Social sårbarhet utifrån ett medborgarperspektiv.

Nieminen Kristofersson, Tuija; Guldåker, Nicklas

2007

LUCRAM
Lund University Centre for Risk Analysis and Management

FRIVA

Framework Programme for Risk and Vulnerability Analysis
Ramforskningsprogram för KBM

Risk- och sårbarhetsanalyser: Utgångspunkt för praktiskt arbete

2007-03-30

Inledning

Denna samling av informationsblad utgör en del av den samlade rapportering av ramforskningsprogrammet FRIVA, som är genomfört under perioden mars 2004 till mars 2007 och finansierat av Krisberedskaps-myndigheten.

Informationsbladens syfte är att beskriva innehåll och slutsatser från FRIVA:s arbete på en form som är anpassat till användares behov. Informationsbladen är tematiska och därför har oftast mera än ett av FRIVA:s vetenskapliga delprojekt bidragit till innehållet. Idén är att beskriva det vetenskapliga innehållet på en enkel och läsbar form, så att det kan utgöra en utgångspunkt för praktiskt arbete.

I denna samling finns samtliga informationsblad från FRIVA:s arbete samlade. Dessa kommer också att finnas på hemsidan, och det är avsikten att kontinuerligt uppdatera informationsbladen. De enskilda informationsbladen är utarbetade, så att de kan används utan koppling till de övriga. Avsikten med detta är att endast de informationsblad som passar in i sammanhanget skall kunna användas på möten, kurer eller vid annan verksamhet.

En slutrapport med redovisning av det vetenskapliga innehållet i samtliga delprojekt samt en henvisning till alla publikationer och annan dokumentation är utarbetat. För övrig information hänvisas till FRIVA på LUCRAM:s hemsida www.lucram.lu.se.

Informationsbladen är utarbetade av forskare, som alla har bidragit till arbetet inom ramforskningsprogrammet FRIVA.

Innehållsförteckning

FRIVA

Några tankar kring analys av krishanteringsförmåga

Författare: Marcus Abrahamsson, Henrik Johansson, Henrik Jönsson

Inledning

Denna skrift är ett av flera informationsblad som redovisar sammanfattade erfarenheter och synpunkter från ramforskningsprogrammet FRIVA (Framework Programme for Risk and Vulnerability Analysis), vilket finansierats av Krisberedskapsmyndigheten under perioden mars 2004 till mars 2007. Informationsbladen skall kunna användas som utgångspunkter för praktiskt arbete när det gäller hantering av risker, sårbarheter, hot, kriser och katastrofer som medför eller kan medföra allvarliga samhälleliga konsekvenser.

Bakgrund

I en ideal värld hade det varit möjligt att förebygga alla händelser som skulle kunna medföra negativa konsekvenser. Tyvärr är detta omöjligt i praktiken eftersom människan inte har förmåga att påverka uppkomsten av vissa fenomen (såsom vissa naturhändelser). Det kan även vara kontraproduktivt att i alltför stor utsträckning satsa resurser på att förebygga uppkomsten av krishändelser eftersom samhällets förmåga att hantera en händelse då den väl inträffar riskerar att degraderas och den totala risken därmed ökas. Ett exempel på försämrad hanteringsförmåga kan ses i vissa delar av samhällets hantering av elavbrott. Idag riskerar samhällskonsekvenserna av ett elavbrott att bli mycket stora, vilket inte var fallet för t.ex. 50-100 år sedan. Detta beror till viss del på att många fler samhällsviktiga system och verksamheter idag är beroende av elförsörjningen än tidigare, men även på att tillförlitligheten i elförsörjningen ökat (d.v.s. elavbrott kan i större utsträckning förebyggas), vilket har inneburit att samhällets hanteringsförmåga inte ställs på prov lika ofta. Att skapa en balans mellan förebyggande åtgärder och en förmåga att hantera händelser då de inträffar torde därmed vara en rationell risk- och krishanteringsstrategi.

Då en kris uppstår utsätts samhället och dess medborgare för påfrestningar, vilket leder till att olika typer av behov måste tillgodoses med syftet att negativa konsekvenser skall undvikas eller begränsas. Vissa behov kan de drabbade själva tillgodose medan andra kräver assistans från olika krishanteringsaktörer (t.ex. offentliga, frivilliga eller privata organisationer). Detta kan bero på att den drabbade befolkningen exempelvis saknar de resurser, kunskaper och förmågor som krävs. Att tillgodose de hjälpbehov som uppstår i en kris kommer att ställa krav på olika aktörers krishanteringsförmåga. Ett sätt för en aktör att bygga upp en god krishanteringsförmåga är att analysera sin befintliga förmåga att hantera händelser av olika slag med syftet att identifiera brister och möjligheter till förbättringar. En sådan analys kan även användas för att förmedla vad en viss aktör tror sig klara av att hantera. Olika krishanteringsaktörer kan på så sätt skaffa sig en uppfattning om andra aktörers förmågor och begränsningar, vilket kan vara viktigt att ha kunskap om, framförallt om det finns starka beroenden mellan aktörerna.

Syfte

I detta dokument presenterar vi några tankar kring vad som är vikigt att tänka på när en aktör ska analysera sin förmåga att hantera en krishändelse. Syftet är inte att vara heltäckande eller presentera någon konkret metod utan endast att belysa några viktiga faktorer då en analys av krishanteringsförmåga skall genomföras.

Vad menar vi med krishanteringsförmåga?

Krishantering delas i en vanligt förekommande modell in i fyra olika faser; förebyggande, förberedande, akut avhjälpande samt återuppbyggande. Ur ett mycket brett perspektiv skulle krishanteringsförmåga därmed kunna ses som förmågan att utföra alla dessa faser. Vanligtvis när man talar om krishanteringsförmåga är det dock förmågan att hantera den akuta fasen av en kris som avses (vilket givetvis beror på eventuellt förebyggande och förberedande arbete). Det är med denna innebörd som krishanteringsförmåga används i detta dokument.

Med krishanteringsförmåga menar vi en eller flera aktörers förmåga att utföra de uppgifter som

aktören/aktörerna har att utföra i en krissituation. Dessa uppgifter syftar ofta till att direkt eller indirekt svara upp mot de behov som uppstår under krisen, och som måste tillgodoses för att undvika eller begräsa de negativa konsekvenserna av krishändelsen. Det är alltså möjligt att tala om krishanteringsförmåga dels för enskilda aktörer, t.ex. en kommunal förvaltning, dels för ett krishanteringssystem i stort, t.ex. samtliga aktörer i en kommun.

Analys och värdering är skilda processer

Det är viktigt att tydligt skilja på *analys* av och *värdering* av krishanteringsförmåga. Att *analysera* krishanteringsförmåga handlar om att på ett så systematiskt sätt som möjligt skaffa sig kunskap om hur väl olika potentiella krishändelser kan hanteras. I detta arbete handlar det om att analysera exempelvis vilka resurser som finns att tillgå, kunskaper och kompetenser som krävs för att lösa uppgifter etc. Att *värdera* krishanteringsförmåga handlar om att ta ställning till huruvida den befintliga förmågan är acceptabel, d.v.s. huruvida förbättringar krävs eller inte. För att kunna göra denna värdering krävs givetvis att en analys av krishanteringsförmågan finns som underlag.

Vi menar att det är mycket viktigt att skilja på dessa två processer eftersom den ena processen handlar om kunskapssökande medan den andra processen handlar om ställningstagande som grundar sig på värderingar och bl.a. relaterar till det ansvar som kan utkrävas av olika aktörer. Att blanda ihop dessa processer tror vi kan leda till problem. I detta dokument behandlar vi endast *analys* av krishanteringsförmåga.

Tre faktorer att tänka på i en analys av krishanteringsförmåga

Vi menar att tre faktorer är speciellt viktiga att ta hänsyn till då en aktör ska analysera sin krishanteringsförmåga. Dessa faktorer är:

- Att förmågor relateras till specifika uppgifter,
- Att det finns mått som kan beskriva hur väl en specifik uppgift kan utföras, och
- Att den kontext som gäller för de bedömningar som görs är beskriven.

Poängen med att tala om specifika uppgifter när förmåga analyseras är att förmåga då relateras till det faktiska händelseförloppet i en kris, vilket gör att det blir möjligt att vara konkret om hur väl uppgiften kommer att kunna utföras. Vi menar att det är viktigt att i en analys sträva mot att de bedömningar som görs av olika förmågor är möjliga att ta ställning till avseende deras giltighet. Att tala om förmåga i mer generella och vaga termer kan leda till tolkningsproblem. Hur uppgifter definieras kommer att bero på det specifika fallet och även vilken detaljeringsgrad som används i analysen. Ett exempel på uppgift för Räddningstjänsten kan vara ”att utfärda varningsmeddelande till allmänheten”.

Vi menar att det är viktigt att man är tydlig med vilka mått som kan användas för att avgöra huruvida en uppgift kan utföras väl. Även detta är ett sätt att konkretisera tankegångarna rörande analysen av förmåga. Ofta kan flera faktorer vara relevanta för att avgöra om en uppgift kan utföras väl. Exempel på mått är hur snabbt uppgiften kan utföras och i vilken utsträckning agerandet motsvarar det behov som finns. För att återknyta till exemplet ovan skulle mått på hur väl uppgiften ”att utfärda varningsmeddelande till allmänheten” utförts exempelvis kunna vara ”hur lång tid det tar innan varningsmeddelandet utfärdas” och ”hur stor andel av befolkningen som nås av meddelandet”.

Den tredje faktorn som är viktig att ta hänsyn till i en analys av krishanteringsförmåga är den kontext som gäller i analysen. Med kontext menar vi förhållandena i omgivningen, exempelvis huruvida det fysiska händelseförloppet har påverkat någon resurs som en aktör är beroende av för att utföra sina uppgifter. Ett tydligt exempel är om telekommunikationen skulle vara utslagen, vilket skulle kunna innebära att kommunikationen inom en organisation eller mellan organisationer försvåras. Detta kan vidare leda till att en aktörs förmåga att utföra olika uppgifter försämras drastiskt. Att ta hänsyn till att kontexten inte alltid är ”optimal” för att lösa en uppgift är ett sätt att öka kunskapen om robustheten i sin krishanteringsförmåga. Eftersom kontexten inte alltid ser likadan ut är det aktuellt att i en analys av krishanteringsförmåga fundera över sin förmåga i olika kontexter.

Framtiden är osäker

Ett problem när man försöker skaffa sig kunskap om framtida händelser är att det föreligger osäkerheter om utfall och händelseutvecklingar. När det gäller analys av krishanteringsförmåga föreligger osäkerhet avseende vilka krav som kommer att ställas på en viss aktör i en krissituation, vilken kontext som råder då aktören ska lösa en viss uppgift och hur väl uppgiften kan lösas givet en viss kontext. Syftet med analys av krishanteringsförmåga är att belysa dessa osäkerheter, t.ex. genom att ta hänsyn till att olika kontext kan råda, och på så sätt skaffa sig så god kunskap som möjligt om hur väl olika uppgifter kan lösas. Hur

lyckad en analys av krishanteringsförmåga blir beror givetvis till viss del på hur utförlig analysen görs, men bara genom att inse att de tre faktorerna ovan är viktiga att tänka på tror vi kan hjälpa en aktör att skapa ett strukturerat arbetssätt och därmed förbättrade analyser.

I många krissituationer kommer det troligtvis att uppstå uppgifter som inte förutsågs eller kanske ens gick att förutse, detta trots att en analys av krishanteringsförmåga genomförts. Vi tror dock att genom att genomföra grundliga analyser kan många viktiga frågor kring framtida krishändelser diskuteras och kunskap om dessa erhållas. Förutsättningarna för att sedan fatta välgrundade beslut om hur förmågorna skulle kunna förbättras är mycket bättre om en utförlig analys finns som grund.

Sammanfattning

I detta informationsblad har vi fört fram tre faktorer som vi tror är viktiga att ta hänsyn till då en aktör, t.ex. en myndighet eller kommunal förvaltning, ska genomföra analyser av sina krishanteringsförmågor. Dessa faktorer är:

- Att förmågor relateras till specifika uppgifter,
- Att det finns mått som kan beskriva hur väl en specifik uppgift kan utföras, och
- Att den kontext som gäller för de bedömningar som görs är beskriven.

Att genomföra en analys av krishanteringsförmåga kan leda till att en aktör skaffar sig värdefull kunskap om hur väl den kan hantera en potentiell framtida händelse och vad den är beroende av för att lyckas lösa uppgifterna väl. Denna kunskap kan sedan användas för att skapa ännu bättre förutsättningar för att hantera sådana händelser och fungera som underlag för beslut om hur förmågan ska förbättras. Genom att analysera krishanteringsförmåga tvingar aktören sig även att tänka sig in i framtida potentiella händelser och vilka krav de kan tänkas ställa, vilket leder till att ett proaktivt tänkande stimuleras i organisationen.

Tips för vidare läsning

- Jönsson, H., Abrahamsson, M. och Johansson, H. (2007), ”An Operational Definition of Emergency Response Capabilities”, Artikel skickad till *The International Emergency Management Society 14th Annual Conference*, Trogir, Kroatien.

Kontakt

För mer information kontakta oss på följande e-post-adresser eller besök FRIVA:s hemsida.

Marcus Abrahamsson
Marcus.abrahamsson@brand.lth.se

Henrik Johansson
Henrik.johansson@brand.lth.se

Henrik Johansson
Henrik.jonsson@brand.lth.se

FRIVA
http://www.lucram.friva.lu.se

FRIVA Sårbarhetsanalys av teknisk infrastruktur

Författare: Jonas Johansson, Henrik Jönsson, Henrik Johansson

Inledning

Denna skrift är ett av flera informationsblad som redovisar sammanfattade erfarenheter och synpunkter från ramforskningsprogrammet FRIVA (Framework Programme for Risk and Vulnerability Analysis), vilket finansierats av Krisberedskapsmyndigheten under perioden mars 2004 till mars 2007. Informationsbladen skall kunna användas som utgångspunkter för praktiskt arbete när det gäller hantering av risker, sårbarheter, hot, kriser och katastrofer som medför eller kan medföra allvarliga samhälleliga konsekvenser.

Bakgrund

Samhället har blivit, och kommer troligen att bli, alltmer beroende av tekniska infrastrukturer och de tjänster som de tillhandahåller. Stormen Gudrun 2005 och stormen Per 2007 har tydligt visat hur beroende samhället är av elförsörjning, telekommunikation och transportsystem samt hur sårbart samhället är för infrastrukturella kollapser. Under *elförmörkelsen* 2003, då elförsörjningen i hela södra Sverige slogs ut, uppdagades beroenden av elförsörjningen som tidigare inte varit särskilt väl belysta, såsom att Öresundsbron tillfälligt fick stängas pga. att övervakningssystemet slutade fungera och att landningar på Kastrups flygplats ej tilläts. Utebliven elförsörjning leder oftast inte till direkta livshotande konsekvenser, men väl till allvarliga ekonomiska konsekvenser och avsevärda olägenheter. Stormen Gudrun kostade de berörda nätbolagen i storleksordningen 2,6 miljarder kronor, då inte inräknat samhällets ekonomiska förluster på grund av utebliven elförsörjning. Elförmörkelsen under 2003 beräknades kosta Sverige i storleksordningen en halv miljard kronor. Dessa stora konsekvenser belyser behovet av att studera de tekniska infrastrukturernas sårbarhet för olika typer av påfrestningar.

Sårbarhet kan ses ur två perspektiv. Ur det ena perspektivet är sårbarhet en systemegenskap, dvs. ett systems oförmåga att stå emot påfrestningar av olika slag. Ur det andra perspektivet är en sårbarhet en kritisk punkt i systemet, dvs. en punkt som om den fallerar ger upphov till stora konsekvenser. Båda perspektiven ger viktig information till arbetet med att reducera tekniska infrastrukturers sårbarhet. För en mer utförlig diskussion om sårbarhetsbegreppet, se ”En operationell definition av sårbarhet” som är ett annat informationsblad från FRIVA.

Syfte

Syftet med detta dokument är att beskriva en metod för sårbarhetsanalys som kan användas för analys av tekniska infrastruktursystem. Beskrivningen ger en översikt av metoden och en steg-för-steg guide. Målet är inte att ge en fullständig redogörelse för metoden och dess bakgrund, eftersom det kräver mycket större utrymme, utan dokumentet ska istället fungera som en inspirationskälla och översikt för hur sårbarhetsanalys kan genomföras i praktiken. I slutet av dokumentet ges några tips för vidare läsning för den som är intresserad av mer information.

Metodöversikt

Den metod för sårbarhetsanalys som presenteras i detta dokument baseras på att det system som analyseras kan modelleras som ett *nätverk*. De tekniska infrastruktursystem som utgör basen för vårt samhälle är uppbyggda i nätverksstrukturer, exempelvis transport-, eldistributions- och vattensystemen, vilket gör att denna metod är väl anpassad för dessa typer av system. Nätverk består av två huvudkomponenter: *noder* och *länkar*. Noderna kan exempelvis vara korsningar i ett vägnät, reservoarer i ett vattensystem eller nätstationer i ett eldistributionssystem och länkarna kan exempelvis vara vägsträckor, vattenledningar eller elledningar.

Sårbarhetsanalysen har två syften. Det ena syftet är att studera systemets förmåga att motstå påfrestningar, dvs. att bibehålla sin funktion trots att det är utsatt för påfrestningar. Detta kallas hädanefter för global analys av sårbarhet. Det andra syftet är att identifiera de punkter eller komponenter i systemet som är kritiska, d.v.s. som om de slås ut leder till stora konsekvenser. Syftet är således att hitta systemets svaga punkter, vilket kompletterar den

globala analysen genom att söka orsakerna till systemets sårbarhet.

Global analys av sårbarhet

För att analysera den globala sårbarheten i de tekniska infrastruktursystemen simuleras påfrestningar och störningar genom att slå ut noder eller länkar i nätverket. Efter varje *utslagningsomgång*, d.v.s. efter det att en nod eller länk har slagits ut, beräknas ett mått på de negativa konsekvenser som uppstår på grund av påfrestningen. Ett system är mycket sårbart om endast en liten påfrestning, t.ex. ett fåtal utslagna komponenter, leder till stora konsekvenser.

En rad olika påfrestningar kan tänkas exponera ett tekniskt infrastruktursystem, t.ex. naturhändelser eller antagonistiska hot. Sårbarheten i ett system måste relateras till en specifik påfrestning för att kunna analyseras, vilket innebär att ett system kan vara sårbart för vissa påfrestningar men robust mot andra. Genom att använda olika typer av *utslagningsstrategier* kan olika påfrestningar mot infrastruktursystemen simuleras. En utslagningsstrategi anger i vilken ordning noderna och länkarna slås ut. Det är vanligt att skilja mellan slumpmässig och riktad utslagning. I en helt slumpmässig utslagning har alla noder och länkar lika stor sannolikhet att bli utslagna i en specifik utslagningsomgång. Denna strategi skulle kunna liknas vid ett naturfenomen som påverkar alla systemets komponenter på likartat sätt eller som normala slumpmässiga komponentfel. Vid riktad utslagning beräknas ett mått på hur viktiga noderna och länkarna är i nätverket, t.ex. hur central en nod eller länk är. Den nod eller länk som är viktigast slås ut i första utslagningsomgången, den som är näst viktigast slås ut i andra omgången etc. Utslagning av mest centrala komponenter kan tänkas likna en antagonistisk påfrestning där någon försöker åsamka så stora skador som möjligt. En tredje typ av utslagningsstrategi är slumpmässig men där noder och länkar har olika sannolikhet att bli utslagna. En sådan påfrestning skulle kunna vara en storm som påverkar ett eldistributionssystem. En lång luftledning har här en större sannolikhet att fallera jämfört med en kort (givet att alla andra förhållanden är lika) men det finns ett inslag av osäkerhet eftersom det inte är säkert att den långa ledningen slås ut först - det är bara mer sannolikt. Ett viktigt steg i analysarbetet är att utveckla utslagningsstrategier som realistiskt återger de påfrestningar som systemet verkligen kan utsättas för.

Identifiering av kritiska komponenter

En kritisk komponent kännetecknas av att den är väldigt viktig för infrastrukturens funktion. För att identifiera kritiska komponenter i ett infrastruktursystem gäller det alltså att identifiera de komponenter som om de slås ut ger upphov till allvarliga konsekvenser. Identifieringen försvåras av att vissa komponenter, om de slås ut enskilt, inte ger upphov till några konsekvenser, men då de slås ut tillsammans med en eller flera andra komponenter ger upphov till allvarliga konsekvenser. En person med god insikt i systemet har troligtvis god kunskap om vilka enskilda komponenter som är kritiska. Kombinationer av komponenter som fallerar är däremot svårare att identifiera eftersom antalet kombinationer ofta är mycket stort. Då krävs en systematisk genomgång av möjliga kombinationer för att hitta de som leder till allvarliga konsekvenser.

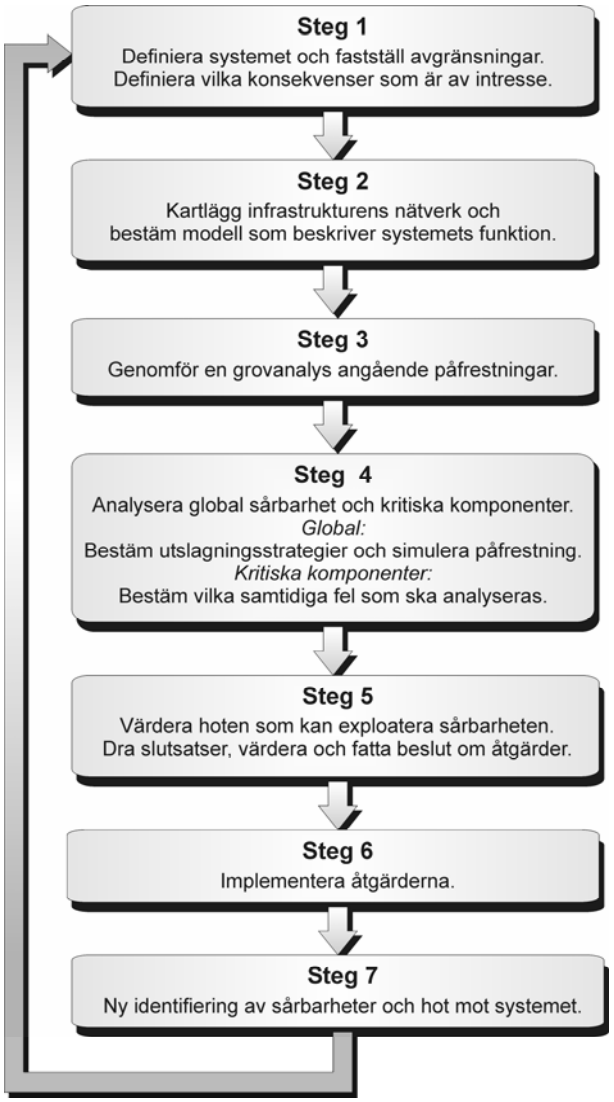
Det ska noteras att en punkt kan vara kritisk för ett system även om sannolikheten för dess felfunktion är liten. Som exempel kan man nämna att kritiska transformatorer i elnät inhyses i låsta byggnader med inhägnad runt. Under senare år har även fjärrövervakning av viktiga stationer introducerats. Säkerhetsåtgärderna har genomförts för dessa stationer just därför att de är kritiska punkter i systemet. Identifierade kritiska punkter kräver därmed vidare diskussioner och analyser för att klarlägga vilka hot som kan bringa dessa ur funktion. För att reducera risken kan förebyggande åtgärder för hotet implementeras *eller* så kan sårbarhetsreducerande åtgärder genomföras, exempelvis med utbyggnad av redundanta system. Det sistnämnda alternativet är troligen det enda realistiska alternativet i fråga om hot som är svåra att förebygga.

Beräkning av konsekvenser

I föregående avsnitt har det antagits att det finns ett sätt att avgöra vilka konsekvenser som uppstår till följd av att noder och länkar i ett nätverk slås ut, dvs. vilka konsekvenser som uppstår givet att systemet befinner sig i ett visst tillstånd. Beräkningen av konsekvenser handlar om att avgöra på vilket sätt ett system påverkas av att komponenter är ur funktion. Topologin, dvs. strukturen, på de infrastrukturella nätverken har stor inverkan på infrastruktursystemens funktionalitet, men det är inte det enda som har betydelse. Viktiga faktorer är även nodernas och länkarnas beskaffenhet och typ av infrastruktursystem. Ofta finns begränsningar i vad noderna och länkarna i ett infrastrukturnätverk klarar av, exempelvis har el- och vattenledningar begränsad kapacitet, inmatningspunkter har begränsningar vad gäller inmatningskapacitet etc. Den konsekvensberäkningsmodell som används för ett specifikt infrastruktursystem måste därmed anpassas till den typ av system som analyseras.

Metodens arbetsgång

I detta avsnitt presenteras en förenklad steg-för-steg guide till hur en sårbarhetsanalys kan utföras, steg 1-4, samt hur den utgör underlag för diskussion och implementering av sårbarhetsreducerande åtgärder, steg 5-7. I Figur 1 ses en schematisk bild över guiden.



Figur 1. Schematisk beskrivning av arbetsgången för en sårbarhetsanalys av teknisk infrastruktur.

Steg 1: Systemdefinition, avgränsningar, fastställa det skyddsvärda

Det första steget i sårbarhetsanalysen är att definiera det system som är av intresse. Det gäller att ha en klar uppfattning om vad som ska analyseras, vad syftet med analysen är och vilka avgränsningar som gäller. Allt detta kommer att påverka hur analysen kommer att gestalta sig, vilka förenklingar och antaganden som är lämpliga etc. Det är även viktigt att de val och överväganden som görs i detta steg dokumenteras eftersom en förståelse för detta steg är en förutsättning för att kunna förstå analysens resultat och de val som gjorts under analysens gång. En viktig del av detta steg är att bestämma sig för vilka konsekvensmått som ska användas. Ska konsekvensmåttet exempelvis avspegla samhällets förluster på grund av utebliven service eller ska det ses ur systemägarens perspektiv och hur den tekniska infrastrukturen påverkas?

Steg 2: Kartlägga och modellera systemet

Steg två handlar först och främst om att kartlägga systemet och skapa en nätverksmodell av det. I många fall kan flera komponenter representeras eller approximeras som *en* nod eller länk, under förutsättning att de ger upphov till samma konsekvenser om de slås ut. För ett elnät kan exempelvis en ledning och tillhörande brytare eller frånskiljare modelleras som en länk.

Utöver nätverksmodellen måste en modell för att uppskatta konsekvenserna till följd av utslagna komponenter tas fram. För att ta fram modellen måste man ha kunskap om hur infrastrukturens funktionalitet påverkas av att komponenter slås ut. Är infrastrukturen ett vägnät måste kunskap om hur trafiken påverkas vid utslagning av en länk (väg) finnas. Är infrastrukturen ett elnät måste kunskap om hur många kunder som förlorar elförsörjning vid utslagning av komponenter finnas. Givetvis måste konsekvensberäkningsmodellen kopplas till det konsekvensmått som fastställdes i steg 1.

Sammanfattningsvis kan sägas att den som utför analysen i detta steg har en mängd val vad gäller detaljeringsgrad, både avseende nätverkets topologi och konsekvensberäkningen. Målet är att specificera en modell som är *tillräckligt* detaljerad och giltig med hänsyn taget till exempelvis syfte och resurstillgång.

Steg 3: Identifieria möjliga typer av påfrestningar

I det tredje steget gäller det att identifiera vilka typer av påfrestningar som kan tänkas exponera systemet. Ställning måste tas till huruvida en heltäckande analys ska genomföras eller om det endast är sårbarheten för någon specifik påfrestning som ska analyseras. För analyser som syftar till att vara heltäckande måste dock ofta en grov sållning av potentiella påfrestningar utföras för att analysen ska kunna genomföras i praktiken, dvs. sålla bort påfrestningar som bedöms som extremt osannolika. För den globala analysen måste de utslagningsstrategier som ska simuleras bestämmas. En utslagningsstrategi kan representera flera påfrestningar, förutsatt att påfrestningarna exponerar systemet på likartat sätt. För identifiering av kritiska komponenter måste det bestämmas hur många samtidiga fel som ska undersökas.

Steg 4: Analysera global sårbarhet och identifiera kritiska komponenter

Detta steg består av två delmoment: global analys av sårbarhet och identifiering av kritiska komponenter. I den globala analysen genomförs simuleringar för varje typ av utslagningsstrategi. De utslagningsstrategier som är probabilistiska (t.ex. slumpmässig utslagning) måste simuleras flera gånger eftersom varje simuleringsomgång kommer att skilja sig åt med avseende på vilka konsekvenser de ger upphov till. En fördelning av värden på konsekvens genereras alltså, vilken kan ligga till grund för beräkning av medelvärden och spridning. Vid identifiering av kritiska komponenter beräknas alla möjliga kombinationer av samtidiga komponenter ur funktion. För ett nät bestående av 800 komponenter innebär detta att 800 konsekvensberäkningar måste genomföras för en komponent ur funktion, ca 320 000 för två samtidiga komponenter ur funktion och ca 85 000 000 för tre samtidiga komponenter ur funktion. Därmed behövs en metod för att ta fram intressanta fall som exempelvis kan baseras på konsekvensen som uppstår i kombination med typ av komponenter som är ur funktion.

Steg 5: Värdera sårbarhet och beslutsfattande

I detta steg gäller det att fundera igenom om sårbarheterna är acceptabla eller om sårbarhetsreducerande åtgärder bör genomföras. Med den globala analysen som grund kan slutsatser dras om vilka typer av påfrestningar som systemet är sårbart för, men för att avgöra huruvida sårbarheten är acceptabel måste hänsyn också tas till hur sannolikt det är att de olika påfrestningarna inträffar. Utifrån analysen av kritiska komponenter måste man fundera igenom huruvida det finns hot som kan tänkas exploatera de identifierade sårbarheterna.

Visar det sig att sårbarheterna är oacceptabla gäller det att fatta beslut om vilka sårbarhetsreducerande åtgärder som bör genomföras. Olika alternativa åtgärder kan reducera sårbarheten olika mycket men även vara olika kostnadseffektiva. Båda dessa faktorer är givetvis viktiga vid val av alternativ. I detta steg kan även slutsatser dras om att mer detaljerade analyser måste utföras, t.ex. genom att förfina modelleringen eller utföra mer ingående investeringsbedömningar.

Steg 6: Implementera åtgärder

I detta steg gäller det att implementera de åtgärder som beslutades om i föregående steg. Detta steg är givetvis mycket viktigt eftersom det är först när åtgärder implementeras som sårbarheterna faktiskt reduceras.

Steg 7: Uppdatera sårbarhetsanalysen

Ett minst lika viktigt steg är att regelbundet uppdatera sårbarhetsanalyserna, inte minst om systemet har vuxit eller förändrats på något sätt. Lika viktigt är det att diskutera om hotbilden har förändrats. Att genomföra nya analyser är även ett sätt att förbättra kvaliteten på de som redan gjorts, t.ex. genom att göra mer detaljerade analyser.

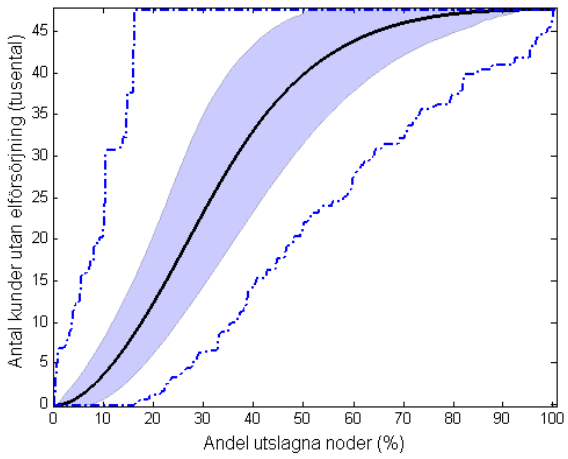
Tillämpning på eldistributionssystem

I detta avsnitt visar vi på tillämpning av den metod för sårbarhetsanalys (steg 1-4) som har beskrivits i detta dokument. Tillämpningen sker på ett eldistributionsnät (10 kV) i en svensk kommun. Noder med koppling till högre spänningsnivåer i elsystemet klassas som inmatningsnoder (transformatorer i mottagningsstationer). Noder med koppling till lägre spänningsnivåer klassas som lastnoder (nätstationer med effektkunder och/eller där nedtransformering till lågspänningskunder sker). Konsekvensen beräknas som antalet kunder utan elförsörjning. I det praktiska genomförandet av analysen användes datorprogram utvecklade av författarna.

Elnätet som analyserades drivs radiellt men är i viss utsträckning byggt maskat eller slingmatat, d.v.s. omkopplingar är möjliga att utföra med syftet att överföra elen via alternativa vägar i de fall då normal matningsväg ej är tillgänglig. I vår nätverksmodell antogs att omkopplingar kunde ske momentant, vilket givetvis är en idealisering. De bortfall av elförsörjning som beräknas i detta exempel kan därmed ses som varaktiga bortfall. Om det hade varit av intresse att även analysera avbrott som är kortvariga kan nätverksmodellen modifieras så att den motsvarar konfigurationen då elnätet drivs radiellt.

Den globala analysen exemplifieras genom att simulera slumpmässig utslagning av noder i nätverket. Eftersom denna typ av utslagning är probabilistisk, d.v.s. i vilken ordning noder slås ut kommer att variera mellan olika simuleringar, så kommer konsekvenserna för varje simuleringsomgång att variera. Det går alltså inte att entydigt uttala sig om vilka konsekvenser som uppstår då exempelvis tre noder har blivit utslagna, utan i vissa fall kommer detta att variera avsevärt. Ett sätt att visa på sårbarheten i nätet är att endast visa konsekvensernas medelvärde över alla simuleringar, men vi menar dock att det även är viktigt att åskådliggöra spridning kring medelvärdet. Resultatet från dessa simuleringar presenteras i Figur 2. De streckade linjerna i figuren anger de högsta respektive de lägsta konsekvenserna som en viss andel utslagna

noder kan leda till, baserat på de fall som simulerades. I värsta fall tappar alla kunderna elförsörjning vid ca 14% utslagna noder och i bästa fall tappar alla kunder försörjningen först när nästan alla noderna är utslagna. Dessa stora skillnader pekar på att slumpen kan ha stor inverkan på om en påfrestning leder till stora eller små konsekvenser.

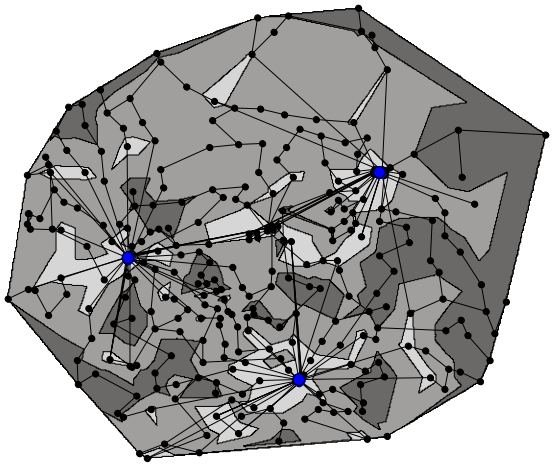


Figur 2. Resultat från en simulering med slumpmässig utslagning av noder. Som konsekvensmått anges antal kunder utan elförsörjning. Den svarta linjen visar medelvärdet av konsekvensen för 50 000 simuleringsomgångar. Det ljusblå området visar det band som 90% av konsekvensvärdena ligger inom. De streckade blå linjerna visar maximal respektive minimal konsekvens för respektive andel utslagna noder.

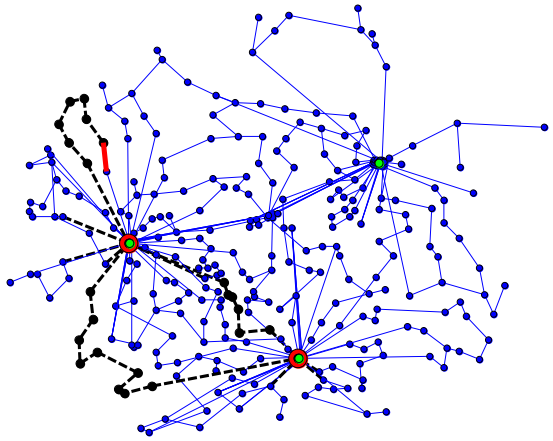
Från den globala analysen går det även att få fram lokala mått som beskriver hur sårbar elförsörjningen är i respektive område av nätet. I Figur 3 ses en karta över det geografiska området där sårbarheten i elförsörjningen för olika områden illustreras. Sårbarheten är baserad på i vilken utslagningsomgång som en nod i genomsnitt tappar matningsmöjlighet från samtliga inmatningspunkter då nätet blir utsatt för en påfrestning – i detta fall en slumpmässig påfrestning.

För att finna de komponenter som är kritiska genomförs en lokal analys. Ett exempel från analysen ges i Figur 4. Figuren visar identifiering utav tre samtidigt utslagna komponenter (exempelvis på grund av två samtidiga fel och ett underhåll) som orsakar stora konsekvenser och därmed anses som kritiska.

När kritiska komponenter har identifierats är nästa steg att analyserna möjligheten för att dessa inträffar samtidigt. När sannolikheten för de identifierade felen har bedömts (kan exempelvis vara en uppskattning på en femgradig skala) ger detta tillsammans med de konsekvenser som uppstår möjligheten för en sammanvägd bedömning av huruvida förbättring måste genomföras eller ej.



Figur 3. Sårbarhetskarta som, i tre nivåer, visar hur sårbar elförsörjningen är olika områden av elnätet. De ljusare områdena är mindre sårbara än de mörkare. De blå noderna är inmatningspunkter och de svarta är noder med kunder kopplade till sig.



Figur 4. Exempel på identifikation utav kritiska komponenter. I figuren har tre komponenter ur funktion markerats i röd färg, vilket ger konsekvensen 5870 kunder utan elförsörjning (15 MW icke-levererad effekt). De noder och länkar som är utan elförsörjning är markerade i svart färg. De gröna noderna är inmatningsnoder till elnätet.

Sammanfattning

I detta dokument har vi beskrivit en metod för sårbarhetsanalys kan användas med syftet att skapa kunskap om hur robust/sårbart ett infrastrukturnätverk är. Vi har visat exempel på tillämpning av metoden på ett eldistributionsnät och även placerat in analysmetoden i ett större perspektiv där kompletterande moment handlar om värdering av analysresultatet samt implementering av sårbarhetsreducerande åtgärder. Vi tror att analyser av denna typ kan komplettera de befintliga, intuitiva kunskaper som ofta finns om infrastruktursystem och på det sättet öka kunskapen om systemens

sårbarhet. I takt med att olika system blir alltmer komplexa tror vi även att behovet av att utföra systematiska sårbarhetsanalyser kommer att öka.

Litteraturtips

- Johansson, J., Jönsson, H. och Johansson, H. (2007), "Analysing the vulnerability of electric distribution systems: a step towards incorporating the societal consequences of disruptions", *Int. J. Emergency Management*, Vol. 4, No. 1, pp. 4-17.
- Jönsson, H., Johansson, J. och Johansson, H. (2007), "Identifying Critical Components in Electric Power Systems: A Network Analytic Approach", Artikel accepterad till *European Safety and Reliability Association 2007, Safety and Reliability Conference*, Stavanger, Norge.

Kontakt

För mer information kontakta oss på följande e-post-adresser eller besök FRIVA:s hemsida.

Jonas Johansson
Jonas.johansson@iea.lth.se

Henrik Jönsson
Henrik.jonsson@brand.lth.se

Henrik Johansson
Henrik.johansson@brand.lth.se

FRIVA
http://www.lucram.friva.lu.se

FRIVA Användning av metoder för risk- och sårbarhetsanalys

Författare: Henrik Johansson, Henrik Jönsson

Inledning

Denna skrift är ett av flera informationsblad som redovisar sammanfattade erfarenheter och synpunkter från ramforskningsprogrammet FRIVA (Framework Programme for Risk and Vulnerability Analysis), vilket finansierats av Krisberedskapsmyndigheten under perioden mars 2004 till mars 2007. Informationsbladen skall kunna användas som utgångspunkter för praktiskt arbete när det gäller hantering av risker, sårbarheter, hot, kriser och katastrofer som medför eller kan medföra allvarliga samhälleliga konsekvenser.

Bakgrund

Enligt förordningen (SFS 2006:942) om krisberedskap och höjd beredskap skall alla statliga myndigheter årligen genomföra risk- och sårbarhetsanalyser. Liknande krav ställs på kommuner i Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap. Dessa analyser genomförs idag med olika metoder och det har konstaterats att analyserna har varierande kvalité (Krisberedskapsmyndigheten 2005; Krisberedskapsmyndigheten 2006). Det är därför intressant att diskutera vad man kan kräva av en risk- och sårbarhetsanalys och även hur man kan gå tillväga för att förbättra de analyser som genomförs. Detta informationsblad redovisar några tips på vad man bör tänka på när man använder olika metoder för risk- och sårbarhetsanalys. Diskussionen rörande tipsen tar sin utgångspunkt i en definition av sårbarhet som först diskuteras kortfattat (en utförligare diskussion finns i informationsbladet ”En operationell definition av sårbarhet”). I rapporten ”Metoder för risk- och sårbarhetsanalys från ett systemperspektiv” (Johansson & Jönsson 2007) finns en mer detaljerad beskrivning av det material som tas upp här.

Olika typer av metoder för risk- och sårbarhetsanalys

Vid en genomgång av metoder för risk- och sårbarhetsanalys finner man att metoderna grovt kan delas in i två grupper, de som kan kallas *scenariobaserade* risk- och sårbarhetsanalysmetoder och de som kan kallas *systembaserade* risk- och sårbarhetsanalysmetoder. De scenariobaserade metoderna är exempelvis ROSA (Länsstyrelsen i Kronobergs län 2003), MVA (Hallin et al. 2004) och IBERO (Länsstyrelsen i Stockholms län 2006). Dessa metoder karaktäriseras av att de är starkt fokuserade på att ta fram ett förhållandevis begränsat antal riskscenarier[1]. Dessa riskscenarier förefaller ofta vara mycket detaljerat beskrivna. De systembaserade metoderna är mer fokuserade på att beskriva det aktuella systemet innan en analys av olika riskscenarier genomförs. Detta innebär att man först skapar någon typ av modell av verkligheten i vilken man beskriver relationer mellan olika element i systemet (exempelvis relationer mellan pumpar och ventiler i ett tekniskt system). Med utgångspunkt i denna modell resonerar man sig sedan fram till vilka olika riskscenarier som kan uppkomma i systemet. Exempel på metoder som tillhör denna grupp är ”traditionella” riskanalysmetoder som felträdsanalys och händelseträdsanalys. Fler exempel på metoder finns i ”Handbok för riskanalys” (Räddningsverket 2003).

I det här informationsbladet används den definition av risk och den definition av sårbarhet som presenteras i informationsbladet ”En operationell definition av sårbarhet”. Risk betraktas där som svaren på frågorna ”Vad kan hända?”, ”Hur sannolikt är det?” och ”Vad blir konsekvenserna?”. Detta är en definition som föreslogs redan på 80-talet och som har använts mycket inom det tekniska området. Fördelen med denna definition är att förutom att vara ganska enkelt formulerad så ger den också vägledning för hur man analyserar risken i ett

[1] Begreppet ”riskscenario” används för att beteckna en händelseutveckling i ett system som leder till någon typ av oönskat tillstånd i systemet.

system, d.v.s. det är en operationell definition. Motsvarande operationella definition av sårbarhet har föreslagits som svaren på frågorna ”Vad kan hända, givet att en specifik påfrestning inträffar?”, ”Hur sannolikt är det, givet denna påfrestning?”, och ”Vad blir konsekvenserna?”. Utifrån de båda definitionerna kan man formulera ett antal önskvärda egenskaper som en riskanalys eller sårbarhetsanalys bör ha. I det här informationsbladet berörs ett antal av dessa egenskaper som bedömts extra viktiga. I Johansson & Jönsson (2007) finns en mer detaljerad redogörelse.

Det är en fördel att inleda en diskussion om önskvärda egenskaper hos risk- och sårbarhetsanalyser med att notera skillnaden mellan risk och sårbarhet. I en riskanalys utgår man från att det system som man är intresserad av att analysera befinner sig i ”normaltillståndet”, d.v.s. att inga oönskade konsekvenser uppstått och sedan undersöker man vad som kan få systemet att avvika från detta tillstånd. En förutsättning för att kunna göra detta är naturligtvis att man beskrivit vad man menar med ”normaltillstånd” och att man beskrivit vad man betraktar som negativa konsekvenser i systemet. I en sårbarhetsanalys, enligt den definition som används här, utgår man däremot från att en specifik påfrestning har inträffat och påverkar systemet i fråga och det som man utreder i analysen är vad som kan hända efter att påfrestningen inträffat, hur sannolikt det är och vad konsekvenserna blir. Skillnaden är alltså att i sårbarhetsanalysen är man inte intresserad av hur sannolikt det är att den aktuella påfrestningen inträffar, bara effekterna av den.

Det finns en annan aspekt av sårbarhet som är viktig att notera när man diskuterar metoder för risk- och sårbarhetsanalys. När begreppet sårbarhet används här avses svaren på de tre frågorna som beskrevs ovan, men begreppet sårbarhet kan också användas för att indikera *ett förhållande eller omständighet* i det system som studeras. Exempelvis kan en olåst dörr betraktas som *en* sårbarhet eftersom någon kan ta sig in den vägen och stjäla något. I det fallet syftar alltså begreppet sårbarhet inte på en systemegenskap i förhållande till en påfrestning, vilket definitionen som presenterades ovan gör. För att identifiera *en eller flera* sårbarheter i ett system är det rimligt att anta att man då måste göra en analys av *systemets* sårbarhet för en eller flera specifika påfrestningar och därmed finns det alltså en koppling mellan de båda användningarna av sårbarhetsbegreppet. Detta diskuteras mer under rubriken ”Några viktiga saker att tänka på då man gör en risk- och sårbarhetsanalys” nedan.

Detta sätt att betrakta begreppen risk och sårbarhet kan innebära att en *risk- och sårbarhetsanalys* är en riskanalys i vilken extra vikt fästs vid att identifiera sårbarheter i systemet. I praktiken kan man även tänka sig att en *risk- och sårbarhetsanalys* är en grov riskanalys som kombineras med en eller flera betydligt mer detaljerade sårbarhetsanalyser.

Riskscenariorymden

Ett annat begrepp som är användbart för att diskutera metoder för risk- och sårbarhetsanalys är *riskscenariorymd*. Riskscenariorymden för ett specifikt system, exempelvis en kommun eller myndighet, utgörs av *samtliga* riskscenarier som kan inträffa i systemet. I Figur 1 finns en illustration av riskscenariorymden som innehåller alla brandscenarier som kan inträffa i en specifik byggnad. Där kan man se att det finns tre olika typer av riskscenarier som kan inträffa i byggnaden (ett område i figuren motsvarar en typ av riskscenario), en typ som innebär att branden börjar i lokal 2, en som innebär att branden börjar i lokal 1 och där sprinklersystemet släcker branden samt en typ där branden börjar i lokal 1 men där sprinklersystemet inte släcker branden. Det kan verka konstigt att påstå att *bara* dessa tre riskscenarier kan inträffa i byggnaden eftersom man kan tänka sig exempelvis ett brandscenario som börjar i lokal två och som släcks av sprinklersystemet. Vad man menar när man säger att de tre riskscenarierna utgör samtliga riskscenarier som kan inträffa i byggnaden är att de tre riskscenarierna *beskriver* eller *representerar* samtliga riskscenarier som har med brand att göra i byggnaden. Riskscenariot som börjar i lokal 2 och som släcks av sprinklersystemet kan beskrivas av ett av riskscenarierna i figuren, nämligen det som innebär att branden börjar i lokal 2.

Figur 1 *Illustration av den del av riskscenariorymden för en byggnad som innebär att bränder börjar i byggnaden.*

Exemplet ovan illustrerar en viktig sak i risk- och sårbarhetsanalyser: ett riskscenario kan *alltid delas upp i mer detaljerade beskrivningar*. En utmaning när

man gör en risk- och sårbarhetsanalys är att göra uppdelningen av riskscenariorymden så att den *representerar* samtliga riskscenarier som kan inträffa i systemet på ett bra sätt.

Några viktiga saker att tänka på när man gör en risk- och sårbarhetsanalys

Med hjälp av begreppet riskscenariorymd kan man diskutera ett antal aspekter som är viktiga att tänka på när man gör en risk- och sårbarhetsanalys. Några av dessa diskuteras kortfattat nedan.

Analysens täckningsgrad

Ett viktigt problem som man bör reflektera över då man gör en risk- och sårbarhetsanalys oavsett vilken metod som används är om man har missat att identifiera några väsentliga riskscenarier. Med analysens täckningsgrad avses hur väl de riskscenarier som identifierats i analysen ”täcker in” allt som kan inträffa i verkligheten. I exemplet med branden i byggnaden som illustrerades i figur 1 är täckningsgraden god om det är så att byggnaden bara har två lokaler (lokal 1 och 2) eftersom det då inte finns några andra ställen som en brand kan börja på i byggnaden. Om det däremot hade funnits en tredje lokal i byggnaden, där det vore möjligt för bränder att starta, hade analysens täckningsgrad inte varit fullständig eftersom den då inte ”täcker in” scenarierna som börjar i lokal 3.

Att hantera täckningsgradsproblemet i en risk- och sårbarhetsanalys är mycket viktigt, speciellt när man använder en scenariobaserad metod eftersom dessa ger mindre vägledning än de systembaserade metoderna när det gäller att identifiera samtliga riskscenarier.

För att reducera detta problem då man genomför en analys med en scenariobaserad metod kan man använda ett enkelt tillvägagångssätt som förhoppningsvis inte gör att analysen blir mycket mer tidskrävande. Tillvägagångssättet bygger på att man identifierar händelser eller omständigheter i det riskscenario som man för tillfället analyserar som är viktiga för hur stora konsekvenserna på grund av riskscenariot blir. När dessa händelser och omständligheter sedan är identifierade går man systematiskt igenom dem och funderar över vad som skulle hända om de aktuella händelserna *inte* inträffade, eller om omständigheterna som man räknat med *inte* gällde.

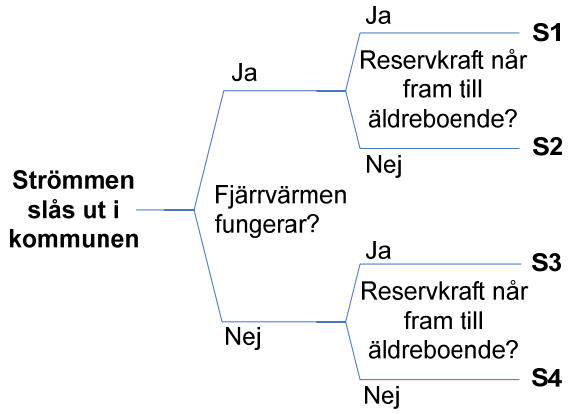
För att illustrera tillvägagångssättet kan ett enkelt exempel i vilket en kommun analyserar konsekvenserna av ett långvarigt strömavbrott användas. I det fallet har kommunen konstaterat att när strömmen försvinner kommer kommunens äldreboenden att sakna möjlighet till uppvärmning eftersom cirkulationspumparna i byggnaderna som driver runt det varma vattnet i radiatorerna inte fungerar då. Om cirkulationspumparna fungerar måste även distributionen av värme via fjärrvärmesystemet fungera för att byggnaderna skall kunna värmas upp (annars finns inget varmt vatten som kan cirkulera i byggnaderna). När personerna som genomfört analysen resonerat kring detta riskscenario kom de fram till att portabla elverk kommer att köras ut till äldreboendena och på så sätt kan byggnaderna försörjas med ström. Vidare konstaterade man att fjärrvärmesystemet kan hållas igång med hjälp av de reservkraftsaggregat som finns installerade i systemet och alltså kommer uppvärmningen av äldreboendena att fungera. Det här riskscenariot innehåller (åtminstone) två viktiga händelser: att de portabla elverken kommer ut till äldreboendena och att fjärrvärmesystemet fungerar.

De händelser som identifierats ovan måste dokumenteras så att man också kan analysera vad som händer om de *inte* inträffar, d.v.s. elverken når inte äldreboendena av någon anledning eller fjärrvärmesystemet fungerar inte av någon anledning. Om man arbetar systematiskt med att identifiera sådana viktiga händelser i ett riskscenario ökar möjligheten att identifiera andra riskscenarier som kan inträffa vilket gör att analysen blir mer heltäckande.

En nackdel med detta arbetssätt är att det krävs en större arbetsinsats för att analysera riskscenarier då man hela tiden måste fundera över vad som händer om viktiga händelser inte inträffar. Den extra arbetsinsatsen behöver dock inte bli alltför betydande, utan det beror på hur noggrant de olika riskscenarierna analyseras. Ofta räcker det med att konstatera att om exempelvis fjärrvärmesystemet inte fungerar måste äldreboendena tömmas på folk och de måste flyttas till byggnader som har värme. Hur detta kan göras kan man vänta med att analysera i detalj tills man har resurser för det, det viktiga är att man identifierat möjligheten att händelseutvecklingen blir en annan än den som man identifierat i det ursprungliga riskscenariot.

Ett bra sätt att illustrera de olika riskscenarier som kan uppstå till följd av en påfrestning är med hjälp av händelseträd. I figur 2 illustreras exemplet med äldreboendena. Trädet inleds med den påfrestning som man analyserar, d.v.s. ”Strömmen slås ut i kommunen” och därefter illustreras de olika viktiga händelserna, d.v.s. om fjärrvärmen fungerar eller ej och om reservkraften når fram till äldreboendena. Resultatet blir ett händelseträd där fyra olika

riskscenarier, S1 till S4, illustrerar olika händelseutvecklingar till följd av påfrestningen.



Figur 2 *Illustration av några viktiga händelser vid påfrestningen "Strömmen slås ut i kommunen".*

Hantering av osäkerhet

Notera att de fyra riskscenarierna i figur 2 svarar på frågan "Vad kan hända, givet påfrestningen att strömmen slås ut i kommunen?". Svaret är alltså att något av de fyra riskscenarierna i figuren inträffar. För att göra en fullständig risk- och sårbarhetsanalys enligt den definition som används här måste analysen också svara på frågorna hur sannolika riskscenarierna är givet påfrestningen och vad konsekvenserna blir för de olika riskscenarierna . När det gäller sannolikheten att de olika riskscenarierna inträffar räcker det troligtvis med att man ger en grov uppskattning av vilket av riskscenarierna som är troligast och möjligtvis också indikerar vilka som är minst sannolika. Det viktiga är inte själva sannolikhetsskattningarna i sig utan det faktum att man noterar att osäkerhet (rörande vilket riskscenario som kommer att inträffa) även förekommer i en sårbarhetsanalys.

Syftet med risk- och sårbarhetsanalys

När man gör en risk- och sårbarhetsanalys är det viktigt att ha klart för sig vad syftet med analysen är. Syftet kan påverka hur analysen utformas och det är inte säkert att en analys som utförs med en viss metod för risk- och sårbarhetsanalys kan uppfylla alla syften som man kan ha med en sådan analys.

Det vanligaste syftet med en risk- och sårbarhetsanalys är, med utgångspunkt i de definitioner av risk och sårbarhet som används här, att svara på de tre frågorna som presenterats ovan. Hur väl man kan uppfylla detta syfte har till stor del att göra med hur man hanterar täckningsgradsproblemet (se diskussionen ovan), d.v.s. hur man ser till att alla relevanta riskscenarier finns med i kartläggningen. Det finns dock andra syften som kan vara förknippade med en risk- och sårbarhetsanalys. Exempelvis kan syftet vara att identifiera *risker och sårbarheter* i systemet för att kunna föreslå sätt att eliminera dessa. Här används begreppen risk och sårbarhet för att beteckna en omständighet i systemet och alltså inte en uppsättning riskscenarier som är den normala betydelsen i detta dokument. Om man vill använda analysen för att uppfylla detta syfte är det rimligt att först identifiera de riskscenarier som kan tänkas uppstå i systemet, deras konsekvenser och sannolikheter och sedan utifrån den informationen försöka identifiera omständigheter i systemet som är *huvudorsakerna till varför dessa riskscenarier kan inträffa*. Ett exempel är att man i analysen av äldreboendena i kommunen som diskuterades ovan konstaterat att om ett långvarigt strömavbrott inträffar i kommunen kommer man att få svårt att få ut reservkraftverk till äldreboendena vilket i sin tur innebär att konsekvenserna för de äldre människorna på äldreboendena kommer att bli allvarliga. Med utgångspunkt i denna typ av riskscenarier kan man sedan konstatera att det är *en sårbarhet* att äldreboendena saknar reservkraftsgeneratorer.

Ett annat exempel på syfte med en risk- och sårbarhetsanalys är att den skall användas som beslutsunderlag för investeringar i riskreducerande och/eller sårbarhetsreducerande åtgärder. I det fallet kan högre krav ställas på att bedömningarna av sannolikheterna för de olika riskscenarierna som kan uppkomma är noggrant utförda och dokumenterade.

Det finns alltså olika syften som man kan ha när man genomför en risk- och sårbarhetsanalys och det är viktigt att detta framgår i en analys. Annars är det mycket svårt att veta om den aktuella analysen är tillräcklig eller ej. Huruvida en analys är tillräcklig eller ej torde bara kunna bedömas med avseende på vad syftet med analysen är.

Analysens detaljeringsgrad och definition av negativa konsekvenser

En annan aspekt av arbetet med en risk- och sårbarhetsanalys som är viktig är hur detaljerat man beskriver de olika riskscenarierna som kan inträffa. I exemplet som illustreras i figur 2 har fyra typer av riskscenarier använts för att representera allt som kan inträffa efter att strömmen i kommunen slås ut. Detta kan för vissa syften vara tillräckligt, exempelvis i en analys av de äldres situation vid en sådan påfrestning, men för andra syften är den förmodligen inte tillräcklig, exempelvis för att analysera hur sårbar räddningstjänstens verksamhet är för ett långvarigt

strömavbrott. Vad som behöver beskrivas i riskscenarierna beror till stor del på syftet med analysen, men också på vad som man i analysen uppfattar som negativa konsekvenser för det aktuella systemet (vilket i sin tur kan bero på syftet med analysen). Vad som uppfattas som negativa konsekvenser är inget självklart och det bör framgå tydligt i en risk- och sårbarhetsanalys vad det är. Exempelvis kan negativa konsekvenser vara antal omkomna människor, men det kan också vara konsekvenser som innebär att vissa samhällsviktiga funktioner inte kan upprätthållas.

Ett bra tillvägagångssätt i en risk- och sårbarhetsanalys är att inleda analysen med att fundera över vad det är som uppfattas som negativa konsekvenser och sedan utgå ifrån det när man identifierar olika riskscenarier. Att successivt ställa frågan ”vad är det som påverkar graden av negativa konsekvenser för en specifik påfrestning?” gör att man kan identifiera de händelser och omständigheter som sedan kan användas för att identifiera olika riskscenarier som kan bli resultatet av den specifika påfrestningen (se figur 2).

Sammanfattning

Sammanfattningsvis kan de metoder för risk- och sårbarhetsanalys som finns tillgängliga grovt delas upp i *scenariobaserade* och *systembaserade*. I praktiken är det sannolikt de scenariobaserade som används mest för statliga myndigheter och kommuner. Oavsett vilken typ av metod som används finns det vissa frågor som bör kunna besvaras när det gäller en analys. Dessa frågor berör de centrala delarna av det som diskuterats tidigare i detta informationsblad:

- Svarar *sårbarhetsanalysen* på frågorna ”Vad kan hända, givet att en specifik påfrestning inträffat?”, ”Hur sannolikt är det, givet denna påfrestning?” och ”Vad blir konsekvenserna?” ?
- Svarar *riskanalysen* på frågorna ”Vad kan hända?”, ”Hur sannolikt är det?” och ”Vad blir konsekvenserna?” ?
- Hur har man säkerställt att risk- och sårbarhetsanalysen inte missat att identifiera relevanta riskscenarier?
- Vilka är de negativa konsekvenserna som man fokuserar på i analysen? Är dessa tillräckliga?
- Är syftet med analysen klart beskrivet? Är detaljeringsgraden i riskscenariobeskrivningarna tillräcklig för att uppfylla syftet med analysen?

Svaren på dessa frågor ger god vägledning för att kunna bedöma om en specifik risk- och sårbarhetsanalys bör utvecklas på något område.

Referenser

Hallin, P.-O., Nilsson, J. & Olofsson, N. (2004), *Kommunal sårbarhetsanalys*, Krisberedskapsmyndigheten, Stockholm.

Johansson, H. & Jönsson, H. (2007), *Metoder för risk- och sårbarhetsanalys från ett systemperspektiv*, LUCRAM, Lunds universitet, Lund.

Krisberedskapsmyndigheten (2005), *Uppföljning av myndigheternas arbete med risk- och sårbarhetsanalyser*, Dnr: 0152/2005, Stockholm.

Krisberedskapsmyndigheten (2006), *Risk- och sårbarhetsanalyser år 2005*, Dnr 0222/2006. Stockholm.

Länsstyrelsen i Kronobergs län (2003), *ROSA - en metod för risk- och sårbarhetsanalyser*.

Länsstyrelsen i Stockholms län (2006), *IBERO Steg för steg – Manual*, Stockholm.

Räddningsverket (2003), *Handbok för riskanalys*, Karlstad.

Kontakt

För mer information kontakta oss på följande e-postadresser eller besök FRIVA:s hemsida.

Henrik Johansson
Henrik.johansson@brand.lth.se

Henrik Jönsson
Henrik.jonsson@brand.lth.se

FRIVA
http://www.lucram.friva.lu.se

FRIVA

En operationell definition av sårbarhet

Författare: Henrik Johansson, Henrik Jönsson

Inledning

Denna skrift är ett av flera informationsblad som redovisar sammanfattade erfarenheter och synpunkter från ramforskningsprogrammet FRIVA (Framework Programme for Risk and Vulnerability Analysis), vilket finansierats av Krisberedskapsmyndigheten under perioden mars 2004 till mars 2007. Informationsbladen skall kunna användas som utgångspunkter för praktiskt arbete när det gäller hantering av risker, sårbarheter, hot, kriser och katastrofer som medför eller kan medföra allvarliga samhälleliga konsekvenser.

Bakgrund

Det finns många olika definitioner av sårbarhet (se exempelvis Hallin m.fl. (2004). När man gör en sårbarhetsanalys är det därför mycket viktigt att klargöra vilken definition av begreppet som används. I det här informationsbladet presenteras en operationell definition av sårbarhet som lämpar sig väl för användning i en sårbarhetsanalys. Med ”operationell definition” avses i det här sammanhanget en definition som även innehåller en beskrivning av en procedur eller operation för hur man kan analysera ett systems sårbarhet. Detta är något som många definitioner av sårbarhet saknar och som gör dem svåra att använda i praktiken. Resultaten som presenteras i det här informationsbladet kommer från delprojekt 2 i FRIVA-projektet och redovisas mer detaljerat i rapporten ”Metoder för risk- och sårbarhetsanalys från ett systemperspektiv” (Johansson & Jönsson 2007).

Vad är sårbarhet, system och negativa konsekvenser?

När det gäller sårbarhetsanalys för ett system, exempelvis en kommun eller en statlig myndighet, går det inte att diskutera ett systems sårbarhet utan att klargöra vilken påfrestning som avses. Detta innebär att man vid en analys av ett systems sårbarhet måste ha en specifik påfrestning som utgångspunkt för analysen. Det går alltså inte att diskutera ett systems sårbarhet *i allmänhet* eftersom systemets sårbarhet kan bero på vilken påfrestning som avses, ett system kan exempelvis vara sårbart för stormar men robust mot epidemier.

Förutom att man måste klargöra vilken påfrestning som man avser vid en analys av ett systems sårbarhet måste man också klargöra vad man menar med ”systemet”. Ett system uppfattas i det här sammanhanget som en uppsättning element som på något sätt bildar en helhet. Vanligtvis funderar man kanske inte så mycket över vad systemet är, utan det uppfattas ofta som självklart. Om systemet är en kommun förväntar sig de flesta att personerna som bor i kommunen är en ”del” av systemet, men är exempelvis personer som bara vistas i kommunen en del av systemet? På sådana frågor finns inget rätt eller fel svar utan det beror på hur man definierar sitt system, vilket illustrerar vikten av att vara tydlig med en systemdefinition när man gör en sårbarhetsanalys. Inom riskanalysområdet är detta mer eller mindre självklart, men när det gäller sårbarhetsanalyser förefaller det inte vara lika uppmärksammat. En anledning till att det är viktigt att presentera en klar systemdefinition är att verkligheten kan beskrivas på i princip ett oändligt antal sätt och det går ofta inte att säga att ett visst sätt är mer ”rätt” än ett annat. Det går exempelvis att beskriva systemet ”kommunen” som bestående av ett antal stadsdelsnämnder, men det går också att beskriva det som bestående av de människor som bor i ett visst geografiskt område.

Hur man väljer att beskriva verkligheten, d.v.s. hur man definierar sitt system, påverkar i högsta grad hur man ser på vad som är negativa konsekvenser i en sårbarhetsanalys. Negativa konsekvenser är något som är centralt både för begreppet risk och för begreppet sårbarhet. Om det inte finns någon möjlighet att det skulle kunna uppstå negativa konsekvenser i ett system finns det heller ingen risk i systemet. På samma sätt som när det gäller definitionen av systemet måste en analys av ett systems sårbarhet för en specifik påfrestning ta sin utgångspunkt i vad som uppfattas som negativa konsekvenser. Eftersom detta kan bero på vilka värderingar som används som utgångspunkt för analysen måste detta framgå vid en analys av ett systems sårbarhet. Man bör notera att negativa konsekvenser kan beskrivas med ett antal *konsekvens-*

attribut, exempelvis antal döda människor, antal skadade människor, skadekostnader, etc. Vilka som används i en sårbarhetsanalys, och hur viktiga attributen är i förhållande till varandra, beror på vilka värderingar som ligger till grund för analysen.

Enligt det sätt att betrakta ett systems sårbarhet som används här måste man alltså ha följande element för att kunna genomföra en sårbarhetsanalys:

- En beskrivning av systemet.
- En beskrivning av påfrestningen som man vill undersöka systemets sårbarhet för.
- Ett sätt att beskriva de negativa konsekvenserna i systemet.

Viktiga begrepp i en riskanalys och i en sårbarhetsanalys

Den definition av begreppet sårbarhet som presenteras i detta informationsblad är inspirerad av en operationell definition av risk som föreslogs i början på 80-talet (Kaplan & Garrick, 1981) och som är den dominerande när det gäller riskanalyser. En av fördelarna med att använda denna definition av risk som utgångspunkt för definitionen av sårbarhet är att riskdefinitionen innefattar en terminologi som är användbar för att beskriva händelser som kan inträffa i framtiden och som kan innebära negativa konsekvenser. Denna terminologi är även användbar för sårbarhetsanalys. Nedan följer en sammanfattning av några av dessa begrepp som sedan används för att definiera vad ett systems sårbarhet är och hur man kan analysera den.

Riskscenario och S_0-scenario

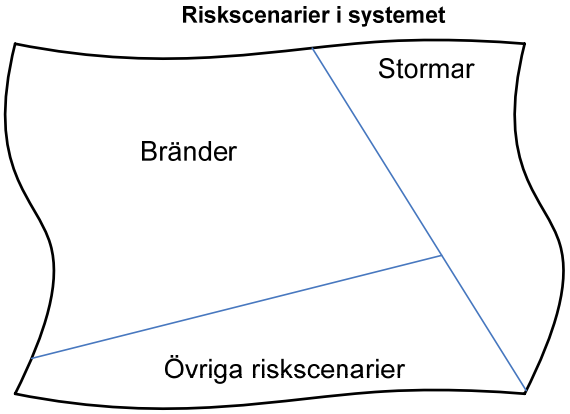
Gemensamt för alla riskanalyser och sårbarhets-analyser är att de berör händelser som kan inträffa i framtiden. Ofta används begreppet *scenario* för att beteckna förändringar i systemet över tid, d.v.s. att någon typ av händelseförlopp sker. För att kunna veta vad som är negativa händelser i ett system utgår man ofta från vad som uppfattas som ”normalt” i systemet, d.v.s. när systemet uppför sig som normalt uppstår inga negativa konsekvenser. För att beteckna ”det normala” i ett system använder man begreppet *S_0-scenariot.* Den beteckningen kommer från den operationella definitionen av risk som har använts som utgångspunkt och den förutsätter att man kan beskriva vad som avses med normalt i ett system. Ibland uppför sig systemet dock inte normalt och då kallar man det för ett *riskscenario*, d.v.s. något händer i systemet som gör att systemet lämnar *S_0-scenariot*.

Inledande händelse

I en riskanalys kallas en händelse som får systemet att lämna *S_0-scenariot* för *inledande händelse* och kan exempelvis vara att ”Brand uppstår i byggnaden”, eller ”En allvarlig storm drabbar kommunen”. Målet med en riskanalys är att identifiera ”alla” inledande händelser som kan få systemet att avvika från *S_0-scenariot* och beskriva de riskscenarier som kan uppkomma som en följd av dessa inledande händelser.

Riskscenariorymd

Samtliga riskscenarier som kan inträffa i ett system kallas för *riskscenariorymden*. Riskscenariorymden kan illustreras med hjälp av ytor, där hela ytan mellan de böjda linjerna i figur 1 representerar alla riskscenarier som kan inträffa i systemet. I figuren syns att denna yta är uppdelad i tre delar, vilka representerar olika *typer* av riskscenarier; bränder, stormar och övriga riskscenarier.



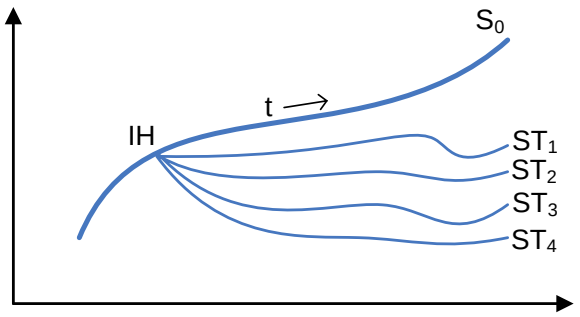
Figur 1 *Illustration av riskscenariorymden i ett system.*

En riskanalys går ut på att göra en uppdelning av riskscenariorymden i olika typer av riskscenarier, d.v.s. att identifiera vilka typer av riskscenarier som kan inträffa i systemet.

När det gäller en analys av ett systems sårbarhet kan man på samma sätt som för en riskanalys betrakta riskscenariorymden som samtliga riskscenarier som kan inträffa *som en följd av den aktuella påfrestningen*. När det gäller sårbarhetsanalysen är riskscenarierna alltså betingade på att den specifika påfrestningen har inträffat.

Olika riskscenarier i ett system brukar även illustreras på det sätt som visas i figur 2. Där representerar den tjockare linjen S_0-scenariot som innebär att systemet befinner sig i ”normaltillståndet”. De grenar som

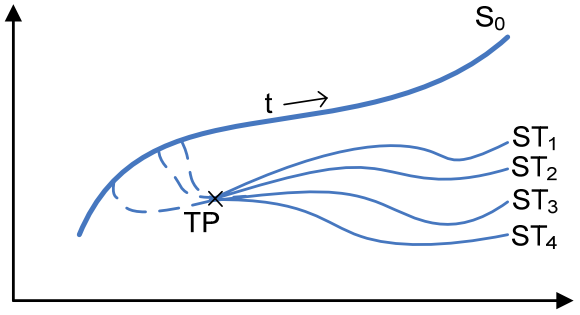
leder ut från S_0-scenariet där det står IH (Inledande Händelse) representerar olika riskscenarier som kan inträffa som en följd av en inledande händelsen. Bokstaven ”t” illustrerar en förändring över tiden. Efter den inledande händelsen kan olika riskscenarier inträffa och dessa representeras i figuren av de olika grenarna som leder ut från IH och slutar i olika sluttillstånd (ST). Ett sluttillstånd innebär att man kan avgöra vad konsekvenserna av riskscenariot blir.



Figur 2 *Avvikelser från S_0-scenariet som resulterar i olika sluttillstånd (ST).*

När det gäller ett systems sårbarhet för en påfrestning kan man använda figur 3 för att illustrera skillnaden jämfört med risken i ett system. I figur 3 illustreras påfrestningen på systemet genom krysset där det står ”TP”. Efter att en påfrestning har drabbat systemet kan olika riskscenarier uppstå, vilket illustreras av de fyra riskscenarierna som resulterar i sluttillstånden ST_1 till ST_4. Notera att det, i detta fall, finns flera olika sätt som den aktuella påfrestningen kan inträffa på (vilket illustreras med hjälp av de streckade linjerna ut från S_0-scenariot).

Skillnaden mellan en riskanalys och en sårbarhetsanalys är att i en riskanalys försöker man identifiera samtliga riskscenarier som kan få systemet att avvika från S_0-scenariot, men i en sårbarhetsanalys *förutsätter* man att en påfrestning som fått systemet att lämna S_0-scenariot har inträffat och man försöker då identifiera alla riskscenarier som kan inträffa *som en följd av den påfrestningen.*



Figur 3 *Illustration av en påfrestning på ett system (TP) och de riskscenarier som uppstår som en följd av påfrestningen.*

Definition av sårbarhet

Med hjälp av de begrepp som presenterats ovan kan man definiera risken i ett system som svaren på frågorna ”Vad kan hända?”, ”Hur sannolikt är det?” och ”Vad blir konsekvenserna?” (detta är den definition som Kaplan och Garrick presenterat tidigare). Svaren på dessa frågor är en beskrivning av ett antal riskscenarier (avvikelserna från S_0-scenariot i figur 2), deras respektive sannolikhet och konsekvens.

På samma sätt kan ett systems sårbarhet för en specifik påfrestning definieras som svaren på frågorna:

- **Vad kan hända, givet att en specifik påfrestning inträffar?**
- **Hur sannolikt är det, givet denna påfrestning?**
- **Vad blir konsekvenserna?**

Svaren på dessa frågor är en beskrivning av *ett antal* riskscenarier, som är betingade av att den specifika påfrestningen har drabbat systemet, deras sannolikheter och konsekvenser. Detta utgör alltså systemets sårbarhet för den aktuella påfrestningen.

Med hjälp av denna information kan man, precis på samma sätt som när det gäller riskbegreppet, skapa olika *mått på sårbarheten*. Ett exempel på ett sådant mått är den maximala negativa konsekvensen till följd av en specifik påfrestning.

Fördelar med definitionen

Det finns ett antal fördelar med att använda den föreslagna definitionen. En fördel är att definitionen är enkel att använda. Visserligen används en del abstrakta begrepp i samband med definitionen, men kärnan i definitionen är förhållandevis enkel att förstå eftersom den kan formuleras som *svaren på de tre frågorna ovan*.

En annan fördel med definitionen är att den ger ett sätt att relatera begreppet risk och begreppet sårbarhet till varandra. Eftersom definitionen av sårbarhet bygger på en definition av risk och eftersom liknande terminologi har använts vid definitionen av sårbarhet som vid definitionen av risk är det enkelt att se hur begreppen förhåller sig till varandra. En analys av risk i ett system utgår från att systemet befinner sig i normalläget och sedan försöker man identifiera riskscenarier som kan få systemet att avvika från detta läge. I en sårbarhetsanalys däremot utgår man från att en påfrestning har

inträffat och sedan försöker man identifiera risk-scenarier som kan bli resultatet av påfrestningen.

Vidare är en fördel med definitionen att den lyfter fram det faktum att det (ofta) råder osäkerhet rörande vad som kommer att hända i ett system efter att det drabbas av en specifik påfrestning. Denna osäkerhet fångas upp genom att det inte bara finns ett riskscenario som är svaret på den första av de tre frågorna ovan, det kan finnas flera. Detta är något som ibland tonas ner i sårbarhetsanalyser där man utgår från att om en specifik påfrestning inträffar så råder ingen osäkerhet rörande konsekvenserna.

Den föreslagna definitionen ger också ett konkret verktyg för att skilja på *ett systems sårbarhet* och *en sårbarhet i systemet*. Ett systems sårbarhet motsvaras av den definition som presenterats här och utgörs alltså av en uppsättning riskscenarier som är betingade av en specifik påfrestning, samt deras sannolikheter och konsekvenser. En sårbarhet i ett system syftar däremot på någonting i det aktuella systemet, ett förhållande eller en omständighet, som gör att konsekvenserna av en påfrestning blir stora. Underförstått är då att om detta förhållande inte fanns skulle påfrestningen inte leda till så stora konsekvenser. Ett exempel är om en byggnad har dåligt inbrottsskydd. Detta kan då sägas utgöra *en sårbarhet* eftersom konsekvenserna om byggnaden skulle utsättas för ett inbrottsförsökt troligtvis blir stora på grund av det dåliga skyddet.

Vad betyder definitionen i praktiken?

Den föreslagna definitionen på sårbarhet innebär att en sårbarhetsanalys i praktiken måste innehålla en dokumentation av de tre punkterna som togs upp på första sidan. Dokumentationen skall alltså bestå av ”En beskrivning av systemet”, ”En beskrivning av den påfrestningen som man vill undersöka systemets sårbarhet för”, samt ”Ett sätt att beskriva de negativa konsekvenserna i systemet”.

Om man är noggrann med detta ökar det möjligheten för andra personer att förstå och granska analysen.

En annan viktig aspekt av den praktiska användningen av definitionen är att den fokuserar på negativa scenarier (riskscenarier), d.v.s. på saker som *kan hända i systemet*. Detta tvingar en person som gör en analys att först fundera på vad som kan hända om en specifik påfrestning inträffar och *därefter* kan han/hon börja fundera på om det finns sårbarheter i systemet som bör åtgärdas. Denna åtskillnad mellan en analys av *systemets sårbarhet* och en *identifiering av sårbarheter* är viktig och definitionen som föreslagits här ger ett tydligt sätt att skilja dessa åt. I praktiken kan man kräva att en sårbarhetsanalys först redovisar en analys av systemets sårbarhet till följd av en specifik påfrestning i form av ett antal riskscenarier som kan inträffa om påfrestningen skulle drabba systemet och först därefter identifierar sårbarheter i systemet och motiverar dessa med hjälp av de riskscenarier som tagits fram.

Ett mycket enkelt exempel som illustrerar hur detta skulle kunna se ut är följande analys av en byggnads sårbarhet för bränder. Antag att byggnaden består av två lokaler, ett förrådsutrymme och en samlingslokal där mycket folk kan samlas. En beskrivning av systemet skulle kunna vara en beskrivning av de olika lokalerna och hur mycket folk som vistas där. Påfrestningen som vi är intresserade av är bränder i byggnaden och de negativa konsekvenserna som är av intresse har att göra med hur många människor som skadas eller dödas i en brand.

Ett resultat från en sådan sårbarhetsanalys skulle kunna vara följande lista (se tabell 3) på brandscenarier där skillnad görs på var branden uppkommer, i förrådet (lokal 1) eller samlingslokalen (lokal 2), om branden växer sig stor eller ej. Notera att sannolikheterna bara angivits som hög, medel eller låg och att konsekvenserna inte har uttryckts i *antalet* döda och skadade. Detta är medvetet eftersom man i en inledande analys kanske inte har tillräcklig information för att använda exakta siffror, men om man får jobba vidare med analysen kan man ersätta beskrivningarna med siffror. Notera att tabellen ger svaren på de tre frågorna som formulerats ovan, d.v.s. vad som kan hända (riskscenarierna), hur sannolikt det är och vad konsekvenserna blir.

Tabell 1 *Exempel på ett antal grovt beskrivna riskscenarier som kan bli resultatet av en brand i en byggnad.*

Riskscenario	Sannolikhet	Konsekvens
Lokal 1/Ej stor	Hög	Ingen
Lokal 1/Stor	Medel	Döda och rökskadade
Lokal 2/Ej stor	Hög	Få rökskadade
Lokal 2/Stor	Låg	Döda och rökskadade

I tabell 1 framgår att konsekvenserna har bedömts bli samma oavsett om branden uppstår i lokal 1 och blir stor eller om den uppstår i lokal 2 och blir stor. Detta beror på att det inte finns någon brandteknisk avskiljning mellan lokalerna och en brand kan alltså börja i förrådet och sedan kan röken obehindrat spridas in i samlingslokalen. En slutsats som kan dras från analysen av systemets sårbarhet för bränder är att det faktum att lokalerna saknar brandteknisk

avskiljning *utgör en sårbarhet*. Om det fanns en brandteknisk avskiljning mellan lokalerna hade det andra riskscenariot i tabellen inte resulterat i några negativa konsekvenser. Denna information kan användas för att ta ställning till om det är värt att göra en sårbarhetsreducerande åtgärd i det aktuella fallet.

När det gäller just förslag på sårbarhetsreducerande åtgärder ger den föreslagna definitionen ytterligare en fördel eftersom den ger möjlighet att klargöra vilka riskscenarier som en eventuell åtgärd skulle kunna reducera konsekvenserna av eller sannolikheterna för. Ett krav som man då kan ställa på förslag på sårbarhetsreducerande åtgärder är att man i ett sådant förslag också presenterar en bedömning av vilka riskscenarier som påverkas, vilket gör det lättare att ta ställning till om det aktuella åtgärdsförslaget är ”kostnadseffektivt” eller ej. Med kostnadseffektivt avses förhållandet mellan hur mycket investeringen kostar och hur mycket den åstadkommer i form av en sårbarhetsreduktion.

Sammanfattning

Definitionen som presenterats i detta informationsblad ger goda möjligheter att systematiskt arbeta med sårbarhetsanalys för olika typer av system. Definitionen innebär att ett systems sårbarhet för en specifik påfrestning uppfattas som svaren på tre frågor:

- Vad kan hända, givet att en specifik påfrestning inträffar?
- Hur sannolikt är det, givet denna påfrestning?
- Vad blir konsekvenserna?

Svaren på frågorna blir en uppsättning riskscenarier som kan inträffa om den aktuella påfrestningen skulle inträffa, tillsammans med en bedömning av riskscenariernas konsekvenser och sannolikheter.

Referenser

Hallin, P.-O., Nilsson, J. & Olofsson, N. (2004), *Kommunal sårbarhetsanalys*, Krisberedskapsmyndigheten, Stockholm.

Johansson, H. & Jönsson, H. (2007), *Metoder för risk- och sårbarhetsanalys från ett systemperspektiv*, LUCRAM, Lunds universitet, Lund.

Kaplan, S. & Garrick, B. J. (1981), On the quantitative definition of risk, *Risk Analysis*, Vol. 1, No. 1, s. 11-27.

Kontakt

För mer information kontakta oss på följande e-postadresser eller besök FRIVA:s hemsida.

Henrik Johansson
Henrik.johansson@brand.lth.se

Henrik Jönsson
Henrik.jonsson@brand.lth.se

FRIVA
http://www.lucram.friva.lu.se

FRIVA

Tankar om krishanteringsövningar

Författare: Jonas Borell, Kerstin Eriksson, Jerry Nilsson

Inledning

Denna skrift är ett av flera informationsblad som redovisar sammanfattade erfarenheter och synpunkter från ramforskningsprogrammet FRIVA (Framework Programme for Risk and Vulnerability Analysis), vilket finansierats av Krisberedskapsmyndigheten under perioden mars 2004 till mars 2007. Informationsbladen skall kunna användas som utgångspunkter för praktiskt arbete när det gäller hantering av risker, sårbarheter, hot, kriser och katastrofer som medför eller kan medföra allvarliga samhälleliga konsekvenser.

Bakgrund

Att genomföra övningsverksamhet, praktiskt inriktad eller i seminarieform, framhävs ofta som ett viktigt verktyg för att undersöka eller öka krishanteringsförmågan i samhället. Övningar involverar ofta många deltagare och för att nå goda resultat krävs genomtänkt planering. Att involvera många deltagare tar både tid och pengar från verksamheten. Därför är det viktigt att man noga tar till vara övningars resultat.

Vår erfarenhet har visat att organisationer ofta missar chansen att dra riktigt stor nytta av övningar som genomförs. Det kan bero på hur man ser på och därmed planerar, genomför och efterarbetar övningar. Ett exempel kan vara att man vid övningar fokuserar specifika skeenden, och inte aktivt letar efter bakomliggande principer.

Syfte

Syftet med denna skrift är att ge några tips och idéer kring vad man kan tänka på när man arbetar med övningar, speciellt ur ett perspektiv där inte bara det skarpa övningstillfället står i centrum. Texten är tänkt att kunna användas av personer som arbetar med övningsverksamhet inom krishanteringsområdet på olika nivåer i samhället. Materialet kommer ur författarnas erfarenheter av olika övningsverksamheter och från litteraturen.

Övningar

Vi har märkt att övningar ibland skulle kunna betraktas i ett vidare sammanhang än vad som görs. Många gånger problematiseras inte övningar och dess syften i förhållande till övriga aktiviteter inom krishanteringssystemet. Vi tror att övningar bör ses i ett större sammanhang, t ex som en väl integrerad del inom en organisations övergripande process för förbättring av krishanteringsförmågan. Hur förhåller sig exempelvis övningen till organisationens arbete med risk- och sårbarhetsanalyser? Hur relaterar den till andra kompetensskapande aktiviteter, t ex utbildningar?

Utsträckning i tiden

Övningar betraktas ofta som en tidsmässigt starkt avgränsad aktivitet där man fokuserar det skarpa tillfälle då deltagarna ”testas”. Förberedelser inför en övning och uppföljning/återkoppling ses ofta som separata moment. Vi vill förorda att man betraktar en övning som något som har en längre utsträckning i tiden än bara utförandet av ”den skarpa fasen”. Vi föreslår att man betraktar faserna före och efter som en del i själva övningen. Ett sådant betraktelsesätt kan dels ge bättre förutsättningar för en processledare[2] att fundera kring syfte och ändamål med övningen, dels ge goda möjligheter för de personer som övas att förstå varför de övas. Ibland är det oklart var gränsen går mot andra aktiviteter och processer – det går inte att säga generellt utan måste (och bör) bearbetas i varje enskilt fall. Varifrån hämtas underlag till övningens innehåll? Vilka aktiviteter och processer ska övningens resultat påverka?

Perspektiv på övningsverksamhet

Övningar kan ses både ur ett organisationsperspektiv och ur ett individperspektiv. Ur ett organisationsperspektiv kan man t ex intressera sig för den process inom vilken en övning skall genomföras eller vilka syften och strukturer organisationen kopplar till en övning. Ur ett individperspektiv är exempelvis kompetensutveckling centralt (erfarenheter ger kunskaper och färdigheter).

[2] Övningar organiseras ofta av individer kallade *processledare.*

Många viktiga aspekter av övningsverksamhet berör samspelet mellan de två nivåerna. Vid genomförandet av en övning skapas och stärks t ex relationer mellan individer. Det kan ses som att ett nätverk utvecklas. För organisationens räkning kan detta nätverks utveckling medföra stärkt krishanteringsförmåga. Ett exempel på en praktisk fråga en processledare kan ställa sig inför en övning är för vilka krishanteringsfunktioner man vill eller behöver utveckla ett starkare personnätverk.

Individers lärande

Ett sätt att betrakta lärande handlar om att se det i relation till förståelse. Om lärande är ett mål med en övning kan man fråga sig vilken förståelse de olika deltagarna tillägnar sig. För att en processledare skall kunna utnyttja en sådan frågeställning bör denne i sin tur förstå att personer lär sig och förstår intryck utifrån den situation de befinner sig i. Sett till praktikerperspektivet handlar detta till stor del om yrkesrollen. En sjuksköterska kommer troligen att ”se” och ”känna” andra saker än en enhetschef gör. Det är viktigt att en processledare ser övningsdeltagarna som unika individer som kommer att förstå övningen utifrån den kontext de rör sig i. Därmed kan processledaren förbereda och ta tillvara övningsresultat på ett mer effektivt sätt. Hur ser man t ex till att alla deltagarna får ut sin del av pusslet av övningen? Vilka olika uppföljande åtgärder krävs för att stämma av vilken kunskap och förståelse som har gett avtryck hos olika övningsdeltagare?

En ständig fråga är den om hur träning i en övningssituation kan ge förmåga att faktiskt hantera en annan, praktisk situation. Det är ju aldrig *precis* de saker som övats som sedan ska göras i praktiken. Denna fråga kan uttryckas annorlunda i termer av validitet – Handlar övningens resultat om det som man avsåg att övningen skulle beröra?

Övningens olika faser

Nedan presenteras tips och idéer över saker man kan tänka på angående krishanteringsövningar. I framställningen indelas övningen i tre faser: *upptakt*, *”den skarpa delen”* och *efterarbete*.

Fas 1 – Upptakt

- Övningar kan vara dyra att genomföra. Därför bör man före en övnings genomförande försöka finna och åtgärda de brister som kan hanteras utan övning. Då slipper man ”slösa” dyrbar övning på trivialiteter.

- Hur ser organisationens övergripande process för förbättrad krishanteringsförmåga ut? Vilken eller vilka delar av denna process berör den aktuella övningen?

- Vad är syftet med övningen på individnivå respektive organisationsnivå? Kan man klart kommunicera syftet med övningen för varje deltagare? För organisationen som helhet? För sig själv (processledaren)?

- Vad är målet med övningen på organisationsnivå? Skiljer sig officiella och inofficiella mål med övningen?

- Vilka är målen med övningen på individnivå? Har processledaren eller andra deltagare några egna mål? Hur relaterar de till organisationens mål med övningen?

- Vad blev resultatet från den senaste övningen? Vilka lärdomar kan dras av den? Vad kan man ta med sig från den till nästa? Vad har samtal med de involverade gett?

- Kan man definiera vad som är en lyckad övning? Hur kan man se till så att övningen blir lyckad? Ett övergripande kriterium för lyckad övning skulle kunna vara att alla ser övningen som givande och att deltagarna bättre förstår sina egna roller i krishanteringsarbetet.

- Det är självfallet mycket viktigt att i förväg noga begrunda vilka som ska övas. Hur vet man i förväg vilka som kan tänkas behöva agera i en kris?

- För mycket övning kan ge en trötthet i organisationen. Detta kan eventuellt kringgås genom att man ändrar formerna för övningen. Vad kan man göra för att stärka de involverade personernas motivation? Är det dags att dela ut någon form av godis?

Fas 2 – Den ”skarpa delen” av övningen

- Övningar kan vara dyra att genomföra. Därför bör man anstränga sig för att genomföra övningar så seriöst som möjligt

- Hur realistisk ska övningen vara? Det påverkar i hög grad hur ”den skarpa delen” arrangeras, vilket i sin tur ger mycket olika förutsättningar för lärandet. Detta bestämmer t ex övningens tempo, förekomst av pauser och tid för reflektion under pågående övning.

- Ska man ha tillgång till mat och dryck? Avvägningen gäller bibringande av erfarenhet av

svåra, realistiska omständigheter kontra god förmåga för individuellt lärande.

- Hur se till så att deltagarna känner av övningens hetta men samtidigt inte sätts på pottkanten?

Fas 3 – Efterarbete

Övningen är inte slut när den ”skarpa fasen” är över. Mycket återstår – det är först nu de värdefullaste delarna kommer.

- Övningar kan vara dyra att genomföra. Därför är det viktigt att man formar en genomtänkt process för efterarbetet, och funderar över hur denna process passar ihop med den överordnade processen för förbättrad krishanteringsförmåga i organisationen.

- Vilka slags aktiviteter ska ingå i efterarbetet? Hur svarar de mot de syften och mål man formulerat för övningen? Ska man t ex arrangera seminarier där man diskuterar och dokumenterar hur den ”spelade” hanteringen föll ut? Arrangera gärna diskussioner där individernas intryck kompletterar och bryts mot varandra.

- Vilka individer bär på värdefull information efter övningen? Det kan även vara andra än de formella övningsdeltagarna. Försök att hitta så många informanter som möjligt inom utvärderingsarbetet!

- Ska information hämtas in från individer var för sig, eller gruppvis? Vilka för- och nackdelar har respektive form? Det kan t ex hända att man inte vill berätta vissa saker om man inte är anonym. Samtidigt innebär gruppsamtal att man lär av varandras erfarenheter.

- Se till att alla inblandade, aktiva övande såväl som motspelare, funktionärer och observatörer, i direkt samband med övningens ”skarpa del” reflekterar och dokumenterar sina reflektioner. Förbered gärna frågor och eventuella formulär.

- Vilka andra organisatoriska enheter eller instanser och vilka individer bör få del av resultat från efterarbetsprocessen? Vad bör de få del av? Hur? För att svara på detta bör man gå tillbaka till de syften och mål med övningen som formulerats. Har kanske nya syften uppdagats?

- Hur dokumenteras och sprids resultatet inom organisationen? Det viktiga är att man verkligen omsätter betydelsefulla fynd. Hur det ska gå till beror på organisationens övergripande process för förbättring av krishanteringsförmågan. Ska information flyttas från övningsprocessen till någon annan utvecklingsprocess, t ex utbildningsverksamhet? Kan man koppla övningen och dess fokus nära vardagen? Kan man koppla ihop lärande från övningen till de ordinarie beslutsprocesserna inom organisationen?

De olika fasernas samverkan

Anledningen till övningen ska forma *vad* som sker och *hur* det sker under övningens ”skarpa fas”. Detsamma gäller för hur resultaten är tänkta att omsättas. Vad som dokumenteras, lärs och leder till åtgärder ska vara i linje med övningens syfte. För att åstadkomma detta kan det krävas att mer än en person funderar över och håller i övningen. Det är tillrådligt att föra en diskussion mellan några personer som kan hjälpas åt med att se behoven och att åstadkomma det önskvärda resultatet.

Litteraturtips

Deverell, Edward och Grönvall, Jesper (kommande). *Utvärderingshandbok– en praktisk guide för utvärdering av stabs- och beslutsövningar*

KBM (2006). *Kommunernas övningsverksamhet – Tre enkla sätt att öva kommunledning och förvaltningar i krishantering*, Krisberedskapsmyndigheten, Stockholm.

KBM (2006). *Så vill vi utveckla övningsverksamheten – En strategi för utveckling av generell krishanteringsförmåga i samhället*, Krisberedskapsmyndigheten, Stockholm

Kontakt

För mer information kontakta oss på följande e-postadresser eller besök FRIVA:s hemsida.

Jonas Borell
Jonas.borell@design.lth.se

Kerstin Eriksson
Kerstin.eriksson@brand.lth.se

Jerry Nilsson
Jerry.nilsson@brand.lth.se

FRIVA
http://www.lucram.friva.lu.se

FRIVA

Belastningsreglering av webbserver för säker kriskommunikation

Författare: Mikael Andersson, Martin Höst

Inledning

Denna skrift är ett av flera informationsblad som redovisar sammanfattade erfarenheter och synpunkter från ramforskningsprogrammet FRIVA (Framework Programme for Risk and Vulnerability Analysis), vilket finansierats av Krisberedskapsmyndigheten under perioden mars 2004 till mars 2007. Informationsbladen skall kunna användas som utgångspunkter för praktiskt arbete när det gäller hantering av risker, sårbarheter, hot, kriser och katastrofer som medför eller kan medföra allvarliga samhälleliga konsekvenser.

En viktig anledning till att informationstjänster på nätet blir överbelastade är att det har inträffat någon typ av kris i samhället. Detta gör att allmänheten söker efter information om krisen till exempel hos tidningars och myndigheters webbsidor. Det finns en risk att om en webbserver blir överbelastad så får ingen besökare någon information, vilket ger ett behov av metoder för att hantera överlasten. Målet med denna instruktion är att diskutera problemet och ge exempel på tillfällen då kriser har orsakat brister i kriskommunikationen i samhället. Vidare ger vi en översikt av de metoder man kan använda sig av för att angripa problemet. En gemensam nämnare för metoderna är belastningsreglering, dvs. metoder för att begränsa belastningen på en webbserver, som till exempel ankomstkontroll, innehållsanpassning, lastbalansering och schemaläggning.

Instruktionen fokuserar på en av metoderna, innehållsanpassning och visar hur den kan användas praktiskt i en webbserver.

Målgruppen som den här texten är anpassad för är systemarkitekter och IT-ansvariga vid myndigheter, kommuner och övrigt berörda instanser. Vi förutsätter att man är bekant med webbservern Apache eftersom texten inte går igenom hur man konfigurerar den.

Bakgrund

Den tilltagande popularitet hos Internet har bidragit till ökade krav på bandbredd och prestanda på Internet. Både bandbredd och prestanda har ökat, men det räcker inte alltid till. Istället för att vara snabbt och användbart, är Internet många gånger tidskrävande. Långa svarstider på Internet behöver inte nödvändigtvis bero på för låg bandbredd eller för långsamma klienter, istället är flaskhalsen ofta serversystemen. Det finns många exempel då webbservrar har överbelastats och lämnat besökarna utan betjäning. Om en webbserver överbelastas, ökar svarstiderna från den, vilket gör att man riskerar att besökarna väljer andra alternativ på Internet, till exempel genom att gå till en annan webbshop eller gå till en annan nyhetssajt. Situationer då dessa problem uppstår är till exempel vid sportturneringar eller politiska val. Webbshoppar kan bli utsatta för kraftig trafik vid reatider på nätet, banker vid lönedagar, vanliga företag när de presenterar nya produkter etc.

Mer allvarliga situationer uppstår vid kriser. En kris genererar ofta ett stort intressse, vilket gör att nyhetssajter blir kraftigt belastade. Även myndigheters, kommuners och andras hemsidor riskerar överbelastning under en kris. Sedan 11:e septemberattacken i New York 2001 har människors medvetenhet om kriser ökat. Inte bara terrorattacken i New York, utan även tsunamin 2004, bombningarna i Londons tunnelbanesystem 2005 har ökat medvetandet om att vi måste vara väl förberedda i en kris.

Ett sätt att förbereda sajter på Internet för kriser är att införa belastningsreglering för dem. Det räcker nämligen inte med att dimensionera en tillräckligt stor kapacitet för alla tänkbara krissituationer, då detta (om möjligt) skulle bli alltför kostsamt. Inom telekommunikationsvärlden har man sedan länge varit medveten om problemet och därför finns det gott om metoder att utgå ifrån. Denna instruktion diskuterar först kort vilka olika sorters metoder som är aktuella, varefter två metoder gås igenom mer i detalj. Sist i texten ges råd om hur man kan få reda på mer om man är intresserad av ämnet.

Belastningsreglering

En mekanism för belastningsreglering är konstruerad för ett system som riskerar att bli överbelastat.

Termen överbelastning är inte entydigt definierad i litteraturen. Ibland betyder det att svarstiderna för ett system är för långa, eller att systemet har kraschat, men det kan också betyda att processorutnyttjningen är nära 100 procent eller att en annan del av systemet är överbelastat, till exempel hårddisken eller nätverkskortet. Emellertid betyder överbelastning generellt sett att ett system, eller en del av ett system, är utsatt för en belastning som är större än systemet eller delsystemet är konstruerat för.

Det finns flera sätt att hantera överbelastning. Fyra vanliga typer av belastningsreglering är beskrivna nedan. Det är inte nödvändigt att använda sig av endast en av de fyra typerna, tvärtom är det vanligt med en kombination av dessa.

Ankomstkontroll (Admission control)

Ankomstkontroll betyder att man begränsar tillträdet till systemet, till exempel genom att endast tillåta 100 samtidiga besökare på en hemsida. De besökare som därmed inte får plats i den tillåtna andelen avvisas från systemet. Det är viktigt att besökaren informeras om att hon har blivit avvisad och anledningen till detta, för att undvika dålig publicitet och potentiella försök att återbesöka systemet.

Innehållsanpassning (Content adaptation)

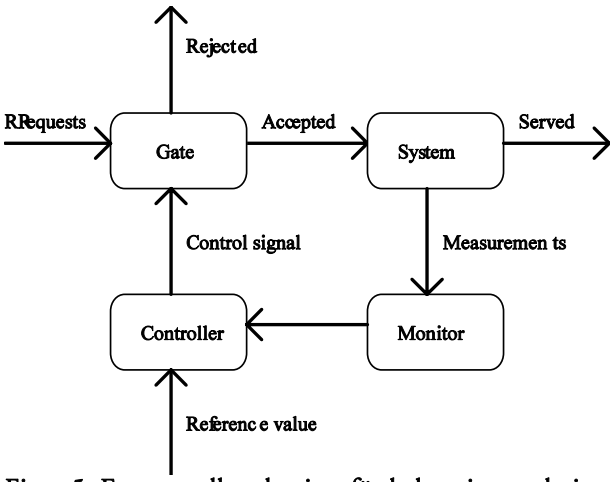
Innehållsanpassning betyder att man, istället för att avvisa besökare till systemet, anpassar den tjänst som besökaren får ta del av. Om belastningen är hög på systemet kommer innehållsanpassningen att se till att varje besökare får en något sämre tjänst. I gengäld kan alla besökare få åtminstone någon tjänst av systemet. Det finns många sätt att konstruera en sådan mekanism, i avsnittet *"Innehållsanpassning i praktiken"* nedan gås ett sådant sätt igenom.

Lastbalansering (Load balancing)

Egentligen är lastbalansering inget sätt i sig att hantera överbelastning. Lastbalansering går ut på att systemet är uppdelat i ett antal identiska delsystem. Lastbalanseringen gör så att varje delsystem får en lagom stor andel av besökarna. Detta gör att alla delsystem blir ungefär lika mycket belastade. Lastbalansering kan med fördel kombineras med någon av de ovanstående teknikerna, och gås inte igenom i denna text.

Schemaläggning (Scheduling)

Schemaläggning går ut på att betjäningen av de för tillfället aktuella besökarna schemaläggs på ett sådant sätt att till exempel den genomsnittsliga betjänings-tiden blir så kort som möjligt, alternativt att de med minst betjäningsbehov blir behandlade först. Vilket sätt man vill schemalägga betjäningen på beror på situationen. Schemaläggning gås inte igenom i denna text.



Figur 5. En generell mekanism för belastningsreglering

En generell modell

För att kunna beskriva en mekanism för belastningsreglering utgår vi ifrån en generell modell av en sådan mekanism. Figur 1 visar ett system som är kopplat till en belastningsreglering bestående av tre delar, Gate, Controller samt Monitor. I korthet fungerar de olika delarna enligt nedan:

System. System representerar systemet som kan bli överbelastat, till exempel en webbserver, men skulle även teoretiskt sett kunna vara en databasserver, en ftpserver eller något annat liknande system.

Gate. Gatedelen är den del som avvisar eller släpper in en besökare till systemet. Delen fungerar på olika sätt beroende på vilken sorts belastningsreglering det handlar om.

Controller. För att Gatedelen ovan ska kunna veta hur många besökare den kan släppa in, eller vilken kvalitet den ska leverera till besökarna, måste den ha en kontrollsignal som reglerar in- och utflödet till systemet. Controllerdelen är den del av systemet som förser Gatedelen med detta. Controllerdelen kan fungera på olika sätt beroende på belastningsreglering

Monitor. Eftersom Controllerdelen tar beslut om hur mycket kraft som ska fördelas av Gatedelen, måste den ha data att utgå ifrån. Monitordelen är den del av mekanismen som hela tiden övervakar systemet ifråga. Regelbundna mätningar görs, t ex på process-orutnyttjande eller bandbredds-utnyttjande, som skickas till Controllern.

Apache och moduler

Apache är den för närvarande mest använda webbservern i världen. Cirka två tredjedelar av

världens webbservrar kör någon version av Apache enligt statistiksajten netcraft.org. Den mekanism för belastningsreglering som beskrivs nedan är tänkta att implementeras som tillägg till just Apache. Förutom att Apache är gratis att använda är även dess arkitektur attraktiv. Mjukvaran är arrangerad i en *kerneldel* och därtill hörande tilläggspaket, så kallade *moduler*. Det gör att vem som helst kan ändra i programkoden och på så sätt skräddarsy sin egen webbserver.

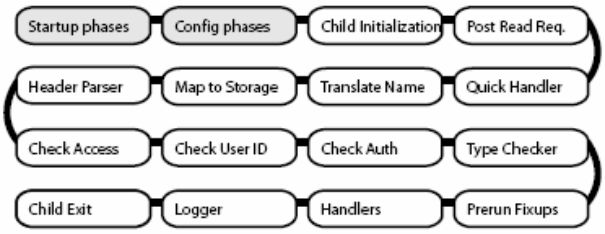
Kerneldelen är ansvarig för att öppna upp inkommande TCP-sessioner, hantera statiska filer och skicka tillbaka resultat. Om något annat än en statisk fil ska hanteras, tar en av de tillhörande modulerna över. En ny modul kan programmeras att hantera en viss typ av förfrågningar, eller alla förfrågningar, genom att den kopplas in i kerneldelen med så kallade *hooks*. En hook är en väl definierad plats i exekveringen av en förfrågan där en modul kan registrera sig. I Apache går varje förfrågan om en hemsida igenom en rad faser, vari olika delar av bearbetningen av förfrågan görs. Exempel på sådana faser är till exempel Child Initialization, Post Read Request, Handlers och Logger. Figur 6 visar några av de faser som finns i Apache. Apache är alltså väl lämpat för att utöka med belastningsregleringsmekanismer. Nedan följer ett exempel på hur man kan använda sig av Apache för att implementera sådana.

Innehållsanpassning i praktiken

Vi har gjort en testimplementation av innehållsanpassning för Apache. I det här avsnittet går vi igenom hur testimplementationen gjordes och vad man bör tänka på.

Syfte

Enligt beskrivningen ovan av innehållsanpassningen är idén att istället för att avvisa vissa besökare kan man sänka betjäningsgraden för alla. I det här exemplet sänker vi betjäningsgraden genom att reducera hemsidornas storlek. Med storlek menas antalet bytes som en komplett hemsida utgör, inräknat stilmallar, bilder och andra tillhörande filer. För att åstadkomma detta krävs att sajten som ligger på webbservern finns i flera olika versioner, där varje fil är olika stor i de olika versionerna. Uppgiften för belastningsregleringen är sedan att välja den mest lämpade versionen av filerna för stunden åt besökarna.



Figur 6. Faserna i bearbetningen av en förfrågan i Apache

Optimeringsrutin

Enkelt uttryckt, vår grundtanke är att det är bättre att ge två filer á 10 kbytes till två besökare, än att ge en fil på 20 kbytes till en besökare. Ett begrepp vi har infört är *nytta.* Nytta är den förtjänst i någon mening det finns med att leverera en viss tjänst till en besökare. Närmare bestämt har vi utgått från att nyttan kan beskrivas med en logaritmfunktion, dvs att nyttan N är logaritmen av hemsidans storlek i bytes, S:

$$N = \log_2(S)$$

Denna definition av nytta stödjer grundtanken om att två små filer är bättre än en stor fil, eftersom att fler besökare får ta del av informationen, det vill säga, ett dokument blir inte dubbelt så bra om det är dubbelt så stort.

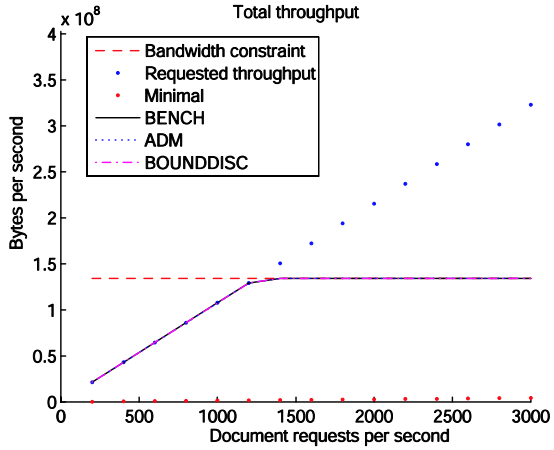
Hur ska man då veta vilka sidor som ska minskas i storlek, och vilka sidor man kan låta vara intakta? Målet med vår belastningsreglering är att försöka *maximera den totala nyttan i varje sekund* som webbservern levererar. Genom att lösa det matematiska optimeringsproblemet kan man få fram en lista över vilka filversioner som är mest lämpliga för stunden. Notera att alla filer inte behöver vara representerade i alla versioner. Listan med tillgängliga versioner och vilka versioner som är optimala för tillfället benämns *optimumtabellen*. Figur 7 visar ett exempel på en sådan tabell. När optimumtabellen därefter används för att välja ut vilka versioner som ska returneras till besökarna blir resultatet att utnyttjandet av bandbredden är konstant, enligt den nivå man bestämt, förutsatt att webbservern är överbelastad.

Till exempel kan man välja att 80 procent av bandbredden får utnyttjas av webbservern. I Figur 8 visas ett exempel där bandbredden utnyttjas på en konstant nivå efter den punkt där webbservern blir överbelastad. Figur 9 visar för samma situation vad som händer med den totala nyttan per sekund. Istället för att plana ut och vara konstant efter den punkt där webbservern blir överbelastad som utnyttjandet av bandbredden gör, fortsätter den totala nyttan att öka, i stort sett i samma grad som den hade gjort ifall webbservern inte hade varit överbelastad.

Document	Available versions				
Doc1.html	1	2	**3**	4	5
Doc2.html	1	2	3	4	**5**
Doc3.html	1		**3**		5
Doc4.html	1		3		**5**
Doc5.html	**1**				

Optimal version =

Figur 7. Exempel på en optimumtabell. Sajten har 5 dokument, där de två första finns representerade i alla fem versionerna, dokument 3 och 4 i tre versioner, samt det dokument 5 som bara finns i originalstorlek. Optimala versioner är inringade.

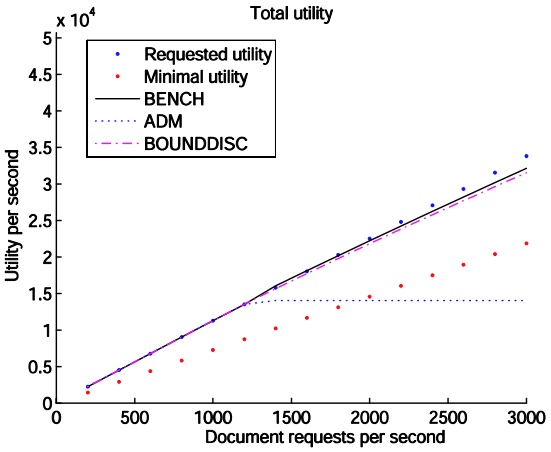


Figur 8. Linjen BOUNDDISC visar hur throughput hålls på en bestämd nivå i regleringen.

I ovanstående beskrivning av en generell mekanism för belastningsreglering beskrivs förutom själva webbservern tre delar, Monitor, Controller och Gate. Detta upplägg passar väl in när man implementerar en innehållsanpassning i en webbserver. Det ingen klar uppdelning i koden, snarare handlar det om metoder eller filer som ansvarar för de olika delarnas ansvarsområden, emellertid fungerar uppdelningen bra för resonemangets skull.

Systemet

Standardinstallation av Apache 2.0 användes. Enligt beskrivningen av moduler och hooks tidigare skrevs en tilläggsmodul för att utföra belastningsreglering, med de tre delarna i. Två hookar användes, en som kopplades till fasen Handlers, samt en som kopplades så sent som möjligt i exekveringskedjan. Den första hooken användes för att omdirigera requests till optimal version och den andra hooken användes för att läsa av requesten när den var färdigbetjänad. Man kan då se hur stor datamängd som levererades, hur lång tid det tog etc. I stort sett går det även bra med tidigare versioner av Apache. Det som skiljer är sättet man registrerar en hook från sin egen modul, samt hur en modul definieras.



Figur 9. Linjen BOUNDDISC visar hur returnerade informationsnyttan praktiskt taget är lika med den informationsnytta som besökarna vill ha trots överbelastning.

Monitor

I det här fallet registrerar Monitor varenda förfrågan som betjänas. Antalet bytes som levereras lagras i en tabell, samt antalet förfrågningar till de olika hemsidorna. Monitor måste lagra tabellen i ett minnesutrymme som alla pågående förfrågnings-exekveringar kan ta del av. Författarna använde sig här av en tilläggsfunktion i Apache för delat minne. Monitordelen kopplades in med en hook i Logfasen i Apache.

Controller

Controller är den del som optimerar bandbredden och tar fram den optimumtabell som sedan används av Gatedelen. Optimumtabellen tas fram genom matematisk optimering, som beskrivs närmare i artikeln ” Content Adaptation Schemes for Web Servers in Crisis Situations”. Ett måste är att optimumtabellen hela tiden beräknas om, eftersom den bara är giltig för en viss trafiksituation. Istället för att räkna ut om trafiksituationen har förändrats, kan man i praktiken låta Controllerdelen optimera om tabellen med jämna intervall. Här anser vi att ett intervall om cirka 5 minuter är lämpligt, eftersom trafiken inte hinner ändra sig så mycket under den tiden. Att göra en optimering kan vara resurskrävande och även tidskrävande beroende på sajtens storlek eftersom problemet är svårare att lösa desto fler versioner och dokument som finns på sajten. Detta kan ställa till problem då belastnings-regleringen är som viktigast när webbservern redan är överbelastad. Man kan dock komma runt det problemet genom att lägga optimeringsarbetet på en extern server som har till uppgift att genomföra beräkningarna, alternativt att man har en samling föroptimerade lösningar som kan användas av Controllerdelen.

Gate

Gatedelen är inkopplade med en hook i Handlersfasen i Apache lämpligtvis. För Gatedelen handlar det om att ta reda på vilken fil som förfrågan avser. Därefter slås filen upp i optimumtabellen, varpå den optimala versionen av filen väljs ut och returneras till besökaren. Ett användbart sätt att returnera en viss sida istället för originalsidan är så kallade redirects i Apache. Man skriver då om den ursprungliga förfrågan till att gälla den optimala versionen av sidan istället.

Diskussion

Den här instruktionen har diskuterat hur man kan gå till väga då man vill implementera en belastningsreglering för en webbserver, närmare bestämt genom att anpassa innehållet som levereras då en besökare ansluter till en hemsida. Det man försöker göra är att optimera nyttan med de hemsidor man levererar till besökarna, genom att utnyttja bandbredden på bästa möjliga sätt. Genom att göra tillägg i en Apache-webbserver är det möjligt att implementera innehållsanpassning. Det räcker dock inte att enbart skriva en modul, eftersom lösningen kräver att hemsidorna finns tillgängliga i flera versioner. Då större sajter uppdaterar sitt innehåll ofta krävs någon form av automatiserad lösning för att generera de olika versionerna, till exempel genom att publiceringssystemen på respektive sajt modifieras. Även om det kan vara ett stort ingrepp i systemet finns det mycket att vinna på att införa belastningsreglering. I en krissituation är information den viktigaste variabeln för en webbserver. Så mycket information som möjligt måste levereras till så många som möjligt. I beskrivningen ovan visas exempel på de vinster som kan fås jämfört med andra lösningar i en krissituation.

Innehållsanpassning är den metod för belastningsreglering som valts i det här exemplet. Metoden passar bra när bandbredden är den begränsande faktorn i webbservern. Vi har även undersökt andra metoder, t ex ankomstkontroll. Ankomstkontrollen implementerade vi på ett liknande sätt som ovan, genom att skriva en modul för Apache. Genom ankomstkontrollen kunde vi då reglera processoranvändningen i webbservern. Hur man implementerar ett sådant system kan man läsa mer om i de artiklar som listas i litteraturtipsen.

Ett sätt att komma igång med arbetet att införa en automatisk belastningsreglering på sin sajt, är att man börjar med att skapa versioner av sina hemsidor. Grundkravet för att innehålls-anpassningen ovan ska fungera är att hemsidorna finns förberedda i ett antal versioner (minst två). Om man inför det kravet har man tagit ett steg i rätt riktning. Fördelen är att man manuellt kan gå över i ett ”krisläge” på webbservern, där endast små versioner av hemsidorna erbjuds, med lägre risk för överbelastning. Därefter kan man fundera på hur man ska införa innehållsanpassning på sin webbserver.

Litteraturtips

Denna text är baserad på forskning som utförts inom ramen för ramverksprogrammet FRIVA. På FRIVAs hemsida kan man läsa mer om forskningen och ladda hem publikationer. Det är även möjligt att ta del av viss programvara som utvecklats i forskningen. Speciellt rekommenderas nedanstående källor:

- Mikael Andersson, Martin Höst, Jianhua Cao, Christian Nyberg and Maria Kihl (2007), “Content Adaptation Schemes for Web Servers in Crisis Situations”
- Maria Kihl, Anders Robertsson, Mikael Andersson and Björn Wittenmark, (2007) “Control Theoretic Analysis of Admission Control Mechanisms for Web Server Systems“, *Artikel accepterad till World Wide Web Journal*.
- Ben Laurie, Peter Laurie (2003), ”Apache, The Definitive Guide” *O’Reilly*.
- Apaches hemsida (http://httpd.apache.org), samt Apaches utvecklarhemsida (http://httpd.apache.org/docs-2.0/developer).

Kontakt

För mer information kontakta oss på följande e-post-adresser eller besök FRIVA:s hemsida.

Mikael Andersson
mikael.andersson@telecom.lth.se

Martin Höst
martin.host@cs.lth.se

FRIVA
http://www.friva.lucram.lu.se

FRIVA

Erfarenheter av GIS i samband med Stormen Gudrun

Författare: Martin Önnerfors, Nicklas Guldåker och Tuija Nieminen Kristofersson

Inledning

Denna skrift är ett av flera informationsblad som redovisar sammanfattade erfarenheter och synpunkter från ramforskningsprogrammet FRIVA (Framework Programme for Risk and Vulnerability Analysis), vilket finansierats av Krisberedskapsmyndigheten under perioden mars 2004 till mars 2007. Informationsbladen skall kunna användas som utgångspunkter för praktiskt arbete när det gäller hantering av risker, sårbarheter, hot, kriser och katastrofer som medför eller kan medföra allvarliga samhälleliga konsekvenser.

Bakgrund

Detta informationsblad syftar till att förmedla resultat som kan vara av betydelse för kommuners och andra aktörers användning av GIS i kris. Innehållet bygger på intervjuer med tjänstemän från tre kommuner och en länsstyrelse som har erfarenheter av tillämpningar av GIS i samband med stormen Gudrun. Det är således en sammanfattning av den kunskap som redan finns hos många kommuner och som är värd att spridas vidare.

GIS-användning i kommunal verksamhet

Den kommunala GIS-användningen i samband med krissituationer bygger till stor del på hur GIS är integrerat kommuners vardagliga verksamhet. Ett resultat visar att kommuner med god vardaglig användning av GIS i olika verksamheter kan tillgodogöra sig systemen på ett bättre sätt i kris. De tre kommunerna som undersökts benämns här A, B och C. Förutsättningarna att tillgodogöra sig GIS i samband med krissituationer skiljer sig åt mellan kommunerna.

Kommun A har 50 000 invånare och tillhör kommunkategorin *övriga kommuner över 25 000 invånare*.[3] Kommunen har länge satsat på att införa och sprida GIS i sin verksamhet och ses som framstående när det gäller GIS-användning och kunnande. Kommunens personal hämtar och lagrar bland annat information centralt i en databas. Databasen uppdateras kontinuerligt både utifrån och inifrån kommunen, t.ex. från fastighetsregistret och SCB. Personalen från olika förvaltningar har olika behörighet och kan komma åt databasen direkt via det interna nätverket. Spridningen av GIS-användning i verksamheten har gjort att kommunen idag använder GIS vid t.ex. planering av skolskjutsar, bygglovshantering, planering av skolverksamhet och sjukvård. Enligt en tjänsteman i kommunen sparar det både tid och pengar genom snabbare handläggningar och ökad kvalitet. Sedan ett par år samverkar kommunen med två angränsande kommuner. Inom ramen för samarbetet har kommunerna bl.a. agerat som en kund i inköp av kartdata, drivit projekt tillsammans, samt lånat personal av varandra och på så vis fått en viss spridning av GIS-kompetens och effektiviserat flera verksamheter. I kommun A: s kommunledning finns ett medvetande kring GIS och dess potential. Detta har gjort att GIS-samordnare och andra tjänstemän kunnat utveckla och sprida GIS-användningen i kommunen.

Kommun B har 70 000 invånare och tillhör kategorin *Större städer*. I kommunen har GIS-verksamheten funnits länge, men man har inte aktivt spritt systemen och kunskapen inom kommunen. Efter krishanteringen i samband med stormen Gudrun uppmärksammades fördelarna och idag satsas det mer på att öka medvetenheten och kunskapen om GIS. GIS används redan idag med god framgång vid t.ex. planering av skolskjutsar. Man försöker även att involvera omsorgs- och kulturförvaltningen i GIS-satsningen.

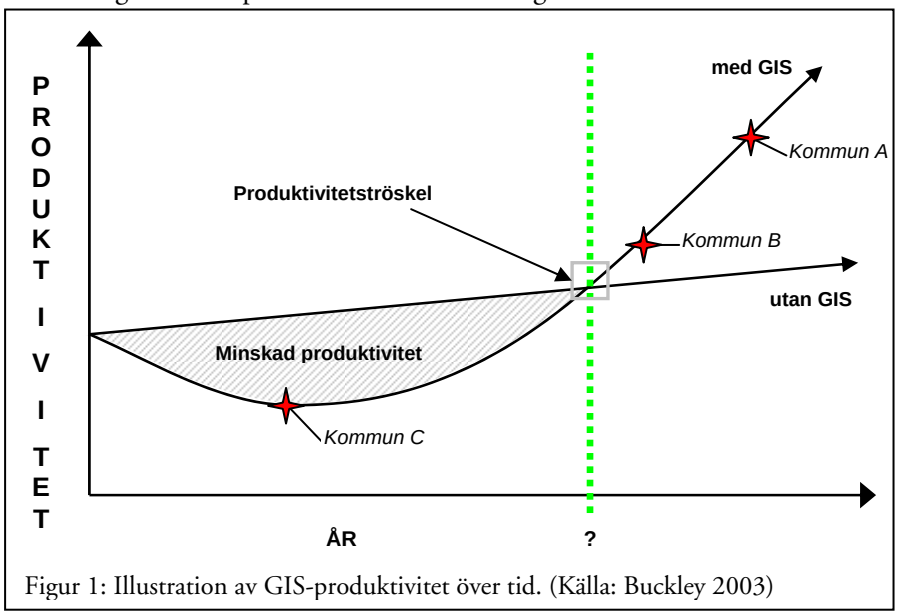
Kommun C har 10 000 invånare och tillhör kategorin *varuproducerande kommuner*. Kommunen har sedan länge ett GIS-system, men kommunens GIS-ansvarige har inte lyckats få gehör för sina förslag på vidare

[3] Kommunkategorierna följer Sveriges kommuner och landstings kommunindelningar (se vidare www.skl.se)

satsningar, varken hos kommunledningen eller i andra förvaltningar. Medvetenheten om vilken kapacitet som finns i systemen är i allmänhet låg inom kommunen. Den låga kunskapen och bristen på engagemang gör att införandet och spridningen av GIS står stilla.

Det finns således stora skillnader mellan de studerade kommunerna och hur de lyckats sprida GIS olika verksamheter. En kommun kan öka avkastningen från sin GIS-investering genom att försöka sprida GIS till andra förvaltningar och därmed få användning på många ställen i kommunen. När systemen väl är inköpta och personal har utbildats, är steget till att använda GIS i andra verksamheter ofta inte långt. I kommun A och kommun B påpekar tjänstemännen att det till en början gäller att få igång rätt ”tänk” i andra förvaltningar, så att de anställda där vet vad man kan göra med GIS. När systemen och kunskapen sedan införts i förvaltningarna kan användningen påbörjas. Det är viktigt att medarbetarna ser den direkta nyttoeffekten, t.ex. i form av sparad arbetstid, personalresurser m.m. En spridning av GIS kan öka produktiviteten i investeringen. En allmän modell för en organisations samlade produktivitet av till följd av en investering (kunskap, kompetens, implementeringsstrategier, prioritet och status av data) i GIS åskådliggörs i figur 1.

Den gröna streckade linjen i figur 1 illustrerar den tidpunkt då produktiviteten i en organisation börjar överstiga en organisation som inte satsat på GIS. GIS-investeringen leder på sikt till effektiviseringar och resursbesparingar. Ett långsiktigt och kontinuerligt engagemang krävs dock för att nå tröskeln för en förbättrad produktivitet. Hur lång tid detta tar varierar. I figuren har de tre kommunerna inplacerats efter hur långt de kommit i processen när det gäller nytta av GIS-användning. Det är viktigt att poängtera att illustrationen inte är en heltäckande bedömning av kommunerna, utan mer en fingervisning om hur olika de lyckas införa och dra nytta av GIS. I figuren hamnar kommun A långt över tröskeln för förbättrad produktivitet, eftersom de har en stor spridning av GIS i olika förvaltningar, ett bra samarbete med andra kommuner och har satsat långsiktigt. Kommun B hamnar en bit ovanför tröskeln, eftersom kommunen fått igång en process, skapat ett medvetande hos kommunledningen och i olika verksamheter, samt visat sig villig att satsa på GIS i framtiden. Kommun C hamnar under tröskeln för positiv produktivitet, eftersom GIS finns men endast används i begränsad utsträckning, och det finns ett motstånd mot spridande av GIS i såväl kommunledning och förvaltning. Kommun C har inte lyckats få en långsiktighet i sin investering, vilket har lett till att den avstannat.



Figur 1: Illustration av GIS-produktivitet över tid. (Källa: Buckley 2003)

De viktigaste erfarenheterna från denna studie angående *införandet* av GIS är att:

– *kunskap om* GIS måste finnas på alla nivåer i kommunen, från de tjänstemän som skall använda det upp till kommunledningen. Gehör från kommunledningen har visat sig särskilt viktigt när det gäller att få pengar för de investeringar som krävs, t.ex. inköp av geografisk information och fortbildning av personal.

– *långsiktiga investeringar* i frågor som gäller GIS är nödvändiga för att få produktivitet i sin GIS-verksamhet. Höga investeringskostnader är i inledningen normalt eftersom det tar tid att arbeta in och få rutin på sin GIS-verksamhet. Att ha uppdaterad statistik och kartdata är avgörande för att göra korrekta och aktuella analyser och införskaffande av detta är löpande kostnader.

– *samarbete mellan kommuner* kan öka kompetensen och minska kostnaderna eftersom de kan delas upp mellan fler parter. Detta är speciellt lönsamt för mindre kommuner, som får tillgång till en teknologi och kompetens som är svår att utveckla med redan begränsade resurser.

Hur använde man GIS i samband med stormen Gudrun?

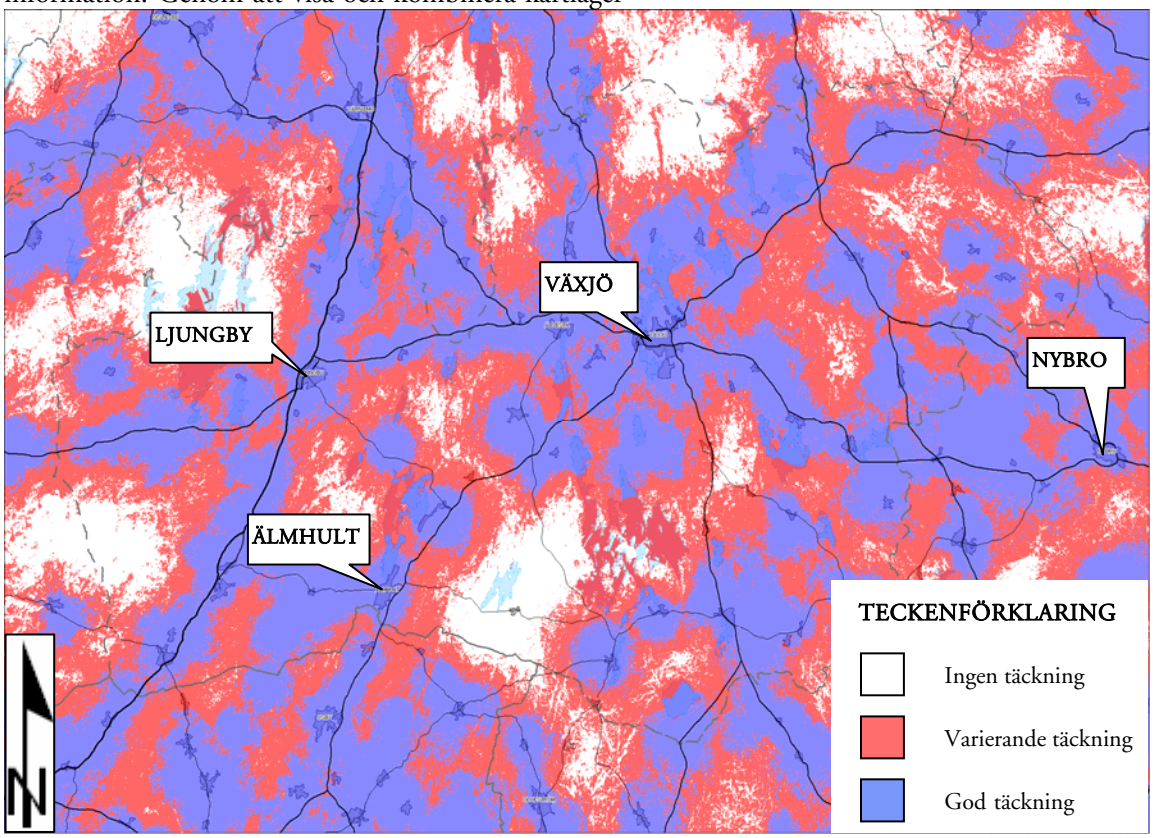
Precis som många extraordinära händelser, kom stormen Gudrun snabbt och oväntat och krävde snabba insatser av de kommuner och länsstyrelser som drabbades. Resultaten visar att det var de

organisationer som arbetat mest med GIS i vardagliga sammanhang som hade lättast att använda teknologin även i kris. Så här såg GIS-användningen ut i de undersökta organisationerna:

– kommun A använde sig av GIS på många olika sätt i samband med krishanteringen av stormen Gudrun. En viktig och välanvänd funktion var att använda GIS och kommuninvånarregistret för att leta upp äldre, strömlösa och potentiellt utsatta individer. Resultatet av denna användning kunde sedan visas och skrivas ut på kartor, tillsammans med vilka vägar som var framkomliga, och användas av bland annat frivilliga resursgrupper i fält för att söka upp och hjälpa invånare. Aktuella kartor med krisinformation visades under krisledningsmöten, vilket underlättade och påskyndade beslutsprocessen. Kartorna visades i ett GIS-program kopplat till en projektor, vilket gav möjlighet till omedelbara justeringar och växlingar mellan olika resultat och analyser av geografisk information. Genom att visa och kombinera kartlager med farbara vägar, strömlöshet, invånare, information från fältet, med mera, skapades en översikt, vilket effektiviserade ledningsgruppernas arbeten.

– kommun *B* använde sig inte av GIS under krishanteringen i samband med stormen. Under arbetet fick dock krisledningen klart för sig att man hade haft stor nytta av GIS för att t.ex. kunna sammanställa och visa all information som kom in från fältet angående farbara vägar och strömlöshet. Detta har lett till att GIS idag används mer än tidigare. Ett antal övningar med GIS har också genomförts i syfte att bland annat öka effektiviteten i krisledningsarbetet. Kommun B har även etablerat en webbaserad informationsportal, som skall göra krisinformationen tillgänglig inom kommunen.

– kommun *C* använde sig av GIS vid ett tillfälle under krishanteringen av stormen Gudrun, då man letade upp och karterade äldre invånare i kommunen som inte var registrerade vårdtagare.



Figur 2: Karta över en mobiloperatörs täckning i Kronobergs län 17 januari, 2005

(Källa: Länsstyrelsen i Kronobergs län 2006).

I övrigt användes inte GIS, och kommunen har till synes inte heller vidtagit några åtgärder för att förbättra GIS-användningen, varken till vardags eller inför framtida krissituationer.

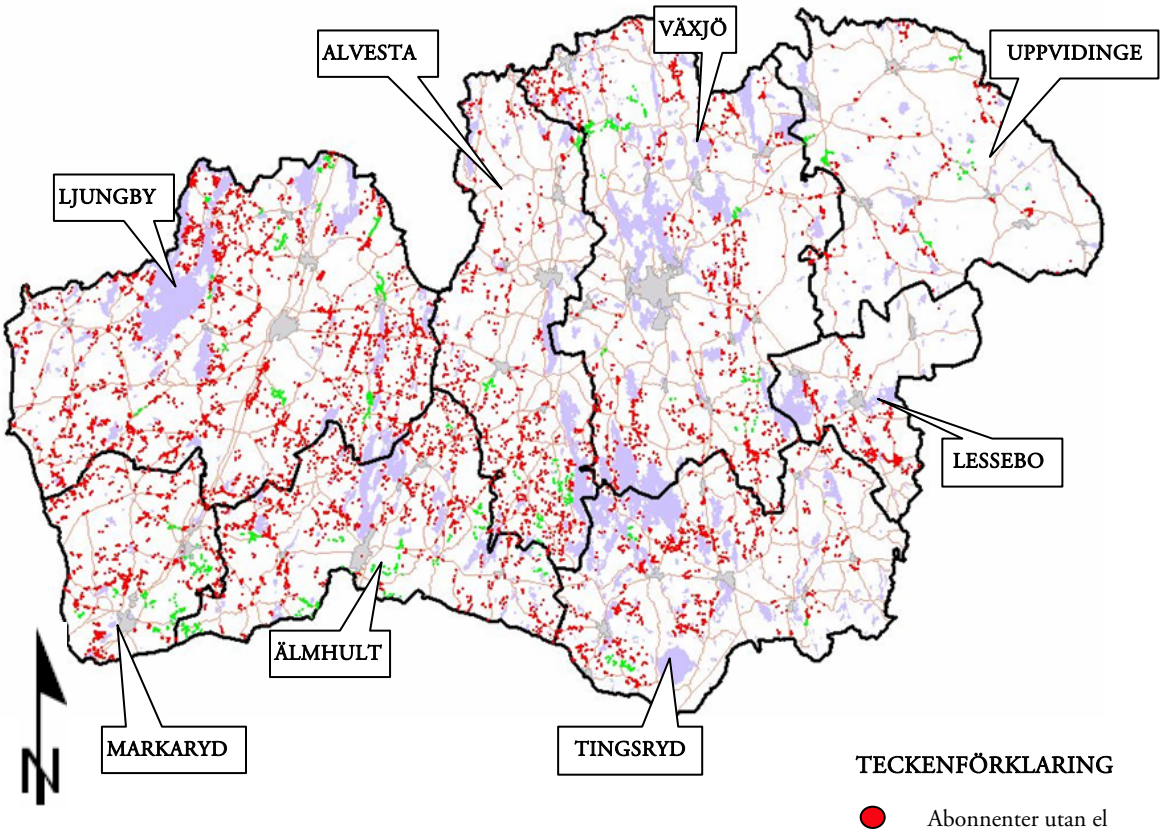
Länsstyrelsen hade en annorlunda roll i krishanteringsorganisationen jämfört med kommunerna, och använde sig därför främst av GIS för att visa krisinformation för ledningsgruppen (på samma vis som i kommun A ovan). Företrädare från länsstyrelsen berättar om aha-upplevelser i krisledningsstaben när man kombinerat och karterat olika sorters geografisk information, t.ex. kombinerades kartlager över det fasta och mobila telenätets täckningar. På så sätt kunde man se vilka områden som helt saknade täckning (de vita) och var det var mest lämpligt att lägga sina resurser på att återställa mobilnätet (se figur 2). I figur 3 ges ytterligare ett exempel på en betydelsefull karta. Kartor som den i figur 3 uppdaterades med dagliga el-prognoser från kraftbolagen, och gav länsstyrelsen i Kronoberg geografiskt underlag för var insatser och resurser skulle inriktas. Kommunnamnen i kartorna skall inte förknippas med ovan beskrivna kommuner A, B eller C.

Några strategier för GIS-användning

GIS är, under förutsättningar att förberedelserna och användandet sker på ett adekvat sätt, ett värdefullt hjälpmedel vid omfattande informationsbehandling. Med GIS-system och kunskap kan oöverskådlig information snabbt summeras upp, vilket underlättar beslutsprocesser i olika tidspressade krissituationer. Här är det vikigt att betona att systemen och kunskapen om dess användning inte kan ersätta lokal kunskap eller erfarenhet. Tillsammans med den lokalkunskap som anställda och invånare i kommunen innehar, kan GIS hjälpa till att minimera konsekvenser i form liv, skador, ekonomi, materiell osv. Ett antal strategier får här sammanfatta informationsbladet:

– ett GIS-system är en *långsiktig investering*, och det är därför viktigt att veta att en period med ökade kostnader är att vänta innan investeringen blir lönsam. En viktig strategi är att genomföra någon form av långsiktig kostnad-nytta-analys. Om man som kommun eller organisation saknar erfarenhet kan man snegla på andra kommuner med mer kunskap om vanliga felsteg och värdefulla tips som minskar risken för missuppfattningar och onödiga kostnader.

– *tillgång till uppdaterad information/data* om kommunen, t.ex. befolkning och infrastruktur, är A



Figur 3: Abonnenter utan el i Kronobergs län den 26 januari 2005 (Källa: Länsstyrelsen i Kronobergs län, 2006).

och O inom såväl GIS som krishantering. Viktigt att tänka på här är att viss data, t.ex. information om vårdtagare, är sekretessbelagd och kräver såväl etiska som regelmässiga överväganden och beslut innan den kan användas. Det är av vikt att se över lagstiftning, t.ex. information om sekretess för vårdtagare med mera. Ofta krockar möjligheterna till användning av sekretess- och integritetsskyddad information med vilka som är behöriga att hantera denna.

– *samarbete mellan kommuner* i GIS-frågor är lönsamt för alla inblandade parter, både i form av minskade utgifter, ökad kompetens och effektivitet. Det finns många kommuner som kan föregå med goda exempel på samarbetsavtal för geografisk information och data.

– GIS-system i krishantering används ibland för att *identifiera sårbara medborgare samt visa och underlätta tidspressade beslutsprocesser*. Dessa två funktioner är effektiva och bidrar till noggrannare krisarbete och säkrare beslut. Det är viktigt att i förebyggande träna på olika geografiska analyser. Det kan vara exempelvis att skapa buffertar kring olika områden och se vilka människor som eventuellt drabbas av giftutsläpp eller översvämningar. GIS-analyser är således användbara i kommunala såväl som regionala risk- och sårbarhetsanalyser.

– Ett sätt att hos *beslutsfattare öka medvetenheten om GIS möjligheter i krissituationer*, är att genomföra scenariobaserade krisövningar där GIS-expertis kan hjälpa till att hantera och summera upp stora mängder information på lättförståeliga kartor och tabeller.

Tips på vidare läsning

Buckley, D. J. (2003): *The GIS Primer. An introduction to Geographic Information Systems.* http://www.innovativegis.com/basis/primer/primer.html. 2007-03-28.

Guldåker, N. (2007 kommande): Stormen Gudrun och hushålls sårbarhet. Meddelande från Lunds Universitets geografiska institutioner, avhandlingar xxx.

Guldåker, N. & Nieminen Kristofersson, T. (2007): *Kommuners arbete och stöd till utsatta medborgare till följd av stormen Gudrun, flodvågskatastrofen och några andra större händelser.* FRIVA informationsblad. Lunds Universitet.

Nieminen Kristofersson, T. & Guldåker, N. (2007): *Social sårbarhet utifrån ett medborgarperspektiv.* FRIVA informationsblad. Lunds Universitet.

Önnerfors, M. (2006): *GIS i hanteringen av stormen Gudrun – en studie av tre kommuner och en länsstyrelse*. C-uppsats i kulturgeografi, Institutionen för kulturgeografi och ekonomisk geografi. Handledare: Tuija Nieminen Kristofersson och Nicklas Guldåker. Publikationen finns på att hämta från http://www.keg.lu.se/forsa

Kontakt

För mer information kontakta oss på följande e-post-adresser eller besök FRIVA:s hemsida.

Martin Önnerfors
Martin@onnerfors.se

Nicklas Guldåker
Nicklas.guldaker@keg.lu.se

Tuija Nieminen Kristofersson
Tuija.Nieminen@keg.lu.se

FRIVA
http://www.friva.lucram.lu.se

FRIVA

Kommuners arbete och stöd till utsatta medborgare till följd av stormen Gudrun, flodvågskatastrofen och några andra större händelser

Författare: Nicklas Guldåker, Tuija Nieminen Kristofersson

Inledning

Denna skrift är ett av flera informationsblad som redovisar sammanfattade erfarenheter och synpunkter från ramforskningsprogrammet FRIVA (Framework Programme for Risk and Vulnerability Analysis), vilket finansierats av Krisberedskapsmyndigheten under perioden mars 2004 till mars 2007. Informationsbladen skall kunna användas som utgångspunkter för praktiskt arbete när det gäller hantering av risker, sårbarheter, hot, kriser och katastrofer som medför eller kan medföra allvarliga samhälleliga konsekvenser.

Bakgrund

Detta informationsblad syftar till att förmedla resultat från flera undersökningar om kommuners och andra aktörers arbete och stöd till utsatta medborgare i samband med större kriser. Informationsbladet kan förhoppningsvis bidra med erfarenheter och idéer till kommuners arbeten med risk- och sårbarhetsanalyser, krisberedskaps- och säkerhetsplaner, övningar och annan typ av krishanteringsrelaterad verksamhet. Innehållet bygger på intervjuer med kommunala tjänstemän som arbetat aktivt med olika kriser och katastrofer från 1990 till 2006. Det är således en sammanfattning av den kunskap som redan finns hos många kommuner och som är värd att spridas vidare.

Uppfattning av och arbete med utsatta medborgare

Stormen Gudrun orsakade långvariga tele- och elavbrott, vilket var en stor påfrestning för kommuner i södra och mellersta Sverige. Undersökningarna visar att kommunala tjänstemän i många fall har en välgrundad uppfattning av vilka grupper som var utsatta (se vidare Guldåker 2007 kommande och Nieminen Kristofersson 2007 kommande). Framförallt omnämner de personer över 70 år, handikappade, sjuka och i viss mån barnfamiljer med små barn. Många skogsägare och hushåll med djurhushållning drabbades. De som redan hade någon form av hemvård lokaliserades relativt snabbt av bland annat socialtjänst, hemtjänst och hemsjukvård. Svårigheten var att snabbt få fram information om var andra utsatta befann sig, det vill säga de som inte får kontinuerlig vård eller omsorg men som av olika anledningar hade det svårt under och efter stormen. Kommunerna anser att sårbarheten hos många medborgare och hushåll påverkas av flera medverkande krafter, bland annat splittring av hushåll, situationsbundenheten, avsaknad av grannar och anhöriga, boendeform, fysisk isolering, brist på alternativa värmekällor, avsaknad av el, telekommunikationer och vatten samt el- och telesystemens avbrottstid. Man uppfattar att de medborgare som klarat sig bäst är de som har haft tillgång till alternativa uppvärmningsmöjligheter (kakelugnar, vedspisar, kaminer, vedeldade pannor med självcirkulationssystem med mera), egna brunnar samt i viss mån har haft god tillång till reservelkraftverk, gasolkök, stearinljus, ficklampor, pannlampor, motorsågar med mera.

Kommunernas krisledningsstaber använde sig av flera strategier för att identifiera och tillgodose vissa gruppers hjälpbehov. Bland annat användes lokala källor, information från Sydkraft/Telia, posten, olika informatörer som arbetade i fält, register och i varierad mån geografiska informationssystem (se vidare informationsbladet *Erfarenheter av GIS i samband med stormen Gudrun* 2007). Arbetet var i många fall långsamt och gav inledningsvis en osäker uppfattning av de utsattas situation. En följd av detta är att det finns ett behov att se över de rutiner som kan effektivisera och förbättra detta arbete. Vid händelser som liknar stormen Gudrun är det väsentligt att så tidigt som möjligt skaffa sig en enhetlig lägesbild. Omedelbara flyg- eller

helikopterinventeringar kan här ge värdefull information om drabbade områden.

Landsbygden var, tillskillnad från tätorterna, bra rustad för långvariga elavbrott till följd av tidigare vana med avbrott på el- och teleledningar. Handlingskraften på landsbygden var också i många fall effektivare och snabbare än hos kommunen eller andra aktörer. Detta märktes inte minst vid upprö jning av små och stora vägar. Förutom behjälpliga materiella resurser har samverkan i och mellan nätverk bidragit till att minska sårbarheten och öka handlingskraften.

Kommunerna utförde, oftast i samverkan med Sydkraft/Eon och räddningstjänsten, insatser för att på olika sätt stödja kommuninvånarna. Större reservelverk sattes vid skolor och äldreboende och andra prioriterade verksamheter och mindre elverk och kaminer distribuerades till privata hushåll. Värmestugor inrättades runt om i kommunerna för att erbjuda invånarna hjälp med praktiska saker som att duscha, tvätta, laga mat, övernatta och inte minst informera sig om den rådande situationen. Erfarenheter visar att de inte alltid utnyttjades i den mån kommunerna trodde, eftersom människor föredrog att i det längsta stanna i sina hem (se vidare informationsbladet *Social sårbarhet utifrån ett medborgarperspektiv 2007*). Förtjänsten av dessa insatser var att det på skapades mötesplatser för socialt umgänge och information. Vissa kommuner hade med andra ord överskattat snarare än underskattat invånarnas hjälpbehov. En annan händelse med ett giftutsläpp bekräftar detta. Det visade sig att de evakueringsmöjligheter som äldreomsorgen då inrättade inte alls utnyttjades. En slutsats av detta är om möjligt att ännu mer försöka rikta insatserna mot människors hem. Det kan exempelvis handla om praktisk service, som att inrätta fler ställen för utlämning av livsmedel, kaminer, elaggregat och andra resurser och tjänster. För att effektivisera förmedling och utnyttjande av reservelaggregat kan man upprätta prioriteringslistor till äldreboende, skolor, värmestugor och andra prioriterade byggnader. Det finns inte alltid aggregat till alla prioriterade byggnader och då tillämpas ofta någon form av roterande bortkoppling, t.ex. att olika byggnader under en viss tidsperiod turas om att utnyttja samma reservelaggregat.

I samband med tsunamin ordnade de flesta kommuner någon form av krismottagning som kunde erbjuda de drabbade psykologiskt stöd. Även på flygplatserna fanns det representanter för kommunala krisgrupper för att möta passagerare från Thailand. Det visade sig dock att alla drabbade inte ville ha detta stöd, utan en del sökte upp hjälp först några månader efter händelsen eller ville bara ha hjälp att finna andra familjer i samma situation. En förklaring till detta har angetts bero på att de drabbade hade fungerande sociala nätverk och ekonomiska resurser och därför klarades mycket på egen hand. En annan orsak som har angetts i intervjuerna skulle kunna vara okunskap eller rädsla. Det är emellertid vanskligt att värdera eller gradera de drabbades skäl till att avböja stöd. Att t.ex. på en flygplats inför alla andra passagerarna välja att gå till en väntande krisgrupp innebär att visa sin sårbarhet på ett sätt som kan kännas obehagligt.

I utformningen av stödet till de drabbade i samband med tsunamin och andra händelser har några kommuner praktiserat det som kallas *empowerment*. Uttrycket kommer från socialt arbete, och betyder att vara lyhörd för den drabbades egna sammanhang och kapacitet att lösa problem.[4] För att kunna göra detta behöver de drabbade information. Ett exempel från en kommun är ett pedofiliärende med flera utsatta barn. Föräldrarna till barnen kallades till informationsmöten där det klargjordes vilket ansvar olika myndigheter har som polisen, åklagaren, psykiatrin och socialtjänsten. Vidare gavs det information om aktuell forskning om hur utsatta barn klarar av att gå vidare och hur föräldrarna påverkas av händelsen. Samtal erbjöds både enskilt och i grupp. Kommunen följde också upp familjerna efter en tid. Samma modell användes sedan för utformningen av stödet efter tsunamin. Utförandet innebär att kunskap och adekvat information om händelserna kan verka läkande för de drabbade. Efter tsunamin ville skolorna erbjuda eleverna möjlighet att tala om händelsen. I de stormdrabbade områdena visade det sig att eleverna i stället ville berätta om vad de hade varit med om i stormen. Detta visar också vikten av förståelse för barnens perspektiv – de är inriktade på det som är närmast deras erfarenhet. Samtidigt är det givetvis viktigt att vara lyhörd för att en så stor katastrof som tsunamin kan beröra många även i de kommuner där det inte fanns omkomna.

Samverkan och nätverk

I samband med stormen Gudrun samordnades krishanteringen i kommunerna ofta utifrån någon form av krisledningsstaber och som i sin tur styrdes av kommunstyrelsen eller i vissa fall krisledningsnämnden. Krisledningscentralerna var många gånger placerade på räddningstjänsten. En betydelsefull erfarenhet visade sig vara när kommunpolitiker besökte staberna och på så sätt fick insyn i praktiska problem som uppstod. Detta visade sig ge en större förståelse för allvaret i händelsen med snabba beslut

[4] Begreppet *empowerment* används här så som det definieras i socialt arbete, se Lundberg & Starrin (1997).

som följd. Politikerna var även informatörer ut mot kommuninvånarna. Kommunerna samverkade med andra aktörer som Länsstyrelser, Sydkraft/Eon, Telia, vägverket, SOS-alarm, försvaret, frivilliga resursgrupper, LRF, Polis, lokala föreningar och hushåll. Stödet till och kontakterna med invånarna sköttes främst genom räddningstjänst, kommunala förvaltningar och bolag. I flera fall var frivilliga resursgrupper (FRG) inblandade, vilka representerades av bland annat Kvinnliga Bilkåren, automobilklubbar, Frivilliga motorcykelkåren, Blå Stjärnan, Frivilliga Flygkåren (FFK), MC-ordonnanser, brukshundsklubbar, Lottakåren, Bilkåristerna, Röda korset och Civilförsvars-föreningen. FRG gav kommunerna möjlighet att sätta in extra personal och resurser. Många frivilliga försvarsorganisationer härrör från försvaret, vilket gör att viktig kunskap och handhavande av materiell, fordon m.m. har bevarats. En nackdel är dock att deras arbetsuppgifter och roller i många fall är oklara. Det finns därför goda strategiska incitament till att se över nuvarande samarbetsformer mellan kommuner och frivilliga resursgrupper och försvars-organisationer. Geografiska och demografiska skillnader är att tänka på. De frivilliga resursgrupperna är ojämnt fördelade över Sverige och i många fall är medelåldern hos medlemmarna hög.

Andra väsentliga aktörer var lokala föreningar och grupperingar som i många fall fungerade som viktiga sambandscentraler inte minst vid arbetet med röjning av vägar och skog, men även vid arbetet med att undsätta utsatta. Många kommuner har insett att konsekvenserna hade förvärrats utan den lokala befolkningens insatser. En fördelaktig strategi är därför att upprätthålla kontinuerlig kontakt med och kunskap om lokala föreningar, byalag, stödgrupper och andra lokalt viktiga kontaktpersoner. Dessa utgör ovärderliga resurser i kriser som liknar stormen Gudrun. Likväl är det av vikt att kommunen informerar sig om lokala materiella och personella resurser. Det kan t.ex. handla om att registrera var sjukvårdskunnig personal bor eller var större privata elaggregat finns stationerade.

Även efter tsunamin erbjöd sig en del frivilliga att göra insatser. Krisgrupperna bedömde att i många fall var de inte lämpliga att ge psykosocialt stöd eftersom de frivilliga hade egna behov att få tala om de händelser som de varit med om. På det sättet skiljer sig tsunamin från många andra extraordinära händelser eftersom behoven mest handlade om att ge psykosocialt stöd. Efter branden i Göteborg 1998 kunde krisgrupperna däremot ta tillvara frivilliga insatser eftersom det fanns praktiska uppgifter som de kunde uträtta som att köra bil eller bre smörgåsar.

I samband med tsunamin och giftutsläppet har betydelsen av samverkan betonats. De personliga kontakterna mellan tjänstemän i olika förvaltningar och myndigheter har framförts som en viktig del för att vissa uppgifter kan lösas snabbt och effektivt. Personlig kännedom ger också möjlighet till improvisationer och snabba åtgärder. Däremot har polisens och resebyråernas fördröjning med passagerarlistor angetts som en svårighet att rätt dimensionera krisgruppernas insatser efter tsunamin.

Information

I samband med stormen Gudrun gjordes stora insatser för att på olika sätt informera drabbade, anhöriga och andra. Internet, radion, posten (lantbrevbärare) och lokala möten var några viktiga informationskanaler. Medborgarträffar sam-organiserades ofta på lokal plats med representanter från kraftbolag och Telia. Erfarenheterna visar på stort behov av kommunala politiker och tjänstemän samt personal från kraftbolag och Telia som är insatta i hur de tekniska systemen och bygderna ser ut. Andra lärdomar visar vikten av att ha kunniga och kända personer som besvarar frågor från allmänheten. I en mindre kommun nyttjades exempelvis en pensionerad tjänsteman för detta ändamål med positivt resultat. När det gäller information via radion är lokalradion att föredra framför länsradion. Inte minst därför att lokalradion kan ge lokalspecifik information. Det finns ett stort behov av lokal information om när elen väntas komma tillbaka och information om reservel, värmestugor och informationsmöten. Det är även av betydelse att dimensionera resurser för att informera media och oroliga anhöriga som hör av sig samt att förbereda sig för att kunna besvara inkommande enkäter och krav på utvärderingar och uppskattning av kostnader från bland annat Länsstyrelsen, Socialstyrelsen och andra myndigheter. Krav på enkätsvar gällde även vid tsunamin då det upplevdes som störande. Flera kommunala tjänstemän har framfört synpunkter på att de själva blev dåligt informerade. Den interna informationen är således lika viktig som den externa. Det är därför viktigt att en informationstjänst motsvarande Krissam i Kronobergs län kan tillhandahålla information internt såväl som till allmänheten, media, andra myndigheter med flera.

Flera aktörer har tagit upp medias roll i krishanteringen. I samband med ett uppmärk-sammat mord upplevde kommunala tjänstemän det svårt att händelsen tolkades som ett rasistiskt dåd i media trots att det inte var det. Både de anhöriga och politikerna fick kraftfullt dementera uppgifterna. I samband med ett giftutsläpp handlade kommunernas insatser framför allt om information, dels om olyckan i sig, dels om de avspärrningar som infördes i

områden närmast utsläppet. En välförberedd informationsfunktion i krisorganisationen var en förutsättning för att kunna ge personliga svar åt dem som ringde kommunen. Kommunens hemsida och lokalradio användes också för att ge information på olika invandrarspråk. Samtidigt fanns det problem att nå vissa utsatta grupper som hörselskadade och utvecklingsstörda i eget boende. Ett dilemma för kommunen med giftutsläppet var att balansera informationen till medborgarna. Utsläppet i sig var inte av det mest allvarliga slaget, men läget var under en tid osäkert och kunde lätt ha förvärrats. Räddningstjänsten bedömde då att det var säkrare att behålla avspärrningarna trots kritik från invånarna i området för att gardera sig för ett ännu större utsläpp.

Prioriteringar, risker och uthållighet

Ett dilemma vid kriser är att ansvar och engagemang för utsatta medmänniskor ibland måste ställas mot den egna personalens säkerhet. Både i samband med stormen Gudrun och giftutsläppet utsatte sig personal från räddningstjänst, hemtjänst, hemsjukvård och andra operativa enheter för risker eftersom de ansåg andra människors behov gå före den egna säkerheten. Incidenter med fallande träd på och omkring tjänstebilar vittnar om detta. I några få fall skadades människor, men olyckstalet var förvånansvärt lågt i relation till insatserna. För hemtjänst och hemsjukvård, som inte har samma skyddsutrustning som räddningstjänst, har följden blivit att de ser över sina resurser inför liknande händelser och inte tillåter t.ex. nattpatruller att köra ut i storm utan eskort. Det i sin tur innebär ett större ansvar för anhöriga till vårdtagarna och patienterna. Detta kan bli en svårighet, eftersom inte alla vård- och omsorgstagare har anhöriga på nära håll och de enligt socialtjänstlagen har rätt till omvårdnad. Bristen på översikt, rykten och människors nyfikenhet och oförmåga att förstå det allvarliga med händelsen medförde att stora resurser fick användas till att undsätta nödställda. Ett exempel var när räddningstjänsten fick sätta in stora resurser för att undsätta en invånare, vars hund hittats men som själv troddes vara försvunnen bland fallna träd. Reflektioner efteråt pekar på större återhållsamhet med personella risker vid liknande framtida händelser. Ett annan vanligt misstag är att inledningsvis sätta in för mycket personal som får arbeta hårt och under långa pass. Följderna kan bli att personalstyrkan tröttas ut. Hemtjänsten, hemsjukvård och räddningstjänst och även andra kommunala enheter var under stormen Gudrun hårt belastade. Att hushålla med personalstyrkan är av särskilt betydelse för små kommuner. Detta gäller också när en kommun involveras i flera händelser efter varandra. Det kan också vara positivt att ha en organisation igång, t.ex. var det psykologiska stödet i form av krisgrupper redan uppstartat till följd av tsunamin när stormen Gudrun inträffade. När giftutsläppet inträffade var den berörda kommunens räddningstjänstpersonal inte fulltalig eftersom en del av den var engagerad i en grannkommun som drabbades svårt av stormen. Händelserna ger med andra ord dominoeffekter som innebär utmaningar i planeringen av personalens insatser. På nationell nivå finns det en erfarenhet från stormdrabbade kommuner att deras svårigheter inte i början togs på allvar på grund av att tsunamin dominerade media.

En annan fråga som har kommit fram i flera kommuner är var gränsen för kommunens respektive den enskilde medborgarens ansvar går. Några beredskapssamordnares erfarenhet är att den största risken i deras arbete är enskilda medborgare som förväntar sig snabb hjälp från myndigheter utan att ha tagit egna initiativ t.ex. genom att själva införskaffa reservelaggregat. Att bosätta sig på landet innebär att se över sin egen beredskap och ta ett ansvar så att man klarar sig medan man väntar på myndigheternas insatser. Tendensen till att förvänta sig snabb hjälp från myndigheterna är tydlig hos yngre medan äldre människor på landet ofta bor i hus med t.ex. alternativa värmekällor. Det är även en medborgerlig skyldighet att ta del av den information som myndigheterna ger på webbsidor och i radions kanal P4. I en av de intervjuade kommunerna har man gjort försök till utbildning om överlevnadskunskap i samarbete med Civilförsvarsföreningen för att öka allmänhetens kunskaper i egen beredskap. Detta väckte dock inte något större intresse och visar på behovet av en allmän debatt om frågorna.

En ytterligare sårbarhet för kommunen och andra myndigheter och organisationer är att vissa nyckelpersoner ofta saknar ersättare och att dessa av personliga skäl kan tvingas stanna hemma för att ta hand om barn, vårda anhöriga eller att sköta om sin privata egendom. Exempel på sådana personer finns lite var stans i kommunen, hos räddningstjänsten eller i vården. En strategi för att undvika dylika kompetensbortfall skulle kunna vara att inrätta någon form av resursuppbackning för att lösa privata angelägenheter. En sådan planering skulle kunna skötas av en så kallad extern analysenhet, i vissa kommuner även kallad ”*omfallgrupp*”, vars främsta uppgift är att under ett aktivt krishanteringsarbete sätta upp olika scenarier för förändrade omständigheter. Under stormen Gudrun användes dessa grupper bland annat för att förbereda kommunerna för eventuella väderomslag. Ett påpekande var att gruppens medlemmar bör vara oberoende och inte ingå i den ordinarie krishanteringsstaben.

Några sammanfattande strategier

Informationsbladet sammanfattas med följande krisberedskaps- och krishanteringsstrategier:

- Kommuner och andra aktörer bör se över de rutiner som kan effektivisera och förbättra arbetet med att identifiera och stödja utsatta gruppers behov av hjälp.
- Kommunen bör om möjligt att ännu mer försöka rikta insatser mot människors hem.
- Kommuner tjänar på att vara lyhörd för den enskildes kapacitet och sammanhang.
- Det är viktigt att kommunpolitiker får insyn i praktiskt krishanteringsarbete.
- Kommuner och andra (t.ex. EON, Telia m.fl.) tjänar på att se över samarbetsformer med frivilliga resursgrupper och med lokala grupper.
- Det kan vara betydelsefullt att dimensionera kanaler för intern och extern information. Att informera utåt med hjälp av personer med god lokal kunskap kan ge ökat förtroende.
- Det är viktigt att spara och inte utsätta den egna personalstyrkan för stora risker.
- Det är nödvändigt fundera över var gränsen mellan kommunens och den enskilde medborgarens ansvar går.
- Nyckelpersoner saknar ofta ersättare. Det är väsentligt att backa upp även det privata.
- Att dimensionera för *omfall* ger möjligheter att förbereda för det oväntade.

Tips på vidare läsning

Guldåker, N. (2007 kommande): Stormen Gudrun och hushålls sårbarhet. Meddelande från Lunds Universitets geografiska institutioner, avhandlingar xxx.

Lundberg, B. & Starrin, B. (red.) (1997): *Frigörande kraft – empowerment som modell i skola, omsorg och arbetsliv.* Stockholm, Förlagshuset Gothia.

Nieminen Kristofersson, T. (2002): Krisgrupper *och spontant stöd – om insatser efter branden i Göteborg 1998*. Avhandling i socialt arbete.

Nieminen Kristofersson, T. (2007 kommande): *Om social sårbarhet i samband med extraordinära händelser – en intervjustudie i 12 kommuner.* Rapport från FRIVA, LUCRAM, Lunds universitet.

Nieminen Kristofersson, T. (2007 kommande): *Hur de som drabbas av katastrofer ser på sin sårbarhet*. Rapport från FRIVA, LUCRAM, Lunds universitet.

Nieminen Kristofersson, T. & Guldåker, N. (2007): *Social sårbarhet utifrån ett medborgarperspektiv.* FRIVA informationsblad. Lunds Universitet.

Önnerfors, M., Guldåker, N. Nieminen Kristofersson, T. (2007): *Erfarenheter av GIS i samband med stormen Gudrun* 2007. FRIVA informationsblad. Lunds Universitet.

Kontakt

För mer information kontakta oss på följande e-post-adresser eller besök FRIVA:s hemsida.

Nicklas Guldåker
Nicklas.guldaker@keg.lu.se

Tuija Nieminen Kristofersson
Tuija.Nieminen@keg.lu.se

FRIVA
http://www.friva.lucram.lu.se

FRIVA Social sårbarhet utifrån ett medborgarperspektiv

Författare: Tuija Nieminen Kristofersson och Nicklas Guldåker

Inledning

Denna skrift är ett av flera informationsblad som redovisar sammanfattade erfarenheter och synpunkter från ramforskningsprogrammet FRIVA (Framework Programme for Risk and Vulnerability Analysis), vilket finansierats av Krisberedskapsmyndigheten under perioden mars 2004 till mars 2007. Informationsbladen skall kunna användas som utgångspunkter för praktiskt arbete när det gäller hantering av risker, sårbarheter, hot, kriser och katastrofer som medför eller kan medföra allvarliga samhälleliga konsekvenser.

Bakgrund

När extraordinära händelser inträffar, handlar de akuta insatserna för de drabbade om livräddning och akutsjukvård. Annan praktisk hjälp t.ex. att åtgärda vattenförsörjning och återställa infrastruktur ingår i kommunernas och andra myndigheters insatser. Sedan slutet av 1980-talet har även det psykologiska och sociala stödet uppmärksammats. I samband med s.k. Kistaolyckan 1988, då skolelever dog i en bussolycka i Norge, blev det tydligt att de drabbades behov av information, psykologiskt och socialt stöd var stort. Efter Kistaolyckan har krisgrupper bildats i kommunerna på rekommendation av socialstyrelsen i form av POSOM-grupper (psykologiskt och socialt omhändertagande).

Syftet med detta informationsblad är att förmedla resultat från några undersökningar som tar upp medborgarnas erfarenheter av hur de fått både praktisk hjälp och psykologiskt stöd i samband med extraordinära händelser. Medborgarnas kunskaper är värdefulla och kan bidra till en bättre krishantering och risk- och sårbarhetsanalys. Undersökningarna berör händelser som stormen Gudrun 2005, tsunamin 2004, branden i Göteborg 1998 och några andra händelser.

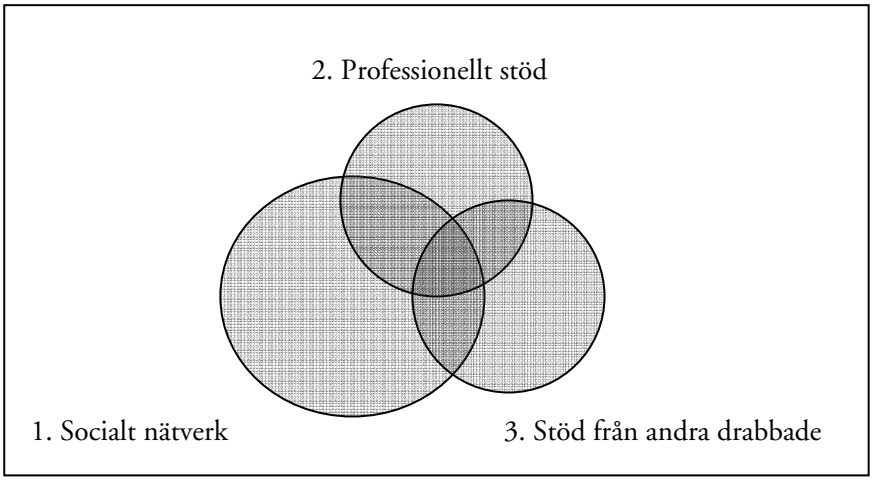
Sårbarhet används ofta som en term i analyser av tekniska system. Begreppet ”social sårbarhet” beskriver hur grupper av människor på olika sätt drabbas av extraordinära händelser. Med socialt sårbara grupper avses av tradition en del äldre, vård- och omsorgstagare, barn och personer med nedsatt funktionsförmåga. Det är grupper som till vardags kan vara beroende av tillsyn, vård eller omsorg och därför är i behov av stöd även i samband med katastrofer. Dessutom kan det hända att grupper som annars inte är sårbara blir det i samband med en katastrof. I samband med en extraordinär händelse drabbas ofta alla medborgare i ett område oavsett om de är sårbara eller inte. I denna text används till stora delar begreppet ”de drabbade” för att markera alla berörda eftersom de intervjuade inte alltid kan räknas bland socialt sårbara.

Stöd i olika dimensioner

Figur 1 illustrerar olika former av stöd i tre olika dimensioner: det sociala nätverket, det professionella stödet och stöd från andra drabbade. Varje dimension i sin tur kan handla om både praktiskt och psykologiskt stöd. Såsom det framgår av figuren kommer stödet i första hand från det sociala nätverket, cirkel nr 1 samtidigt som det överlappas av stöd från professionella, cirkel 2, och andra i samma situation, cirkel 3.

Stöd från det sociala nätverket

De drabbades behov av stöd från omgivningen i samband med extraordinära händelser skiftar under tiden. Omedelbart efter en händelse handlar behoven om akutvård, information och praktisk hjälp. Det var svårt att vänta på säkert besked om anhöriga i samband med diskoteksbranden i Göteborg och tsunamin. I detta osäkra och påfrestande skede betyder den närmaste kretsen av det sociala nätverket, d.v.s. anhöriga, vänner och släktingar, mycket. Tillsammans med dem sökte de drabbade information hos myndigheter och media. Det är också de närmaste som kan hjälpa med praktiskt stöd som att röja vägar och bära in ved efter stormen eller handla och laga mat efter branden i Göteborg. När till exempel bostaden förstörs av brand eller blir oåtkomlig efter ett giftutsläpp föredrar de flesta att flytta till sina närmaste.



Figur 1 Olika former av stöd i samband med extraordinära händelser

Det starka behovet av att vara tillsammans med sina nära kallas för anknytningsbeteende, och handlar om det känslomässiga engagemanget inom familjen som räknas till våra s.k. primärgrupper tillsammans med närmaste vänner och släktingar. Anknytningsbeteendet gör att människor kan störta in i brinnande hus för att rädda familjemedlemmar eller som i Göteborg då ungdomar sprang tillbaka till diskotekslokalen för att hämta ut sina kamrater.

Efter stormen Gudrun kunde LRF:s stödgrupper och andra lokala organisationer, föreningar och spontana grupper organisera uppröjning av kraftledningsgator och vägar och samtidigt ta reda på hur de avlägset boende mådde. På landet finns det enligt intervjupersonerna ett naturligt intresse för grannarna eftersom man har förutom en social gemenskap även ekonomiska frågor att lösa t.ex. underhåll av gemensamma vägar.

Många lokala insatser styrdes upp och understöddes av personer som inte kunde vara med ute och röja skog. Dessa, ofta äldre personer eller anhöriga med tidigare vana att leda organisationer, såg bl.a. till att skogsarbetare kom hem och att de inte var för trötta, att varm mat lagades och att lokala informationsmöten med kommunala tjänstemän, skogsbolag, tele- och kraftbolag anordnades. Samhörigheten och den sociala gemenskapen på landsbygden har i många fall stärkts. Även efter branden upplevde många drabbade i Göteborg en ökad samhörighet som dock klingade av efter en tid.

De som således blir mycket sårbara är de som inte får stöd eller hjälp av sina anhöriga och vänner. Det kan röra sig om grupper som nyinflyttade på orten eller invandrare utan släkt i Sverige som t.ex. efter en brand blev beroende av socialtjänsten för att få ny bostad. Ofta har dock invandrare stora sociala nätverk som utgör ett viktigt känslomässigt och praktiskt stöd. Däremot kan de sakna det som kallas för informationsstöd. Det innebär att släkt och vänner hjälper med värdefull information om hur samhället fungerar t.ex. hur man tar kontakt med myndigheter och försäkringsbolag efter brand eller trafikolyckor. När de drabbade eller deras sociala nätverk inte förmår att på egen hand sköta dessa kontakter är de hänvisade till krisgrupper. Den sociala sårbarheten kan också handla om hushåll och familjer som av olika anledningar inte klarar av händelsens påfrestning. Ett exempel från banden i Göteborg var ett par svenska föräldrar som på grund av skilsmässa inte kunde kommunicera med varandra. Det var därför svårt för dem att förbereda det omkomna barnets begravning. De fick dock stöd från en socialsekreterare som var anknuten till en krisgrupp och kunde också följa upp familjen under en längre tid.

Det professionella stödet

Som det framgår av figur 1 pågår stödet från det sociala nätverket delvis samtidigt som myndigheter och krisgrupper utför sina insatser (där cirklarna nr 1 och 2 lappar över varandra). Det kan t.ex. betyda att de grupper som redan är beroende av vård och omsorg har kvar sitt omsorgsberoende som dessutom kan öka i samband med extraordinära händelser. Ett annat exempel är identifiering av omkomna. Efter branden i Göteborg 1998 var föräldrarna tacksamma att det fanns stöd från krisgrupperna vid detta svåra tillfälle även om de också hade stöd av sina anhöriga. Vid enstaka olyckor där enskilda ombetts att identifiera sina omkomna anhöriga har de framfört kritik mot att de inte haft stöd av professionella just vid denna svåra uppgift.

Efter svåra olyckor kan stödet från myndigheter och krisgrupper handla dels om praktisk hjälp som enskilda inte kan ordna på egen hand t.ex. vattenförsörjning, dels om psykologiskt stöd. Olika krisgrupper kan öppna kriscentra dit de anhöriga kan vända sig såsom det skedde efter tsunamin och branden i Göteborg. Krisgrupperna kan erbjuda samtal med professionellt utbildade kuratorer, socialsekreterare och psykologer. Många drabbade har uppskattat detta slags stöd. Både efter branden i Göteborg och efter tsunamin har de drabbade påpekat att mycket krisstöd erbjöds med detsamma då behovet inte var så stort, och det sociala nätverkets stöd fungerade. Behovet av dessa samtal blir tydligt efter några månader efter händelsen. Då har släkt och vänner ”tröttnat” på att höra de drabbade berätta samma sak om och om igen (Nieminen Kristofersson 2002, SOU 2005:104).

Därför är det viktigt att det psykologiska krisstödet, oavsett om det erbjuds av krisgrupper eller av den ordinarie verksamheten som socialtjänsten har ett längre tidsperspektiv än bara några veckor efter en händelse. Detta ordnades efter branden i Göteborg med hjälp av de stödcentra som under två år gav stöd åt de drabbade. Samtidigt betonar de drabbade att de inte vill bli betraktade som psykiskt sjuka eller i behov av psykiatrisk vård bara för att de har råkat ut för en katastrof. Detta kan vara orsaken till att en del av de drabbade efter tsunamin avböjde stödet från krisgrupperna. Deras situation handlar om existentiell sårbarhet. De har frågor om t.ex. varför händelsen har inträffat och varför just de har drabbats och väljer att tala om dessa frågor i sina nätverk i stället för med professionella.

Ett resultat av undersökningarna är att när flera händelser inträffar nära varandra i tiden har de som drabbats av dem möjlighet att jämföra myndigheternas insatser. Detta kan skapa förväntningar t.ex. på att alla ska ha samma psykologiska eller ekonomiska stöd. Det kan också innebära att en del drabbade tonar ner sina behov av stöd. När stormen Gudrun inträffade var det flera boende på landsbygden som jämförde sin situation med dem som varit med om tsunamin. Få förolyckades eller blev skadade under stormen. Med tsunamin som relief var förstörelsen av skog och annan egendom enligt dem en mild konsekvens.

Stöd från andra drabbade

Den tredje delen i stödet för de drabbade är möjligheten att få träffa andra i samma situation. Det illustreras av cirkeln nr 3 i figur 1. Även här kan denna form av stöd för en del drabbade pågå samtidigt som stöd nr 1 och 2, cirklarna överlappar varandra i figuren. Efter extraordinära händelser är det vanligt att de drabbade erbjuds att delta i samtalsgrupper. Ofta är det präster och diakoner från Svenska kyrkan som leder grupperna. En del av de drabbade har framfört att detta slags gruppsamtal också bör erbjudas i neutralt regi med psykologer som ledare eftersom alla inte vill träffa representanter för ett religiöst samfund. Gruppsamtal och stöd från andra drabbade förekommer även spontant. Efter stormen Gudrun diskuteras fortfarande händelsen i samband med olika möten i byalag och lokala föreningar. Ett annat spontant inslag är alla de anhörigföreningar som bildats efter stora katastrofer. Det myndigheterna kan göra för dessa föreningar är att t.ex. upplåta lokaler för sammankomster. Efter branden i Göteborg erbjöds anhörigföreningen till samarbete kring minnesstunderna och hur brandlokalen skulle bevaras för framtiden.

Platsens betydelse

Förutom ovan nämnda delar i krisstödet handlar den sociala sårbarheten också om platsen, både konkret och symboliskt. Katastrofer och olyckor och dess konsekvenser inträffar alltid på en bestämd plats eller över ett bestämt område. Detta i sin tur får följder för de enskilda. Även om en del av kommunerna erbjöd evakuering eller alternativt boende ville de flesta efter stormen Gudrun vara kvar i sina hem. Detta eftersom man var rädd för inbrott och att lämna husen i kylan. Det egna hemmet har en känslomässig betydelse för de flesta människor, det är där vi lever våra privata liv. Även landskapets förändring efter stormen påverkade många. En del skogsägare kunde bli apatiska när de såg förstörelsen. Förlusten av skogen har dessutom även blottat en ekonomisk sårbarhet hos många skogsägare.

Efter tsunamin erbjöds de anhöriga att resa till Thailand för att besöka platsen där deras nära omkom. Efter trafikolyckor och mord bildas det spontana minnesplatser där t.ex. kamrater till de omkomna samlas såsom skedde på Backaplan i Göteborg. Detta i sin tur innebar att sörjande ungdomar rörde sig och uppehöll sig på offentliga platser. Medvetenheten om platsens betydelse kan underlätta myndigheterna att rätt bemöta de drabbade. Visualiseringen av den nerblåsta skogen med hjälp av kartor och GIS[5] (se vägledningen om GIS) underlättade för myndigheterna och framför allt för politikerna att fatta snabba beslut för att hantera konsekvenserna av stormen Gudrun.

Samtalsgrupper i kyrkans regi kritiserades av en del drabbade efter branden och tsunamin också på grund av att de inte ville vara i ett religiöst symboliskt rum som de inte kände samhörighet med.

En annan aspekt på platsens betydelse handlar om skillnaden mellan tätort och landsbygd vilket blev tydligt i samband med stormen Gudrun. I tätorterna kom strömmen och telefonin tillbaka efter en kort tid medan de boende på landsbygden kunde vara flera veckor utan ström och fungerande telefon. Det innebar stora problem i det dagliga livet för många. För barnfamiljer blev belastning extra stor, både fysiskt och psykiskt. Hushåll upplevde kontrasterna mellan hem och arbete som stora och tärande ju längre avbrotten varade. Allmänheten och politikerna i tätorterna hade svårt att förstå vilka problem det blev på landsbygden. I flera fall kände landsbygdsbor sig kränkta (se även Hemström 2005; Länsstyrelsen i Kronbergs län 2005:2)

Däremot finns det en robusthet på landsbygden. Särskilt äldre bor i hus med alternativa värmekällor

[5] GIS står för geografiska informationssystem.

och klarade sig därför bättre än en del barnfamiljer med elvärme eller moderniserade värmesystem. Alla system för t.ex. vatten och avlopp är inte elberoende och det innebär att de inte är lika känsliga för störningar som i tätorterna. Frågor om t.ex. arbetsskydd som kommunerna måste beakta när de skickar ut folk till att röja vägar tog bönderna och andra som hanterade motorsåg inte alltid hänsyn till. Det i sin tur innebar att röjningsarbetet efter stormen kom igång omedelbart.

Både manualer och lokal kunskap

De drabbades erfarenheter kan sammanfattas med hjälp av en teori om manualer och lokal kunskap. Manualer, lagstiftning, regler och beredskapsplaner bildar tankefigurer, rutiner och modeller som hjälper organisationer att utföra insatser för dem som drabbas av katastrofer. Lokal kunskap innebär improvisation och anpassning till nya situationer med hänsyn till det sammanhang där katastrofen inträffar. En viktig poäng med teorin är att en organisation, oavsett vilken uppgift den har, behöver både manualer och lokal kunskap (Tilly 2000).

De drabbades erfarenheter i samband med extraordinära händelser utgör delar av lokal kunskap. Kunskapen är alltid knuten till de drabbade och deras sociala förhållanden och nätverk. Myndigheternas krisstöd utgår däremot till stora delar från beredskapsplaner, risk- och sårbarhetsanalyser och lagstiftning på området.

Stödet från professionella och myndigheter har fungerat när det förutom de krisplaner som använts också har tagit hänsyn till lokal kunskap. Efter branden i Göteborg ville ungdomarna vara tillsammans på Backaplan och övernatta hos vissa krisgrupper. Då anpassade sig krisgrupperna till deras behov. Ett annat exempel är hur kommunerna efter stormen tog tillvara de lokala organisationernas som LRF:s kunskap om vägarna och framför allt om grannar som bodde i avlägsna hus. Utan denna lokala kunskap hade det tagit längre tid för kommunerna att söka upp de utsatta.

De drabbade har också erfarenheter av hur myndigheterna, i alla fall till en början, följt krisplaner och tankemodeller utan lokal kunskap. En sådan modell är uppfattningen att alla efter en extraordinär händelse vill ha psykologiskt stöd från krisgrupper eller psykiatrin. Detta har lett till omfattande mobilisering av krisgrupper omedelbart efter en händelse trots att det stora behovet av samtal kommer först efter några månader. Det har också visat sig att det primära behovet inte alltid är samtal utan hjälp med praktiska problem. En annan tankemodell som en del av de drabbade varit tveksamma till är erbjudandet av samtalsgrupper för anhöriga i Svenska kyrkans regi. Erfarenheterna från både tsunamin och branden har visat att de drabbade är känsliga för om samtalen sker i sammanhang som de inte känner sig hemma i. Ytterligare ett exempel på hur en tankemodell kan bli missriktad är en barnfamiljs erfarenheter efter stormen Gudrun. Kvinnan i familjen höll på att bära in vatten till hushållet då en militär kom och bad henne att fylla i en enkät.

Sammanfattningsvis betyder den lokala kunskapen i form av de drabbades erfarenheter att den fungerar som ett viktigt komplement till kommunal krishantering. Det stöder de resultat som visat att i stället för färdiga fastlåsta krisplaner betonar myndigheterna själva processens, och därmed den lokala kunskapens, betydelse i framtagandet av planerna.

Tips på vidare läsning

Guldåker, N. & Nieminen Kristofersson, T. (2007): *Kommuners arbete och stöd till utsatta medborgare till följd av stormen Gudrun, flodvågskatastrofen och några andra större händelser.* FRIVA informationsblad. Lunds Universitet.

Guldåker, N. (kommande): *Stormen Gudrun och hushållens sårbarhet.* Meddelande från Lunds Universitets geografiska institutioner, avhandlingar xxx.

Hemström O. (red.) (2005): *Stormen. Berättelser från en katastrof*. Carlsson Bokförlag.

Länsstyrelsen i Kronobergs län (2005:2): *Utvärdering av krishanteringsarbetet efter orkanen Gudrun i Kronobergs län vintern 2005*.

Nieminen Kristofersson, T. (2002): Krisgrupper *och spontant stöd – om insatser efter branden i Göteborg 1998* Lund Dissertations in Social Work 7, Lunds universitet.

Nieminen Kristofersson, T. (2006): ”Från olycksplats till minnesplats”, Artikel i *Katastrof! Olyckans geografi och antropologi.* Årsboken Ymer (2006) Svenska Sällskapet för antropologi och geografi.

Nieminen Kristofersson, T. (2007 kommande): *Om social sårbarhet i samband med extraordinära händelser – en intervjustudie i 12 kommuner* rapport från FRIVA, LUCRAM, Lunds universitet

Nieminen Kristofersson, T. (2007 kommande): *Hur de som drabbas av katastrofer ser på sin sårbarhet* rapport från FRIVA, LUCRAM, Lunds universitet

Socialstyrelsen (1991/1996): *Psykiskt och socialt omhändertagande vid stora olyckor och katastrofer.*

Allmänna råd från Socialstyrelsen 1991:2, reviderad upplaga 1996.

SOU 2005:104: *Sverige och tsunamin – granskning och förslag.* Huvudrapport från 2005 års katastrofkommission. Stockholm, Statens Offentliga Utredningar.

Tilly, C. (2000): *Beständig ojämlikhet.* Översättning Sven-Erik Torhell Lund, Arkiv förlag.

Önnerfors, M., Guldåker, N. Nieminen Kristofersson, T. (2007): *Erfarenheter av GIS i samband med stormen Gudrun* 2007. FRIVA informationsblad. Lunds Universitet.

Kontakt

För mer information kontakta oss på följande e-post-adresser eller besök FRIVA:s hemsida.

Tuija Nieminen Kristofersson
Tuija.Nieminen@keg.lu.se

Nicklas Guldåker
Nicklas.guldaker@keg.lu.se

FRIVA
http://www.friva.lucram.lu.se

FRIVA

Informationsblad till MVA Mappsystem Del 1 av 5: Introduktion

Författare: Ana Gil Solá, Jerry Nilsson, Per Olof Hallin

Inledning

Denna skrift är ett av flera informationsblad som redovisar sammanfattade erfarenheter och synpunkter från ramforskningsprogrammet FRIVA (Framework Programme for Risk and Vulnerability Analysis), vilket finansierats av Krisberedskapsmyndigheten under perioden mars 2004 till mars 2007. Informationsbladen skall kunna användas som utgångspunkter för praktiskt arbete när det gäller hantering av risker, sårbarheter, hot, kriser och katastrofer som medför eller kan medföra allvarliga samhälleliga konsekvenser.

Handledningens struktur

Detta är den första och introducerande delen i *Informationsblad till MVA-metoden och MVA Mappsystem.* Handledningen är uppdelad i fem delar:

- Denna första del introducerar MVA-metoden och sammanhanget i vilken metoden utvecklades och används, mappsystem och arbetssätt samt den samlade risk- och sårbarhetsrapport och det bibliotek som arbetet inom MVA-metoden utgör underlag för.
- Del 2-5 innehåller handledningar för de fyra analyser som MVA-metoden erbjuder stöd för: Värdegrund och oönskade händelser (del 2), Översiktlig analys (del 3), Djupanalys (del 4) samt Återkoppling (del 5). Dessa handledningar finns bl.a. på FRIVA:s hemsida http://www.friva.lucram.lu.se och på projektets hemsida www.keg.lu.se/forsa.

Varför sårbarhetsanalys?

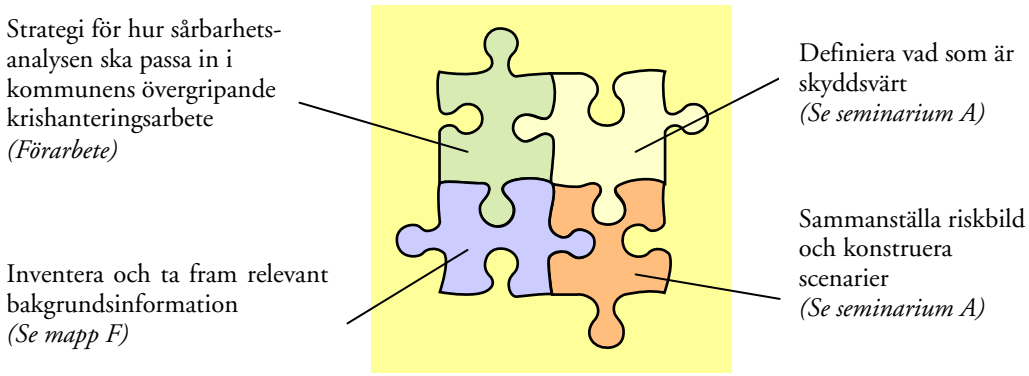
Enligt lag[6] ska kommuner genomföra risk- och sårbarhetsanalyser. I en riskanalys identifieras och beräknas dels sannolikheten för att en eller flera oönskade händelser ska inträffa och dels dess konsekvenser. Med hjälp av en riskanalys är det därmed möjligt att identifiera några av de oönskade händelser som skulle kunna leda till kriser i kommunen samt att reducera sannolikheten och/eller konsekvensen av dessa. Det är dock inte troligt att man lyckas identifiera alla händelser som kan inträffa och övergå i kriser. Det finns därför ett behov av att också upprätthålla en krishanteringsförmåga för oförutsedda händelser eller händelser vars sannolikhet inte kan elimineras. En sådan förmåga kan utvecklas genom att arbeta med sårbarhetsanalyser. Syftet med sårbarhetsanalyser är att identifiera och klarlägga brister i förmågan att motstå och hantera specifika påfrestningar som kan drabba det som är skyddsvärt i samhället.

Som ett led i den samhällsprocess som har växt fram, genom bland annat den nya lagstiftningen, har ett behov uppstått av att utveckla metoder som kommuner och andra organisationer kan använda för att genomföra ändamålsenliga risk- och sårbarhetsanalyser. Ett av de verktyg som har utvecklats med detta syfte är MVA-metoden[7].

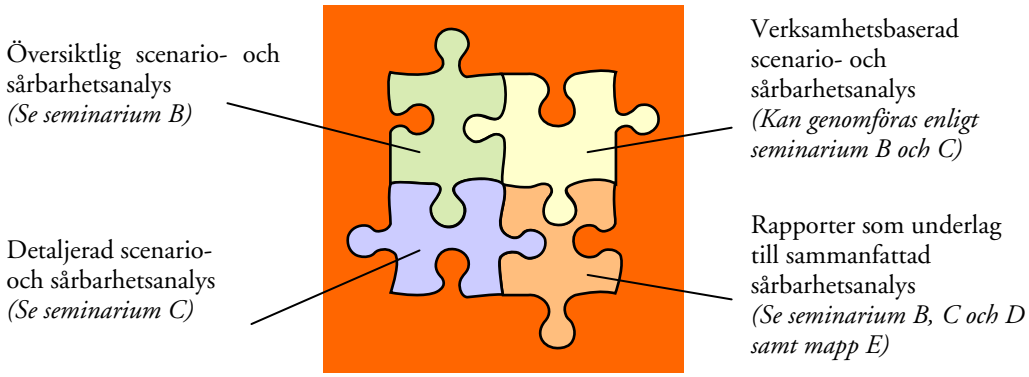
[6] Bland annat Lag (2003:778) om skydd mot olyckor och Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap. Flera lagar och förordningar reglerar krisberedskapsarbetet, se www.krisberedskapsmyndigheten.se > Krisberedskap > Lagar och förordningar och www.krisberedskapsmyndigheten.se > Stöd från KBM > För kommuner > Lagstiftning.

[7] MVA är förkortning för *Municipal Vulnerability Analysis.*

Figur 1. Förberedande moment



Figur 2. Analys



MVA-metoden

MVA är en processinriktad metod för att analysera kommuners och regioners sårbarhet ur ett brett perspektiv. Till metoden finns tre olika IT-stöd: ett mappsystem för Utforskaren (Windows), ett Internetbaserat stöd för att ladda ner formulär och manualer, samt ett program med databashanterare. Denna handledning avser mappsystemet för Utforskaren. Metoden inbegriper bl.a. scenario-metodik och analyserna genomförs i seminarieform. Grundläggande för arbetssättet är 3att sårbarhets-analyserna sätts in i ett helhetsperspektiv, och lika viktigt som att genomföra analyserna är att från starten ha tänkt igenom hur dessa ska passa in i krishanteringsarbetet.

Genom MVA-metoden kan en kommun eller organisation bland annat:

- Bedöma hur sårbar den är mot oönskade händelser.
- Utveckla en informations- och kommunikationsplattform.
- Arbeta fram underlag till förbättringar.
- Utveckla och förstärka personliga nätverk.

MVA-metoden uppfyller följande krav

Metoden ska:

- Kunna tillämpas i alla kommuner och organisationer och ge resultat som kan jämföras.
- Snabbt kunna uppdateras.
- Ge en allsidig bedömning av hot, risk och sårbarhet.
- Värdera förmågan att hantera de behov och uppgifter som har sitt upphov i oönskade händelser.
- Vara förhållandevis enkel att genomföra och lätt att förstå, dvs. att stora krav ställs på presentation av resultat.

MVA-metodens logiska uppbyggnad

För att få till stånd en framgångsrik sårbarhetsanalys är olika moment viktiga att genomföra. Dessa moment kan antingen ses som led i en process eller användas mer som fristående byggstenar. I arbetet med kommuner och MVA-metoden har vissa moment visat sig vara värdefulla att arbeta med, se figur 1 och 2 ovan.

Seminarier och IT-stöd inom MVA-metoden

MVA-metoden fokuserar på en grupprocess som syftar till lärande och organisationsutveckling. Användning av ett datorstöd som är anpassat till metoden underlättar dock strukturering av arbetet och dokumentation av arbetsprocessen. Att dokumentera är viktigt då det ger en spårbarhet i analysen. Kommuner, förvaltningar och andra organisationer kan vid behov också arbeta med MVA-metoden utan att använda något av de utvecklade datorstöden.

Då metoden syftar till att skapa en inlärningsprocess hos kommunerna ingår i metoden olika analyser/seminarier i flera steg, se figur 3 nedan. De olika delarna i figur 3 illustrerar även mappar i MVA Mappsystem och hur dessa hör ihop, se figur 4 nedan.

MVA Mappsystem

Syftet med mappsystemet är att ge en översiktlig struktur till MVA-metodens olika steg/moduler. Mappsystemet innehåller:

- Handledning för MVA-arbete i form av manualer, scenariotexter, formulär, figurer, arbetsmaterial till seminarier samt rapportexempel.
- En struktur till organisationens digitala material för beredskaps- och krishanteringsarbete.

I mappsystemet finns följande mappar vilka illustrerar de olika stegen i arbetet:

A. *Värdegrund och oönskade händelser* – Innehåller anvisningar och mallar för seminarium där grundvalar för risk- och sårbarhetsarbetet lyfts fram.
B. *Översiktlig analys* – Innehåller anvisningar och mallar för en mer översiktlig sårbarhetsanalys.
C. *Djupanalys* – Innehåller anvisningar och mallar för en mer djupgående och detaljerad sårbarhetsanalys.
D. *Återkoppling* – Innehåller anvisningar och mallar till seminarium som syftar till att förankra resultat från sårbarhetsanalys i verksamheten.
E. *Risk- och sårbarhetsrapport* – Innehåller anvisningar för sammanställning av risk- och sårbarhetsrapport.
F. *Bibliotek* – Samlar viktig information om kommunen. Informationen utgör underlag för risk- och sårbarhetsrapport, exempelvis farligt godsleder, farliga anläggningar, tekniska försörjningssystem, naturrisker, utrymnings- och samlingsplatser, gemensamma resurser, social struktur, utförda riskanalyser och riskbild, möjliga oönskade händelser, viktiga aktörer, dokumentation av arbetssätt och process.

I mappar A-D finns tre undermappar – *Arbetsmaterial*, *Mallar* och *Rapportexempel*. I mappen *Mallar* finns allt förberett material inför seminarierna, i mappen *Rapportexempel* hittas exempel på hur en rapport från respektive seminarium kan se ut, och under *Arbetsmaterial* kan användaren lägga sitt eget arbetsmaterial.

Hur verksamheten kan arbeta med MVA-metoden

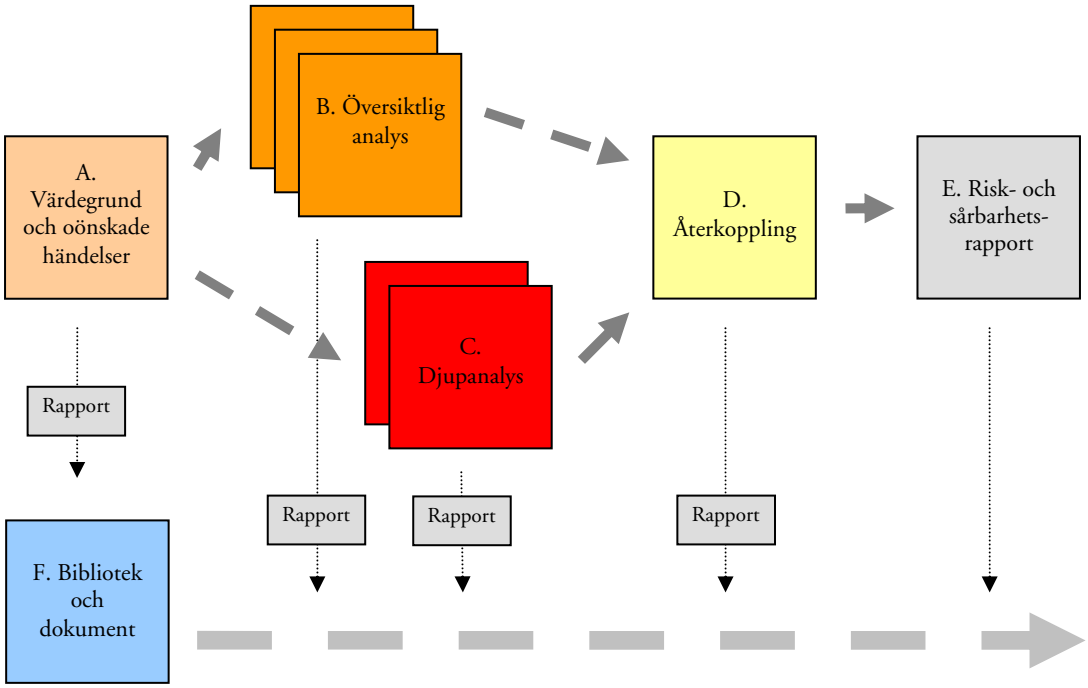
Detta kapitel beskriver flera möjliga sätt att arbeta med materialet i mappsystemet. Anvisningarna kan följas första gången varpå man senare kan hoppa över vissa steg, beroende på kommunens eller organisationens mål och behov.

Initiativ till risk- och sårbarhetsarbetet kan komma underifrån (enskilda förvaltningar) såväl som ovanifrån (övergripande ledning). Krishanteringsorganisationen bör starta med att bestämma strategi för hur sårbarhetsanalysen ska passa in i kommunens övergripande krishanteringsarbete. Därefter kan man bestämma vilka delar av organisationen som ska genomföra sårbarhetsanalyser, varpå dessa bestämmer vilken analys de vill genomföra. Både enskilda förvaltningar och kommunens övergripande funktioner bör involveras i beredskaps- och krishanteringsarbetet.

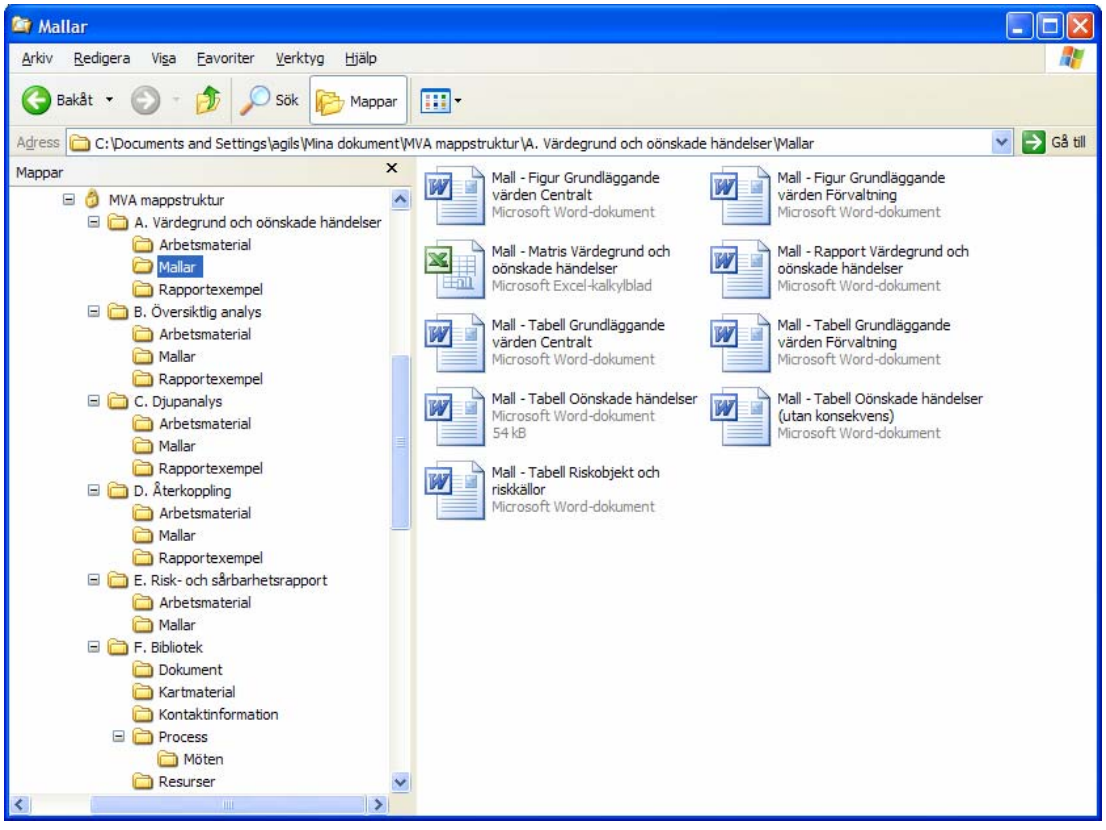
Det första seminariet behandlar organisationens värdegrund, det vill säga vilka värden och objekt som man ser som viktiga eller skyddsvärda för verksamheten. På seminariet lyfts även oönskade händelser som kan drabba kommunen/-organisationen fram, liksom möjliga riskkällor och riskobjekt i kommunen. I samband med att det första seminariet genomförs kan organisationen starta arbetet med att samla material till ett bibliotek. Materialet ska inbegripa sådant som är användbart i beredskaps- och krishanteringsarbetet och bör samtidigt kunna uppdateras kontinuerligt för att även i en akut krissituation vara tillförlitligt.

Utifrån scenarier som konstrueras med utgångspunkt i resultat från värdegrundsseminariet kan organisationen välja att genomföra en översiktlig sårbarhetsanalys eller en djupanalys. I mappsystemet finns en scenariobank som innehåller scenarier utvecklade utifrån olika kommuners värdegrunds-seminarier och önskemål. Dessa kan exempelvis användas i analyserna eller som inspiration för författande av nya scenarier. I mappsystemet finns även uppgifter som har identifierats under sårbarhetsanalyser i olika kommuner, vilka finns i filen *Exempeluppgifter till Djupanalys och Översiktlig*

Figur 3. Block i MVA-metoden



Figur 4: Mappsystem i Utforskaren



analys och kan användas av moderatorn (se nedan) som inspiration.

Både översiktliga sårbarhetsanalyser och djupanalyser bör följas upp av ett återkopplingsseminarium. Under ett sådant seminarium diskuteras och preciseras förslag på åtgärder för att förbättra kommunens krishanteringsförmåga, vilka sedan ligger till grund för en handlingsplan.

När samtliga delar av organisationen har genomfört sina analyser kan dessa sammanfattas i en *Risk- och sårbarhetsrapport*. Inom en kommun skulle detta exempelvis kunna vara Krisledningsgruppen, Vård- och omsorgsförvaltningen, Tekniska förvaltningen samt Kultur- och skolförvaltningen. Den samlade rapporten bör även innehålla material om risker, skydd mot oönskade händelser, process och arbetssätt, mm. Slutligen kan alla färdiga rapporter samlas i ett *Bibliotek* (mapp F) medan allt arbetsmaterial samlas i andra mappar (mappar A-E).

Förberedelser inför seminarierna

Ett av de första stegen i förberedelserna är att välja vilka som ska delta i seminarierna:

- *Gruppdeltagare* – Dessa bör ha ett operativt ansvar för verksamheten som studeras. På så sätt får personer som i en krissituation kommer att leda organisationen bedöma hanteringsförmågan för oönskade händelser samt bättre insikt i verksamhetens sårbarheter.
- *Moderator* – Denne bör ha erfarenhet av att leda grupper samt vara något insatt i verksamheten.
- *Sekreterare* – Den som nedtecknar diskussionen kan vara någon som är insatt i verksamheten, men som inte deltar aktivt i seminariet.

Under seminarierna

Under seminarierna kan moderatorn skriva upp stödord på en tavla för att strukturera diskussionen medan sekreteraren antecknar diskussionen i de formulär som finns tillgängliga för respektive analys. För att gruppen inte ska begränsas av de matriser som används bör de endast få se dem i efterhand.

Formulärmallar och figurer kan användas som riktlinjer för seminariets innehåll och struktur. Dock behöver allt i formulären inte tas upp och de kan gärna ändras för att bättre passa kommunens syfte och arbetssätt. Som minnesstöd kan även diktafon användas samt eventuellt tavlan fotograferas med digitalkamera.

Risk- och sårbarhetsrapport

Mapp E innehåller förslag på disposition och innehåll i en risk- och sårbarhetsrapport. Syftet med texten är att ge riktlinjer för hur kommuner och andra verksamheter kan skriva risk- och sårbarhetsrapporter. I mappen finns även två undermappar – *Arbetsmaterial* och *Mallar* som kan användas när rapporten författas.

Bibliotek

Syftet med mappen är att på ett lättillgängligt sätt samla uppdaterad information för beredskaps- och krishanteringsarbetet.

I mappen ska kontinuerligt viktig information om kommunen samlas, exempelvis farligt godsleder, farliga anläggningar, tekniska försörjningssystem, naturrisker, utrymnings- och samlingsplatser, gemensamma resurser, social struktur, utförda riskanalyser och riskbild, möjliga oönskade händelser, viktiga aktörer, dokumentation av arbetssätt och process. För att materialet ska hållas uppdaterat bör en eller flera ansvariga utses. Är flera ansvariga bör de ansvara för var sin del.

I samband med att det första seminariet *Värdegrund och oönskade händelser* genomförs kan organisationen starta arbetet med att samla material till biblioteket. Följande innehåll kan läggas in i respektive mapp:

- *Dokument* – Krisledningsplan, Informationsplan, mm.
- *Kartmaterial* – Uppdaterat kartmaterial kopplat till aktualiserad statistik.
- *Kontaktinformation* – Kontaktinformation till aktörer inom och utanför kommunen, exempelvis till Krisledningsgruppen, lokalradio, regionens tjänsteman i beredskap, mm.
- *Process* – Mötesanteckningar och protokoll från möten inom krisberedskapsorganisationen. Syftet med materialet är att skapa en minnesbank för både nya och gamla medverkande att gå tillbaka till.
- *Resurser* – Andra resurser att använda i beredskaps- och krishanteringsarbetet, exempelvis flygbilder över kommunen, statistik över befolkning och andra skyddsvärda objekt, mm.

Kontakt

För mer information kontakta oss på följande e-post-adresser eller besök FRIVA:s hemsida.

Ana Gil-Sola
ana.gil-sola@keg.lu.se (t.o.m. 2007-04-30)

Jerry Nilsson
jerry.nilsson@brand.lth.se

Per-Olof Hallin
per-olof.hallin@keg.lu.se

FRIVA
http://www.friva.lucram.lu.se

FRIVA Ett arbetsmönster att använda i arbetet med en kommuns beredskapsplanering

Författare: Marcus Abrahamsson, Lars Fredholm, Kerstin Eriksson

Inledning

Denna skrift är ett av flera informationsblad som redovisar sammanfattade erfarenheter och synpunkter från ramforskningsprogrammet FRIVA (Framework Programme for Risk and Vulnerability Analysis), vilket finansierats av Krisberedskaps-myndigheten under perioden mars 2004 till mars 2007. Informationsbladen skall kunna användas som utgångspunkter för praktiskt arbete när det gäller hantering av risker, sårbarheter, hot, kriser och katastrofer som medför eller kan medföra allvarliga samhälleliga konsekvenser.

Bakgrund

När en oönskad händelse av något slag drabbar samhället har ofta den kommunala nivån ett stort ansvar att svara upp mot de behov som då kan tänkas uppstå. Att beredskapsplanera för det breda spektrum av oönskade händelser som kan drabba en kommun är en mångsidig och viktig uppgift som ställer stora krav på inblandade aktörer. Att sträva efter att på ett systematiskt sätt söka kunskap om potentiella oönskade händelser som skulle kunna drabba kommunen, samt vilka konsekvenser dessa skulle kunna leda till, torde kunna utgöra en bra grund för ett sådant arbete.

Syfte

I denna skrift presenteras översiktligt ett förslag på arbetsmönster som kan användas på kommunal nivå vid planering och förberedelser inför hantering av oönskade händelser som kan drabba kommunen. Arbetsmönstret kan användas:

- för inventering och analys av möjliga krishändelser,
- som underlag till löpande ledning av krisberedskap, samt
- som underlag till utveckling av hanteringsförmåga.

Översikt av arbetsmönster

Arbetsmönstret bygger på hur en s.k. grovanalys kan göras avseende det breda spektrum av risker och hot en kommun kan ställas inför. Det ger möjlighet till att generera scenarier vilka kan vara objekt för noggrannare analys. Underlaget för arbetsmönstret utgörs av:

- en kategorisering av händelser (olycka, sjukdomsspridning, kriminell handling, social oro, infrastruktursvikt),
- en kategorisering och underlag för bedömning (i fem graderingar) av konsekvenser (för liv och hälsa, för miljö, för ekonomi, för livs- och funktionsmöjligheter, för konstitutionell värdestruktur, för anspråk på samhällets resurser), samt
- en skala (i fem steg) för sannolikhets-bedömning.

Ett huvudproblem vid all analys av risker och hot som kan drabba ett system (exempelvis en kommun) har att göra med frågan hur väl man lyckas belysa den variation av tänkbara påfrestningar man kan komma att ställas inför. För att understödja identifiering och beskrivning av händelser inom hela det breda spektrum en kommun skulle kunna drabbas av har ett antal händelsekategorier definierats vilkas innebörd förklaras kortfattat nedan:

- *Olycka* är en plötsligt inträffad händelse som har medfört eller kan befaras medföra skada. Dit räknas händelser som beror på företeelse i naturen eller på människors handlande eller underlåtenhet att handla, t.ex. bränder, explosioner, skred, ras, översvämningar, oväder och utflöden av skadliga ämnen.
- *Sjukdomsspridning* utgörs t.ex. av epidemier bland människor eller epizootier bland djur.

- *Kriminell handling* innebär ett olagligt beteende som kan leda till påfrestningar i samhället. Terrorhandlingar räknas hit. Ageranden som syftar till att förstöra olika infrastrukturella system räknas hit.
- *Social oro* innebär exempelvis att det uppstår motsättningar, ryktesspridning eller förtroendeförluster mellan befolkningsgrupper eller mellan befolkningsgrupper och myndigheter.
- *Infrastruktursvikt* innebär att ett viktigt system i samhället för samhällelig funktion eller försörjning slutar att fungera (eller avsevärt försämras) genom t.ex. ett tekniskt fel, mänsklig felhandling eller yttre påverkan. Det kan handla om elförsörjning, vattenförsörjning, järnvägsnät, informationsöverföringssystem, system för social omsorg, räddningstjänst etc.

I rapporten ”En studie av risker och sårbarheter i Stenungsunds kommun” (se ”Litteraturtips”) finns exempel på checklista som kan fungera som stöd vid identifiering av tänkbara scenarier inom de olika händelsekategorierna ovan.

Det är också av stor vikt att klargöra vad som uppfattas som negativa konsekvenser av en oönskad händelse. Detta kan givetvis variera mellan olika kommuner och i olika sammanhang men nedan ges en kort beskrivning av sex konsekvenskategorier som kan användas som utgångspunkt:

- *För liv och hälsa* avser om en händelse kan medföra dödsfall, svårt skadade eller sjuka människor, människor i behov av vård etc.
- *För miljö* handlar om hur stora miljöeffekter en skadehändelse kan medföra avseende geografisk och tidsmässig utbredning, möjlighet till återställande etc.
- *För ekonomi* avser såväl kortsiktiga som långsiktiga effekter på hela ”systemet” kommun, d.v.s. påverkan på bl.a. industri, samhälle och invånare inkluderas.
- *För livs- och funktionsmöjligheter* avser hur stor del av samhällets invånare och näringsliv som får sina livsbetingelser och möjligheter att fungera normalt avsevärt försvårade eller omintetgjorda.
- *För konstitutionell värdestruktur* handlar om i vilken utsträckning en skadehändelse skulle kunna medföra ohörsamhet mot demokratiska principer och samhälleliga lagar och bestämmelser.
- *För anspråk på samhällets resurser* handlar om i vilken utsträckning samhälleliga resurser kommer att krävas för att hantera en skadehändelse och dess effekter.

I rapporten ”En studie av risker och sårbarheter i Stenungsunds kommun” (se ”Litteraturtips”) finns för varje konsekvenskategori en femgradig skala med beskrivning av vilken konsekvensnivå som motsvarar de olika stegen på skalan. På motsvarande sätt finns en femgradig skala att använda som stöd för bedömning av sannolikheten för de identifierade scenarierna.

Avsikten är att modellen skall ge en uppfattning av det totala utfallsrum (händelsetyper, konsekvensbelastningar och uppskattade sannolikheter) av kriser som kan drabba en kommun.

Inventering och analys av möjliga krishändelser

Med arbetsmönstret som underlag kan en kommuns för beredskapsplanering ansvariga tjänstemän och politiker (i form av en arbetsgrupp) komma fram till ett panorama av sådana krissituationer som kan drabba kommunen. Arbetet innebär att systematiskt arbeta sig genom de olika kategorierna av händelser (olycka, sjukdomsspridning, kriminell handling, social oro, infrastruktursvikt) och för varje kategori

- identifiera möjliga kommunpåfrestande händelser,
- uppskatta möjliga konsekvenser för varje identifierad händelse (inom kategorierna liv och hälsa, miljö, ekonomi, livs- och funktionsmöjligheter, konstitutionell värdestruktur, anspråk på samhällets resurser), samt
- bedöma sannolikhet för identifierad händelse.

På detta sätt kan kommunens för krishantering ansvariga politiker och tjänstemän bilda sig en uppfattning om det panorama av kriser som kan drabba kommunen. Med detta som underlag kan både förebyggande och förberedande åtgärder vidtas.

Löpande ledning av krisberedskap

Det finns ett behov av att en kommun löpande kan leda en verksamhet som syftar till att upprätthålla krisberedskap. För att bygga upp en sådan i kommunen integrerad ledande verksamhet (ett ledningssystem) kan en grund eller ram behövas utifrån vilken krissituationer kan identifieras och

analyseras, mål för krishanteringen formuleras samt nödvändiga resurser identifieras. Det ovan beskrivna arbetsmönstret kan vara en sådan grund eller ram. Med utgångspunkt i identifierade händelser, konsekvenser och sannolikheter inom de olika händelsekategorierna kan

- krishanteringsmål formuleras,
- ansvarsfördelning ske mellan olika förvaltningar,
- organisering och koordinering inom och mellan förvaltningar ske med avseende på uppgifter i krishantering,
- uppföljning av resurser och förmåga ske, samt
- en inom kommunen ansvarig funktion för löpande ledning av krisberedskap få en grund att utforma sin verksamhet från.

Utveckling av hanteringsförmåga

Med utgångspunkt i de scenariobeskrivningar som kan åstadkommas inom respektive händelsekategori kan vidare analys ske av hur resurser och förmåga skall utvecklas för att akut kunna hantera kriser i kommunen. De identifierade möjliga scenarierna kan bli underlag för att definiera

- vilka generella hanteringsproblem som är gemensamma för alla skadehändelser,
- vilka specifika hanteringsproblem som uppstår p.g.a. olika händelser, samt
- specifika, av lokala omständigheter betingade, hanteringsproblem.

Med detta som underlag kan sedan analyser göras av hur

- organisering (inom och mellan förvaltningar) av responsinsatser för hantering av respektive generella och specifika hanteringsproblem bör ske,
- hur planering bör utformas, samt
- hur utbildning och övning bör genomföras.

Litteraturtips

Ovan angivna förslag är mycket kortfattade. En utförligare beskrivning av arbetsmönstret och hur det kan användas i en kommun finns i rapporten

➢ Abrahamsson, M. & Johansson, H. (2007) ”En studie av risker och sårbarheter i Stenungsunds kommun”, LUCRAM rapport 1009, Lunds Universitet.

En beskrivning på engelska finns även i

➢ Abrahamsson, M., Johansson, H., Fredholm, L., Eriksson, K., & Jacobsson, A. (2007) ”Analytical Input to Emergency Preparedness Planning at the Municipal Level – A Case Study”, skickad till TIEMS2007 *Disaster Recovery and Relief: Current & Future Approaches* 5-8 Juni, Trogir, Kroatien

Kontakt

För mer information kontakta oss på följande e-post-adresser eller besök FRIVA:s hemsida.

Marcus Abrahamsson
marcus.abrahamsson@brand.lth.se

Lars Fredholm
lars.fredholm@srv.se

Kerstin Eriksson
kerstin.eriksson@brand.lth.se

FRIVA
http://www.friva.lucram.lu.se/

FRIVA

IT Systems in Emergency Management

Författare: Kim Weyns, Martin Höst, Per Runeson

Introduction

This document is one in a series of information sheets summarizing the results from the FRIVA (Framework Programme for Risk and Vulnerability Analysis) research programme, funded by the Swedish Emergency Management Agency from March 2004 until March 2007. The information sheets are intended to be used as a baseline for applied work with risk and vulnerability management for threats that can lead to serious consequences for society.

Background

Swedish municipalities have an important operative role in crisis situations. In recent years municipalities have become more and more dependant on IT systems for their everyday work. This evolution has made that also for their responsibilities in a crisis situation they have come to rely more and more on all kinds of IT systems. This evolution poses special requirements on these IT systems, and some recent examples have shown that sometimes IT systems are not as reliable as they were believed to be, when they were suddenly critically needed.

For example in the aftermath of the storm Gudrun, many municipalities noticed that they had become very dependant on the public mobile phone networks for their communication. When these networks were damaged by the storm, this caused serious delays in the crisis relief efforts. Better planning and awareness of this vulnerability could have prevented many of those problems.

Another example is that when a serious accident happens in a municipality and the emergency managers wish to publish urgent information to the general public on the municipality's public webpage, it can turn out that it takes much longer than they thought to make the information available online. In this case this problem could have been discovered with better communication between emergency managers and the personnel responsible for the website. If the problem had been detected before the crisis occurred, the systems could have been changed to allow the faster publication of crisis information.

Many different kinds of IT systems can turn out to be critical in crisis relief. Examples of these systems are of course all communication systems (such as both internal and public telephone networks or even the internet or email), networking components that are required for reaching shared information (such as routers and file servers) and of course all systems needed by the personnel with operative responsibilities during a crisis. Emergency services like the fire department usually have access to special systems like RAKEL that have been built with special crisis requirements in mind, and these systems can be depended on much more than everyday systems like desktop computers that have not been built to be used in critical circumstances. However, in crisis situations both kind of systems might turn out to be very critical.

The evolution of IT systems at most municipalities has gone very fast, and the use of IT will probably continue to change quickly. More and more important information is stored electronically on a distant server instead of locally on paper. When all systems continue to function perfectly, this creates many possibilities for improvements in crisis relief, although this evolution also means an increased risk. To avoid unexpected problems with IT systems in the aftermath of a crisis it is important that these risks are identified before a crisis occurs and that measures can be taken to reduce the dependence on systems that could be unreliable.

This kind of risk analysis requires the sharing of information between emergency managers (who perform risk and vulnerability analysis), users (who know best how much they depend on the different IT systems) and IT personnel (who have the most understanding of how dependable IT systems are). In many municipalities there is too little communication between these different actors, and therefore critical information is not available to take into account the reliability of the IT systems in risk analyses for crisis situations.

To completely analyse the reliability of a certain system or even the exact dependency on a certain IT system is often very difficult and most

municipalities lack the resources to do such a detailed risk analysis. However, even with very limited resources a lot can be done by motivated IT personnel, users and emergency managers that are aware of possible problems. The next sections present some of the simpler measures that can be taken to reach a higher level of reliability of IT systems in crisis situations.

Purpose

This set of guidelines is meant to help municipalities identify some of the weaknesses in the preparedness of their IT systems for crisis situations. Further it explains the importance of some simple measures that can be taken to better prepare the IT systems and the IT organisation for possible crises.

For a municipality as a whole to reach a higher level of dependability for its IT systems requires a focused IT strategy supported by an IT organisation that can efficiently handle these issues. Therefore the next section first deals with IT organisational issues. Then the next section focuses on how risk and vulnerability analyses can take IT dependability into account. The last section discusses some of the responsibilities of IT personnel that can contribute to a higher reliability of IT systems in crisis situations.

IT organisation

The position of IT personnel in the organisational structure of a municipality can differ a lot from one municipality to another. As IT systems have become more important, many municipalities have chosen to centralise their IT services to some degree. In some municipalities all IT personnel has been brought together in one IT organisation that serves all departments, and many IT services are shared with the whole organisation. In other municipalities some large departments like schools or health care services still have their own IT personnel with little cooperation between the different IT units.

The centralisation of IT services can have both positive and negative effects on the dependability of the IT systems. On the positive side, it becomes much easier to share critical resources such as backup servers or power generators that can increase the reliability of the IT systems, and all the technical knowledge of all the IT personnel becomes available to all departments. But on the negative side, centralisation usually decreases the personal contact between users and IT personnel, which makes it much harder for IT personnel to understand the needs of the users. This could lead to a situation where, although the IT systems might be technically more reliable, they do not fulfil the needs of the users as well.

No matter which organisational structure a municipality has, it is crucial for the treatment of dependability issues that the organisational structure reflects the increased importance of IT. IT has become so closely connected to all the responsibilities of a municipality that it should be an essential part of the strategy of a municipality. Most commercial companies have by now realised the importance of IT for their organisation and often the Chief Information Officer (CIO) or a similar function is part of the top management. Some municipalities on the other hand lack the organisational structure to lift strategical IT questions up to the highest level of the organisation. This is often the case when the highest level of management has not realised that IT is of much higher strategical importance than most other technical tools in an organisation.

Another important organisation issue is the relation between the IT unit and the rest of the organisation. The IT systems can be seen as an internal service from the IT unit to all other units within the municipality. At large companies the IT department often signs formal service level agreements (SLAs) with the other departments that specify the level of service offered. This formal way of working is probably too cumbersome for most Swedish municipalities, but the lack of any kind of discussion about the service level can lead to confusion about the level of service offered by the IT personnel. For example, when a crisis should occur outside the normal working hours, it can be very important to know if and how IT support can be reached at any time. Service level agreements offer a perfect forum to discuss these issues, but even if no formal agreements are written, it is important that the level of IT service is understood and agreed upon by both parties (users and the IT personnel) to avoid surprises in a critical situation.

Another important part of the relationship between the IT unit and the rest of the organisation is the division of responsibilities. Often there is confusion about who is the main responsible for a certain IT system, and especially who is responsible for issues such as reliability. Often users consider this a responsibility of the IT unit because they themselves do not have enough technical knowledge about the system. While the IT personnel on the other hand consider this a responsibility for the users, since they themselves do not have enough understanding of how the systems are supposed to be used. This results in the issues being neglected and never being

discussed. Therefore IT dependability requires that a main responsible is explicitly defined for every system and this person is responsible for collecting the necessary information from all involved parties to be able to judge if the system fulfils the necessary reliability requirements.

A final issue in the organisation of IT services is how the municipality deals with external suppliers of services and IT systems. With suppliers the writing of a clear service agreement is crucial. And the level of service ordered, should be in relation to how dependant an organisation is on the services or systems concerned. When this dependence on the systems changes the level of service should of course be re-evaluated.

Risk Analysis

This section focuses on the responsibilities of emergency managers (or other personnel in a municipality responsible for conducting risk and vulnerability analyses and making emergency plans) in ensuring IT dependability during crisis situations.

Emergency managers are in the best position to identify which of the municipality's many IT systems are most critical during different possible crisis situations. When making emergency plans and risk analyses the information flow is always a critical factor. The information flow often depends both on people and on a critical set of IT systems, which can be identified by going in detail over the emergency plans. For each of these systems it should be considered how critical they are under those situations. If the emergency managers are unsure of how much certain users depend on different IT systems, they should make sure this information is collected since it is an essential part of the emergency plan.

A second responsibility of the emergency managers is then to inform themselves with the IT personnel, with the suppliers of the systems or with some other experts, on the expected reliability of these systems under specific emergency conditions. The emergency managers probably do not have the detailed technical knowledge about the systems to make this judgement themselves. But requesting the information from people who could know is an important task of the emergency managers. With this information they can then decide if the reliability of the systems is sufficient for how critical the systems are.

If the reliability is thought to be insufficient the solution could be to make the systems more reliable or to make the systems less critical by making sure backup systems or other ways to reach the information are available.

In most municipalities emergency plans are made for a possible power blackout. It is easy to see that most IT systems will not function for a long time during a blackout unless a backup generator is available, and this is often reflected in many emergency plans. However, in many cases the emergency plans do mot take into account that there are many other reasons such as overload or software failures that could make an IT system fail. Software reliability is much more complex than power failures, and therefore it is important that experts with more IT knowledge are consulted to make the judgement on the reliability of a system.

An important part of this responsibility is to keep track of changes in the IT systems or in how the systems are used. In these cases the emergency plans need to be updated accordingly. For example a transition from analogue to IP telephony can have severe implication for the reliability of the phone system in different crisis situations. In this case the effects should preferably be studied before the transition is made, but also afterwards the effects have to be re-evaluated. In this particular example, a more detailed technical discussion of these issues can be found in a report published by PTS in 2005, available on their webpage.

IT support

This section focuses on some of the responsibilities of IT personnel in ensuring IT dependability during crisis situations. As discussed in the previous section, the IT personnel is in the best position to make a judgement on the reliability of the IT systems they service. For this purpose it is important that they take the time to collect detailed failure statistics about all failures they discover. This information is of very high value for making strategical IT decisions and for making any kind of risk analyses that include IT systems. For example information on how many hours per year the telephone system, the internal network or the public website of the municipality are inaccessible if important in crisis planning. For the same reason it can be very important to know from experience how long it actually takes to restore a computer or server from the last backup.

The IT personnel are also responsible for the maintenance of the IT systems during a crisis. In these situations, for example after a short power blackout when many systems have to be restarted, it is important to be able to effectively prioritise the maintenance work. This can only be done when the

priority of the systems has been agreed upon with the users before the crisis occurs. During the crisis it is often too late and it might be very hard for the IT personnel to know which systems need the most urgent attention.

Another important matter to consider for IT personnel is the criticality of the systems they do regular maintenance operations on. Often major updates are performed on evenings or in weekend to not disrupt the normal workflow of the municipality, but when a crisis occurs during these updates it is important that the operative personnel always have access to the necessary systems when they are called in on short notice. For example, the desktop computers of the administrative department can probably be taken offline for maintenance for a whole Saturday without disrupting any important work activities, but the computers of the emergency managers can be needed suddenly and unexpectedly on any given day or night.

The IT personnel are also the ones that can most easily keep track of the changes in the IT infrastructure. Usually the usage of IT is continuously increasing and with this the workload of the IT personnel increases also. It is important that the IT unit increases accordingly. Because often strategic work on software reliability is the first thing that is dropped when the workload becomes too high and all time is spent on solving problems that continuously pop up.

Conclusions

For a municipality to evaluate its dependence on its different IT systems requires a coordinated risk analysis, taking into account the effects of possible crises on those systems and an estimate of the reliability of these systems under crisis conditions. This risk analysis requires cooperation between the emergency managers, the users of the systems who know how dependent they are on the systems and the IT personnel who take care of the maintenance of the IT systems.

This document has presented a short list of relatively simple measures that can be taken to improve the software dependability at a municipality during a crisis. The measures are grouped in three areas: IT organisation, risk analysis and IT support. Many of the measures relate to improving the communication between users, emergency managers and IT personnel. This is absolutely the most critical factor. No single person has all the information required to judge if the dependability level is acceptable, but when a strong incentive can be created to discuss these with all involved parties, inconsistencies and shortcomings in the preparation for a crisis can be discovered more easily. This incentive can be created by the introduction of service level agreements, prioritisation of IT systems, or simply by appointing a clear responsible for these matters, but most effectively by a combination of many of the measures discussed in this document.

The practical implementation of these measures is not always an easy task and reaching a higher level of dependability is a slow process. When a municipality wants to make a coordinated approach to improve in this field it is important that one responsible is appointed to coordinate the whole process. It will be his task to agree on short and long term goals with all the different personnel involved and to follow up on how well these goals have been reached. For this purpose some useful process improvement models are available.

Recommended Reading

KBM has previously published a number of documents that are related to the issues discussed here:

- **Basnivå för informationssäkerhet (BITS)**, utgåva 3, KBM Rekommenderar, 2006
- **Kommunal sårbarhetsanalys**, Per-Olof Hallin, Jerry Nilsson, Nicklas Olofsson, KBM:s Forskningsserie, 2004
- **Samhällets krisberedskap - Inriktning för verksamheten 2007**, Planeringsprocessen 2005:3

Each of these documents is available for download on KBM's homepage::
http://www.krisberedskapsmyndigheten.se/

or can be ordered from them directly.

- Further a more detailed technical report on the same topic will soon be published by the same authors

Contact

Kim Weyns
kim.weyns@telecom.lth.se

Martin Höst
martin.host@telecom.lth.se

Per Runeson
per.runeson@telecom.lth.se

FRIVA
http://www.friva.lucram.lu.se/

FRIVA Psykologisk och teknisk beredskap gentemot extrema väderhändelser

Författare: Anders Bengtsson, Georg Lindgren

Inledning

Denna skrift är ett av flera informationsblad som redovisar sammanfattade erfarenheter och synpunkter från ramforskningsprogrammet FRIVA (Framework Programme for Risk and Vulnerability Analysis), vilket finansierats av Krisberedskapsmyndigheten under perioden mars 2004 till mars 2007. Informationsbladen skall kunna användas som utgångspunkter för praktiskt arbete när det gäller hantering av risker, sårbarheter, hot, kriser och katastrofer som medför eller kan medföra allvarliga samhälleliga konsekvenser.

Bakgrund och syfte

Denna vägledning är skriven med tanke på sådana konsekvenser för samhällsplaneringen och för samhällets beredskap som kan bli resultatet av klimatförändringar och andra förändrade förutsättningar. Exemplet med väderhändelser är valt med tanke på att det är konkret och aktuellt, men tankegångarna är inte begränsade till naturhändelser. Liknande problem uppstår naturligtvis varje gång villkoren för planeringen ändras. Som illustration till den allmänna problematiken har vi valt att beskriva behovet av balans mellan olika intressen i samband med översvämningsskydd, och jämfört med ett exempel på stormskadorna vid Gudrun-stormen.

Det regelverk som styr planeringen av samhällets beredskap mot tekniska kriser är baserat på långvarig erfarenhet. Ökad kunskap, t ex om ett miljögift, eller inträffade olyckor och incidenter, har ofta gett upphov till förändringar i regelverket. I idealfallet skyddar det tekniska regelverket samhället mot allvarliga kriser, och frågan kan uppstå om det finns en god balans mellan beredskapsnivån, uttryckt i olika slags kostnader, och de allvarliga skador som en kris kan orsaka.

Det finns all anledning att i en kommunal analys av samhällets känslighet för skadehändelser också inkludera en psykologisk beredskap inför de osäkerheter som alltid finns bakom icke-planerade händelser.

Klimatförändringar och långsiktig planering

Kunskapen om klimatförändringarnas effekter på samhällsplaneringen håller på att byggas upp, men mycket är ännu osäkert. Detta gäller de storskaliga effekterna såväl som de lokala, på ner till detaljerad kommunnivå. De kraftiga stormar och översvämningar, som inträffat de senaste åren kan tjäna som exempel. Stormarna har orsakat mycket allvarliga störningar i samhällsfunktionerna, större än man tidigare upplevt i liknande situationer.

Man skulle då kunna fråga sig vad som ligger bakom att störningarna av de inträffade stormarna blivit så allvarliga och vilka slutsatser man skall dra i det korta och i det långa perspektivet.

- Om det är så att förutsättningarna för verksamheten och beredskapen har ändrats som konsekvens av klimatförändringarna kan man behöva göra stora förändringar i rutiner och beredskapsplaner.
- Om det å andra sidan är förändrade samhällsstrukturer, försummat underhåll eller dålig planering, som gjort konsekvenserna så allvarliga, så blir åtgärderna naturligtvis annorlunda.

Psykologiskt är det en stor skillnad mellan de båda alternativen och behoven av kunskap olika. Den första punkten ryms inom den forskning som bedrivs eller planeras om klimatförändringarnas konsekvenser. Säkerheten i slutsatserna kan sannolikt graderas, kanske det också är möjligt att värdera kostnader för specifika åtgärder. Det är också väsentligt att de punkter markeras där slutsatserna är osäkra och ett tydligt handlingsalternativ inte direkt framträder.

En viktig fråga är hur länge den uppmärksamhet som klimatrisker just nu åtnjuter, håller i sig. Det finns många exempel på att minnet av tidigare kriser orsakade av naturhändelser bleknar och det senast inträffade tas som det normala. Den statistiska analysen av Gudrun-stormen visar t ex att skogsskadorna blev av en omfattning som

statistiskt sett bör kunna inträffa en gång på 80 år, vilket inte på något sätt kan sägas vara extremt – det är bara ovanligt! Förväntningarna på samhällets krisplanering är höga och kraven på väl underbyggda beslut stora. Det kollektiva minnet av det som tidigare generationer upplevt är en svårhanterlig ingrediens i krishanteringen, där ny, och ibland osäker, kunskap måste kombineras med tidigare erfarenheter.

Översvämning – ett historiskt Danskt exempel

Det pågår nu en intensiv planering inom många kommuner inför möjliga ökade översvämningsrisker, med åtföljande konsekvenser. Varje sådan planering kräver långsiktighet och uthållighet i avvägningar mellan olika intressen.

Exemplet handlar om skydd mot stormflod och högvatten vid danska västkusten omkring och i städerna Ribe och Tönder. De intressanta momenten är

- Bedömning av risker och konsekvenser av katastrof
- Avvägning av risker mellan olika verksamheter, jordbruk industri, stadssamhälle
- Psykologiska överväganden vid val av säkerhetsnivå rörande trygghet, kulturbevarande etc., samt risk för skada till liv och hälsa i förhållande till ekonomisk och social nytta.

Geografisk och historisk bakgrund

Längs Nordsjökusten finns större och mindre landområden, som vunnits från havet och som ligger så lågt att de är torra vid lågvatten och översvämmas vid högvatten. Områdena skyddas av vallar mot havet och omfattar i Sönderjylland drygt 30 000 ha. Syftet med invallningen, vilka påbörjades på 1500-talet, har i första hand varit att säkra odlingsmark, i andra hand att säkra bebyggelse. Kostnaderna har burits lantbefolkningen och inte av stadsborgarna. Det är först i sen tid som man tagit hänsyn till skydd av kulturvärden i Ribe, Danmarks äldsta stad, vilken varit drabbad av flera stora översvämningar.

De svåra stormfloder, som vållade omfattande katastrofer i Holland, England och Tyskland under 1950- och 60-talen berörde inte Danmark i någon större utsträckning. De satte emellertid igång ett noggrant utredningsarbete och en omfattande utbyggnad av vallskyddet.

Risk för katastrof

Med katastrof menas brott på en vall i samband med högvatten, vilket så gott som säkert leder till en stor översvämning och omfattande skador. Risken för översvämning beror självfallet på vallens tekniska kvalitet, höjd och profil. Dessa faktorer anses som kontrollerbara, även om vallens åldring inte helt kan förutses. De icke-kontrollerbara faktorerna som bestämmer risken är

- Tidvattensorsakat högvatten i kombination med storm
- Sådan vidstyrka och vindriktning att vallen eroderas
- Varaktigheten av storm

I utredningsarbetet studerade man historisk vattenståndsstatistik och beräknade de statistiska riskerna för de olika riskerna, och fick därmed fram säkerhetsgraden hos olika alternativ för utbyggnad av vallsystemet. Säkerhetsnivåerna anges som förväntade tiden mellan katastrofer, exempelvis 30 år, 100 år, etc. Man kan då betänka att om det i medeltal går 100 år mellan katastrofer så risken ett enskilt år ca 1 %, medan risken för katastrof minst en gång under de kommande 100 åren är ca 63 %. Utredningen föreslog en utbyggnad till en säkerhetsnivå på 200 år, vilket skall jämföras med säkerhetskraven i Holland, som ligger på 10 000 år.

Konsekvenser av katastrof

En överraskande översvämningskatastrof medför alltid risk för förlust av människoliv, I och med att man var beredd att acceptera en så låg nivå som 200 år accepterade man också tanken på att en katastrof kan uppstå. Man försökte därför också minimera risken för förlust av människoliv genom omfattande varningssystem. Därmed ansåg man det försvarbart att koncentrera konsekvensberäkningarna till de ekonomiska förlusterna.

För att få en ledtråd till valet av säkerhetsnivå jämförde man nyttan, beräknad som inbesparade ekonomiska förluster på grund av översvämning, och kostnaderna, d.v.s. kostnaden för investeringar och långsiktigt underhåll. Förhållandet mellan nytta och kostnad visade sig med detta räknesätt var fördelaktigt vid just 200 års säkerhet.

Riskpsykologi

Vad har de olika risknivåerna för innebörd för samhällets psykologiska beredskap? De säkerhetsnivåer, som figurerar i sammanhanget, d.v.s. 30-45 år för de gamla vallarna, 200 år för det nya förslaget

och 10 000 år för en ”säker” utbyggnad, har i hög grad olika innebörd, både vad gäller de teoretiska beräkningarna och för det dagliga livet.

Val av säkerhetsnivå

- *30-45 år:* De nu levande generationerna riskerar att drabbas, och måste anpassa sig till att leva med hög risk. Beräkningarna har god tillförlitlighet. Frekvensen av framtida katastrofer är så hög att det kan vara försvarbart att grunda beslut på kombinationen av sannolikhet och konsekvens. Huruvida risken accepteras av dem som utsätts för risken är en annan, men viktig, fråga.
- *200 år:* Risken för katastrof under nuvarande och nästa generation är inte försumbar; våra barn eller deras närmast efterkommande kan med stor sannolikhet komma att drabbas, och samhället måste upprätthålla en hög beredskap. De sannolikhetsteoretiska beräkningarna är på gränsen till tillförlitliga, men är dock grundade på erfarenhetsmaterial. Man kan säga att samhället försökt skaffa sig en respittid under vilken man hoppas hinna få säkrare underlag.
- *10 000 år:* Man har ”gjort allt i mänsklig makt” för att undvika katastrof, d.v.s. man har tagit hänsyn till allt man nu vet om riskerna. Man skulle vilja säga att systemet är helt säkert – under förutsättning att förhållandena är desamma i framtiden som nu. Tillförlitligheten i beräkningarna kan vara ganska hög, men bygger delvis på osäkra framtidsutsikter.

Ytterligare en faktor har naturligtvis påverkat de olika valen av säkerhetsnivå: i Danmark drabbas en ganska liten del av befolkningen som själva valt bosättningsort, medan i Holland är det landets existens som står på spel.

Avvägning mellan olika slags förluster

De förluster som är aktuella är de direkt ekonomiska, förluster av liv och hälsa samt förluster av kulturella värden.

Vad gäller *egendomsförluster* gjorde man en noggrann kalkyl över direkta skador och förlorade intäkter, men satte inget pris på förlorade människoliv. Inte heller studerade man alternativ användning av nedlagda resurser.

Liv och hälsa behandlades så att man, genom en omfattande säkerhetstjänst, innefattande ett avancerat hydrologiskt och statistiskt varningssystem, som skall kunna evakuera samtliga invånare i området. Detta förutsatte att ett sådant varningssystem fungerar tillfredsställande och utan alltför många felaktiga, falska eller uteblivna, larm. Det är svårt att uttala sig om allmänhetens förtroende för systemet när det inte satts på något ordentlig prov.

Kulturella värden finns huvudsakligen i den gamla staden Ribe. En allvarlig översvämning kommer att totalskada så gott som alla historiskt värdefulla byggnader där. Följande citat är hämtat från en specialstudie av situationen i Ribe:

> *Ribe kan ikka tåle en eneste alvorlig oversvømmelse. Spörgsmålet er ikke, hvor tit man kan affinde sig med, at den oversvømmes, men hvor lang en statistisk levetid man vil tilstå byen. … Det ægte, gamle Ribe ville under alle omstændigheder være gåed håblöst og definitivt tabt.*

Gudrun-exemplet – Stormskador på skog

De senaste årens stormarskador på skog belyser på ett tydligt sätt flera av de frågeställningar som tas upp ovan. Är dessa stormskador en konsekvens av en pågående klimatförändring eller är de en del av den naturliga variationen eventuellt i kombination med ett förändrat skogsbruk?

Stormen Gudrun, den 8-9 januari 2005, orsakade större stormskador på skog än någonsin tidigare i Sverige. Totalt 270 000 hektar skog, eller 70 Mm^3, skadades, huvudsakligen i Götaland. De omfattande skadorna resulterade också i sekundära skador på viktig infrastruktur som kraftnät, telekommunikationer, väg och järnvägsförbindelser. Detta ledde till en kraftig och bitvis ganska hätsk kritik kring hur framförallt elsäkerheten hanterats, och många röster höjdes för en omfattande och kostsam omläggning av elnätet från luftledningar till jordkabel.

Två år senare, den 14 januari 2007, drabbades i stort sett samma område av en ny storm, kallad Per, som orsakade skador på 12 Mm^3 skog. Också denna storm ledde till skador på elnätet, dock i betydligt mindre omfattningen än Gudrun. Kritiken från allmänheten mot nätbolagen uteblev i stort sett denna gång.

En sammanställning av tillgängligt material över rapporterade stormskador under de senaste dryga hundra åren visar på en kraftigt ökande trend både med avseende på storlek såväl som frekvens av rapporterade skogsskador. Osäkerheten kring de tidiga rapporterna är dock stor med brister både vad gällande omfattning och frekvens.

Resultaten från en statistisk extremvärdesanalys av stormskadorna i Sverige år 1965 till 2007 visar på att även om stormen Gudrun var extrem så kan stormskador av denna storleksordning förväntas inträffa i genomsnitt en gång var åttionde år utifrån periodens stormskadeklimat. I Tabell 1 ges de framräknade skadekvantilerna för risknivåerna 5, 10, 20 % och för tidsintervallen 1, 2 och 5 år. Analysen visar också att det inte finns någon tydlig och ökande trend varken för storleken på skadorna eller frekvensen under perioden, men eftersom antalet stora stormskador av naturliga skäl är litet så är osäkerheten i trendanalysen relativt stor.

Risk	1 year	2 years	5 years
20%	3.1	7.2	19
10%	7.7	16	42
5%	17	34	87

Tabell 1. Skadekvantiler (Mm^3) för olika tidsintervall beräknat utifrån rapporterade stormskador under perioden 1965 till 2007. Sannolikheten för att en stormskada överstigande 3.1 Mm^3 skall inträffa inom ett år är 20% osv.

Analysen visar också på att de svåraste stormskadorna har stor spridning. Ett exempel på detta är den beräknade medianen för nästa värsta stormskada, dvs. den stormskada som kommer att överträffa Gudrun. Medianen för en sådan skada är 140 Mm^3, dubbelt så mycket som Gudruns 70 Mm^3. Detta kan jämföras med de två hittills värsta stormskadorna, januari 2005 och novemberstormen 1969, där stormen år 2005 orsakade ungefär 2.5 gånger så stora skador som stormen 1969. Denna variabilitet för de extremaste skadorna kan också till en del förklara överraskningsmomentet i samband med Gudrun.

Redan utifrån dagens stormskadeklimat är alltså återkomsttiden för skador av Gudruns storlek så kort att sannolikhets- och konsekvensberäkningar har en tillförlitlighet som gör det möjligt att ta med dem i framtida beslut.

Kontakt

För mer information kontakta oss på följande e-post-adresser eller besök FRIVA:s hemsida.

Anders Bengtsson
ab@maths.lth.se

Georg Lindgren
georg@maths.lth.se

FRIVA
http://www.friva.lucram.lu.se/