförallt att genomföra följande aktiviteter:

- Identifiera viktiga verksamheter och processer
- Kartlägga deras beroenden av resurser (personer, varor, tjänster etc.)
- Bestämma vad som är acceptabel avbrottstid för respektive process/verksamhet
- Genomföra åtgärder som minskar risken för störningar
- Skapa planer och reservrutiner/alternativa arbetssätt för att hantera de störningar som ändå kan uppstå.

Samhällsviktiga verksamheters beroende av och krav på återställningstid sätter krav på hur snabbt it-stödet ska kunna hantera störningar. Av naturliga skäl är det därför nödvändigt att verksamheterna är tydliga i sin kravställning. Är it-verksamheten intern ska kraven kommuniceras på det sätt som är etablerat i organisationen. Om driften är extern sker det ofta via tjänsteavtal, där SLA (Service Level Agreement) styr nivåer av tillgänglighet för it-tjänster.

När störningar inträffar för en digital tjänst börjar it-verksamheten arbeta i enlighet med sin kontinuitetshantering och de kontinuitetsplaner som finns för att hantera störningar.

MSB har ett omfattande stöd till aktörer för deras arbete med kontinuitetshantering som finns publicerat i form av en verktygslåda. Här finns även vägledning om kontinuitetshantering för informationstillgångar.

Läs mer

Kontinuitetshantering (msb.se)

Kontinuitetshantering för informations-tillgångar (informationssakerhet.se)

Katastrofplanering inom it-verksamheter

It-verksamheters hantering av särskilt allvarliga händelser beskrivs ofta i en ”katastrofplan”. Den beskriver bland annat vilka system/tjänster som är högst prioriterade att upprätthålla/återställa funktionalitet i, vilka som kontaktas vid störningar, intern- och externkommunikation med mera.

En del i katastrofplaneringen handlar ofta om alternativa sätt att upprätthålla drift av åtminstone grundläggande it-infrastruktur och de viktigaste verksamhetssystemen vid en störning i ordinarie serverhall (till exempel brand eller vattenskada).

Beroende på verksamhetens krav och kommunens risktolerans finns olika lösningar. De bästa men också mest kostsamma är att ha speglade serverhallar på olika geografiska platser. Om den ena går ner ska den andra sömlöst kunna ta över driften. Avbrottstiden blir då i stort sett inte märkbar. Ett alternativ är att ha en förberedd alternativ hall med hårdvara på plats men som inte är aktiv utan aktiveras vid en störning. En sådan lösning innebär en avbrottstid vars längd bestäms av den specifika lösningen som valts. Ett tredje alternativ är att ha en site som är förberedd med den grundläggande infrastrukturen för att kunna fungera som serverhall men utan faktiska servrar. Utrustning köps/hyrs in och installeras vid behov.

En redundant lösning måste inte nödvändigtvis driftas av den egna kommunen. Externa leverantörer kan som molntjänst leverera en redundant serverlösning inklusive lagring av backup. Innan en sådan lösning kan väljas görs en noggrann riskanalys och krav regleras med leverantören. Det kan också vara nödvändigt att ingå säkerhetsskyddsavtal.

Vilken lösning som väljs bestäms bland annat av hur långa avbrott som kan accepteras. Är kraven mer eller mindre kontinuerlig drift? Kan avbrott på några timmar tolereras? Eller klarar sig kommunen utan fungerande it-drift i flera dagar/veckor?

Det måste också avgöras vilka system och tjänster som kommunen driftar som ska finnas i en sådan redundanslösning. Ju fler system, desto mer kostsam blir lösningen.

För att snabbt och effektivt kunna nå ut till dem som är berörda av en störning inkluderar en katastrofplan också kommunikationsaspekter. Här finns kopplingar till kommunens kriskommunikationsplan särskilt vad gäller internkommunikation. Kriskommunikationsplanen innehåller rutiner för när, hur och av vem som medarbetare och ansvariga ska få information vid samhällsstörningar. Vid en del it-incidenter kommer tänkta kommunikationssätt inte vara tillgängliga, till exempel intranät eller e-post. It-verksamhetens katastrofplan kan innehålla viktig information om hur de planerar att nå medarbetare i sådana situationer.

It som stöd inom krisberedskapsområdet

Avsnittet beskriver hur hantering av en samhällsstörning kan vara beroende av fungerande it-stöd. Det beskriver både den egna kommunens behov men också aspekter kring det geografiska områdesansvaret på lokal nivå.

Det ger förståelse för att olika it-stöd är viktiga i hantering av samhällsstörningar samt förståelse för hur sådana kan identifieras och vikten av att dessa kravställs och hanteras på lämpligt sätt.

Kommunal krisberedskap och krisledningsförmåga är beroende av en rad it-system, teknisk utrustning och digitala tjänster. Några exempel på det inom viktiga funktioner inom krisledningsförmåga ges nedan:

- Kriskommunikation: telefoni, webbplats, intranät och sociala medier.

- Analys: geografiska informationssystem (GIS) samt information/fakta som är lagrad digitalt.
- Samverkan: WIS och e-post.

Det är viktigt med en förståelse för hur det totala beroendet ser ut. Lämpligt kan då vara att först identifiera alla kritiska produkter och tjänster för krisledningsarbetet. Där identifieras sannolikt både direkta beroenden av it-stöd i form av enskilda resurser (till exempel mjukvara i form av WIS, e-postklient, GIS-lösningar, extern webbplats och intranät men också hårdvara i form av datorer, projektorer och nätverksutrustning) men också indirekta beroenden eftersom andra kritiska resurser kan vara beroende av it för att vara tillgängliga (till exempel informationstillgångar som är digitalt lagrade internt eller externt).

När viktiga resurser identifieras bör det, efter att maximala avbrottstider fastslagits, säkerställas att dessa har en tillräckligt hög grad av robusthet så att de kan användas också under störda förhållanden. Det bör också säkerställas att det finns acceptabla reservrutiner om resurserna inte är tillgängliga. Hur höga kraven ska vara på it-resurserna avgörs av bland annat vilka tolerabla avbrottstider krisledningsorganisationens aktiviteter kan acceptera. Vanliga lösningar för att öka tillgängligheten är att duplicera data på flera speglade diskar och att nätverks- och kommunikationsutrustning är dubblerad. För kommunikation på längre avstånd gäller dels flera vägar, exempelvis flera fiberkablar, olika tekniker samt radio eller satellit som alternativa vägar. Analoga reservalternativ bör finnas.

Inte bara tillgänglighet är viktigt att säkerställa även krav på konfidentialitet och riktighet måste beaktas. Om information förvanskas kan stora konsekvenser uppstå i form av försämrade förutsättningar att hantera samhällsstörningen. Det kan också leda till problem efter hanteringen av en händelse, till exempel om beslutsgrunder har förvanskats eller dokumentation över fattade beslut inte överensstämmer med de faktiska besluten.

Planering av it-stödet bör inkludera att krishantering kan behöva ledas både från ordinarie och från en alternativ plats. It-avdelningen eller sourcingpartnern behöver vara med i en sådan planering. De bör också vara med på krishanteringsövningar.

Särskilda förutsättningar för inriktnings- och samordningsfunktion (ISF)

ISF är en tillfälligt sammansatt aktörsgemensam funktion för att sluta överenskommelser om inriktning och samordning vid hantering av en samhällsstörning. På lokal nivå leds den av kommunen. Vid de tillfällen ISF:en liknar en gemensam stab där externa aktörer ingår ansvarar kommunen för att ge lämpligt tekniskt stöd. Det handlar bland annat om nätverk med internettillgång, lösningar för gemensam fillagring och skrivartjänster samt att möjliggöra för externa parter att använda egen utrustning såsom dator/telefon från en gemensam lokal.

Kraven på tekniska lösningar varierar beroende på om en ISF ska bedrivas fysiskt och/eller på distans. Oftast behöver dokument och inte minst loggböcker vara tillgängliga från flera platser samtidigt. Det är inte osannolikt att vissa parter kan behöva ansluta till gemensamma möten på distans. Det måste därför finnas förberedda lösningar i form av video- eller telefonkonferensutrustning och mjukvarulösningar för mötet. Det bör finnas flera sätt att bedriva möte på distans för att skapa redundans.

Det måste vara tydligt överenskommet om det finns begränsningar kring vilken typ av information som kan hanteras i olika tekniska lösningar; framförallt information som är sekretessbelagd sätter gränser. Några exempel är att WIS inte är byggt för att hantera sekretessbelagd information samt att det som skickas via post måste anses vara helt oskyddat.

Samtidigt måste en riskavvägning göras – i vissa lägen är det viktigare att snabbt få fram information än att skydda informationen från obehörig åtkomst. Då kan känslig information behöva överföras i tjänster som till vardags inte ska användas för sådan information.

Hur aktörerna i en ISF ska arbeta tillsammans med stöd av it-lösningar behöver förberedas, gärna aktörsgemensamt. Att tillsammans identifiera hur samarbetet ska stödjas av it-lösningar och sedan förbereda dessa minskar risken att under en pågående samhällsstörning behöva ta fram sådana lösningar.

Läs mer

Samlingssida för material om Lokal ISF (msb.se)

Planering av it-stöd för stabsarbete

Nedan följer några konkreta råd som är bra att ta med i förberedelserna för att hantera en samhällsstörning. Råden utgår från att någon form av stabsfunktion används. Typiskt sett är det stabens sambandsfunktion som ansvarar för arbetet nedan:

- ☐ Förbered funktionsinloggningar för datorer/konton i den egna it-miljön. Dessa ska kunna användas av både egen personal i stab samt samarbetspartner från andra organisationer/frivilliga (dock krävs konton med olika behörigheter). Konton som inte är knutna till en specifik person underlättar ofta samarbete.
- ☐ Förbered funktionsinloggningar för datorer/konton i den egna it-miljön. Dessa ska kunna användas av både egen personal i stab samt samarbetspartner från andra organisationer/frivilliga (dock krävs konton med olika behörigheter). Konton som inte är knutna till en specifik person underlättar ofta samarbete.
- ☐ Samarbetspartner lånar dator och loggar in med ett särskilt gästkonto. Dessa får endast tillgång till gemensamma fillagringsytor som används för samarbetet organisationerna emellan, skrivarresurser, internet och eventuella andra samarbetslösningar. Om samarbetspartner arbetar i egna datorer går det inte att säkerställa driftsäkerhet, att det tas backup för att undvika informationsförlust med mera.
- ☐ Förbered med funktionsadresser (e-post) för respektive funktion i staben. Om det är en liten organisation kanske det räcker med en brevlåda för hela staben. Vid en händelse måste det hela tiden vara tydligt vem som ansvarar för att bevaka den.
- ☐ Organisationens stab bör ha funktionstelefoner/-telefonnummer. Gärna en telefon per roll i en stab. Eller som lägstanivå ett telefonnummer in till staben (om det är en liten stab/begränsad händelse).
- ☐ Planera för var information ska lagras och hur alla berörda aktörer (om möjligt och lämpligt även externa) får tillgång till en sådan lagringsyta.
- ☐ Förbered att kunna hantera händelser från alternativa lokaler. Det innebär att bland annat kunna sätta upp ett trådlöst nätverk (kommuninternt och gästnät), skrivare, utrustning för distansmöten, projektorer och internetaccess.

Vid hantering av en samhällsstörning är det viktigt att så snart som möjligt ta in resurser från it-avdelningen/sourcingpartnern för att kunna hantera eventuella behov av it-stöd. Länsstyrelsen kan också kontaktas för att få hjälp från andra myndigheter. MSB:s förstärkningsresurser för samverkan och ledning kan också vara aktuella att kontakta.

Informationssäkerhetsrisker vid hantering av en samhällsstörning

Att arbeta under en samhällsstörning kan öka informationssäkerhetsrisker. Nya arbetssätt, annan personal, nya samarbetspartner och en ökad stress öppnar upp för sårbarheter. Det kan exempelvis handla om

- ökad risk för mänskliga misstag, till exempel att sprida känslig information till fel personer/aktörer
- risk att bli utsatt för bedrägerier (också kallat social ingenjörskonst)
- risk att viktig information inte hanteras på ett sätt som gör att tillgången till den säkras. Exempelvis att det inte finns backup på viktig information eller att den inte går att nå när den behövs. Något som kan bli följden till exempel när information lagrats lokalt på en stabsmedlems dator och hen inte är tillgänglig.

En analys över denna typ av risker bör göras i det förberedande krishanteringsarbetet. Det bör påverka utformningen av både de tekniska och de organisatoriska lösningarna som väljs.

Incidenthantering

En it-incident kan beskrivas som en oönskad och oplanerad it-relaterad händelse som kan påverka säkerheten i organisationens informationshantering och/eller kan innebära en störning i organisationens förmåga att bedriva sin verksamhet. En it-incident kan vara en händelse som påverkar till exempel hård- eller mjukvara, informationstillgångar, kommunikation eller drift.

Hantering av incidenter görs vanligtvis både av den som är ansvarig för drift av den påverkade tjänsten/funktionen och av den verksamhet som är beroende av tjänsten/funktionen. De förstnämnda arbetar för att återställa funktionaliteten medan de senare arbetar efter sin kontinuitetsplan. Vid allvarliga incidenter kan en kommuns krishanteringsorganisation behöva aktiveras.

Rekommenderade processer för att hantera it-incidenter innehåller i stort sett samma moment oavsett vilken organisation som föreslagit dem. Standarden ISO 27035 föreslår följande:

1. Planera och förbereda. Bland annat att ha tydliga rutiner samt att ha utpekade och övade funktioner för incidenthantering.
2. Detektera och rapportera. Bland annat aktiviteter för att upptäcka sårbarheter och händelser samt att samla information om och rapportera dem.
3. Bedöma och besluta. Att samla in och analysera information samt besluta om det skett en incident.
4. Hantera. Att stoppa incidenten, undanröja problemet, kommunicera med interna och externa parter samt återgå till normala förhållanden.
5. Utvärdera och lära. Identifiera lärdomar, se över informationssäkerhetsåtgärder, se över incidenthanteringsprocessen samt att dela resultat med betrodda parter.

Den som arbetar med kommunal krisberedskap bör ha kunskap om den egna kommunens incidenthanteringsprocess. Det är också bra att ha dialog med driftansvariga om hur deras process kopplar an till kommunens planering för hantering av samhällsstörningar.

När allt fler tjänster driftas av externa leverantörer behöver det också finnas tydliga rutiner för deras incidenthantering i relation till kommunen. När ska kommunen kontaktas, vem ska kontaktas och hur den fortsatta hanteringen i kommunen ser ut är sådant som behöver överenskommas.

Det är viktigt att ha olika system och tjänster listade i rangordning och vilka korsvisa beroenden som finns så att system kan återstartas i rätt ordning. Prioriteringen kan variera över säsong eller tid (exempelvis runt bidrags- och lönekörning etc.).

Läs mer

Incidenthantering (informationssäkerhet.se)

Krav på incident-rapportering

Kommunen omfattas av olika rättsliga krav på rapportering av incidenter som rör it-stöd och digitala tjänster. De som finns inom NIS-direktivet och säkerhetsskyddslagen är mest aktuella att känna till för kommuner.

Enligt NIS-direktivet ska leverantörer av samhällsviktiga tjänster rapportera incidenter som orsakar störningar vilka får betydande inverkan på kontinuiteten i tjänsten. Vilka incidenter som ska rapporteras och till vilken myndighet styrs av MSB:s föreskrifter. Dessa incidenter kan även ge upphov till samhällsstörningar (t ex allvarliga störningar i el- eller dricksvattenförsörjningen) och därav behov av att aktivera kommunens krisledningsorganisationen.

Säkerhetsskyddsförordningen ställer i sin tur krav på rapportering av så kallade säkerhetshotande händelser. Anmälan görs till Säkerhetspolisen om något av följande har hänt:

1. En säkerhetsskyddsklassificerad uppgift kan ha röjts.
2. Om det inträffat en incident i ett informationssystem som kommunen är ansvarig för och som har betydelse för säkerhetskänslig verksamhet och där incidenten allvarligt kan påverka säkerheten i systemet.

Kommunens säkerhetsskyddsanalys visar vilka säkerhetsskyddsklassificerade uppgifter som finns och hur de hanteras samt information om eventuell säkerhetskänslig verksamhet.

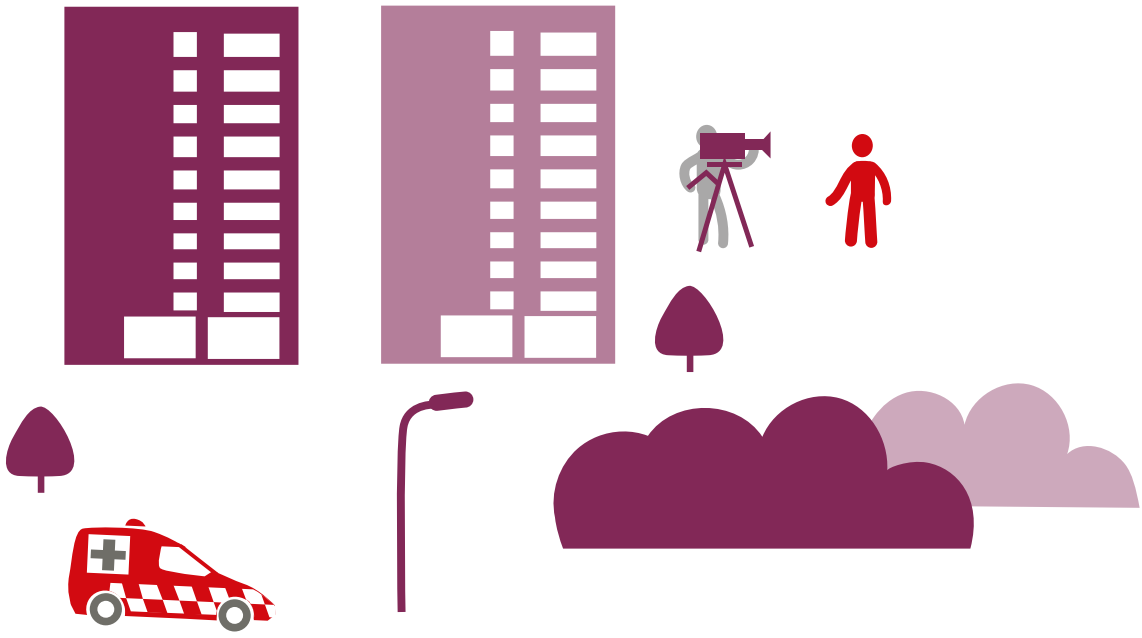
Utöver dessa rapporteringskrav kan kommunen frivilligt anmäla incidenter till CERT-SE.

Läs mer

Incidentrapportering för leverantörer av digitala tjänster (msb.se)

Anmälan vid säkerhetshotande händelser och verksamhet (sakerhetspolisen.se)

Säkerhetsskyddsförordning (2018:658) (riksdagen.se)



Risker och sårbarheter

Här beskrivs kopplingar till kommunens övergripande arbete med risk- och sårbarhetsanalyser (RSA). Det ges också exempel på typer av risker som är relevanta ur ett krisberedskapsperspektiv. Avsnittet avslutas med information om statliga myndigheters rapportering av it-incidenter.

Risk- och sårbarhetsanalys kopplat till it-stöd

I den kommunövergripande risk- och sårbarhetsanalys som finns beskriven i MSB:s föreskrifter 2015:5 ingår bland annat att identifiera samhällsviktig verksamhet inom kommunens geografiska område och att identifiera kritiska beroenden för kommunens samhällsviktiga verksamhet. It-stöd kan både vara en samhällsviktig verksamhet i sig men även utgöra kritiskt beroende till andra samhällsviktiga verksamheter. När sådana beroenden identifieras är det lämpligt att inte bara riskhantera utan också kontinuitetshantera verksamheten, något som beskrivs i avsnittet Planering.

I risk- och sårbarhetsanalysen ingår också att identifiera och analysera risker inom kommunens geografiska område. Större störningar i it-relaterat stöd kan vara något som leder till samhällsstörningar, varför risker kring it-stöd med fördel ingår i RSA-arbetet.

Det ställs också högre krav på riskhantering i it-stöd för vissa samhällsviktiga verksamheter. NIS-regleringen innebär krav på systematiskt riskhanteringsarbete för it-stödet inom bland annat el- och dricksvattenförsörjning samt hälso- och sjukvård. Likaså innehåller elberedskapslagen (1997:288) krav på producenter och distributörer av el att upprätta risk- och sårbarhetsanalyser av säkerheten i den egna verksamheten. Livsmedelsverkets föreskrifter om dricksvatten (SLVFS 2001:30) innebär i sin tur krav på VA-huvudmannen att bedriva riskhantering. Både affärssystem och cyberfysiska system är relevanta att bedriva riskhantering för, sett till dessa lagstiftningar.

Att ensa de olika riskhanteringsprocesserna ger resurseffektivitet och minskar arbetsbördan för berörda verksamheter.

Risker inom området

Samhällets beroende av fungerande it-stöd ökar. Tidigare gick det att tillfälligt återgå till manuella rutiner och arbetssätt, men digitaliseringen har nu gått så långt att fungerande it-system allt som oftast måste ses som nödvändigt för att bedriva en verksamhet. En naturlig följd av det är att störningar i it-miljön riskerar att få allt större konsekvenser och leda till samhällsstörningar.

Nedan ges exempel på några olika risker som kan leda till samhällsstörningar. Fokus ligger på störningar i tillgänglighet och till viss del informations riktighet. Men det finns också risker utifrån konfidentialitet, vilket också är relevant ur ett krisberedskapsperspektiv.

Cyberattacker

En cyberattack utförs av en angripare. Det kan till exempel vara brottslingar motiverade av ekonomisk vinning eller aktörer kopplade till stater som agerar utifrån sina nationella intressen. Attacker kan vara riktade mot en viss organisation och/eller mer slumpmässigt eller urskillningslöst attackera olika funktioner i samhället.

I nedan fördjupningsmaterial ges en översikt kring hotaktörer och vilka metoder de kan använda sig av. samt rekommendationer om vilka grundläggande åtgärder som bedöms minska sårbarheterna.

Läs mer

Nationellt center för cybersäkerhet (msb.se)

Cybersäkerhet i Sverige 2020 – Hot, brister, beroenden och metoder (pdf, msb.se)

Cybersäkerhet i Sverige 2020 – Rekommenderade säkerhetsåtgärder (pdf, msb.se)

Nedan ges ett par exempel på vanliga cyberattacker.

Överbelastningsattack

En överbelastningsattack (också kallad denial of service (DoS)-attack) syftar till att göra tjänster onåbara/oanvändbara. En sådan attack kan både rikta sig mot tjänster som riktar sig till att ge medborgare information, mot tjänster som används för att styra och övervaka delar av it-miljön eller mot samhällsviktiga verksamheters digitala tjänster.

Ofta rör det sig om så kallade DDoS-attacker (Distributed Denial of Service) som innebär att många olika internetanslutna enheter kontaktar en webbplats med skräpdata i syfte att överbelasta och därmed göra den otillgänglig. Ett exempel är från valdagen 2018 då Valmyndighetens webbplats inte gick att nå under sammanställningen av röstresultaten.

För en kommun kan denna typ av attack störa åtkomsten till viktiga tjänster riktade mot invånarna, såsom webbplats eller e-tjänsteportal. Om en sådan attack utförs när kommunikationsbehovet är stort, som under en samhällsstörning, kan den få omfattande konsekvenser. Det är bra att ha en planering för hur sådana situationer ska hanteras samt ha skydd mot att det händer.

Det kan innebära allvarliga konsekvenser för dricksvatten- eller elförsörjning om en överbelastningsattack ger störningar i övervakningen eller styrningen av styrsystemen (eller andra cyberfysiska system såsom IoT-enheter).

Ibland används överbelastningsattacker för att dölja det egentliga syftet hos en angripare. När en attack hanteras är det därför viktigt att fortsatt arbeta på bredden med säkerhetsarbetet och inte endast fokusera på att hantera den pågående attacken.

Läs mer

Denial of Service (DoS) guidance (ncsc.gov.uk)

Avsiktlig attack släckte valsajt i Sverige (svt.se)

Skadlig kod med fokus på utpressningsprogram

Skadlig kod är ett vanligt hot mot it-miljön och kan påverka de system och tjänster som används samt hårdvara och information. Skadlig kod kan sprida sig snabbt, ändra sig efter behov och ta sig in via slutanvändares utrustning, e-postbilagor, webbsidor, molntjänster och bärbara lagringsmedier. Modern skadlig kod har också utvecklats för att undgå, angripa eller inaktivera säkerhetsfunktioner.

Ett vanligt sätt att få in skadlig kod är genom att lura användaren att klicka på en länk, ladda ner en bilaga eller köra vissa funktioner i ordbehandlings- och kalkyldokument.

Utpressningstrojaner (ransomware) är en nu mycket vanlig typ av skadlig kod med ett mål att kryptera informationstillgångar och därmed göra dessa otillgängliga. Angreppet kan även utformas att stjäla information. Vanligtvis får den drabbade organisationen information om att en lösensumma måste betalas för att återfå kontroll över sin information. Det finns även exempel på när syftet varit att göra informationen permanent oläsbar, det vill säga det finns ingen dekrypteringsnyckel oavsett om en lösensumma skulle ha betalats.

I en kommun skulle utpressningsprogram kunna leda till att viktig information och it-system inte går att använda vilket kan ge upphov till en samhällsstörning. Det kan också leda till att känslig information om invånare[6] eller samhällsviktig verksamhet förstörs eller sprids till obehöriga.

Ett exempel är en svensk kommun som under 2019 drabbades av ett utpressningsprogram. Incidenten uppstod genom en kombination av att medarbetare lurades att ladda ner en bilaga eller klicka på en länk i e-post samt att det fanns en sårbarhet i en viss mjukvara som kommunen använde. Konsekvenserna blev omfattande trots en effektiv hantering. Bland annat ominstallerades en stor del av alla datorer.

Ett exempel på internationell nivå är att under 2017 utsattes ett stort antal organisationer runtom i världen för utpressningsprogrammen WannaCry och NotPetya. Även organisationer i Sverige angreps. Angreppen möjliggjordes av en sårbarhet i Windows som utnyttjades för att installera den skadliga koden. Microsoft hade publicerat en säkerhetsuppdatering ett par månader innan den skadliga koden spreds, men många organisationer hade inte installerat den och var alltså sårbara.

För att ha en it-miljö så säker som möjligt mot angrepp är det bästa att alltid ha den senaste säkerhetsuppdateringen installerad på varje enskilt informationssystem. Vissa informationssystem kan dock vara svåra att uppgradera, till exempel utifrån de störningar själva uppgraderingsarbetet kan innebära eller att det finns beroenden till andra informationssystem som är svåra att hantera. Det kan exempelvis vara fallet med äldre cyberfysiska system i kommunalteknisk infrastruktur. Går det inte att göra viktiga uppdateringar måste kompensatoriska åtgärder vidtas, till exempel att placera systemet där det inte är nåbart från internet eller organisationens administrativa nätverk.

Läs mer och konkreta råd

Utpressningsvirus trendar (cert.se)

Öka motståndskraften mot ransomware (pdf, msb.se)

Mitigating malware and ransomware attacks (ncsc.gov.uk)

Pågående ransomware-kampanj (WannaCry/Wcry/WannaCrypt0r) (cert.se)

Kryptomaskar och deras konsekvenser. Åtgärder för cybersäkerhet utifrån fallen WannaCry och NotPetya. (foi.se)

6. Många patienter till ett terapiföretag i Finland drabbades av att deras journaler spreds under hösten 2020. https://www.svt.se/nyheter/utrikes/tusentals-journaler-lackta-fran-finskt-terapiforetag

Driftstörningar

När it-stöd inte levereras enligt verksamheternas och samhällets behov riskerar det att leda till samhällsstörningar. Det finns en stor mängd olika sorters driftstörningar och de kan drabba både egen it-verksamhet och leverantörer av produkter och tjänster. Nedan ges några exempel på sådana störningar.

Driftstörning it-infrastruktur

Med it-infrastruktur avses här de tekniska lösningar som är nödvändiga för leverans av it-stöd. Infrastrukturen består både av hårdvara såsom servrar och nätverksutrustning och av den mjukvara som behövs för att it-miljön ska fungera. Infrastrukturen har i sin tur beroenden till sådant som el, elektronisk kommunikation och personal.

It-infrastrukturen kan påverkas av en stor mängd hot. Störningar i beroenden mellan olika informationstillgångar är en kategori av hot. Mjukvarurelaterade problem är en annan. En tredje kategori utgörs av fysiska risker såsom brand, översvämning och elavbrott.

Vad gäller just fysiska hot mot it-infrastruktur har MSB tagit fram en vägledning om fysisk säkerhet i it-utrymmen. Den beskriver både hur analyser kring fysisk säkerhet kan genomföras samt vilka åtgärder som kan vara lämpliga.

Läs mer

Vägledning för fysisk informationssäkerhet i it-utrymmen

Driftstörning i cyberfysiska system

Samhällsviktig verksamhet är i allt högre grad automatiserad och digitaliserad. Detta bland annat genom så kallade cyberfysiska system (it-system som i slutändan styr någon form av fysisk process). Det ger möjlighet till sådant som att på distans läsa av nivåer i reservoarer och styra produktion och distribution av dricksvatten. Andra exempel finns inom fastighetsautomation, skalskydd och modern välfärdsteknik.

Tekniken kan öka både effektivitet och driftsäkerhet men medför också risker som måste hanteras, precis som med övrig digitalisering. Avbrott kan medföra störningar i de processer systemet stödjer. Obehörigt intrång i systemen kan ge angripare möjlighet att allvarligt störa verksamheten, till exempel genom att stänga av elförsörjningen eller påverka dricksvattenkvaliteten. Det kan i sin tur ge upphov till en samhällsstörning. Om systemen inte fungerar ställer det ökade krav på bemanning eller rondering av anläggningar vilket i sin tur kräver reservplaner och resurser.

I NIS-regleringen ställs krav på ett systematiskt och riskbaserat informationssäkerhetsarbete. Kommunala verksamheter som kan omfattas av regleringen är bland annat dricksvatten- och energiförsörjning samt vårdverksamhet. Oavsett om kommunens verksamhet omfattas av direktivet eller inte är det viktigt att bedriva ett riskbaserat systematiskt säkerhetsarbete med sina nätverks- och informationssystem. Stöd för kommuners arbete med detta finns via MSB och berörda tillsynsmyndigheter.

Under 2015 och 2016 drabbades delar av Ukraina av flera elavbrott. Dessa var orsakade av intrång i cyberfysiska system inom elsektorn. Intrånget resulterade i avbrott i elförsörjningen. Det stängde också ute elleverantörens medarbetare från systemet, något som gjorde det svårare att hantera angreppet. Angreppet 2015 möjliggjordes genom att anställda hos elleverantören via e-post lurades att ladda ner bilagor. Angreppet 2016 möjliggjordes troligen genom att angriparen fortfarande hade viss åtkomst till it-miljön efter 2015 års angrepp.

Läs mer

NIS-direktivet (msb.se)

Samlad informations- och cybersäkerhets-handlingsplan för åren 2019–2022 : redovisning 2020 (msb.se) en nationell satsning som inkluderar tekniska, förebyggande, förmågehöjande och koordinerande aktiviteter i syfte att öka säkerheten i industriella informations- och styrsystem och sakernas internet (IoT). Säkerhet i cyberfysiska system (msb.se)

Viktiga lärdomar från elavbrotten i Ukraina: skyddet av industriella informations- och styrsystem (ICS) måste stärkas (msb.se)

Vägledning för robust & Säker IoT på Robust digital infrastruktur (ssnf.org)

Driftstörning eller annan störning hos en viktig leverantör

Det finns alltid beroenden till externa leverantörer av utrustning eller tjänster. Det är viktigt att alla upphandlingar görs med tydliga och av verksamheten satta krav på servicenivå.

Störningar hos leverantörer kan också påverka kommunens verksamheter. Ett exempel är när delar av internet-trafiken slogs ut av en denial-of-service attack hösten 2016. Ett annat är när företaget Tietos driftanläggning år 2011 drabbades av problem vilket ledde till avbrott i både samhällsviktiga tjänster men också permanent förlust av information.

Problem hos en extern leverantör kan också leda till förtroendeförluster som också är relevant ur ett krisberedskapsperspektiv. När en extern leverantör genom ett misstag gjorde att flera miljoner telefonsamtal innehållandes hälsouppgifter gick att nå för obehöriga drabbade det Region Stockholm, Sörmland, Värmland och Gotland samt 1177. Även om problemet uppstår hos en leverantör är det kommunen som är verksamhetsansvarig inklusive har ansvar för sekretess.

Läs mer

Major cyber attack disrupts internet service across Europe and US (theguardian.com)

1177-läckan (svt.se)

Statliga myndigheters rapportering av it-incidenter

Statliga myndigheter ska rapportera it-incidenter som inträffar i myndighetens informationssystem eller i tjänster som tillhandahålls åt en organisation.[7] Incidenterna som ska rapporteras är de som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för. Kommuner uppmanas att frivilligt rapportera incidenter till MSB/CERT-SE men det finns inget krav.

Incidentrapporteringen sammanfattas framförallt i årliga rapporter. Dessa sammanställningar kan tjäna som inspiration för att se vilka typer av incidenter som vanligen inträffar.

I rapporterna över både 2018 och 2019 konstateras att de incidenter som gett störst konsekvenser finns inom områdena ”störning i driftmiljö” respektive ”oönskad eller oplanerad störning i kritisk infrastruktur”. ”Störning i driftmiljö” omfattar bland annat när it-system av olika anledningar inte fungerar som de ska. Gällande ”oönskad eller oplanerad störning i kritisk infrastruktur” förekommer ofta olika varianter av avbrott. Det kan handla om elförsörjning, elektroniska kommunikationer (exempelvis telefoni och internet-förbindelser) eller kylsystem.

Läs mer

It-incidentrapportering för statliga myndigheter (msb.se)

7. Enligt förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

Utbildning och övning

Avsnittet ger exempel på de utbildningsmöjligheter som finns inom området samt ger förslag på hur kommunen kan öva kring krisberedskap och it-stöd.

Utbildningsmöjligheter

Utbildningar relevanta för it-stödets roll inom krisberedskapsområdet finns till viss del, både på den privata och den offentliga marknaden. Framförallt i form av utbildningar kring it-säkerhet och styr- och kontrollsystem relevanta för kommunalteknisk infrastruktur.

Totalförsvarets forskningsinstitut bedriver ett antal olika utbildningar inom området industriella styr- och kontrollsystem.

Övningsverksamhet

Liksom inom övrigt krisberedskapsarbete är övning nödvändigt för att både utveckla och testa förmåga. Övningsverksamheten kan bygga på de två olika perspektiv som genomsyrar den här texten i stort – it-stödets roll för att hantera samhällsstörningar samt hur störningar i it-stödet kan leda till samhällsstörningar.

Övningar av denna typ erbjuder också goda möjligheter att öka samverkan mellan it-avdelningen/en extern it-leverantör och kommunens övriga verksamheter.

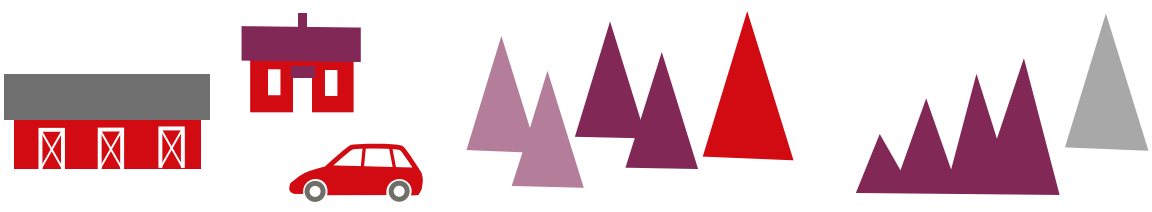
Öva it-stödets funktion och roll vid normala krishanteringsövningar

Det finns två grundläggande behov som kan omhändertas via övning:

- Deltagare i krisledningsorganisationen måste effektivt kunna använda de it-stöd som ska användas vid en samhällsstörning.
- It-avdelningens personal måste ha förståelse för sin roll. Detsamma gäller en extern leverantörs personal om kommunen har utkontrakterat drift av it-stöd.

Dessa behov skulle kunna ske både genom riktade funktionsövningar och genom kommunens normala krishanteringsövningar.

Funktionsövningar handlar om att pröva en eller flera specifika funktioner, till exempel larmning och eskalering, stabsfunktion eller som i detta fallet it-stöd. En funktionsövning skulle kunna vara inriktad på att testa att den planerade användningen av it-stödet är genomförbar rent tekniskt samt att all berörd personal har kunskap om hur lösningarna ska användas. Det kan handla om att testa förmågan att använda WIS, att genomföra effektiva distansmöten med flera parter, att ovan nämnda funktionskonton- och telefoner fungerar etc.



När kommunen genomför sina vanliga krishanteringsövningar bör it-stöd också övas (i den mån det går). Om det är en simuleringsövning blir det ingen praktisk övning/träning men det kan ändå ingå att deltagarna identifierar behoven av it-stöd för att lösa olika uppgifter. I en simuleringsövning kan det däremot ingå att rent praktiskt etablera och använda it-stöden.

Stöd för att genomföra krishanteringsövningar finns bland annat i MSB:s metodstöd ”Öva enkelt” samt FSPO:s metodstöd. Det senare är förvisso skrivet mot aktörer inom det finansiella området men vägledningen fungerar även för andra organisationer. I FSPO:s (Finansiella Sektorns Privat-Offentliga Samverkan) vägledning om kontinuitetshantering i appendix F finns en kortare del om övning och test kopplat till it.

Läs mer

Öva enkelt! (msb.se)

6 STEG TILL BÄTTRE ÖVNINGAR (pdf, fspos.se)

FSPOS Vägledning för Kontinuitetshantering (pdf, fspos.se) se Appendix F

Öva hantering av it-relaterade samhällsstörningar

Detta perspektiv kan omhändertas exempelvis genom att öva genomförandet av en katastrofhanteringsplan för it-avdelningen eller att öva störningar i it-system som samhällsviktiga verksamheter är beroende av.

Katastrofhanteringsplanen kan övas antingen i sin helhet eller enskilda moment. Det sistnämnda skulle kunna innebära att exempelvis öva återläsning av backup-data, kommunens lösning för redundant serverdrift eller internkommunikation.

Övningar kring störningar i it-system kan med fördel genomföras tillsammans med berörda verksamheter. Exempelvis tillsammans med VA-avdelningen/-bolaget vad gäller störningar i styr- och kontrollsystem för dricksvattenförsörjning eller vårdverksamheten vid storskaliga störningar i sådant som journalsystem eller larm- och trygghetslösningar.

Stöd för att genomföra övningar finns bland annat hos Storbritanniens cybersäkerhetscenter. De har tagit fram ett utbildningskoncept riktat mot just it-stöd (kallat ”Exercise in a box”). Det innehåller ett antal förberedda scenarier samt stöd för genomförandet av övningar. Scenarierna är dock inte skrivna utifrån perspektivet samhällsstörning utan handlar om mer begränsade it-säkerhetsrelaterade händelser.

ISO 27301, kapitel 8.1.3 innehåller en övergripande beskrivning av processer för övning inom ramen för kontinuitetsarbete inom it-området. Standarden kan ge input till vilken typ av övningar som kan vara relevanta att genomföra samt förslag på en övergripande övningsstrategi.

Övningar på nationell nivå

På nationell nivå finns övningsserien Nationell informationssäkerhetsövning (NISÖ) som hanteras av MSB. NISÖ syftar till att stärka samhällets förmåga till krishantering och samhällets förmåga att hantera it-relaterade samhällsstörningar. Övningsverksamheten ska även stärka samverkan på bred front i krishanteringssystemet. Den senaste övningen genomfördes 2018. Under övningen identifierades två huvudsakliga utvecklingsområden: samverkan och systemförståelse samt informationsdelning och lägesbild. Vad gäller den lokala nivån lyftes det under punkten Systemförståelse att andra aktörer i samhället behöver större förståelse för den lokala nivån och hur it-relaterade händelser påverkar och hanteras. Nästa övning genomförs 2021.

Läs mer

NISÖ 2018: erfarenhetsrapport (msb.se)

Ett samarbete mellan:

Myndigheten för samhällsskydd och beredskap

Sveriges Kommuner och Regioner

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB1682 - mars 2021 978-91-7927-097-1