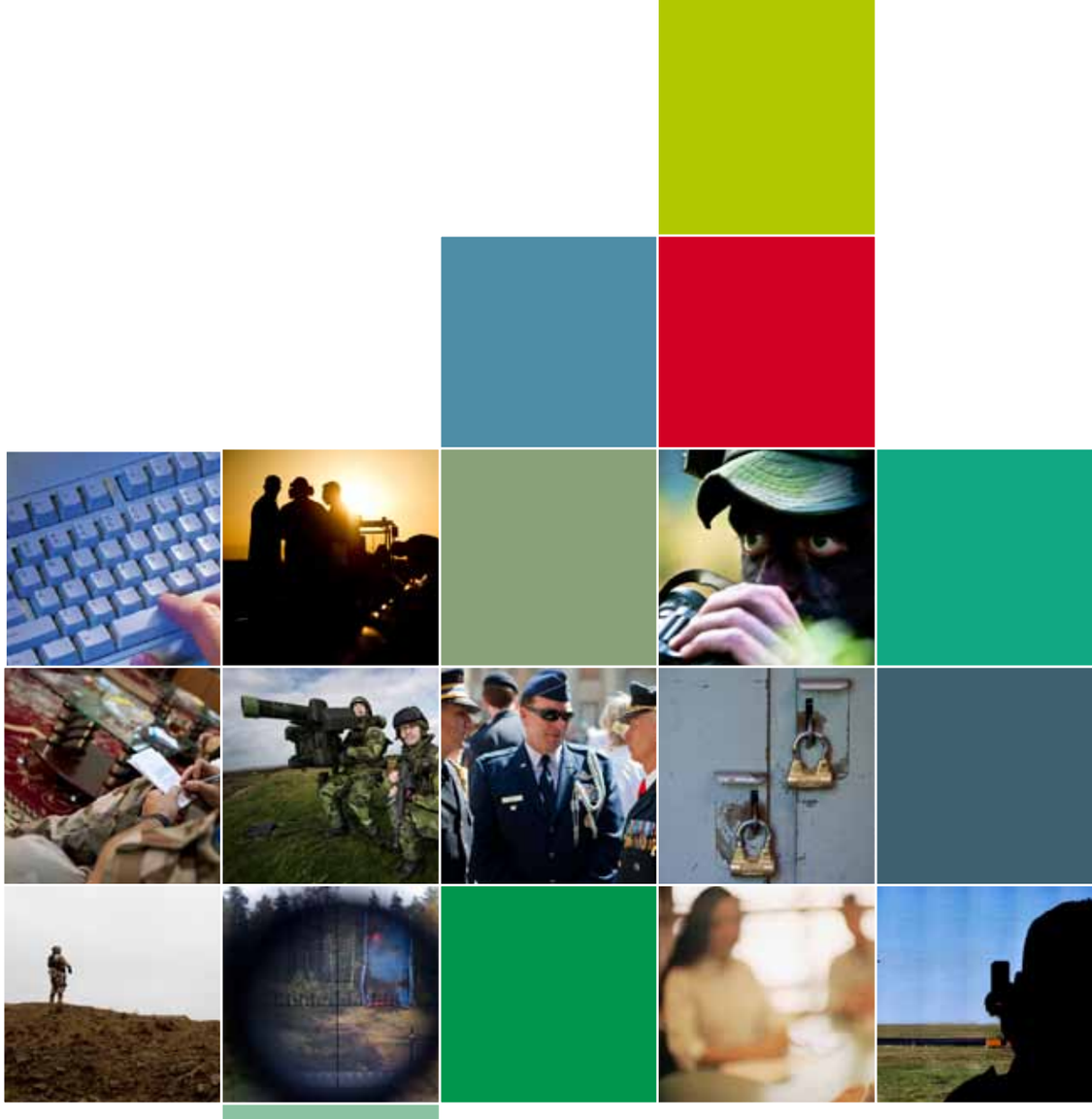


ÅRSRAPPORT

SÄKERHETSTJÄNST 2011

FÖRSVARSMAKTEN
MILITÄRA UNDERRÄTTELSE- OCH SÄKERHETSTJÄNSTEN

107 85 Stockholm Telefon: 08-788 75 00 Fax: 08-788 77 78 www.forsvarsmakten.se

Årsrapport säkerhetstjänst 2011

Militära underrättelse- och säkerhetstjänsten, MUST

FÖRSVARSMAKTEN

MILITÄRA UNDERRÄTTELSE-
OCH SÄKERHETSTJÄNSTEN

INNEHÅLL

Foto: Försvarets mediaportal
Övriga bildkällor: www.office.com/bilder
Formgivning: MUST, Säkerhetskontoret
Tryck: FMLOG APSA, Grafisk produktion Stockholm

FÖRORD

Utvecklingen i det svenska närområdet påverkar hotbilden mot Försvarsmakten och därmed utformningen av vårt säkerhetsskydd. Såväl Ryssland som NATO genomför idag regelbundet övningar och spaning i närområdet. Den ryska militärreformen, med ökad operativ förmåga som mål, fortsätter. Östersjöns betydelse för energitransporter ökar. Konkurrensen om Arktis hårdnar till följd av relativt höga energi- och råvarupriser och ett krympande istäcke.

Sveriges deltagande i internationella militära insatser kommer fortsatt att vara en viktig uppgift för Försvarsmakten, både på underrättelse- och säkerhetstjänstsidan. Planerade reduceringar av svensk och annan utländsk trupp i Afghanistan, liksom gradvis förändrade arbetsuppgifter för ISAF-missionen, ger konsekvenser i säkerhetsavseende. Dessa analyseras och skyddsåtgärderna anpassas löpande därefter.

Förutsättningarna för den militära säkerhetstjänstens arbete präglas också av den snabba IT-utvecklingen i samhället. Efterfrågan på IT-baserade informationssystem ökar - så även inom försvarssektorn - och vi blir mer beroende av tekniska lösningar för att hantera information, vilket kvalificerade motståndare utnyttjar.

Det finns uppenbara säkerhetshot, risker och sårbarheter kopplat till IT-tekniken. Exempelvis med smarta mobiltelefoner, sociala medier och bärbara lagringsmedier som laptops och USB-minnen. Att minska det IT-säkerhetsmässiga gapet - genom att bl.a. höja personalens medvetenhet, stärka signalskyddet, revidera rutiner och ta fram säkrare IT-lösningar - är en angelägen uppgift och utmaning för Försvarsmakten och som säkerhetstjänsten ständigt måste ha i fokus.

Säkerhetstjänst är i mångt och mycket en lärande process. MUST:s tillsyns- och kontrollverksamhet utgör en hjälp för både Försvarsmakten i stort som det enskilda förbandet. Resultaten från kontrollerna ska tas tillvara och omsättas till konkreta åtgärder. Ett framgångsrikt säkerhetstjänstarbete kräver inte bara säkerhetschefens utan hela ledningens engagemang.

Denna årsrapport ger en bild av den militära säkerhetstjänstens verklighet och verksamhet 2011. Jag rekommenderar dig varmt att läsa vidare.

Stockholm i juni 2012

Stefan Kristiansson
Generalmajor

Chef militära underrättelse- och säkerhetstjänsten

DEN MILITÄRA SÄKERHETSTJÄNSTEN

Den militära säkerhetstjänsten bidrar till att skydda Sveriges nationella oberoende genom att tillvarata de säkerhetsintressen som rör Försvarsmakten och dess tillsynsområden. Säkerhetsintressena omfattar personal, materiel, information, anläggningar och verksamhet både nationellt och internationellt.

Den militära säkerhetstjänsten bedrivs inom tre huvudområden:

Säkerhetsunderrättelsetjänst identifierar och klarlägger säkerhetshot som riktas mot Försvarsmakten och dess intressen inom och utom landet.

Säkerhetsskyddstjänst förebygger bl.a. att uppgifter som omfattas av sekretess och som rör rikets säkerhet inte röjs, ändras eller förstörs, att obehöriga får tillgång till hemliga uppgifter och att personer som inte är pålitliga från säkerhetssynpunkt deltar i verksamhet som har betydelse för rikets säkerhet.

Signalskyddstjänst förhindrar att obehöriga får insyn i, eller kan påverka totalförsvarets telekommunikationer. Signalskydd innefattar även användning av kryptografiska funktioner i IT-system.

Den militära säkerhets- och underrättelsetjänsten har medarbetare inom en rad olika yrkeskategorier, bland annat analytiker, kryptologer, statsvetare, ekonomer, översättare, personalvetare, jurister, administratörer, systemvetare och IT-specialister. Andelen kvinnor är 30 procent. Cirka 26 procent av medarbetarna är officerare.

Den militära säkerhetstjänsten leds från central nivå av chefen för den militära underrättelse- och säkerhetstjänsten (C MUST) som är Försvarsmaktens säkerhetsskyddschef och informationssäkerhetschef. C MUST ansvarar även för ledning och samordning av signalskyddstjänst inom totalförsvaret.

Insatschefen i högkvarteret leder säkerhetstjänsten i internationella militära insatser samt den territoriella säkerhetstjänsten med stöd av säkerhetsorganisation på regional nivå.

På lokal nivå, vid insatsförband och i basorganisationen, representeras den militära säkerhetstjänsten av säkerhetschefer, IT-säkerhetschefer, säkerhetsmän och signalskyddschefer.

Vår främsta uppgift är att utarbeta och delge säkerhetshotbedömningar, ange normer för säkerhetsskydds- och signalskyddstjänsten.

Genom rådgivning, utbildning och kontroller säkerställer vi att hotbilden uppfattas rätt, att normerna följs samt att säkerhetsmedvetandet hos våra medarbetare ligger på en hög nivå.

Dessutom ansvarar vi för att utveckla, godkänna och upprätthålla signalskyddssystem för totalförsvaret samt att godkänna IT-säkerhetsmekanismer för Försvarsmakten.

Försvarsmakten utövar, genom den militära säkerhetstjänsten, tillsyn av säkerhetsskydd, över bland annat Försvarets materielverk, Försvarets radioanstalt, Försvarshögskolan, Totalförsvarets forskningsinstitut, Rekryteringsmyndigheten, Försvarsexportmyndigheten och Fortifikationsverket.

Den militära säkerhetstjänsten leder och samordnar signalskyddstjänsten inom totalförsvaret. Arbetet inkluderar säkra kryptografiska funktioner och föreskrifter inom signalskyddsområdet. Inom ramen för detta genomför vi även administrativa och tekniska kontroller.

Framtiden

Nu har 2011 passerat och vi kan i backspegeln se att resultaten varit goda, även om förbättringar alltid kan göras. De erfarenheter vi dragit av det gångna året tar vi med oss in i verksamheten för 2012.

Några av våra viktigaste utmaningar och fokusområden är; hur kan det IT-säkerhetsmässiga gapet minskas? Hur ska säkerhetstjänsten bli en mer naturlig del av verksamheten så att chefer och medarbetare upplever det som en självklar del?

Kan vi förbättra uppföljning och granskning av säkerhetsskyddad upphandling med säkerhetskyddsavtal (SUA)? Vi ser en ökad användning av civila underleverantörer och privata aktörer med kopplingar till Försvarsmakten.

Hur förbereder vi oss när det beslutas om insats med kort varsel? Där tillkommer också Försvarsmaktens nya personalförsörjning som ställer stora krav på en strukturerad säkerhetsprövning. Metoder finns men behöver nå ut i organisationen.

Sist men inte minst, hur stödjer vi den nya organisationen för Försvarsmakten 2013 och vad kommer det att innebära ur ett säkerhetstjänstperspektiv?

SÄKERHETS-UNDERRÄTTELSER

Den militära säkerhetstjänsten gör bedömningen att ett tiotal länder bedriver aktiv underrättelse-inhämtning mot Försvarsmaktens förmågor och kapacitet.

Inhämtning av information sker på många skilda sätt och vid många olika tillfällen. En del av informationsinhämtningen bedrivs genom öppen laglig verksamhet av försvarsattachéer, som vi samarbetar med. Men det sker också illegalt och dolt, eller som det står i brottsbalken; "*hemligen eller med användande av svikliga medel*" för att få tillgång till önskad information.

Metoderna för inhämtning av information varierar. En skicklig underrättelseofficer kan få svar på sina underrättelsebehov genom att inhämta fragment av svaren från olika individer vilka då heller inte uppfattar att de avslöjat någon sekretessbelagd information.

I samtal med en skicklig underrättelse-officer upplevs samtalet många gånger som intressant och givande och inte minst uppfattas han eller hon som mycket trevlig och intresserad. Underrättelseofficeren kan också ställa raka och specifika frågor som kan upplevas som provokativa, för att få målpersonen ur balans, och genom kroppsspråk och minspel omedvetet svara på frågor.

Under året som gått har ett flertal försök till IT-angrepp upptäckts och hanterats. Angripare har försökt sprida skadlig kod i försvarsmaktsanställdas datorer med syfte att inhämta information. Säkerhetstjänsten har noterat en ökad medvetenhet inom Försvarsmakten för denna typ av attacker, som sker bland annat via e-post. Det har resulterat i att hot kunnat avvärjas utan att information gått förlorad.

Genom att avsändare och dokumentets innehåll ser legitimt ut försöker angriparen få mottagaren att öppna bifogade filer i e-postmeddelanden. När en fil av denna typ öppnas kan en bakdörr etableras i mottagarens dator. Svagheter, i bland annat Microsofts och Adobes programvaror, utnyttjas för att extrahera information ur datorns innehåll till angriparens server. Det är viktigt att man är vaksam när man hanterar e-post och webblänkar.

Några av dem som varit föremål för denna typ av angrepp har tjänstgjort utomlands, men det förekommer även att information inhämtats genom exempelvis sändlistor eller visitkort. På detta sätt har angriparen fått kontaktuppgifter som kan utnyttjas. Främmande makts långsiktiga personbaserade inhämtning är bland annat inriktad mot insamlande av biografisk information. Denna typ av inhämtning kan t.ex. ske i samband med inkommande delegationsbesök till Försvarsmakten.

Säkerhetstjänsten har under året observerat inkommande delegationer som agerat konspirativt, genom att vi upptäckt försök till dolda aktiviteter vid sidan av det officiella programmet.

Kunskapen och medvetenheten om att underrättelseinhämtning sker mot Försvarsmakten, våra förmågor och kapacitet finns hos vår personal. Den militära säkerhetstjänsten har under de senaste åren kunnat konstatera ett ökat antal rapporteringar av upplevda försök till underrättelseinhämtning. Förmågan hos våra anställda att uppfatta och återge detaljer vid dessa händelser har utvecklats och vi har under senare år erhållit ett stigande antal säkerhetsrapporter.

Rapporterna har uppnått en allt högre kvalitet med större detaljredovisning och utgör ett bra underlag för analyser om främmade makters specifika intressen och deras inhämtningsmetoder mot Sverige och Försvarsmakten.

DEN MÄNSKLIGA FAKTORN

Medarbetarnas lojalitet är oerhört viktigt för alla organisationer. I Försvarsmakten blir det ännu tydligare med tanke på vilka uppgifter medarbetarna hanterar. Av det skälet synas varje ny potentiell medarbetare inför anställning, och sedan löpande under sin anställningstid.

– Det finns ett antal riskområden som kan påverka en person att bli illojal mot sin arbetsgivare och lämna ut information. Riskfaktorer kan t.ex. vara stora förändringar i livssituationen, som dödsfall i nära relation, skilsmässa eller otrohet, berättar Tuula som är psykolog och arbetar med säkerhetsprövning vid den militära säkerhetstjänsten. Hon har bred kunskap om frågor som rör säkerhetsprövning, lojalitet och insiders.

Dubbla lojaliteter, d.v.s. att man har lojaliteter även gentemot en annan person, organisation eller nation är också en riskfaktor. Inom Försvarsmakten arbetar vi numera mer intervjubaserat och individfokuserat, från att tidigare ha varit mer registerkontrollfokuserad. Vi har en inarbetad rutin för hur en säkerhetsprövningsintervju ska genomföras och för att se till att den genomförs.

– Vårt mål är att ha en säkerhetsprövning som fungerar optimalt; initialt och uppföljande, nationellt och internationellt.

Bitterhet gentemot arbetsgivaren kan uppstå om man t.ex. blivit förbigången vid en förväntad befordran eller att man står i negativ beroendeställning till någon.

– Det kan också vara att man får försämrad ekonomi, drabbas av girighet, eller att man har blivit förledd och smickrad av en person som vill komma åt information, säger Tuula.

Vi har även börjat utbilda på kravet att följa upp medarbetare från säkerhetssynpunkt. Uppföljningen bör ske av någon i den anställdes närhet för att få en så komplett bild av individen som möjligt, men också för att uppfatta när något inte verkar stämma.

Under hösten 2012 startar Försvarsmakten ett forskningsprojekt med Brottsförebyggande rådet, BRÅ, där flera andra myndigheter kommer att delta. Fokus för projektet är att urskilja förändringar och faktorer hos individer som riskerar att bli insiders.

Forskningsprojektet kommer att använda sig av en liknande modell som den som används för att utreda om en person är i riskzonen för att få hjärtinfarkt. Vid hjärtinfarkt kan man ofta se en koppling till vissa riskfaktorer som höga blodfetter, högt blodtryck etc. När en eller flera faktorer uppträder så kan man i ett tidigt stadie vidta åtgärder som skydd för att hjärtinfarkten inte ska bli ett faktum. På samma sätt hoppas projektetet kunna identifiera riskfaktorer för att tidigt kunna upptäcka individer som riskerar att bli insiders.

– Vi arbetar ständigt med att utveckla säkerhetsprövningen. Dels för att inte utsätta individer för sårbarheten som det innebär att hantera information som de kanske inte är lämpade att hantera, och dels för att skydda oss mot och upptäcka medarbetare som riskerar att bli insiders. Vårt mål är att ha en säkerhetsprövning som fungerar optimalt; initialt och uppföljande, både nationellt och internationellt, säger Tuula.

Försvarsmakten är nu inne i en historisk transformering av personalförsörjningssystemet från ett traditionellt värnpliktsförsvar till ett modernt insatsförsvar med tillsvidare- och kontraktsanställda medarbetare. Det ställer ökade krav på funktionen säkerhetsprövning i och med att fler individer kontinuerligt behöver prövas när det gäller pålitlighet ur säkerhetssynpunkt. Den militära säkerhetstjänsten deltar i transformeringen och har en aktiv roll.

UTBILDNING

En grundläggande förutsättning för ett bra säkerhetsskydd är en positiv attityd till säkerhetstjänst och ett högt säkerhetsmedvetande. Det skapar vi bland annat genom utbildning.

Utvecklingen vid den militära säkerhetstjänsten har gått från att vara enbart informerande till att aktivt ta fram utbildningsmaterial med presentationer och lärarhandledning för att ge ett bättre stöd för säkerhetsarbetet på lokal nivå. Reaktionerna har varit mycket positiva och vi kommer att fortsätta i samma riktning framöver. Under 2012 presenterar vi bland annat utbildning i grundläggande säkerhetstjänst samt fördjupningsutbildningar inom säkehetskydd.

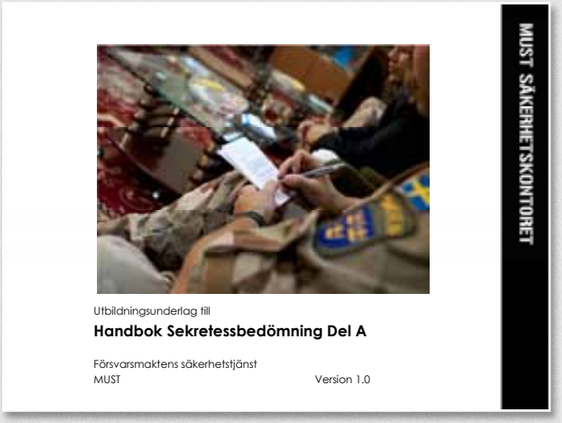
Det är viktigt att den kunskap som finns vid den militära säkerhetstjänsten sprids till de som behöver det. Vi kommer därför även i fortsättningen att delta som föreläsare och utbildare, såväl inom Försvarsmakten som vid externa aktiviteter som mässor, seminarier och i utbildningsinsatser vid försvarsmyndigheterna. Allt för att förbättra attityden och öka kunskaperna om säkerhetsarbete.

EXEMPEL PÅ UTBILDNINGSINSATSER 2011

>150 **inom säkerhetsunderrättelsetjänst**

>150 **inom säkerhetsskyddstjänst**

>20 **inom signalskyddstjänst**



Exempel på utbildnings- och informationsunderlag från den militära säkerhetstjänsten 2011; *Geografisk positionering genom Smartphones och sociala medier*, som togs fram för att öka kunskapen om riskerna med geografisk positionering genom smarta telefoner och sociala medier, ***Utbildningsunderlag till Handbok sekretessbedömning del A***, som stöd till handboken och handlar om sekretessbestämmelser och informationsklassificering, samt ***Säkerhet och mobiltelefoni***, för att öka kunskapen om de risker användning av smarta telefoner kan innebära.

UTBILDNINGSINSATSER GER RESULTAT

Mängden personärenden har genom utvecklade metoder och omfattande utbildningsinsatser minskat under 2011. Personärenden innebär att man bedömer om en person är lojal och pålitlig från säkerhetssynpunkt enligt säkerhetsskyddslagen och är en av många uppgifter för säkerhetsprövningssektionen.

Den militära säkerhetstjänsten har bedrivit omfattande utbildningsinsatser som rör Försvarsmaktens metod för säkerhetsprövning, såväl internt inom myndigheten som externt vid t.ex. Rikspolisstyrelsen, Regeringskansliet och Riksdagsförvaltningen. Resultatet av dessa insatser inom myndigheten börjar redan ge effekt i form av att antalet personärenden minskar.

Under året har vi deltagit med expertkompetens inom säkerhetsprövningsområdet i en konferensserie inom EU. Syftet med konferenserna har varit att jämföra olika nationella system för säkerhetsprövning inom EU.

Metoder och rutiner för säkerhetsprövning har fortsatt att utvecklats under 2011. Den militära säkerhetstjänstens produktionsstöd till Försvarsmakten för registerkontroller och intyg om genomförd säkerhetsprövning (*Personnel Security Clearance, PSC*) ligger kvar på en fortsatt hög nivå.

Betydelsen av att ha personal som är pålitlig från säkerhetssynpunkt gör att den militära säkerhetstjänsten kontinuerligt arbetar med utveckling inom säkerhetsprövningsområdet. Vi kommer bland annat att fokusera på att göra en översyn av hur säkerhetsprövning fungerar vid lokal rekrytering i internationella militära insatser, beskriva hur säkerhetsprövning ska genomföras vid SUA samt att besluta om hur uppföljande säkerhetsprövning ska utföras.

2011 SÄKERHETSPRÖVNING

6880 Security Clearance

11414 Registerkontroller

2419 Registerkontroller av företag (SUA)

75 Skyddssamtal

INFORMATIONSKAMPANJER

Under 2011 tog den militära säkerhetstjänsten fram foldrar med olika teman. Budskapen är korta och manar till eftertanke inom olika områden.

Foldrarna har bl.a. behandlat säkerhet och sociala medier, säkerhet och mobiltelefoner, samt säkerhet och USB-minnen. De har spridits utanför Försvarsmakten vid t.ex. mässor och myndighetssamverkan och fått positiv uppmärksamhet.

För att öka säkerhetsmedvetandet och uppmuntra Försvarsmaktens medarbetare att fortsätta rapportera om säkerhetshotande verksamhet och brister i säkerhetsskyddet har även planscher tagits fram.

Allt informationsmaterial från den militära säkerhetstjänsten kan inom Försvarsmakten beställas via Grafisk produktion, FMLOG, Stockholm.

Utomstående myndighet kan kontakta MUST Säkerhetskontor på 08-788 75 00.

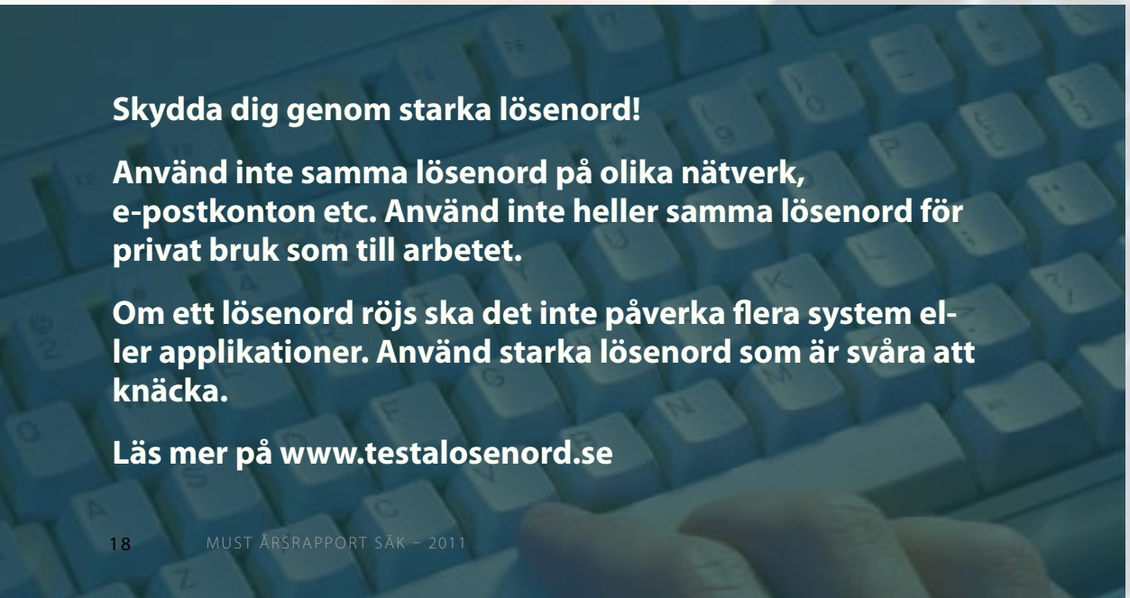
SÄKERHET OCH SOCIALA MEDIER

Sociala medier som t.ex. Facebook, Google+, Tumbler, Twitter och bloggar är för många ett naturligt och enkelt sätt att kommunicera och hålla kontakten med familj, vänner och bekanta på. De kan vara användbara på många sätt, men attacker riktas i princip mot alla de stora nätverken.

En av de mest ökända är masken och botnätet Koobface, där masken bland annat infekterade offrens Facebook-konton genom att sprida falska videolänkar på användarnas väggar medan botnätkoden gav hackare möjlighet att fjärrstyra offrens datorer.

Under 2011 ökade attackerna mot sociala medier lavinartat. På grund av att vi ägnar mer tid av våra liv på nätet, och använder oss av inloggningar och lösenord på allt fler sajter, tyder mycket på att trenden kommer att hålla i sig.

Sociala medier används av främmande underrättelsetjänst, kriminella och terrorister för att inhämta värdefull information. Information som kan användas för att påverka dig och dina anhöriga. Genom att vara medveten om riskerna kan du förhindra att värdefull information kommer i orätta händer.



Skydda dig genom starka lösenord!

Använd inte samma lösenord på olika nätverk, e-postkonton etc. Använd inte heller samma lösenord för privat bruk som till arbetet.

Om ett lösenord röjs ska det inte påverka flera system eller applikationer. Använd starka lösenord som är svåra att knäcka.

Läs mer på www.testalosenord.se

SÅ SKYDDAR DU DIG

Flera typer av skadlig kod är specialskrivna för sociala medier som t.ex. Facebook. De som står bakom attackerna imiterar vårt beteende på Internet vilket gör attackerna svåra att urskilja. Var försiktig med länkar och nedladdningsbara filer. Om meddelandet med länken kommer från en vän som brukar skriva på svenska, men nu har skrivit på engelska kan det t.ex. vara en varningssignal.

Håll ditt antivirusprogram uppdaterat. Ett bra antiviruspaket skyddar både mot virus, nätfiske och identitetsstöld.

Kontrollera och ändra vid behov sekretess- och säkerhetsinställningarna i de sociala nätverk du är medlem i så att du verkligen är skyddad på det sätt du själv önskar. Det är säkrare att börja restriktivt och successivt utöka informationen än tvärtom. De flesta sociala nätverk kan blockeras från företagsdatorer.

Att kartlägga så mycket som möjligt om en person underlättar både målsökning och inhämtning. För den som arbetar med känslig information är det viktigt att inte berätta för andra vilken information man har tillgång till och som omfattas av sekretess.

Inom Försvarsmakten har hot riktats mot såväl personal i utlandsstyrkan som mot anhöriga. Var medveten om risken att lägga ut kontaktinformation eller andra uppgifter som kan identifiera dig, dina anhöriga eller kollegor.

Tänk efter innan du publicerar texter och bilder på Internet. Information som du tror är skyddad kan bli offentlig på grund av att nätverkets allmänna villkor och policyregler ändras, attacker från hackers eller som ett resultat av att företag säljer eller delar med sig av uppgifter om användare.

Information som du har lagt ut på nätet kommer alltid att finnas kvar på nätet!

SÄKERHET OCH MOBILTELEFONER

Mobiltelefonens många användningsområden gör den till en viktig informationskälla. Den kan innehålla information om samtal, SMS, MMS och e-post – det vill säga information om dig, ditt kontaktnät, vilken information du sökt efter och om var du befinner dig. I vår informationsbroschyr "Säkerhet och mobiltelefoner" ger vi råd och riktlinjer för säkrare användning av mobiltelefoner. Här presenteras några av dem.

Mobiltelefoner kan spåras, övervakas och avlyssnas. En dyr telefon är attraktiv för ficktjuvar och den är lätt att tappa bort. Det går snabbt och lätt att installera spionprogram och annan skadlig kod, särskilt om mobiltelefonen i ett oövervakat tillfälle hamnar i fel händer.

Skydda din telefon genom att stänga av funktioner som gör det möjligt för andra att koppla upp sig på din telefon, som t.ex. Bluetooth och trådlösa nätverk, när du inte använder dem.

Acceptera inte oväntade programinstallationer via MMS, Bluetooth eller liknande. Återställ din mobiltelefon till fabriksinställningar om den uppför sig konstigt. Gör det svårare för obehöriga att komma åt informationen på din mobil genom att aktivera både telefonlås (skärmlås) och PIN-kod (SIM-kortet).

Idag finns utrustning och teknik lättillgänglig för den som vill avlyssna, störa ut, koppla vidare eller på andra sätt påverka ett mobiltelefonsamtal.

Med fler funktioner i mobiltelefonerna ökar angreppssätten. Det är inte längre enbart statsaktörer som kan ha resurser att följa Försvarsmaktens mobilkommunikation, utan även kriminella och andra som kan ha intresse av vår information.

RISKER MED SMARTA TELEFONER

Risken för nätfiske och elakartad kod är lika stor på en smart telefon som på en dator. Använd samma försiktighet på din smarta telefon som du gör på din dator. Se till att ha den senaste mjukvaran installerad och installera bara program från källor du litar på. Klicka inte på länkar i e-post och SMS om du inte är säker på vad det är.

Att ladda ner appar är vanligt, men kan även medföra risker. Varje månad upptäcks appar som innehåller skadlig kod.

Skadlig kod kan användas för att stjäla information, avlyssna samtal, sms eller göra att mobiltelefonen fungerar som en mikrofon. Den kan även resultera i höga telefonräkningar eller att kontokortsnummer och koder stjäls och används för bedrägerier av olika slag. Ladda därför inte ner en app hur som helst. Ladda bara ner från kända platser, i praktiken Google Play och Apples App Store.

Stäng av synkroniseringen innan du knappar in nya kontakter eller importerar kontakter från ditt gamla SIM-kort. Annars finns risken att alla kontakter automatiskt synkroniseras mot t.ex Google och därigenom lagras på internet.

Skydda din smarta telefon på samma sätt som du skyddar en bärbar dator. Se till att du har ett bra antivirusprogram och de senaste uppdateringarna. Sök igenom systemet regelbundet och gör backup på den information du vill spara.

Var rädd om din mobiltelefon!
Låt inte obehöriga få tillgång till den.

SÄKERHET OCH USB-MINNEN

Lagringsmedier med USB-teknik används i stor omfattning. USB-minnen, externa hårddiskar, digitalkameror, mobiltelefoner, GPS-mottagare, surfplattor, MP3-och MP4-spelare använder USB-teknik.

Med USB-minnen kan stora mängder information på ett enkelt och snabbt sätt flyttas mellan olika IT-system. USB-minnen innebär många fördelar, men medför även flera säkerhetsrisker. Att endast radera filer på ett USB-minne ger inget skydd eftersom informationen kan återskapas.

För att vara säker på att raderad information inte kan återskapas krävs att USB-minnet destrueras. Det finns idag inget godkänt överskrivningsverktyg för USB-minnen. Inom Försvarsmakten beslutar MUST om vilka överskrivningsverktyg som får användas.

USB-minnen förvaras ofta i väskan, fickan eller i datorn. De är därför lätta att tappa bort och enkla att stjäla.

Om USB-minnet stjäls eller tappas bort kan mängden information som förloras bli mycket stor.

Förlust av lagringsmedium kan leda till att information röjs för obehöriga, ändras eller går förlorad.

USB-minnen kan användas för att sprida skadliga program som virus, maskar och trojaner. De kan även infektera IT-system som inte är anslutna till nätverk eller Internet.

SÅ SKYDDAR DU DIG

Den militära säkerhetstjänsten har tagit fram riktlinjer för säkrare användning av USB-minnen och andra digitala lagringsmedier till försvarsmaktsanställda. Flera av säkerhetsråden är generella och kan enkelt följas av alla organisationer för att skydda sin information. Ytterligare bestämmelser förekommer för lagringsmedier som innehåller hemlig, utrikesklassificerad eller sekretessklassificerad information.

USB-minnet bör användas för tillfällig lagring av information.

Använd aldrig upphittat eller på annat sätt okänt USB-minne i arbetsgivarens IT-system.

Ta bort information du inte behöver, men tänk på att informationen kan återskapas.

USB-minne som inte längre används ska förstöras på ett säkert sätt.

Var uppmärksam på hur du använder USB-minnen. Kontrollera vilka bestämmelser som gäller för det IT-system du arbetar i.

USB-minne som du inte längre behöver, t.ex. då du byter befattning eller lämnar din anställning, ska återlämnas till arbetsgivaren.

HANDBÖCKER 2011

Under 2011 publicerade den militära säkerhetstjänsten två handböcker.

Handbok Sekretessbdömning Del A beskriver Försvarsmaktens informationsklassificeringsmodell och ger bl.a. den teoretiska grunden för offentlighet och sekretess samt en beskrivning av sekretesskategorierna hemliga, utrikesklassificerade och sekretessklassificerade uppgifter. Till handboken hör även ett utbildningsmaterial med bildspel och lärarhandledning.

Handbok Sekretessbedömning Del B är under produktion och ges ut kapitelvis i PDF-format på säkerhetstjänstens säkerhetsportal på Försvarsmaktens intranät. Handboken kompletterar Del A med specifika ämnesområden för informationsklassificering, t.ex. inom insatsverksamhet och underrättelsetjänst.

En ny handbok säkerhetsskyddad upphandling med säkerhetsskyddsavtal (Handbok SUA) togs fram till årsskiftet 2010/2011, som ett stöd för det praktiska säkerhetsarbetet i samband med säkerhetsskyddad upphandling. Ett nytt utbildningsmaterial kopplat till handboken kommer att tas fram under 2012.

NOLL TOLERANS

MOT INFORMATIONSFÖRLUSTER

Ett högt säkerhetsmedvetande hos personalen är en förutsättning för ett bra säkerhetsskydd och är något som genomsyrar Försvarsmaktens verksamhet.

Trots detta sker informationsförluster. En del är av ringa omfattning och medför ingen, eller endast liten skada. Andra är mer omfattande och kan medföra skada både för Försvarsmakten och för rikets säkerhet.

För att minska förlusterna tog vi under 2011 fram ett utbildningsmaterial som stöd för att höja säkerhetsmedvetandet.

Utbildningsmaterialet visar på flera faktiska händelser och några viktiga åtgärder för att minska risken för informationsförluster.

Händelserna i underlaget har, i förekommande fall, varit föremål för polisanmälan och anmälan internt i Försvarsmakten eller vid annan statlig myndighet. För att inte peka ut enskilda är händelserna anonymiserade och i vissa fall förenklade.

KONTROLL

Regeringen har tilldelat Försvarsmakten uppgiften att kontrollera säkerhetsskyddet vid de myndigheter som Försvarsmakten har tillsynsansvar för.

Försvarsmakten har även uppgiften att kontrollera det egna säkerhetsskyddet vid enheter både nationellt och internationellt. Kontrollverksamheten är ett medel för att uppnå fullgott säkerhetsskydd där många aspekter kan belysas. Fokus ligger alltid på att hitta den svagaste länken i en kedja och stärka denna. Erfarenheter visar att det är svårt att se egna brister och därför behövs externt stöd för att genomföra kontroller. Kontrollresultaten visar ofta att den svagaste länken är den enskilde individen och att bristerna enkelt kan rättas till med utbildning och tydligare arbetssätt.

Under 2011 har vi märkt en positiv förändring av attityden till kontrollverksamhet. Chefer på olika nivåer förstår allt mer betydelsen av ett fullgott säkerhetsskydd för att övrig verksamhet ska fungera.

När det gäller Försvarsmaktens tillsyn av totalförsvarsmyndigheterna är syftet att kravet på säkerhetsskydd ska uppfyllas. Utmaningen ligger i att genomföra kontrollen på ett sådant sätt att den ger ett användbart stöd och uppfattas som värdefull i myndighetens säkerhetsskyddsarbete.

Den militära säkerhetstjänsten genomför kontinuerligt utvärderingar av tillsynsverksamheten. Den senaste utvärderingen, som omfattar åren 2006-2011, har visat att ett bra säkerhetsskydd bygger på en anpassad säkerhetsorganisation, kontinuerlig internutbildning, regelbunden internkontroll och ett aktivt attitydarbete.

Vi har under året genomfört ett antal säkerhetsskyddskontroller och säkerhetsskyddsbesök bl.a. vid Försvarets radioanstalt, Totalförsvarets forskningsinstitut, Rekryteringsmyndigheten, Försvarsexportmyndigheten och Försvarsunderrättelsedomstolen samt vid centrala delar inom Försvarsmakten.

Betydelsen av att ha ett bra säkerhetsskydd ökar ständigt och gör att vi bland annat kommer att fokusera på att utveckla enklare metoder att genomföra såväl interna- som externa kontroller, snabbare uppföljning av brister i säkerhetsskyddet, ett utökat samarbete och ett proaktivt arbetssätt.

2011 KONTROLL

9 INTERNA SÄKERHETSSKYDDS-KONTROLLER INTERNATIONELLT OCH NATIONELLT

30 SIGNALSKYDDSKONTROLLER AV ANDRA MYNDIGHETER

9 SIGNALSKYDDSDIALOGER MED ANDRA MYNDIGHETER

5 SÄKERHETSKYDDSBESÖK VID ANDRA MYNDIGHETER

VÅR ROLL I NATIONELLT IT-FÖRSVAR

Den militära säkerhetstjänsten kan konstatera att det så kallade IT-säkerhetsmässiga gapet i samhället ökar. Det vill säga att IT-utvecklingen i stort går så fort att säkerhetsåtgärder för skydd av system och information har svårt att hålla samma utvecklingshastighet.

Den militära säkerhetstjänsten utgör en central del av Försvarsmaktens IT-försvarsförmåga som är en delkomponent i den svenska förmågan att hantera allvarliga IT-incidenter. Vi har under året utökat samarbetet med SÄPO och Försvarets radioanstalt i syfte att tillsammans utveckla förmågan.

Under året har ett antal tekniska och administrativa kontroller genomförts såväl internt inom Försvarsmakten, som till stöd för annan myndighet för att höja skyddet mot IT-incidenter.

Tekniska utredningar har genomförts där säkerhetstjänstens nationella spetskompetens inom området använts för att stödja andra myndigheter i tekniska utredningsarbeten.

Den militära säkerhetstjänsten är Försvarsmaktens representant i samverkansgruppen för informationssäkerhet, SAMFI, som arbetar för att förbättra informationssäkerheten i samhället.

RISKER MED OUTSOURCING

Privatisering av statlig verksamhet och det ökade behovet av att upphandla varor och tjänster som medför att hemliga uppgifter hanteras av privata aktörer ställer krav på Försvarsmakten och övriga försvarsmyndigheter. Det är viktigt att kontroll sker av säkerhetsskyddsavtalen som följer av de säkerhetsskyddade upphandlingarna.

Försvarsmakten har under 2011 genomfört ett projekt för att samordna försvarsmyndigheternas lägesbild för de företag som myndigheterna har säkerhetsskyddsavtal med (s.k. SUA-företag), där målet är att samordna kontrollen av företagen.

Till stöd för att utveckla verksamhet som rör säkerhetsskyddad upphandling tog den militära säkerhetstjänsten i slutet av 2010 fram en ny handbok SUA. Vi bedriver också kontinuerlig uppföljning av projekt inom Offentlig Privat Samverkan (OPS), för att bevaka att säkerhetsfrågorna blir omhändertagna när statlig verksamhet privatiseras. Ett exempel på sådan verksamhet var utredningen av en eventuell outsourcing av Försvarsmaktens ammunitionshantering.

Kraven på ökad effektivitet i statsförvaltningen kan medföra omstruktureringar av myndigheternas verksamhet, där stödjande funktioner och verksamheter läggs ut på entreprenad. Inom Försvarsmakten bedrivs denna inriktning bl.a. genom OPS. Det innebär att historiskt sett statliga verksamheter konkurrensutsätts och övertas av privata aktörer.

Utvecklingen kräver att staten är tydlig med vilka säkerhetskrav som gäller för verksamheten. Dessutom måste det analyseras om ytterligare säkerhetsskyddsåtgärder kan bli nödvändiga vid övergången från statlig till privat verksamhet. Vid dåligt utformade avtal eller upphandlingar finns risk för såväl informations- som sekretessförluster. Det måste även tydliggöras att staten ska avstå från privatisering om säkerhetsfrågorna inte kan lösas.

Den militära säkerhetstjänsten kommer att ägna fortsatt uppmärksamhet åt företag som är upphandlade med säkerhetsskyddsavtal (SUA). Avsikten är främst att undersöka om företagen har ett adekvat säkerhetsskydd för de hemliga uppgifter som de hanterar för Försvarsmaktens del. Metoder och rutiner kommer att utvecklas i samarbete med andra myndigheter för att bl.a. göra uppföljningen mer effektiv.


tsarkiv | Tieto bekräftar driftstörningar

baka

Tieto bekräftar driftstörningar

PUBLICERAD: 27 NOVEMBER 2011
DEN HÄR ARTIKELN HANDLAR OM: PRESSMEDDELANDE

TIETO ABP MEDDELANDE 27 november 2011 KL 14.40

På grund av ett hårdvarufel i ett av Tietos svenska datacenter har bolaget för närvarande driftstörningar. Tieto för en dialog med berörda kunder och arbetet med att återställa funktionerna pågår. Dessa kommer att återstartas fortlöpande.

För ytterligare information, kontakta;
Krister Högne, vice VD, Tieto, +46 730 20 8432
Kristina Westerlind, kommunikationschef, Tieto Sweden, +46 703 32 6330

TIETO ABP

DISTRIBUTION
Centrala media

Tieto är det ledande IT-tjänstföretaget i norra Europa och erbjuder IT- och produktutvecklingstjänster. Våra specialiserade IT-lösningar och -tjänster ger, tillsammans med en stark plattform av tekniska lösningar, en konkret affärsnytta för våra lokala och globala kunder. Vi arbetar nära våra kunder, förstår deras unika behov och är en betrodd partner i transformationer. Med cirka 18 000 specialister är vårt mål att bli en ledande integratör av tjänster och därmed skapa den bästa tjänsteupplevelsen med IT. www.tieto.com

DELA: MER

I november 2011 drabbades IT-driftleverantören Tieto av ett omfattande daorhaveri som ledde till långvariga datastopp för ett 50-tal kommuner, myndigheter och företag och därmed tusentals användare. Försvarmakten, FRA och Regeringskansliet var några av Tietos kunder.

TALA ÄR SILVER, KRYPTO ÄR GULD

Försvarsmakten har i uppgift från regeringen att leda och samordna signalskyddstjänsten för de s.k. totalförsvarsmyndigheterna. I det ingår också granskning och godkännande av signalskyddssystem och produktion och distribution av kryptonycklar, aktiva kort och certifikat. Dessutom ska signalskyddstjänsten vid myndigheter som tilldelats eller anskaffat signalskyddssystem kontrolleras.

Det betyder också att Försvarsmakten stödjer Regeringskansliet i frågor som rör kryptoverksamhet och annan signalskyddsverksamhet. Det behövs utbildning, behörighet, kryptonycklar m.m. för att få ett kryptosystem att fungera.

Sverige har mer än 50 års erfarenhet av utveckling av kryptosystem. Det gör att vi har en god grund för vår utveckling.

– Det som gör att vi har en särställning är att vi inte enbart betraktar kryptoproblematiken utan också tar med IT-säkerhetsaspekter i vårt arbete. I många länder görs det här på olika delar i deras organisation, fortsätter Cem.

Att vi betraktas som en duktig kryptonation fick vi kvitto på när Sverige i november 2011 fick ett internationellt erkännande genom att vi blev medlem i den exklusiva grupp om sex nationer som benämns AQUA, Appropriately Qualified Authorities. Det innebär också i sig att vi får ytterligare möjligheter för kunskapsuppbyggnad.

Det vi tar fram ska oftast kunna fungera i allt från kontorsmiljö på regeringskansliet ut till den enskilde soldaten, mitt i sandstormen i Afghanistan.

– Trots att Sverige är ett litet land och vi är få som jobbar med detta, står vi oss mycket bra jämfört med andra stora kryptonationer i Europa och världen både erfarenhetsmässigt och i kompetensnivån på våra kryptologer och IT-säkerhetsexperter, säger Cem som är ansvarig chef för granskningen av nya kryptosystem vid den militära säkerhetstjänsten.

VI ÄR EN DEL AV EUROPAS KRYPTOELIT

I november 2011 fick Sverige ett internationellt erkännande genom att vi blev medlem i den exklusiva grupp om sex nationer som benämns AQUA, Appropriately Qualified Authorities.

I Sverige utgörs den nationella kryptogodkännande organisationen av den militära säkerhetstjänstens avdelning för krypto och IT-säkerhet.

AQUAs uppgift är att godkänna andra medlemsstaters godkända krypton så att de uppfyller EU:s bestämmelser för skydd av säkerhetsskyddsklassificerade (hemliga) EU-uppgifter. Ett nytt kryptosystem ska först godkännas av en AQUA-medlem innan produkten godkänns av EU-rådet. AQUA består nu av Storbritannien, Frankrike, Tyskland, Holland, Italien och Sverige.

Hur går det till att ta fram ett kryptosystem? Bestämmer MUST själv när det är dags att ta fram ett nytt krypto eller kommer krav från någon annan?

– Kraven kommer alltid från verksamheten, dvs den som upplever att det saknas ett skydd. Naturligtvis är vi också ute i verksamheten och snappar upp de behov som finns inom Försvarsmakten eller inom totalförsvaret när vi genomför kontroller och därigenom bidrar till att ett arbete för kravställning sätter igång, säger Cem.

Ett avancerat kryptosystem med hög skyddsnivå kan ta flera år att utveckla. Den militära säkerhetstjänsten utvecklar aldrig några system på egen hand. När ett krav på nytt kryptosystem ställs från Försvarsmakten eller någon av totalförsvarsmyndigheterna får FMV i uppdrag att upphandla det gentemot industrin.

– Upphandlad kryptoindustri tar sedan fram förslag på design som måste godkännas av oss innan vidare utveckling. Granskningar av varje ”etta och nolla” i ett system görs löpande under utvecklingen för att till slut uppnå ett godkännande, säger Cem.

Det är en ständig balansgång att möta behovet från användaren och få förståelsen av att hela önskelistan inte kan få plats i ett system. Det vi tar fram ska oftast kunna fungera i allt från kontorsmiljö på regeringskansliet ut till den enskilde soldaten, mitt i sandstormen i Afghanistan.

>1000 000

kryptonycklar har producerats och levererats till Försvarsmakten och totalförsvarsmyndigheterna under 2011

KRYPTO UNDERLÄTTAR SAMVERKAN OCH SKYDDAR UPPGIFTERNA

Informations- och kommunikationssystem är viktiga och strategiska resurser för alla organisationer – både internt och för samverkan med andra myndigheter och aktörer. För att skydda informationen i systemen kan kryptering användas.
KSU är kryptosystem som kan användas av alla organisationer.

KSU står för Krypto för skyddsvärda uppgifter. Det är inte ett speciellt kryptosystem utan en kvalitetsstämpel för att kryptosystemet är godkänt av den militära säkerhetstjänsten. Under 2011 har ett KSU godkänts med benämningen KGAI.

Behovet av att skydda information från obehöriga är ständigt aktuellt, inte bara inom Försvarsmakten. KGAI är benämningen på ett krypto som tillsammans med ett regelverk är nationellt godkänt av Försvarsmakten för skydd av information som rör skyddsvärda uppgifter.

Det har länge funnits önskemål om ett krypto som är användarvänligt och tillgängligt för den enskilde handläggaren. Ett krypto som täcker behovet att skydda känslig information, men som inte behöver lika starkt skydd som uppgifter som rör rikets säkerhet eller utrikesklassificerade uppgifter.

Styrkan med KGAI är att det är en kontrollerad produkt som kan användas av olika myndigheter. De som t.ex. arbetar i ett projekt mellan olika myndigheter kan med krypto skydda informationen under arbetets gång.

Det är ett traditionellt krypto där avsändare och mottagare av ett meddelande får tillgång till en gemensam kryptonyckel.

Programvaran för krypot sparas exempelvis på datorns skrivbord. Man krypterar enkelt meddelandet genom att klicka och dra det till programvarans ikon på skrivbordet, som krypterar innehållet. Sedan kan man skicka meddelandet krypterat med e-post till mottagaren.

Beroende på uppgifternas skyddsvärde så väljer användaren hur starkt nyckeln ska skyddas. Är det inte så högt skyddsvärde så kan den krypterade nyckeln t.ex. skickas med separat e-post. Är behovet av skydd högre kan nyckeln överföras manuellt t.ex. brevledes. Allt avgörs av användarens organisation.

Ett grundläggande regelverk finns framtaget men ger också respektive myndighet en möjlighet att verksamhetsanpassa det för just sitt behov.

KSU
Krypto för skyddsvärda uppgifter är kryptosystem som har granskats och godkänts av Försvarsmakten och som kan användas av alla organisationer.

KSU ska användas för sekretessbelagda uppgifter, men inte för information som gäller rikets säkerhet eller utrikesklassificerade uppgifter.

Det kan t.ex. användas för patientsekretess inom hälso- och sjukvården, företagssekretess eller en myndighets risk- och sårbarhetsanalyser.

FÖRSVARA OCH FÖRVARA SKYDDSVÄRD INFORMATION

Försvarsmakten bedriver verksamhet som tilldrar sig intresse från flera olika aktörer. Det kan vara enskilda stater, internationella organisationer, sammanslutningar av människor för särskilda syften, eller individer som av olika skäl har ett intresse i Försvarsmaktens olika aktiviteter.

Riktade attacker mot informationssystem och informationstillgångar kan genomföras när som helst. Angreppen kan utgöras av olika former av skadlig kod eller intrångsförsök i informationssystem i syfte att stjäla, kopiera, förstöra eller förvanska.

Ett exempel på en sådan riktad attack är den skadliga koden Stuxnet som konstruerades för att slå ut specifika mål. Stuxnet angriper system som använder Siemens WinCC, ett program för industriella styrsystem vilka används i t.ex. kraftverk, kärnkraftverk, oljeplattformar och vattenreningsverk. Det var Stuxnet som angrep Irans kärnanläggningar.

Men vad gör Försvarsmakten för att skydda sig så obehöriga inte tar sig in i våra system?

– Att bygga ett IT-system är komplext och svårt. Dessutom ska systemet vara säkert ur många olika perspektiv. Försvarsmakten har många olika typer av IT-system som används och allt beror på vilken information som ska behandlas i systemet, berättar Jan som arbetar med granskningen av IT-system ur säkerhetsperspektiv inom Säkerhetstjänsten.

Försvarsmakten har en stor bredd av system. Några är inbyggda i vapenplattformar som fartyg, flyg och marksystem, medan andra är vanliga kontorssystem för att hantera hemliga handlingar och är helt administrativa. Till exempel tittar vi nu på hur och om varje anställd ska kunna ta emot sin e-post i telefonen eller på sin hemdator. Då handlar det inte om överföring av hemliga uppgifter men alla uppgifter kan och ska betraktas som känsliga eftersom en stor samlad informationsmängd tillsammans kan bli hemlig. Men det ska också vara användarvänligt och inte kosta för mycket för arbetsgivaren.

Under 2011 genomförde den militära säkerhetstjänsten trettio yttranden inför ackreditering av IT-system

I huvudsak sköter FMV all upphandling utifrån kraven som bestämts av Försvarsmakten.

– På ett sätt bygger alla våra system på kommersiella komponenter, det vi brukar kalla COTS, men ofta gör FMV eller deras leverantörer egna anpassningar. För de system som hanterar hemliga uppgifter är säkerhetskraven högre. Då krävs det ofta att COTS-produkterna kompletteras med säkerhetskomponenter som är utvecklade specifikt för Försvarsmakten, säger Jan.

För att bestämma om ett system är säkert granskar vi olika funktioner.

– Vem som ska ha tillgång till informationen och hur säkerställer man att det är rätt person som tar sig in i systemet? Kan informationen kommas åt av utomstående eller överföras till ett annat system och hur ser den eventuella övergången ut, är den virusskyddad, är frågor vi ställer, fortsätter Jan.

Några av de största utmaningarna brukar uppstå i samband med utbyte av information med eller mot andra system, d.v.s. när man tar emot eller skickar information eller kopplar ihop sig med annat system på något vis.

Det är den kravställandes behov av säkerhetsegenskaper som vi hjälper till att testa och granska. Till vår hjälp så har vi en kravkatalog för de olika funktionerna men vi ser också till att göra en helhetsbedömning, t.ex. vad systemet ska klara av och i vilken miljö den ska verka.

Varför är det så viktigt att systemet är ackrediterat, d.v.s. har godkända säkerhetsfunktioner?

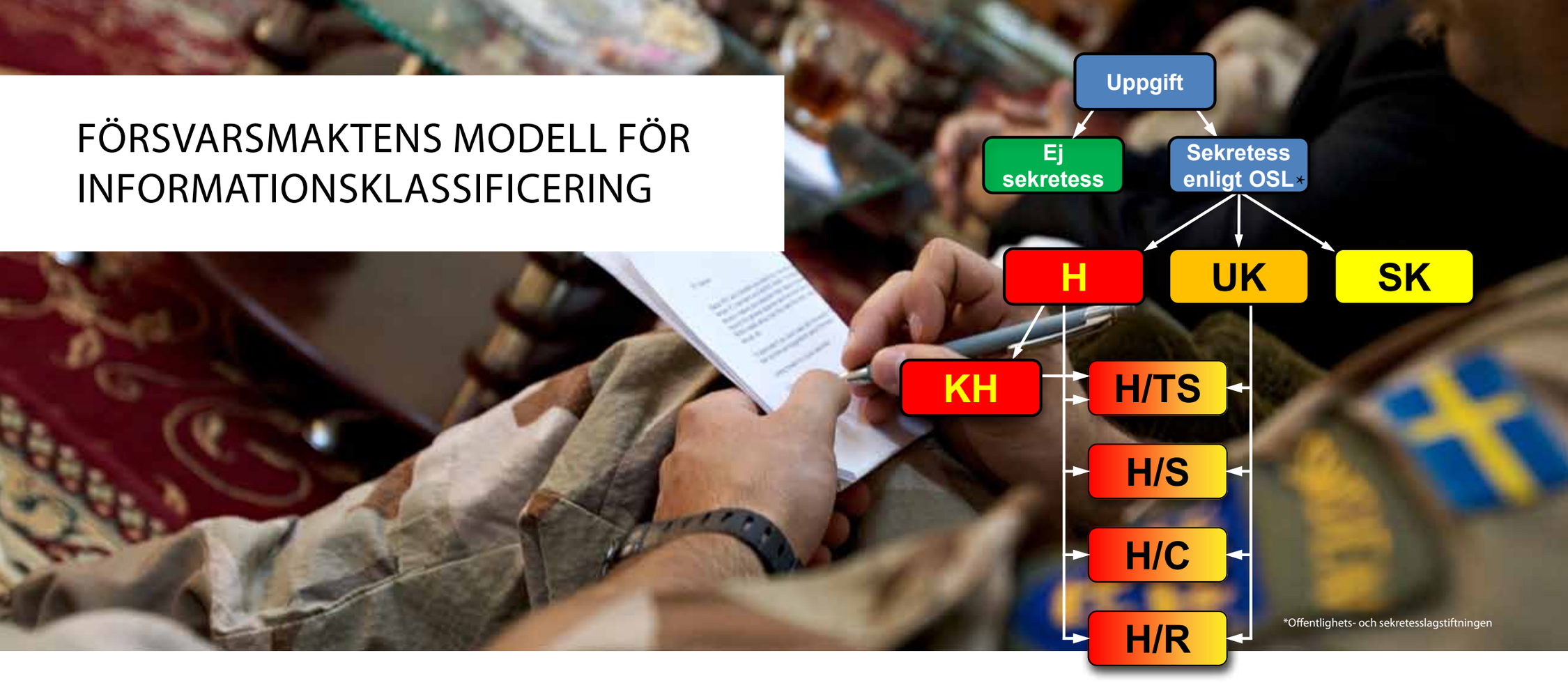
– Om du beställt ett system för din verksamhet behöver du kunna ta ställning till om det fungerar för vad det är avsett för. På säkerhetskontoret gör vi en granskning och översyn, ur säkerhetssynpunkt, av det underlag vi får från tillverkaren och det som beställaren gjort. Med den bedömningen som grund beslutar sedan beställaren om de risker vi pekat på är värda att ta och därför godkänna systemet eller inte, säger Jan.

En vanlig missuppfattning är att MUST är den som bestämmer om ett system får användas eller inte. Vi beslutar om säkerhetsfunktionerna är godkända eller inte. Om de är godkända är det sedan beställaren som avgör om systemet kan användas. Vår roll är att ge en så bra beskrivning vi kan av de risker vi ser i systemet så att beställaren har ett bra beslutsunderlag. Om säkerhetsfunktionerna inte är godkända får endast ÖB fatta beslut om driftsättning av systemet.

Att ha en kompetent personal är naturligtvis en förutsättning för att lyckas med utmaningarna som uppstår.

– Vi har haft tur och kunnat rekrytera bland de bästa i Sverige som kan det här området och arbetet är både tillräckligt lockande och utmanande så vi har nöjd och professionell personal. Kompetensutveckling är ett måste för att hänga med i allt nytt som kommer och där har Försvarsmakten en bra policy som vi tror ger ett försprång gentemot civila arbetsgivare, säger Jan.

FÖRSVARSMAKTENS MODELL FÖR INFORMATIONSKLASSIFICERING



Försvarsmakten har under lång tid anpassat informationssäkerheten för att ge ett bra stöd, både vid nationell och internationell verksamhet. Grunden för en god informationssäkerhet utgörs av rätt klassificerad information.

För att på ett bättre sätt kunna anpassa Försvarsmaktens informationssäkerhetsarbete med uppgifter som förekommer i internationell verksamhet tog den militära säkerhetstjänsten 2011 fram en handbok som beskriver Försvarsmaktens informationsklassificeringsmodell.

Handbok Sekretessbedömning Del A ger bl.a. den teoretiska grunden för offentlighet och sekretess samt en beskrivning av sekretesskategorierna.

Genom Försvarsmaktens informationsklassificeringsmodell följer myndigheten EU:s och Nato informationsklassificering i den mån det är möjligt med dagens säkerhetsskyddslagstiftning.

MISSION SECRET

Begreppet används framförallt inom NATO och har inom Försvarsmakten ibland felaktigt uppfattats som att skyddsåtgärder inte behöver vara lika omfattande som normalt, eftersom det kan vara begränsat geografiskt och/eller tidsmässigt, oftast kopplat till en internationell insats.

Det som styr omfattningen av skyddsåtgärder för information avgörs uteslutande av uppgifternas informationsklassificering.

Våra svenska informationsklasser har motsvarigheter i andra länder och organisationer som vi samarbetar med och inplaceras därefter. Mission Secret är ingen informationsklass.

Mission Secret avser uppgifter inom ramen för en insats. Uppgifterna kan ofta delges direkt på plats efter beslut av insatsens befälhavare (Force Commander) istället för att först passera den formella beslutsgången inom NATO.

INTERNATIONELL VERKSAMHET

Internationaliseringen och det alltmer ökade utbytet av information mellan Sverige och andra länder ställer krav på den nationella hanteringen av andra länders och organisationers skyddsvärda information.

Den militära säkerhetstjänsten förhandlar internationella säkerhetsskyddsöverenskommelser mellan Sverige och andra länder vars uppgift är att säkerställa ett informationsutbyte med fullgott säkerhetsskydd.

Signalskyddsöverenskommelser tecknas i de fall där Sverige planerar att låna ut eller sälja svenska signalskyddssystem till andra nationer eller internationella organisationer, eller då andra nationer eller internationella organisationer lånar ut eller säljer signalskyddssystem till Sverige.

En förhandling innebär att berörda parter ska vara överens om hela avtalets innehåll och innebörd. Varje nation har sin egen organisation där ärendet ska handläggas och erfarenheten säger att det tar minst tolv månader att förhandla fram ett generellt säkerhetsskyddsavtal.

Under 2011 genomfördes förhandlingar med Tyskland, Kroatien, Estland, Irland och Slovenien. Den militära säkerhetstjänsten har även rollen som nationell säkerhetsmyndighet (National Security Authority – NSA) i bilaterala säkerhetssamarbeten och har i denna roll fått hantera uppkomna säkerhetsfrågor.

Internationella signalskyddsöverenskommelser (COMSEC Agreements) är skriftliga, oftast bilaterala, avtal som förhandlas och ingås av Försvarsmakten eller annan myndighet på bemyndigande av regeringen.

En signalskyddsöverenskommelse reglerar bl.a. vilka signalskyddssystem som ska användas, hur kryptonycklar och signalskyddsmateriel ska hanteras och förvaras, distribution/transporter, åtgärder vid signalskyddsincidenter, signalskyddsutbildning, behörigheter och ansvar.

MAZAR-E-SHARIF 2011 Svenska stridssjukvårdare övar medevac tillsammans med amerikansk blackhawk och besättning strax utanför Camp Marmal inte långt ifrån svensk-finska Camp Northern Lights i Mazar-e-Sharif. Sverige bidrar med soldater till Isaf, International Security Assistance Force, i norra Afghanistan. Isaf etablerades 2001 och arbetar under ett mandat av FN:s säkerhetsråd och ett avtal mellan Isaf-styrkan och den afghanska regeringen. Sverige leder sedan mars 2006 ett Provincial Reconstruction Team i Mazar-e-Sharif i Balkh-provinsen. Ansvarsområdet omfattar fyra provinser i den norra delen av landet. Den sammanlagda ytan motsvarar ungefär en femtedel av Sveriges. I det svenskledda styrkan ingår även personal från Finland. *Fotograf och bildtextförfattare: Henrik Klingberg FS21, Försvarsmakten*

Försvarsmakten har sedan tidigare ett stående regeringsbemyndigande att förhandla och ingå signalskyddsöverenskommelser med de länder eller internationella organisationer som Sverige har generella säkerhetsskyddsöverenskommelser med. Om ingen generell säkerhetsskyddsöverenskommelse finns måste ett regeringsbemyndigande sökas i varje enskilt fall innan en signalskyddsöverenskommelse får börja förhandlas.

Under 2011 har ett avtal tecknats med Finland för nyttjande av svenska signalskyddssystem vid insatsen i Kosovo samt ett avtal tecknats med Kroatien för användning av svenska signalskyddssystem inom ramen för Nordic Battle Group.

Fördjupade internationella samarbeten innebär också en ökad nationell specialisering och därmed ökade beroenden av viktiga funktioner för försvaret av Sverige. Särskilt påtagligt är detta inom försvarsmaterielsektorn där utvecklingen alltmer går mot att inhemsk utveckling och produktion ersätts av internationella upphandlingar.

Detta ställer krav på förtroendet för utländska leverantörer t.ex. när det gäller leveranssäkerhet i en förhöjd krisnivå. I detta sammanhang måste Sverige vara en trovärdig partner och ge ett relevant skydd för uppgifter som Sverige får från andra länder och organisationer. Samtidigt måste Sverige ställa krav på att svensk information ges ett fullgott skydd när den delges för andra länder, mellanfolkliga organisationer och för utländska företag.

LIBYEN-INSATSEN FL 01

2011 genomfördes den första internationella flyginsatsen, FL01-insatsen över Libyen. Säkerhetskontoret gav stöd, både vid förberedelserna och under genomförandet av insatsen.

Insatsen var ledd av NATO och hela insatsen planerades under mycket korta tidsförhållanden. Stödet utgjordes bl.a. av att säkerhetskontoret lämnade in en begäran hos NATO om att få svensk tillgång till de NATO-kryptonycklar som senare användes för säker kommunikation mellan Sverige och övriga deltagande länder i insatsen OUP (Operation Unified Protector).

Målet för säkerhetstjänsten vid en insats är att alla avtal, nycklar eller system ska vara klara och framtagna när beslutet kommer. Av det skälet var FL01 viktig eftersom den insatsen skedde med mycket kort framförhållning. Erfarenheten av det använder vi oss av för att fortsätta att utvecklas och för att kunna ge ett ännu bättre stöd i morgon.