Myndigheten för
samhällsskydd
och beredskap

Vägledning för säker och robust samverkan

Vägledning för säker och robust samverkan

VERSION 1.0

Vägledning för säker och robust samverkan

Myndigheten för samhällsskydd och beredskap (MSB)

Avdelningen för utveckling av beredskap

Illustrationer: Martin Ek
Produktion: Advant Produktionsbyrå

Publikationsnummer: MSB1285 - november 2018
ISBN: 978-91-7383-881-8

Innehåll

Vägledningen

Vägledningen

Syfte

Vägledningen är ett stöd till dig som behöver hjälp att välja verktyg för säker och robust samverkan. Vägledningen beskriver, på en övergripande nivå, vad säker och robust samverkan omfattar och varför dessa aspekter är viktiga.

Vägledningen fungerar som ett stöd när din organisation ska identifiera vilka verktyg som ni ska använda utifrån era behov av säker och robust samverkan.

Vägledningen syftar också till att vara ett underlag att använda i diskussioner med de ni samverkar med för att tillsammans komma fram till vilka verktyg ni behöver använda för att uppnå säker och robust samverkan. Matrisen i vägledningen ger en förenklad bild av hur olika verktyg förhåller sig till varandra. Tanken med matrisen är att den ska kunna fungera som underlag till diskussion om vilka verktyg som är lämpliga i aktörgemensam samverkan utifrån aspekterna robusthet och sekretess.

För att kunna fatta beslut om vilket verktyg som ska användas för aktörsgemensam samverkan måste respektive aktör först ha gjort en analys över sitt eget ansvar, sina samverkansbehov, vilken information som ska delas i samverkan och hur skyddsvärd den informationen är.

Målgrupp

Alla aktörer som har ett ansvar vid en samhällsstörning och som behöver stöd i valet av verktyg för säker och robust samverkan kan använda denna vägledning.

Geografiskt områdesansvariga aktörer på nationell och regional nivå (MSB respektive länsstyrelserna) bör ha ett särskilt ansvar i att avgöra val av verktyg för samverkan och informera om desamma vid olika typer av händelser beroende på vilken typ av händelse som hanteras och hur skyddsvärd informationen är som ska delas.

Definitioner och avgränsningar

I vägledningen betyder begreppet ”verktyg” en tjänst, funktion eller applikation som en aktör kan nyttja. Ordet ”aktör” är en formell organisation, antingen offentlig, privat eller ideell, eller ett spontant socialt nätverk, som har betydelse för hanteringen av samhällsstörningar. ”Samverkan” betyder att aktörer åstadkommer inriktning och samordning av tillgängliga resurser genom att komma överens. Begreppet ”aktörsgemensam samverkan” betyder samverkan över organisationsgränser, i kontrast till aktörsintern.[1]

Vägledningen omfattar endast verktyg som tillhandahålls av MSB och som bygger på elektroniska kommunikationer. Några av verktygen i denna vägledning har en begränsad användarkrets vilket innebär att de endast kan användas av vissa organisationer. I kapitlet ”Verktyg för säker och robust samverkan” finns övergripande information om respektive verktyg och vilka som kan använda dem.

1. Definitionerna kommer från *”Gemensamma grunder för samverkan och ledning vid samhällsstörningar”* MSB ISBN-nummer: 978-91-7383-507-7.

Vikten av att samverkan är säker och robust

Vikten av att samverkan är säker och robust

Det är viktigt att din organisation är förberedd att kunna hantera händelser när de inträffar. För detta krävs att din organisation kan samverka och leda, att ni är utbildade och övade, att ni har väl fungerande metoder och att ni har tekniska stödsystem som fungerar. Er möjlighet till samverkan och ledning måste även finnas under störda förhållanden där till exempel system för elförsörjning och elektroniska kommunikationer är starkt negativt påverkade. Detta ställer krav på att de kommunikationsverktyg ni avser att använda är robusta och fungerar utan avbrott även i en störd miljö och att informationen hanteras på rätt sätt beaktande av sekretess.

Det är viktigt att ni i förväg tar ställning till vilka verktyg som ska användas vid aktörsgemensam samverkan så att detta fungerar när en händelse inträffar. Det är även bra att ha en plan för redundans vid bortfall av något av de verktyg som behövs vid samverkan.

En kedja är inte starkare än sin svagaste länk

För att uppnå säker och robust samverkan är det viktigt att förstå hela kedjan i informationsdelningen. Det räcker inte att använda ett verktyg i denna vägledning för att säkerställa att samverkan kan ske säkert och robust utan ni måste se över alla ingående delar för att säkerställa att de håller lämplig nivå. Det handlar till exempel om att införa och förvalta administrativa regelverk så som policys och riktlinjer, tekniskt skydd med bland annat brandväggar och kryptering samt fysiskt skydd med till exempel skal- och brandskydd. Det krävs även både kunskap och utbildning för de personer som ska delta i informationsdelningen. En säker och robust samverkan förutsätter att det ställs krav på alla länkar i kedjan.

Innan val av verktyg för samverkan

Innan val av verktyg för samverkan

För att välja rätt verktyg för säker och robust samverkan måste respektive aktör först svara på vilka ni ska samverka med och om den information ni ska dela med andra är skyddsvärd.

Vilka ska ni samverka med?

I *"Gemensamma grunder för samverkan och ledning vid samhällsstörningar"*[2] finns hjälp om hur varje aktör kan ta reda på sitt behov av samverkan och hur denna samverkan bör gå till. Det är viktigt att respektive aktör utgår från den "helhetssyn" som beskrivs i *"Gemensamma grunder för samverkan och ledning vid samhällsstörningar"*. Helhetssynen är ett förhållningssätt som stöder aktörer i att använda samhällets resurser så effektivt som möjligt.

I vägledningen *"Rätt person på rätt plats – Vägledning för myndigheters arbete med krigsorganisation och krigsplacering"*[3] finns stöd i hur ni kan analysera din organisations ansvar under höjd beredskap och ta fram en krigsorganisation. Vägledningen riktar sig specifikt till myndigheter men går även att använda av andra aktörer. Genom arbetet med att ta fram en krigsorganisation planerar ni för vilka delar av verksamheten som ska bedrivas vid höjd beredskap och hur verksamheten behöver anpassas för att fungera.

Det är även viktigt att respektive aktör tar ställning till hur ofta ni ska dela information med andra, hur tidskritisk den är och vilken typ av information som ska delas (bild, text eller tal) då detta också påverkar val av verktyg.

Läs mer på www.msb.se.

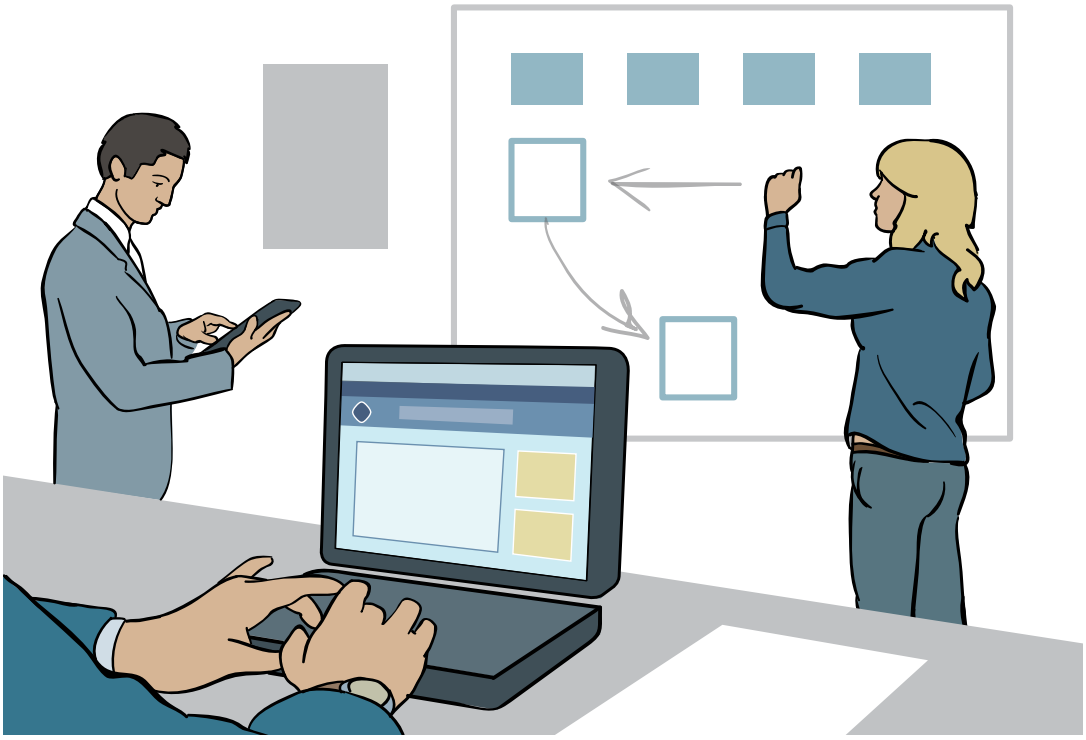
2. *"Gemensamma grunder för samverkan och ledning vid samhällsstörningar"* MSB ISBN-nummer: 978-91-7383-507-7.
3. *"Rätt person på rätt plats – Vägledning för myndigheters arbete med krigsorganisation och krigsplacering"*, MSB ISBN-nummer: 978-91-7383-807-8.

Hur skyddsvärd är informationen ni delar med andra?

Information är värdefullt och behöver skyddas efter behov. Ett bra informationssäkerhetsarbete som utgår från etablerade standarder är en förutsättning för effektiv och korrekt informationshantering så väl i vardagen som i en krissituation. Detta skapar förtroende både inom och utanför organisationen. Det är viktigt att informationen som delas i samverkan med andra är klassad utifrån vilket skyddsvärde informationen har och att ni väljer rätt verktyg som motsvarar den klassning ni gjort.

MSB:s metodstöd för systematiskt informationssäkerhetsarbete riktar sig till dig som arbetar med informationssäkerhet i en organisation, oavsett verksamhetsområde och storlek på organisation. Metodstödet ska kunna användas om din organisation står i startgroparna för att införa det systematiska arbetssättet men också om din organisation redan har mycket på plats. Metodstödet bygger på standarden ”*SS-EN ISO/IEC 27001 Ledningssystem för informationssäkerhet*”. En del i metodstödet handlar om att göra en klassning av organisationens informationstillgångar utifrån den konsekvens otillräckligt skydd ger. Därefter kan ni besluta om vilka skyddsåtgärder som behöver göras, exempelvis vilka verktyg som ska användas.

Läs mer på www.informationssäkerhet.se.



Robust samverkan

Robust samverkan

Begreppet ”robust” går att definiera på många olika sätt och kan omfatta krav på exempelvis tillgänglighet, uthållighet, redundans och reservkraft. Den gemensamma nämnaren är att robusthet handlar om förmågan att motstå störningar och avbrott.

AVBROTTSTIDER VID STÖRNING

	Avbrottstid	FOI:s typfall
1	El- och telenät drabbas av avbrott i upp till tre timmar (<3 h).	Inget typfall beskriver denna situation, detta är normalläge.
2	El- och telenät drabbas av avbrott i upp till 24 timmar (<24 h).	**Typfall 5:** Utdragen och eskalerande gråzonsproblematik (ej höjd beredskap).
3	El- och telenät drabbas av avbrott i upp till 7 dagar (<7 dagar).	**Typfall 3:** Angrepp med fjärrstridsmedel m.m., huvudsakligen mot militära mål. **Typfall 2:** Angrepp med fjärrstridsmedel m.m., huvudsakligen mot civila mål. **Typfall 5:** Utdragen och eskalerande gråzonsproblematik (ej höjd beredskap).
4	El- och telenät är utslagna i 3 månader.	**Typfall 4:** Angrepp som omfattar landstigning och luftlandsättning mot viktiga områden i Sverige.

I tabellen finns en eskalerande skala över de störningar som kan pröva robustheten eller motståndskraften i elektronisk kommunikation. I matrisen på sida 19 används skalan för att kategorisera de olika verktygens motståndskraft mot störning. De angivna avbrottstiderna återfinns i *”Vägledning för samhällsviktig verksamhet: att identifiera samhällsviktig verksamhet och kritiska beroenden samt bedöma acceptabel avbrottstid”*[4], Post- och telestyrelsens, nedan PTS, föreskrifter (PTSFS 2015:2) om krav på driftsäkerhet[5] samt Försvarsberedningens rapport *”Motståndskraft – Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025”*.[6]

För att få en uppfattning om vilka omständigheter dessa avbrott kan uppstå under finns hänvisning till FOI:s typfall i *”Hotbildsunderlag i utvecklingen av civilt försvar”* och *”Typfall 5: Utdragen och eskalerande gråzonsproblematik”*[7].

4. *”Vägledning för samhällsviktig verksamhet: att identifiera samhällsviktig verksamhet och kritiska beroenden samt bedöma acceptabel avbrottstid”* MSB ISBN-nummer: 978-91-7383-392-9.
5. Post- och telestyrelsens föreskrifter om krav på driftsäkerhet (PTSFS 2015:2).
6. *”Motståndskraft – Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025”*, Ds 2017:66.
7. *”Hotbildsunderlag i utvecklingen av civilt försvar”* FOI Memo 5089 och *”Typfall 5: Utdragen och eskalerande gråzonsproblematik”* FOI Memo 6338.

Säker samverkan

Säker samverkan

Säker samverkan innebär att den information som delas med andra aktörer inte röjs till obehöriga. Vägledningen omfattar från helt öppen information till uppgifter som rör rikets säkerhet.

SKYDDSNIVÅ FÖR INFORMATION			
0	**Ingen skyddsnivå** Förlust av information medför inte någon negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	4	**Begränsat hemlig** Ringa skada för Sveriges säkerhet kan uppstå om uppgifterna röjs.
1	**Grundläggande skyddsnivå** Förlust av information innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	5	**Konfidentiell** Inte en obetydlig skada för Sveriges säkerhet kan uppstå om uppgifterna röjs.
2	**Utökad skyddsnivå** Förlust av information innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	6	**Hemlig** Allvarlig skada för Sveriges säkerhet kan uppstå om uppgifterna röjs.
3	**Hög skyddsnivå** Förlust av information innebär allvarlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	7	**Kvalificerat hemlig** Synnerligen allvarlig skada för Sveriges säkerhet kan uppstå om uppgifterna röjs.

I Offentlighets- och sekretesslagen (2009:400), nedan OSL, finns särskilda bestämmelser om sekretess till skydd för uppgifter som rör rikets säkerhet. Om uppgifter omfattas av OSL och rör rikets säkerhet är de hemliga uppgifter enligt säkerhetsskyddsförordningen (1996:633).[8] Hemliga uppgifter ska enligt säkerhetsskyddslagen (1996:627) ges ett säkerhetsskydd.[9] I den nya säkerhetsskyddslagen (2018:585), som träder i kraft 1 april 2019, ställs det upp krav på säkerhetsklassning av sådana uppgifter.[10] Hemliga uppgifter måste hanteras på ett särskilt sätt och får krypteras endast med kryptosystem som har godkänts av Försvarsmakten[11], så kallade signalskyddsystem.

Som ett stöd för aktörer att hantera hemliga uppgifter så kommer MSB under 2018 att publicera tre vägledningar. Dessa avser hantering av hemliga uppgifter i digitalt format, vad man ska tänka på vid upprättande av en dator för bearbetning av hemliga uppgifter samt vägledning kring att bygga fysiska rum för muntlig delgivning av hemliga uppgifter.

Nivå 0, 1, 2 och 3 i tabellen handlar om att informationen som delas är skyddsvärd utifrån aspekterna riktighet, tillgänglighet och konfidentialitet. Sådan information behöver inte omfattas av sekretess men kan likväl vara skyddsvärd ur ett informationssäkerhetsperspektiv. Dessa omfattar inte information som rör rikets säkerhet. Nivåindelningen kommer från MSB:s metodstöd för systematiskt informationssäkerhetsarbete.

Nivå 4, 5, 6 och 7 i tabellen omfattar uppgifter kopplade till rikets säkerhet och utgår från säkerhetsskyddsklasserna enligt den nya säkerhetsskyddslagen. Läs mer om samverkan som omfattar uppgifter som rör rikets säkerhet i kapitlet *”Signalskyddssystem godkända av Försvarsmakten”*.

8. Se 4 § första stycket punkten 1 säkerhetsskyddsförordningen.
9. Se 5 och 6 §§ säkerhetsskyddslagen.
10. Se 2 kap. 5 § i nya säkerhetsskyddslagen.
11. Se 9–13 §§ i säkerhetsskyddsförordningen.

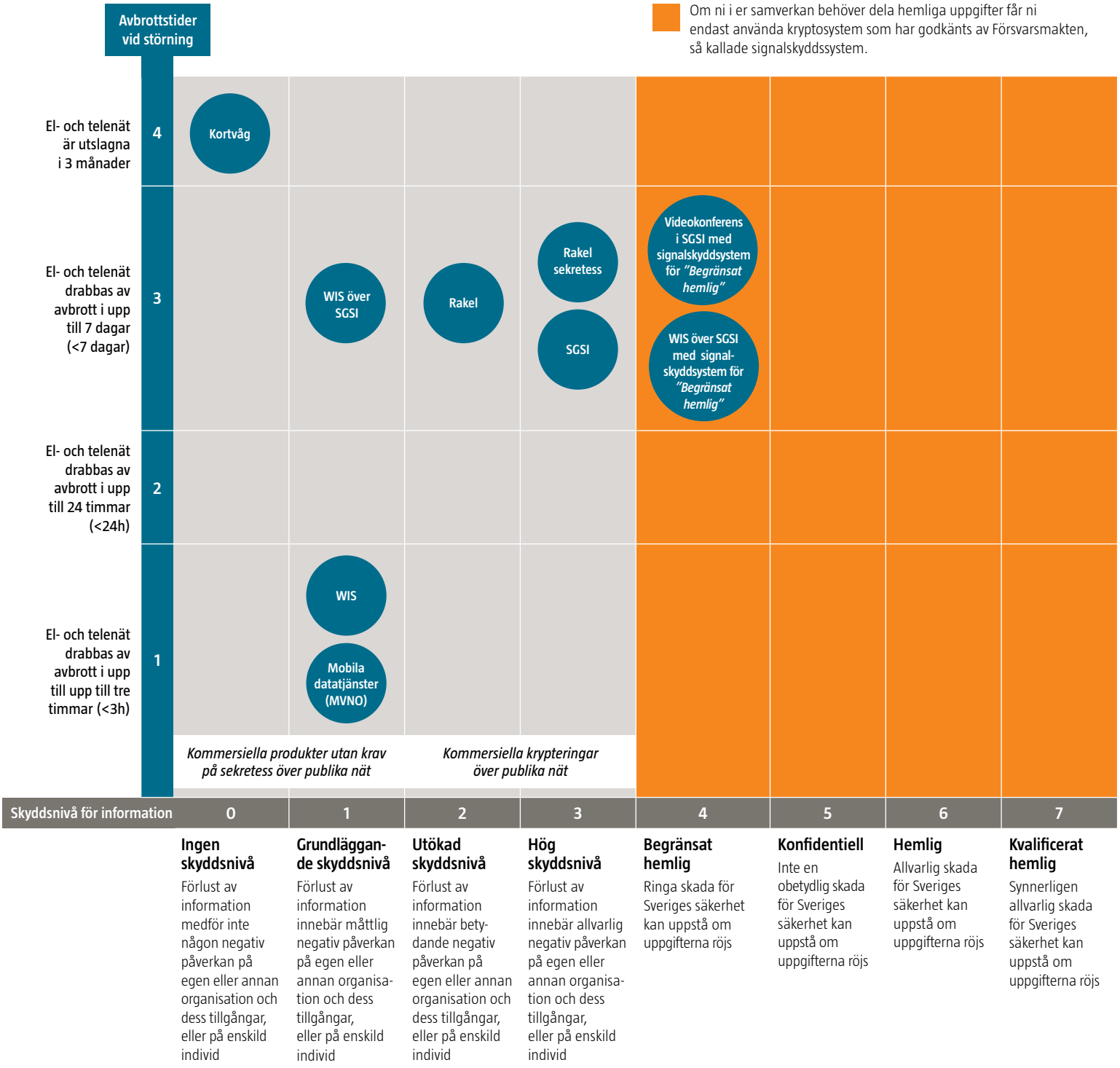
Matris med verktyg för säker och robust samverkan

Matris med verktyg för säker och robust samverkan

Matrisen nedan visar hur olika verktyg förhåller sig till varandra utifrån aspekterna robusthet och sekretess.

Matrisen kan vara ett underlag i diskussioner med de ni samverkar med för att tillsammans komma fram till vilka verktyg ni behöver använda för att uppnå säker och robust samverkan.

Matrisen innehåller de verktyg som MSB tillhandahåller idag eller kommer att tillhandahålla under 2019.



Verktyg för säker och robust samverkan

Verktyg för säker och robust samverkan

Kapitlet innehåller de verktyg som MSB tillhandahåller idag eller kommer att tillhandahålla under 2019. Alla verktygen finns i matrisen i kapitlet *”Matris med verktyg för säker och robust samverkan”*.

Rakel

Rakel är ett kommunikationssystem för trygg och säker kommunikation mellan medarbetare inom samhällsviktiga verksamheter. Med Rakel går det att tala i gruppsamtal, individuella samtal mellan två personer, ringa och ta emot samtal från det vanliga telefonnätet, göra nödsamtal som går direkt till lednings- eller larmcentral, sända information om position, sända textmeddelanden, ta emot och sända filer och data, som till exempel medicinska data som EKG och komma åt databaser som körkortsregister. Det går även att sköta tekniska funktioner med Rakel som till exempel att öppna portar, sätta på/stänga av och övervaka driften av tekniska system till exempel för el-, vatten-, och värmeförsörjning. Vid elavbrott finns reservkraft för upp till sju dagar. Rakelsystemet täcker 99,84 procent av Sveriges befolkning och 95 procent av landets yta, undantaget fjällvärlden.

I framtiden kommer Rakel att förstärkas och kompletteras med ny teknik för ökad datakapacitet.

VILKA FÅR ANVÄNDA RAKEL?

Rakel har en begränsad användarkrets som omfattar aktörer inom allmän ordning, säkerhet och hälsa.

Rakel sekretess

Tilläggstjänsten ”Rakel sekretess” gör det möjligt att kommunicera information med en hög skyddsnivå i det robusta Rakelnätet. Tjänsten ska lanseras under 2019.

VILKA FÅR ANVÄNDA RAKEL FÖRSTÄRKT SÄKERHET?

Tjänsten har samma användarkrets som Rakel.

Rakel kompletteras med mobila datatjänster

Genom ett samarbete mellan MSB och Trafikverket kommer Rakel kompletteras med en lösning för mobila datatjänster som exempelvis bild- och dataöverföring. Tekniken innebär att man skapar en mobiloperatör utan ett eget radionät och gör det möjligt att överföra data via kommersiella nät. Tjänsten ska lanseras under 2019.

Eftersom lösningen använder publika nät bör detta verktyg endast användas till sådan samverkan som inte är verksamhetskritisk.

Lösningen är en brygglösning i väntan på ett beslut om en framtida kommunikationslösning som fullt ut tillgodoser aktörernas behov och krav gällande robusthet, tillgänglighet, säkerhet och sekretess.

VILKA FÅR ANVÄNDA LÖSNINGEN?

Lösningen ska inledningsvis kunna användas av statliga myndigheter som är anslutna till SGSI. MSB arbetar långsiktigt med att få till stånd en lagändring för att på sikt kunna erbjuda denna lösning till hela Rakels användarkrets.

SGSI

SGSI (Swedish Government Secure Intranet) är ett intranät, skiljt från internet, för säker och krypterad kommunikation mellan myndigheter i Sverige och i Europa. Nätet är utformat för att klara höga krav på tillgänglighet och driftsäkerhet. Med SGSI kan man få åtkomst till andra anslutna myndigheters databaser, skicka skyddad e-post och ha videokonferenser. För att få ansluta sig till SGSI ställs höga krav på IT-säkerheten. Syftet är att skapa tillit och förtroende mellan de myndigheter som utbyter skyddsvärd information.

VILKA FÅR ANVÄNDA SGSI?

SGSI får endast användas av myndigheter som uppfyller gemensamt framtagna säkerhetskrav. En ackreditering krävs för att en myndighet ska få ansluta sig till SGSI.

Videokonferens i SGSI med signalskyddsystem för ”Begränsat hemlig”

MSB utvecklar en videokonferenstjänst i SGSI där skyddet möjliggör hantering av sekretess upp till och med informationssäkerhetsklass ”Begränsat hemlig”. Tjänsten ska lanseras under 2019.

VILKA FÅR ANVÄNDA VIDEOKONFERENS VIA SGSI MED SIGNALSKYDDSYSTEM FÖR ”BEGRÄNSAT HEMLIG”?

Videokonferens i SGSI med signalskyddssystem för ”Begränsat hemlig” får endast användas av myndigheter som är berättigade att använda SGSI och som är godkända att hantera signalskyddssystem för ”Begränsat hemlig”. Detta ställer bland annat krav avseende skalskydd, tillträdeskontroll, registerkontroll med mera.

WIS

WIS är ett nationellt webbaserat informationssystem som underlättar för aktörer att dela information före, under och efter samhällsstörningar. Alla inblandade ska enkelt och effektivt kunna skapa sig en samlad lägesbild, genom att aktivt dela information. Varje aktör äger sin egen information och väljer själv vilka man vill dela den med. Det går bra att använda WIS för att dela information enbart inom egen organisation. WIS går över internet.

VILKA FÅR ANVÄNDA WIS?

Myndigheter, kommuner, landsting, frivilligorganisationer och privata aktörer med ansvar under en kris får använda WIS.

WIS över SGSI

Under normala förhållanden fungerar internet utmärkt för den typ av informationsdelning som sker i WIS. Under störda förhållanden behöver alternativa accessvägar vara tillgängliga. WIS över SGSI ökar möjligheterna till informationsdelning och upprätthållande av lägesbilder under störda förhållanden. Tjänsten ska lanseras under 2019.

VILKA FÅR ANVÄNDA WIS ÖVER SGSI?

De WIS-användare som även är berättigade att använda SGSI kan använda denna lösning.

WIS över SGSI med signalskyddsystem för ”Begränsat hemlig”

WIS över SGSI med signalskyddssystem för ”Begränsat hemlig” ökar möjligheten till robust och säker samverkan.

MSB utvecklar en separat och anpassad version av WIS, för bruk i SGSI och hantering av sekretess upp till och med säkerhetsskyddsklassen ”Begränsat hemlig”. För att uppnå denna nivå behöver en separat instans/installation av WIS, med särskilda krav på informationssäkerhet, realiseras. Denna anpassade version av WIS kan endast användas på skyddade platser, och återanvänder på ett effektivt sätt den teknik och de metoder som redan är etablerade och används inom det svenska krishanteringssystemet.

VILKA FÅR ANVÄNDA WIS ÖVER SGSI MED SIGNALSKYDDSYSTEM FÖR ”BEGRÄNSAT HEMLIG”?

De WIS-användare som även är berättigade att använda SGSI med signalskyddssystem för ”Begränsat hemlig” kan använda denna lösning. Detta ställer bland annat krav avseende skalskydd, tillträdeskontroll, registerkontroll med mera.

Kortvågsradio

MSB utreder om kortvågsradio kan vara ett reservsystem för samband när alla andra kommunikationsverktyg fallerar.

Kommunikation via kortvågsradio förutsätter att de som behöver samverka har utrustning som är kompatibla och att man i förväg har kommit överens om vilka frekvenser som ska användas vid vilken samverkan. Kortvågsradio är inte beroende av en särskild infrastruktur.

Kommersiella produkter

Det finns många produkter för samverkan att köpa hos kommersiella aktörer. Dessa går att få med olika grad av robusthet beroende på hur kravställningen ser ut. Det finns även möjlighet att få olika lösningar för hanterande av säkerheten i form av kryptering. Viktigt att komma ihåg är dock att dessa inte är godkända lösningar för att skydda information som är hemlig med hänvisning till rikets säkerhet.

Mer information om hur man kan ställa krav på säkerhet vid val av dessa verktyg finns på Post- och telestyrelsens webbplats.

Under 2019 kommer MSB publicera mer information om hur man kan ställa krav på säkerhet vid val av olika verktyg på www.informationssäkerhet.se.

Signalskyddssystem godkända av Försvarsmakten

Signalskyddssystem godkända av Försvarsmakten

Signalskydd är åtgärder som syftar till att förhindra obehörig insyn i och påverkan av informationssystem med hjälp av kryptografiska metoder och övriga signalskyddsåtgärder. Signalskyddssystem är främst framtagna för att skydda information som är hemlig med hänvisning till rikets säkerhet men kan också användas för att skydda annan skyddsvärd information.

Ett signalskyddssystem är ett av Försvarsmakten godkänt kryptosystem som består av tre samverkande enheter:

- Signalskyddsmateriel.
- Tillhörande kryptonycklar och/eller aktiva kort.
- En instruktion för hur systemet ska hanteras.

Till detta så finns tillgång till användarstöd och anpassad utbildning.

De flesta signalskyddssystem kan oftast kopplas ihop med befintliga nät vilket gör att signalskyddet behöver bli en integrerad del i kommunikationslösningen. Här gäller det att tänka till och skaffa sig kunskap så att skyddet för informationen som ska kommuniceras blir så bra och säkert som planerat.

Det finns flera myndigheter som har olika roller och ansvar inom området signalskydd. Försvarsmakten leder och samordnar signalskyddsverksamheten och har bemyndigats att ge ut föreskrifter inom detta område (FFS 2016:3). Försvarsmakten har också till uppgift att granska och godkänna kryptosystem.

MSB inriktar och samordnar civila myndigheters signalskyddsverksamhet. MSB ger även ut kompletterande föreskrifter inom området till exempel om civila myndigheters kryptoberedskap (MSBFS 2009:11).

Försvarets radioanstalt, FRA, stödjer de myndigheter som enligt MSB ska tilldelas signalskyddssystem. Totalförsvarets signalskyddsskola, TSS, utbildar personal i hantering av olika signalskyddssystem. Utbildningen sker till befattningar såsom signalskyddschef, signalskyddslärare, kortadministratör aktiva kort och till systemoperatör för praktisk drift av olika signalskyddssystem.

Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB1285 - november 2018 ISBN 978-91-7383-881-8