Myndigheten för samhällsskydd och beredskap

Modellering och mätning avseende informationssäkerhet

En populärvetenskaplig sammanfattning av projektet COINS

FORSKNING

MSB:s kontaktpersoner:
Jan Byman, 010-240 43 76

Publikationsnummer MSB 334-2011
ISBN 978-91-7383-178-9

Förord

År 2007 utlyste Krisberedskapsmyndigheten (KBM) forskningsmedel inom området informationssäkerhet. Syftet med utlysningen var att stödja kunskapsutvecklingen kring problemställningar inom området. Baserat på utlysningen startades, under 2008, forskningsprojektet COntrolled INformation Security (COINS) som ett samarbete mellan Totalförsvarets forskningsinstitut (FOI) och Institutionen för data- och systemvetenskap (DSV) vid Stockholms universitet. Genomförandet av projektet har finansierats av KBM och, från och med 2009, Myndigheten för samhällsskydd och beredskap (MSB).

De som har deltagit i de genomförda studierna har en stor del i det resultat som presenteras i denna rapport. Projektgruppen vill därför tacka alla de som ställt upp på intervjuer, deltagit vid seminarier samt medverkat vid framtagandet av metriker.

Denna rapport presenterar en översikt av vad som har gjorts inom COINS. De rapporter som har producerats finns tillgängliga på hemsidorna www.foi.se/coins och https://secprj.dsv.su.se/coins.

Linköping, november 2011

Jonas Hallberg

Projektledare

Innehållsförteckning

Sammanfattning

Att uppnå en lämplig nivå avseende informationssäkerhet är en svår uppgift. Inom projektet COntrolled INformation Security (COINS) har ett antal modeller skapats. Syftet med modellerna är att visa hur informationssäkerhet kommuniceras inom organisationer. Från modellerna går det också att skapa en bild av arbetet med informationssäkerhet inom organisationer. För att utvärdera modellerna genomfördes dokumentstudier och ett flertal intervjuer vid en svensk myndighet. Baserat på modellerna genomfördes beräkningar som visar vilket fokus den studerade myndigheten har för sitt arbete med informationssäkerhet. Från intervjuerna drogs slutsatser om hur arbetet med informationssäkerhet på den studerade myndigheten utvecklades under projektets gång.

Utöver detta genomfördes även en studie av hur den nya standarden ISO/IEC 27004 kan användas för att bygga upp ett mätprogram. Standarden beskriver hur mätvärden för uppföljning av organisationens informationssäkerhetsprogram ska tas fram. Studien visade att metoden som presenteras i standarden fungerar bra. Dock krävs det att vissa egna tillägg och tolkningar görs innan metoden kan appliceras.

Slutligen togs det inom projektet fram ett ramverk som kan användas för att jämföra informationssäkerhetsarbetet mellan två organisationer. Detta ramverk är inte tänkt att användas för att visa vilken organisation som är ”bäst” utan är menat som en startpunkt för diskussion kring informationssäkerhetsfrågor mellan organisationerna.

1. Introduktion

Hur visar en organisation att den information den förvaltar hanteras på ett säkert sätt? Detta är en fråga som många organisationer ställer sig. För tillfället finns det inte några entydiga svar.

Frågan utgjorde grund för det forskningsprogram som skapades 2008 av dåvarande KBM, numera MSB, där forskningsprojektet COINS (COntrolled INformation Security) ingick som en del. COINS fokuserade på lärande om, förståelse för, samt styrning av informationssäkerhet.

Denna rapport är en populärvetenskaplig sammanfattning av några av de resultat som framkom inom projektet COINS. Projektet genomfördes som ett samarbete mellan Totalförsvarets forskningsinstitut (FOI) och Institutionen för data- och systemvetenskap (DSV) vid Stockholms universitet. Syftet med rapporten är att ge läsaren en sammanställning av vad som gjordes i projektet samt att locka till ytterligare läsning och dialog med de forskare som deltagit i COINS.

Inom projektet studerades hur modeller kan användas för att öka förståelsen för vad informationssäkerhet är. För att förankra modellerna i verkligheten inleddes ett samarbete med en svensk myndighet. Vidare studerades hur mätningar kan användas som ett verktyg för att utvärdera en organisations informationssäkerhetsarbete. Slutligen studerades hur jämförelse av informationssäkerhet mellan organisationer kan genomföras.

En mer ingående sammanfattning av projektets samtliga delar presenteras i projektets slutrapport[1]. Denna innehåller även referenser till alla publikationer som producerades under projektet.

I återstoden av rapporten presenteras:

- en kort sammanfattning av resultaten från den kvalitativa studien som genomfördes
- två av de modeller som togs fram inom projektet
- en studie av användbarheten hos standarden ISO/IEC 27004
- ett ramverk för jämförelse av organisationers informationssäkerhetsarbete
- kortfattade slutsatser från projektet.

[1] Slutrapporten *Controlled Information Security: Results and conclusions from the research project,* FOI-R--3187--SE, finns att hämta från www.foi.se

2. Kvalitativa analyser

Som en del i projektet genomfördes en fallstudie vars syfte var att utforska inställningen till informationssäkerhet vid den studerade myndigheten. Fallstudien bestod av en dokumentstudie samt tre omgångar med intervjuer. Under 2008 genomfördes tre intervjuer. Dessa följdes sedan upp med ytterligare tre intervjuer 2010 samt två intervjuer 2011.

De dokument som studerades var myndighetens informationssäkerhetspolicy samt dokument som var viktiga för myndighetens arbete med information. I fallstudien användes dokumenten för att skapa en förståelse för vilket stöd de anställda hade vid arbete med informationssäkerhet vid myndigheten.

Intervjuerna genomfördes med personer på olika befattningsnivåer vid myndigheten. Detta gav möjlighet att studera hur olika nivåer inom organisationen såg på informationssäkerhet. I följande avsnitt presenteras några av de observationer som gjordes under fallstudien.

2.1 Utbildningsmaterial

Vid intervjuerna 2008 framkom att myndigheten saknade material som beskrev hur informationssäkerhet skulle upprätthållas. Detta problem hade åtgärdats till 2010 genom att utbildningsmateriel hade tagits fram. Materialet uppskattades och blev efterfrågat av de anställda. Vid intervjuerna 2011 framkom även att detta material höll på att uppdateras.

2.2 Syn på informationssäkerhet

Ifrån 2008 års intervjuer framgick att den allmänna synen på informationssäkerhet var otydlig, enkelspårig och teknikfokuserad. Denna syn fanns till viss del kvar 2010 men nu talades det även om administrativ informationssäkerhet. 2011 var det igen huvudsakligen teknik som var i fokus. Skillnaden mot 2008 var att de intervjuade 2011 medvetet motiverade teknikfokuseringen med att myndighetens uppgifter i grunden är teknikorienterade. Ändringen i synsätt mellan 2008 och 2011 kan bero på att andelen teknik i informationssäkerhetsprogrammet var för hög 2008 och att en bättre balans mellan teknik och administration hade uppnåtts 2011, varpå myndigheten 2011 kunde arbeta med teknisk informationssäkerhet och vara medvetna om varför.

2.3 Fördelning av ansvar

Vid intervjuerna 2008 framkom det även att det inte fanns någon fördelning av ansvar mellan olika organisatoriska roller. Detta fortsatte i stort sett att gälla 2010 med undantag för små justeringar såsom att ansvar för uppdatering av intranätet fastslagits. Den omorganisation som genomfördes till 2011 hade mer djupgående inverkan på ansvarsfördelningen för olika roller. I den nya organisationen är roller mer väldefinierade med tydligare kopplingar till informationssäkerhetsarbete inom myndigheten.

3. Modeller

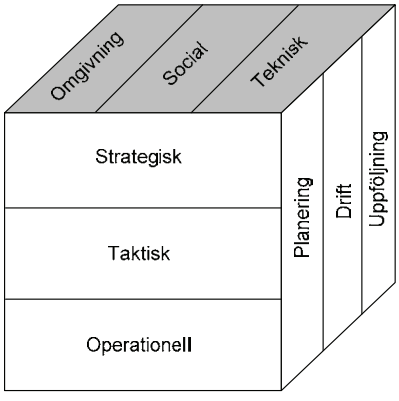
Inom ramen för COINS skapades flera modeller avseende hur informationssäkerhet kommuniceras inom organisationer. Från modellerna går det att ta fram en bild av hur väl arbetet med informationssäkerhet fungerar i en organisation. Nedan beskrivs två av dessa modeller samt hur de kan användas.

3.1 Kubmodellen med tolkningar och metriker

Kubmodellen skapades för att ge en kompakt men ändå förståelig bild av kommunikation avseende informationssäkerhet i en organisation. Kubens tre dimensioner är kopplade till *vad* som kommuniceras, *vilken organisatorisk nivå* kommunikation relaterar till samt *när i informationssäkerhetsprogrammets livscykel* kommunikationen troligen uppstår.

För att förenkla förklaringen av modellen illustreras i Figur 1 samtliga lager i kubmodellen. Vad som kommuniceras delas upp i kommunikation relaterad till tekniska aspekter, sociala aspekter samt kommunikation med omgivningen. De organisatoriska nivåerna representeras av de tre lagren strategisk, taktisk och operationell. Slutligen delas livscykeln upp i de tre delarna planering, drift och uppföljning.

Användning av kubmodellen utgår från en uppsättning utsagor. Detta kan exempelvis vara de krav som finns uppställda i en organisations informationssäkerhetspolicy. Genom att klassa en utsaga till att tillhöra ett av de tre lagren för varje dimension kopplas den till en av de 27 delkuber som tillsammans bildar hela kuben. När alla utsagor har placerats i kuben ger det en bild av det material som utsagorna hämtades från.



Figur 1: Kubmodellens olika lager.

Syftet med kubmodellen är att kunna identifiera eventuella luckor i en organisations informationssäkerhetsarbete. För att göra detta behövs en referenspunkt att jämföra med. Denna referenspunkt kan utgöras antingen av en förståelse hos den som analyserar resultatet eller en fastställd referens. Ett exempel på en sådan referens är de åtgärder för bättre informationssäkerhet som presenteras i standarden ISO/IEC 27001 appendix A. Genom att fylla kubmodellen med utsagor från ISO/IEC 27001 appendix A ges en bild av den referens organisationens arbete med informationssäkerhet kan jämföras mot.

3.2 Referensmodellen med tolkningar och metriker

Referensmodellen används för att jämföra beskrivningar av en organisations arbete med informationssäkerhet mot en given referens. Som referens vid jämförelser används appendix A ur standarden ISO/IEC 27001.

Innan en jämförelse kan genomföras måste det nuvarande arbetet med informationssäkerhet beskrivas i textform. Användning av referensmodellen inleds med att texten delas upp i ett antal utsagor, dvs. små delar som omfattar en eller några meningar. Utsagorna kopplas sedan till det eller de kapitel i bilaga A i standarden som bäst motsvarar utsagornas innehåll. Efter detta räknas antalet förekomster av 229 olika säkerhetsrelaterade termer för varje utsaga. Förekomsten av termerna i utsagorna som kopplats till respektive kapitel summeras sedan ihop. Därmed erhålls 11 värden, där varje värde representerar hur stor vikt som beskrivningen av arbetet med informationssäkerhet lägger på respektive kapitel i standarden.

Genom att använda referensmodellen till att räkna förekomsterna av ord i den standard som klassningen utgår från, kan referensvärden för varje kapitels relativa vikt räknas ut. Dessa referensvärden kan sedan jämföras med de värden som räknats fram för beskrivningen av arbetet med informationssäkerhet.

4. Metriker 27004

Den standard för skapande av ett ledningssystem för informationssäkerhet som för närvarande är gällande i Sverige, SS-ISO/IEC 27001, gavs ut 2005. I denna standard finns det ett krav på att effekten av de åtgärder som införs för att förbättra informationssäkerheten ska följas upp genom mätningar. Hur dessa mätningar ska genomföras fanns dock inte beskrivet förrän en ny standard, ISO/IEC 27004, gavs ut i slutet av 2009.

För att undersöka hur väl denna nya standard fungerar genomfördes under projektet ett försök där fem metriker skapades enligt metoden i ISO/IEC 27004. En metrik beskrivs i detta fall i ett dokument som i detalj redogör för hur mätningar ska genomföras, hur insamlad data ska sammanställas, hur sammanställningarna ska tolkas samt hur resultatet ska presenteras. Försöket genomfördes vid den svenska myndighet som studerades inom ramen för COINS. Metrikerna skapades med deltagande design genom att såväl de tilltänkta användarna som designers av metrikerna var med vid framtagandet.

Skapandet av metrikerna skedde i flera steg. Det första steget var att identifiera de åtgärder för bättre informationssäkerhet – tagna från bilaga A i standarden ISO/IEC 27001 – som skulle ligga till grund för metrikerna. Framtagandet av dessa utgick från en behovsanalys som tidigare genomförts inom projektet. Från denna analys kunde 25 relevanta åtgärder identifieras och från dessa 25 valdes de slutliga 5 ut av en representant från den studerade myndigheten. Denna representant identifierade även 4 personer som arbetade inom de valda områdena och som var villiga att delta i försöket.

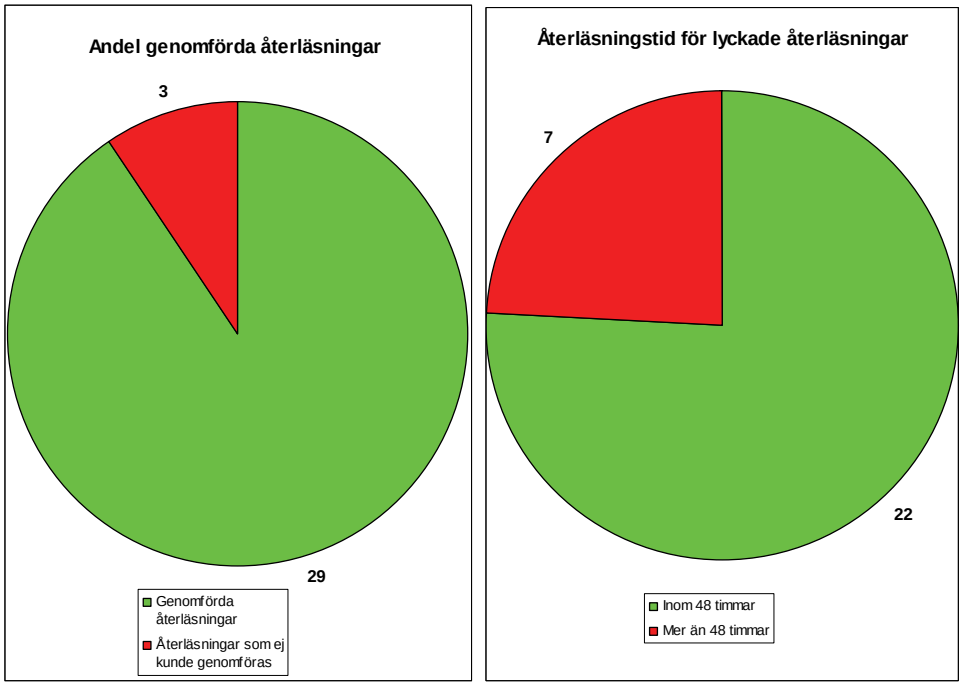
Framtagandet av metrikerna skedde med fokus på genomförbarhet och användbarhet. Detta innebar att metrikerna skulle kunna skapas på den korta tid som studien pågick och att de mätningar som skapades skulle ge ett resultat som var användbart för myndigheten.

Underlaget till metrikerna togs fram vid två omgångar med intervjuer. Vid den första omgången diskuterades vad som borde mätas och var data för dessa mätningar kunde hittas. Vid den andra omgången diskuterades hur olika möjliga mätresultat skulle tolkas och vilka åtgärder som skulle vidtas baserat på resultaten.

Mellan de två intervjuomgångarna strukturerades informationen från intervjuerna och förslag till möjliga tolkningar togs fram. Efter andra omgången intervjuer färdigställdes metrikerna.

När metrikerna var färdiga genomförde respondenterna de överenskomna mätningarna. Data från dessa mätningar

sammanställdes av forskargruppen till en uppsättning rapporter vilka skickades tillbaka till respondenterna.



Figur 2: Resultat för metriken relaterad till återläsningar.

Ett exempel på ett resultat från en av de framtagna metrikrapporterna visas i Figur 2. Mätningarna som gjordes handlade i detta fall om återläsning av säkerhetskopior.

Organisationen har ett krav på att det ska gå att återställa ett system från säkerhetskopior. Att detta inte alltid är möjligt beror troligast på att säkerhetskopian är skadad eller att det system som begärts återläsning för inte har anslutits till säkerhetskopieringstjänsten. Det vänstra diagrammet visar att 3 av 32 begärda återläsningar inte kunde genomföras under mätperioden.

För de återläsningar som genomförs sattes ett krav på att de skulle ske inom 48 timmar. Det högra diagrammet visar att 7 av de 29 återläsningar som genomfördes, tog längre tid att göra än gränsvärdet 48 timmar. Den åtgärd som är kopplad till detta resultat säger att en undersökning av skälen till att återläsningarna tog för lång tid ska genomföras.

Några av de slutsatser som framkom i försöket presenteras i kapitel 6.

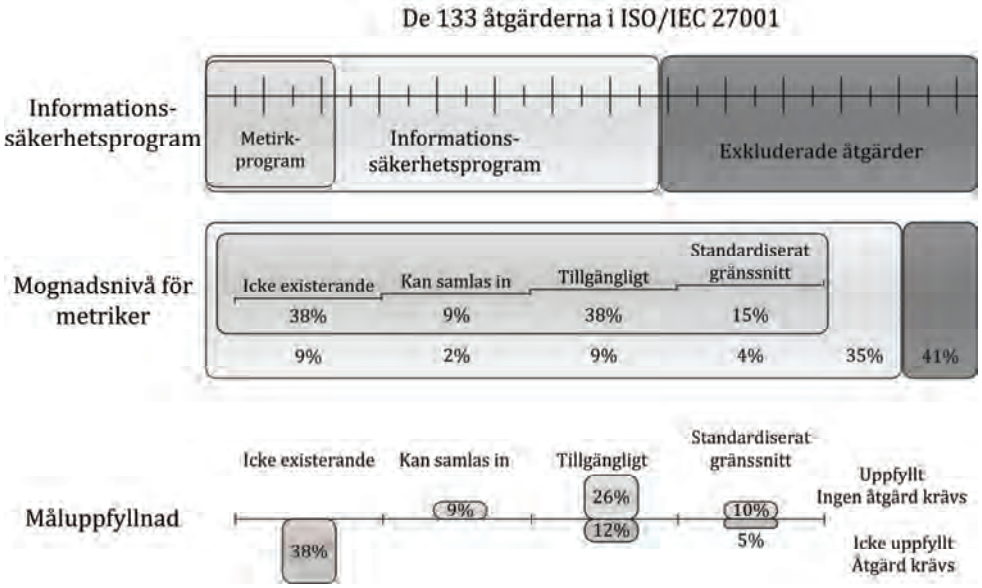
5. Ramverk för jämförelse mellan organisationer

För att ge stöd åt svenska myndigheter i uppföljningen av deras arbete med informationssäkerhet togs ett ramverk för visualisering av informationssäkerhet fram. Ramverket kan användas för att se hur en organisation utvecklar sitt informationssäkerhetsprogram över tiden. Det kan även användas för att jämföra två organisationers arbete med informationssäkerhet.

Ramverket består av tre faser. Ett exempel på hur det skulle kunna se ut då ramverket används visas i Figur 3. Exemplet i figuren är inte taget från verkligheten utan siffrorna är valda för att illustrera hela ramverket.

Utgångspunkten för ramverket är de 133 åtgärder som återfinns i appendix A av standarden ISO/IEC 27001. Dessa åtgärder är den gemensamma grund som används för jämförelser mellan organisationer ska vara möjlig.

I den första fasen fokuseras det på omfattningen på organisationens säkerhetsprogram. Här visas hur stor andel av de åtgärder en organisation anser är nödvändiga som faktiskt kontrolleras med mätningar. Det översta diagrammet i Figur 3 visar hur stor andel av de 133 åtgärderna som organisationen valt att ta med i, samt exkludera ur, sitt säkerhetsprogram. Vidare visar diagrammet också hur stor andel av de åtgärder som valts att ta med som följs upp regelbundet genom ett metrikprogram av den typ som beskrevs i kapitel 4.



Figur 3: Ramverk för illustration av informationssäkerhet.

Ramverkets andra fas handlar om hur mogna de gjorda mätningarna avseende informationssäkerhet är. Detta visas i det mittersta diagrammet i Figur 3. För att ta fram diagrammet måste alla metriker som används för att göra mätningarna klassas utifrån hur lätt det är att få tag på data som metrikerna behöver. Tillgången på data till mätningarna är det som anges på trappstegen diagrammet. De procentsiffror som syns inom området med trappstegen visar hur metrikprogrammet är fördelat över mognadsgraderna. De procentsiffror som finns under dessa, utanför rutan med trappan, visar hur mognadsgraderna förhåller sig till hela informationssäkerhetsprogrammet.

Den sista fasen i ramverket handlar om hur stor andel av de mätningar som genomförs som uppnår de mål som har satts för mätningarna. Detta illustreras av det nedersta diagrammet i Figur 3. Procentsiffrorna i detta diagram visar fördelningen för de åtgärder som det finns metriker till.

Som nämndes i början av kapitlet kan ramverket användas för att visa hur en organisation utvecklar sitt informationssäkerhetsprogram över tiden. Detta kan göras genom att skapa en bild lik den i Figur 3 exempelvis för varje månad och sedan jämföra den med tidigare månader. På detta sätt kan organisationen se hur informationssäkerhetsprogrammet utvecklas.

För att jämföra två organisationer skapas först en bild av respektive organisation. En direkt jämförelse av bilderna ger en förståelse för vilken organisation som genomför flest mätningar samt hur mogna dessa mätningar är. Jämförelsen som ramverket tillhandahåller är på en mycket övergripande nivå. Detta är ett avsiktligt designval för att bilderna ska kunna användas utan att avslöja vilka informationssäkerhetsområden som för tillfället håller på att förbättras.

Den största nyttan med ramverket vid jämförelse mellan organisationer är inte att se vilken organisation som är ”bäst”. Nyttan utgörs av att ramverket ger en startpunkt för en diskussion mellan informationssäkerhetsansvariga vid olika organisationer. Hur detta skulle kunna gå till presenteras i slutsatserna i kapitel 6.

6. Slutsatser

Från projektet som helhet kan det konstateras att det är svårt att ta fram modeller som på ett tydligt sätt beskriver hur informationssäkerhet kommuniceras inom organisationer. Det är också svårt att mäta informationssäkerhet på en övergripande nivå. En orsak är att såväl information som säkerhet är abstrakta begrepp. Vidare anses ofta säkerhet vara ett nödvändigt ont som måste hanteras medan det ”riktiga” arbetet utförs.

I den kvalitativa studien framkom det att de manualer för informationssäkerhet som tagits fram på myndigheten blev efterfrågade av de anställda när de väl fanns tillgängliga. Detta tyder på att personalen har behov av att veta vad som förväntas av dem samt hur saker ska göras för att det ska ske på ett säkert sätt. Vidare visar det att personalen gärna tar eget ansvar för sin kunskap inom området, bara möjligheter för detta ges.

Det framkom också att ansvarsfördelningen för informationssäkerhet är ett område som behöver klargöras. På den studerade myndigheten ledde en omorganisering till en förbättring. I den nya organisationen gavs de anställda, som hanterade informationssäkerhetsfrågor, befogenhet och ansvar som motsvarade deras arbetsuppgifter.

Från metrikstudien som presenterades i kapitel 4 drogs slutsatsen att den metod som beskrivs i standarden ISO/IEC 27004 kan användas för att ta fram användbara metriker. Dock är standarden inte heltäckande i sin beskrivning av vad som ska göras vilket leder till att en del egna tolkningar behövs.

Resultatet från mätningarna med metrikerna visade att enkla mätningar kan ge värdefulla resultat. De mätningar som genomfördes gick huvudsakligen ut på att sammanställa och visualisera lättillgänglig data. Trots detta fanns det resultat som förvånade mottagaren och som ledde till att omedelbara åtgärder vidtogs.

Det ramverk för jämförelse som togs fram inom projektet är, som nämndes i kapitel 5, inte tänkt att användas för att se om en organisation är bättre än en annan. Ramverket ska istället användas som en startpunkt för diskussion, där en organisation med hög mognadsgrad kan stödja en med lägre om vilka steg som togs för att uppnå den högre nivån. Ett annat exempel är att två likvärdiga organisationer diskuterar, med mer ingående detaljer, vad de har valt att inkludera i säkerhetsprogrammet och vad som är mest relevant att mäta. Det viktiga är att diskussionerna leder till erfarenhetsutbyte och utveckling inom den egna organisationen

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB 334-2011 ISBN 978-91-7383-178-9