Bilaga till
dnr: 03200:3419/10:11

Utformning av ett tekniskt detekterings- och varningssystem för samhällsviktig verksamhet och kritisk infrastruktur

Redovisning av regeringens uppdrag
till Försvarets radioanstalt
(2010-04-14, Fö nr. 14)

Förord

Den tekniska utvecklingen har på några decennier gjort IT-användningen till en naturlig del av vardagen, vilket också har medfört nya hot och risker. För att kunna fortsätta utveckla IT-användandet som ett fundamentalt stöd i vår nationella infrastruktur måste arbetet med framtagandet av skyddsåtgärder följa samma takt som den övriga teknikutvecklingen.

Att ha en god förmåga att i realtid kunna detektera och varna för IT-angrepp är en väsentlig del av Sveriges skydd av samhällsviktig verksamhet och kritisk infrastruktur. För att åstadkomma det och för att få en god effekt inom detta område krävs såväl teknik och information som kompetenser inom flera olika discipliner, och ett brett samarbete mellan olika aktörer.

FRA har särskilda kunskaper och tillgång till unik information på området. Regeringen gav den 14 mars 2010 FRA i uppdrag att senast den 1 mars 2011 lämna förslag på hur ett tekniskt detekterings- och varningssystem för samhällsviktig verksamhet och kritisk infrastruktur kan utformas och införas. FRA redovisar sitt förslag i denna rapport. Arbetet har skett under koncentrerade former och synpunkter har inhämtats från andra myndigheter med särskilt ansvar inom informationssäkerhetsområdet.

Stockholm i februari 2011

Ingvar Åkesson
Generaldirektör

Jan Donnér
Chef informationssäkerhetsavdelningen

Sammanfattning

Denna rapport är ett svar på regeringens uppdrag den 14 april 2010, Fö nr 14, till Försvarets radioanstalt (FRA) att senast den 1 mars 2011 lämna ett förslag angående hur ett tekniskt detekterings- och varningssystem för samhällsviktig verksamhet och kritisk infrastruktur kan utformas och införas, samt att bedöma kostnaden för skapandet av ett sådant system.

Ett tekniskt detekterings- och varningssystem består mycket förenklat av sensorer, en kommunikationslösning och en central funktion för analys. Det är i första hand inte frågor av teknisk natur som avgör huruvida ett tekniskt detekterings- och varningssystem kommer att vara ett effektivt system. Även om det tekniska systemet är kapabelt i sig, så är det tillgången till värdefull kompetens, en bred informationsinhämtning och samverkan mellan olika discipliner som ger goda möjligheter att skapa ett slagkraftigt system.

Internet är idag en del av det svenska samhällets kritiska infrastruktur, och får anses så väsentlig att ett IT-angrepp i form av förstörelse, avbrott eller felaktigt utnyttjande skulle kunna ha en allvarlig effekt på Sveriges nationella säkerhet och ekonomiska välstånd. En av de unika aspekterna av IT-angrepp är att de kan initieras var som helst i världen. Antalet angrepp har ökat kraftigt de senaste åren. Därför är en väsentlig och kritisk aspekt av informationssäkerhetsarbetet att balansera resurstilldelningen mellan proaktiva och reaktiva skyddsmekanismer. Angriparna behöver bara hitta en enda sårbarhet som fungerar för deras syften, medan de proaktiva skyddsåtgärderna måste finna samtliga sårbarheter för att uppnå målet att skydda systemet. IT-system kommer alltid att bli angripna och en del av angreppen kommer att lyckas; därför måste en väsentlig del av skyddet bestå av just förmågan att upptäcka befintliga angrepp. Ett tekniskt detekterings- och varningssystem utgör således en väsentlig del av en verksamhets skydd.

En viktig framgångsfaktor för att åstadkomma ett verkningsfullt tekniskt detekterings- och varningssystem är utveckling av effektiva detekteringsverktyg. Ett sådant arbete underlättas av ett stort informationsutbud från olika källor. Information som har ett mervärde är bland annat information om faktiska IT-angrepp, kända och publikt okända sårbarheter samt aktörsspecifika detaljer. Tillgången till användbar information kan påverkas på flera sätt; genom att flera sensorer används, omvärldsbevakning, resultat från IT-säkerhetsrevisioner, egen forskning och underrättelsearbete, särskilt signalspaning.

Ett svenskt cyberförsvar syftar till att skydda Sverige och svenska intressen mot IT-angrepp från de mest resursstarka aktörerna. Med begreppet ”cyberförsvar” avses en nationell förmåga, som i sin helhet omfattar flera samverkande och enskilt nödvändiga komponenter, som krävs för att kunna svara mot den totala angreppsbilden som är mycket komplex. Utmaningen med att hantera IT-angrepp är mångfacetterad och för att skapa ett kvalificerat och dynamiskt cyberförsvar krävs kompetens från olika discipliner. Att kombinera kompetenser inom traditionellt informationssäkerhetsarbete med signalunderrättelseverksamhet ger unika möjligheter att skapa ett effektivt tekniskt detekterings- och varningssystem.

Innehållsförteckning

Förord **2**
Sammanfattning **3**
Innehållsförteckning **4**
1 Uppdrag, läsanvisning och begrepp **5**
1.1 Uppdrag 5
1.2 Läsanvisning 5
1.3 Begrepp 5
2 Inledning **8**
2.1 Hot mot samhällsviktig verksamhet och kritisk infrastruktur 8
2.2 Syftet med ett varnings- och detekteringssystem 9
2.3 Att förebygga och hantera IT-angrepp 9
2.4 Cyberförsvar 9
3 Förslag på en teknisk lösning **12**
3.1 Inledning 12
3.2 Introduktion till ett TDV 12
3.3 Tekniklösning 13
3.4 Detektering 16
3.5 Olika typer av system 18
3.6 Krav på systemet 19
3.7 Övrigt 20
4 Kostnader **21**
4.1 Utveckling av ett TDV 21
4.2 Drift och vidareutveckling 21

1 Uppdrag, läsanvisning och begrepp

1.1 Uppdrag

Den 14 april 2010 fick Försvarets radioanstalt (FRA) i uppdrag av regeringen att den 1 mars 2011 lämna ett förslag hur ett tekniskt detekterings- och varningssystem för samhällsviktig verksamhet och kritisk infrastruktur kan utformas och införas[1]. I uppdraget ingår även att FRA ska bedöma kostnaden för skapandet av ett tekniskt detekterings- och varningssystem.

Uppdraget har genomförts av en arbetsgrupp inom FRA. Arbetsgruppen har inledningsvis inhämtat kunskaper och erfarenheter från andra länder, däribland Norge, vilka har detekterings- och varningssystem i drift. Under arbetet har representanter för de myndigheter som ingår i Samverkansgruppen för informationssäkerhet (SAMFI) kontaktats och beretts tillfälle att lämna synpunkter. Försvarsdepartementet har under arbetets gång informerats om hur uppdraget framskridit.

Frågan om vilka aktörer som bör få tillgång till ett tekniskt detekterings- och varningssystem behandlas av Myndigheten för samhällsskydd och beredskap med anledning av det uppdrag regeringen gav myndigheten den 14 april 2010, Fö nr 13.

1.2 Läsanvisning

Ett tekniskt detekterings- och varningssystem kommer fortsättningsvis i rapporten att benämnas TDV.

Inledningsvis beskriver rapporten hotet mot det svenska samhället, dess samhällsviktiga verksamhet och kritiska infrastruktur. Vidare beskrivs syftet med ett TDV. Därefter följer en redogörelse för begreppet cyberförsvar, med en beskrivning av ett TDV:s roll i ett sådant sammanhang.

I kapitel 3 redogörs för hur ett TDV kan utformas. Initialt ges en introduktion till området, därefter följer en teknisk beskrivning. Vidare förklaras hur arbetet med detektering går till och några olika typer av system presenteras. Avslutningsvis följer en närmare beskrivning av vilka krav som bör ställas på ett TDV samt en kort beskrivning av vad det skulle kunna bidra med utöver detektering och varning.

I kapitel 4 följer avslutningsvis en redogörelse kostnader för skapande av ett TDV.

1.3 Begrepp

Många begrepp som är relaterade till detektering av och varning för IT-angrepp saknar entydiga definitioner. I detta avsnitt beskrivs kortfattat ett antal av de viktigaste begreppen och vilken betydelse de har givits i denna rapport.

[1] Fö nr 14

1.3.1 IT-angrepp

IT-angrepp är en bred term som omfattar alla IT-relaterade angreppsformer, såsom skadlig kod och tillgänglighetsangrepp. Många IT-angrepp utnyttjar en sårbarhet i målsystemet.

1.3.2 Skadlig kod

Med skadlig kod avses ett program som syftar till att utföra oönskade åtgärder på ett datorsystem. Begreppet skadlig kod omfattar alla former av elakartad kod, till exempel trojaner, maskar, rootkits och virus. Oönskade konsekvenser av skadlig kod kan till exempel vara otillåten åtkomst av information och otillåten fjärrstyrning av datorer.

1.3.3 Sårbarhet

En sårbarhet, i ett system, är någon form av fel som tillåter en angripare att kompromettera data eller tillskansa sig privilegier som inte uttryckligen beviljats, även när systemet används på rätt sätt.

1.3.4 Tekniskt detekterings- och varningssystem (TDV)

Angreppsdetektering är en process för att bevaka ett datornätverk eller datorsystem i syfte att upptäcka och identifiera förekomst av IT-angrepp eller förberedelse inför potentiella IT-angrepp. Ett TDV är ett system som automatiserar detektering av och varning för IT-angrepp.

1.3.5 Tillgänglighetsangrepp

Tillgänglighetsangrepp syftar till att begränsa eller helt stoppa möjligheterna för målsystemet att fungera som avsett. Ett exempel på denna form av angrepp är när många datorer instrueras att skicka stora mängder trafik till en enda dator[2].

1.3.6 Detektering av IT-angrepp

Detektering syftar till att upptäcka bevis eller indikationer på IT-angrepp. Själva detekteringen utförs genom att analysera den nätverkstrafik som inkommer till TDV. Vid detektering av IT-angrepp kan larm genereras som indikerar vilken typ av angrepp som pågår.

Metoder för detektering av IT-angrepp
De två huvudgrupperna av detekteringsmetoder som används är signatur- och avvikelseanalys. Definitionerna av dessa grupper är breda och i viss mån även överlappande. Metoderna kan användas antingen separat eller i kombination beroende på ändamålet. Ett bra TDV innehåller båda varianterna av detekteringsmetoder för att tillgå en så bred detekteringsarsenal som möjligt.

Avvikelseanalys
Avvikelseanalys används för att finna anomalier från vad som kan anses vara normalt för en viss sorts händelse, till exempel vid beteendeanalys av standardiserade nätverksprotokoll. En djupanalys av till synes normal trafik kan upptäcka om ett nätverksprotokoll används på ett annat sätt än vad som är avsett. Avvikelseanalys kan utnyttjas för att upptäcka okända och dolda kommunikationskanaler som används för att fjärrstyra IT-angrepp.

[2] Distributed Denial-of-Service attack (DDoS-attack).

Metoden syftar inte på en allmän statusundersökning som till exempel information om huruvida nätverkstrafiken ökar med ett visst antal procent mot ett givet datorsystem. Sådan information ger en analytiker mycket små möjligheter att avgöra om avvikelsen kan bero på ett IT-angrepp då indikationerna blir för grova.

Denna analysform är även lämplig för att identifiera okända angreppsformer. Tillgång till stora informationsmängder kan även möjliggöra identifiering av bakomliggande aktörer.

Signatur
En signatur är ett sökmönster som representerar karakteristiska egenskaper för ett sökt objekt. Signaturerna jämförs mot observerad nätverkstrafikr för att identifiera IT-angrepp.

Signaturer kan bestå av allt från enkel information till komplexa sökmönster där flera enskilda signaturer kombineras. Signaturer är en effektiv metod för att upptäcka kända angrepp, men relativt ineffektiv för att finna okända angreppsformer och varianter av en redan känd angreppsform.

Detekteringsverktyg
Ett detekteringsverktyg utgörs av ett program som implementerar en viss typ av analysmetod, till exempel ett program som genomsöker data efter givna signaturer.

2 Inledning

2.1 Hot mot samhällsviktig verksamhet och kritisk infrastruktur

Datorer och kommunikationsteknik har utvecklats enormt i hastighet och förmåga de senaste decennierna och dramatiskt ändrat det sätt på vilket människor interagerar med varandra och sin omgivning. Detta har också lett till en signifikant utveckling av betydelsen av datorkommunikation som en väsentlig funktion för såväl ekonomin som det sociala och politiska välmåendet i mer utvecklade länder. De separata tekniska elementen, individuella datorer och kommunikationssystem, stöttar många av våra dagliga aktiviteter, både under arbetstid och i privatlivet. De är fundamentala i stödet av vår nationella infrastruktur och informationshantering.

Internet är idag en del av det svenska samhällets infrastruktur, på samma sätt som järnväg, vägtrafik, flyg och sjöfart. Den kritiska infrastrukturen kan anses så väsentlig att angrepp i form av förstörelse, avbrott eller felaktigt utnyttjande skulle kunna ha en allvarlig effekt på Sveriges nationella säkerhet och ekonomiska välstånd. Ett avancerat IT-angrepp kan ha olika stor påverkan på en nation beroende på hur väl utvecklat landet är och hur stort beroendet av Internet är för olika samhälleliga tjänster. Sverige är i hög grad beroende av Internet för att många olika verksamheter ska fungera, som till exempel myndigheternas service till medborgarna, transporter, kraftförsörjning och de finansiella systemen. Därför är det viktigt att ha ett väl utvecklat skydd för den kritiska infrastrukturen och samhällsviktiga verksamheter.

En av de unika aspekterna av IT-angrepp är att de kan initieras var som helst i världen. Datorer kan komprometteras och användas som plattformar för att angripa system som återfinns i andra länder. Även svenska system utnyttjas systemägaren ovetandes som verktyg i angrepp riktade mot system runt om i världen. Detta medför att en identifiering av en aktör bakom en attack är komplicerad och svår. IT-angrepp kan vara billiga, enkla att iscensätta och svåra att spåra. Antalet angrepp har ökat kraftigt de senaste åren och anledningen till ökningen är en kombination av flera faktorer, bland annat att:

- antalet personer som har fått tillgång till Internet och har tillräckliga kunskaper ökar
- utvecklingen av och tillgången till fritt tillgängliga verktyg för att skapa avancerade former av skadlig kod ökar
- antalet aktörer har ökat m.a.a. att stora monetära värden är möjliga att exploatera genom IT-angrepp.

Den ökande frekvensen och målinriktningen av IT-angrepp inkluderar tillgänglighetsangrepp, spionage, propaganda och informationsstöld. Många länder arbetar därför med att integrera offensiva och defensiva IT-förmågor i de nationella strategierna för att förbättra skyddet av den kritiska infrastrukturen.

Sverige är inte mindre utsatt än andra länder. Vårt land är ett tydligt mål för en mängd av dessa olika angrepp och angreppen är globala. IT-angrepp mot svenska intressen pågår kontinuerligt. Det finns idag ingen samlad lägesbild av IT-angrepp och ingen analys av trender avseende angrepp mot samhällsviktiga verksamheter och kritisk infrastruktur. Det nuvarande säkerhetsskyddet bygger till stor del på att de enskilda verksamheterna själva upptäcker incidenter. Varierande nivå på kompetens och tekniska

lösningar gör dock att möjligheten att upptäcka incidenter varierar stort mellan olika verksamheter.

2.2 Syftet med ett varnings- och detekteringssystem

Syftet med ett TDV är att upptäcka och möjliggöra skyddsåtgärder mot IT-angrepp riktade mot svensk samhällsviktig verksamhet och kritisk infrastruktur.

Ett TDV ska inte fungera som ersättning för olika verksamheters befintliga säkerhetsåtgärder, som till exempel kommersiella produkter, utan är att betrakta som ett förstärkt skydd.

2.3 Att förebygga och hantera IT-angrepp

I arbetet med att förhindra IT-angrepp måste hänsyn tas till viktiga aspekter som angreppsformer, vanliga och viktiga sårbarheter, angripare och motiv. För att på bästa sätt kunna kartlägga och hantera angrepp behövs en helhetssyn, som sammanställer en lägesbild baserad på en bred informationsinhämtning och analys vilket resulterar i konkreta skyddsåtgärder.

De aktörer som ägnar sig åt att angripa IT-system och nätverk är väl införstådda med att de hela tiden måste förnya sina metoder i syfte att undkomma de nya skydds-mekanismer som applicerats runt målsystemet. Detta resulterar i en ständig katt-och-råtta-lek där angriparna alltid försöker ligga steget före. Angriparna behöver bara hitta en enda sårbarhet som fungerar för deras syften, medan de proaktiva skyddsåtgärderna måste finna samtliga sårbarheter för att uppnå målet att skydda systemet. Därför är en väsentlig och kritisk aspekt av informationssäkerhetsarbetet att balansera resurstilldelningen mellan proaktiva och reaktiva skyddsmekanismer.

Det behöver givetvis finnas adekvata rutiner för att säkra upp informationssystemen inklusive kontinuerliga och skyndsamma säkerhetsuppdateringar av kända sårbarheter, men det är också av yttersta vikt att det finns adekvata mekanismer som upptäcker såväl misstänkta angreppsförsök som lyckade angrepp. IT-system kommer alltid att bli angripna och en del av angreppen kommer att lyckas. Därför måste en väsentlig del av skyddet bestå av just förmågan att upptäcka befintliga angrepp. Ett TDV utgör därför en väsentlig del av en verksamhets skydd.

2.4 Cyberförsvar

Ett cyberförsvar syftar till att skydda Sverige och svenska intressen mot IT-angrepp från de mest resursstarka aktörerna. Begreppet ”cyberförsvar” står i detta sammanhang för en nationell förmåga som i sin helhet omfattar flera olika, sinsemellan samverkande och enskilt nödvändiga komponenter.

Den totala angreppsbilden är mycket komplex då den består av flera olika typer av aktörer med varierande motiv, angreppsmetoder och nivåer av skicklighet. Av den anledningen behöver det svenska cyberförsvaret svara upp mot komplexiteten i sin helhet, med flera nivåer och olika kombinationer av funktioner och resurser. Det finns ingen enskild del i samhället som självständigt kan ansvara för hela cyberförsvaret utan det kräver en aktiv och effektiv samverkan mellan alla delansvariga. Det krävs förmågor på följande nivåer:

1. Strategisk styrning och planering
2. Samverkan och koordinering
3. Operativa skyddsåtgärder.

Den strategiska nivån upprätthåller en överblick över den totala förmågan och behoven inom hela området. Den följer upp att relevanta funktioner, kontaktytor och samarbeten upprättas och fungerar. På denna nivå sammanställs och framförs förbättringsbehoven uppåt och nedåt avseende resurstilldelning, reglering och policy.

Nivå två består huvudsakligen av ett samverkansorgan med tilldelade resurser från de viktigaste kunskaps- och ansvarsinstanserna. Samverkansorganet utgör den initiala kontaktytan gentemot det övriga samhället för IT-relaterade angrepps- och skyddsfrågor. Denna nivå samlar kunskaper från alla involverade, sammanställer hotbildsbedömningar och trendanalyser, bereder policyfrågor samt informerar och upprätthåller en mycket god operativ samverkan och sammantagen lägesbild.

Den operativa nivån hanterar den tekniska kompetensen, realtidsdetekteringen och lämnar förslag till skyddsåtgärder inom olika områden såsom nationellt samhällsviktiga informationssystem och kritisk infrastruktur. Detta innefattar bevakning och larm till berörda parter för omedelbar åtgärd, samt sammanställning och rapportering av incident-, aktörs- och trendanalyser. Här ingår även kompetenser och funktioner för policytillämpning samt proaktiva och reaktiva skyddsåtgärder.

Så länge det finns luckor på någon av dessa tre nivåer är cyberförsvaret bristfälligt.

2.4.1 Aktörer och motiv

De mest resursstarka aktörerna är huvudsakligen statliga eller statsunderstödda men kan även utgöras av andra formationer. Det som utmärker dessa aktörer är en stor tillgång till kompetenser, teknik och ekonomiska medel. De upprätthåller en kontinuerligt hög förmåga att kringgå befintliga skyddsmekanismer, vilket medför att det är exceptionellt svårt att skydda sig mot deras angrepp. De angrepp som lyckas kan bland annat medföra allvarliga konsekvenser för Sveriges samhälleliga förmåga att tillgodose våra behov i såväl fred, kris som krig. Vidare så kan dessa företeelser påverka svenska företags möjligheter att växa och frodas i en global marknad på lika villkor, vilket även i en förlängning kan komma att påverka hela det svenska samhället på ett negativt sätt.

De finns många olika avsikter med att genomföra IT-angrepp, varav de allvarligaste ur ett nationellt perspektiv kan delas in i fyra huvudsakliga inriktningar:

- ekonomisk brottslighet (elektronisk stöld)
- industrispionage
- underrättelseinhämtning (statlig/statsunderstödd)
- påverkan (alltifrån manipulation av information till sabotage och utslagning av hela samhällsfunktioner).

Uppbyggnaden av ett robust och komplett cyberförsvar kräver att de olika angreppsmotiven behandlas med en korrekt inbördes balans avseende faktisk skadeverkan för svenska intressen. Den sista punkten har hittills relativt sällan förekommit mot svenska intressen och endast i förhållandevis hanterlig skala. Men

sådana IT-angrepp kan komma att användas mot vårt land och åstadkomma stor skada. De tre första punkterna förekommer ständigt i allt ökande omfattning och det finns goda skäl att befara att dessa företeelser idag medför förluster av ansenliga värden för det svenska samhället.

2.4.2 Ett nationellt TDV i ett svenskt cyberförsvar

Ett adekvat detekteringssystem larmar både för intrångsförsök och för pågående, lyckade intrång, till exempel när den skadliga koden för ut information från nätverket. När så sker krävs att respektive verksamhet har funktioner och rutiner som gör det möjligt att inte bara stoppa det pågående utflödet utan även lokalisera den specifika komponenten i systemet som är infekterad. Detta främst för att sanera infektionen, men även för att i vissa fall kunna göra en forensisk analys[3] och menbedömning av händelsen.

Utmaningen med att hantera IT-angrepp är mångfacetterad och för att skapa ett kvalificerat och dynamiskt cyberförsvar krävs kompetens från olika discipliner. En viktig framgångsfaktor är möjligheten att kombinera kompetenser inom traditionellt informationssäkerhetsarbete med information som kan erhållas genom säkerhets- och underrättelsetjänst, särskilt signalspaning. Ett nationellt tekniskt detekterings- och varningssystem är en viktig del i ett svenskt cyberförsvar.

[3] I syfte att säkra bevis från digitala medier.

3 Förslag på en teknisk lösning

3.1 Inledning

I detta kapitel redogörs för hur ett TDV kan utformas. Initialt ges en introduktion till området, som följs av en teknisk beskrivning. Vidare förklaras arbetet med detektering och några olika typer av system presenteras. Avslutningsvis följer en närmare beskrivning av vilka krav som bör ställas på ett TDV och en kort beskrivning av vad det skulle kunna bidra med utöver detektering och varning.

Det bör noteras att det i första hand inte är frågor av teknisk natur som avgör huruvida ett TDV kommer att vara ett effektivt system. Även om det tekniska systemet är kapabelt i sig, så är det tillgången till värdefull kompetens, en bred informations-inhämtning och samverkan mellan olika discipliner som ger goda möjligheter att skapa ett slagkraftigt system.

Skydd av information i IT-system är mest effektivt när olika skyddsnivåer kombineras. För samhällsviktiga verksamheter och kritisk infrastruktur erfordras fler än två komponenter[4] i ett väl fungerande säkerhetsskydd, såsom ett system för att upptäcka angrepp. Ett TDV ska inte fungera som ersättning för annan säkerhetsfunktionalitet, som till exempel kommersiella produkter, utan är att betrakta som ett förstärkt skydd.

3.2 Introduktion till ett TDV

Angreppsdetektering är en process för att upptäcka och identifiera förekomst av IT-angrepp eller förberedelse inför potentiella IT-angrepp. Ett detekteringssystem är ett program som automatiserar detektering, som i sin tur kan leda till varningar. Dessa kan bidra till att verksamheter som har drabbats av IT-angrepp kan vidta skyddsåtgärder. Ett TDV består mycket förenklat av sensorer, en kommunikationslösning och en central funktion för analys.

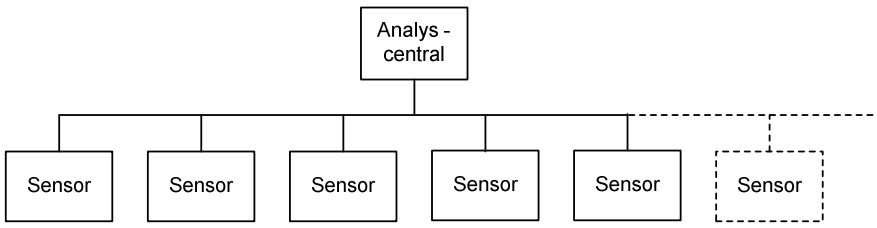

Bild 1: Enkel beskrivning av ett TDV

Sensorerna i ett TDV analyserar trafik som passerar i nätverk. Då trafik inkommer till sensorn så undersöks den för att identifiera IT-angrepp. Det sker med hjälp av olika detekteringsmetoder såsom signatur- och avvikelseanalys. Detekteringsmetoderna undersöker de olika protokollagren (IP, TCP, mm) i OSI-modellen[5] och informationsinnehållet i trafiken för att försöka upptäcka IT-angrepp. Ofta kombineras olika detekteringsverktyg för att uppnå högre effekt och undvika falska detekteringslarm. När ett IT-angrepp upptäcks skickas ett larm som kan gå såväl till den

[4] Som exempelvis brandvägg och antivirusprogram.
[5] OSI-modellen är en konceptuell modell för datorkommunikation och består av sju lager.

verksamhet som är utsatt för IT-angreppet som till analyscentralen. Med larmet bifogas också information om IT-angreppet som den angripna verksamheten kan använda till att åtgärda sårbarheter samt återställa skadade datorsystem.

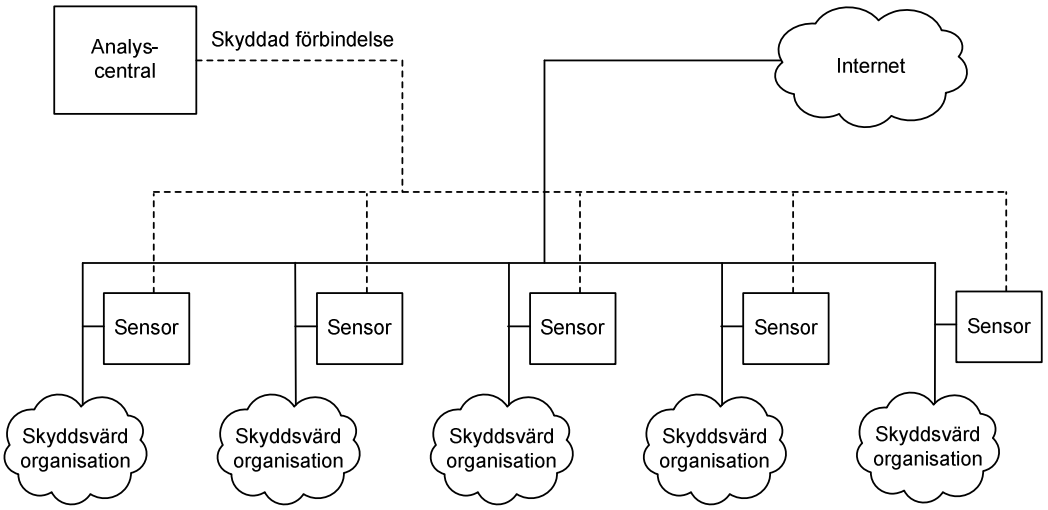

Bild 2: En installation av ett TDV

Ett nationellt TDV bör vara distribuerat, anpassningsbart och säkert. Delarna i ett TDV utgörs av sensorer som, via säkra förbindelser, är kopplade till en central funktion**.** Sensorerna bör vara modulärt uppbyggda för att kunna anpassas efter varierande behov och verksamheter. De moduler som återfinns i respektive sensor kan använda olika former av avancerade detekteringsmetoder. Ett TDV måste kunna hantera stora trafikmängder och därutöver är det viktigt att systemets integritet säkerställs.

3.3 Tekniklösning

3.3.1 Beskrivning av en sensor

Detta avsnitt ger en övergripande beskrivning av hur en sensor kan utformas och hur den kan samverka med övriga delar i ett TDV.

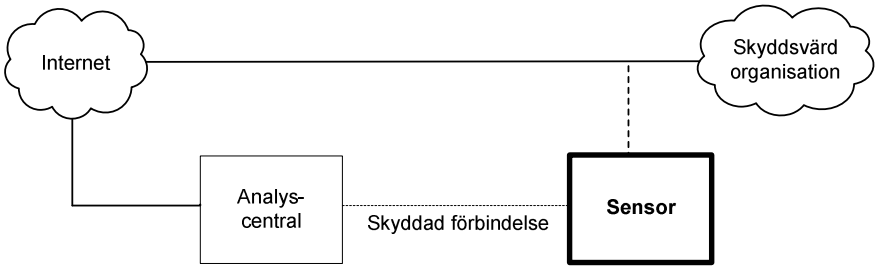

Bild 3: Sensorns roll i ett TDV

Sensorn är den komponent som svarar för detektering och larm. Sensorn analyserar ett trafikflöde och en analysprocess, som kan involvera en eller flera olika analysmoduler, utför detekteringen. En analysmodul kan till exempel innehålla signaturer som kan

användas för att identifiera skadlig kod. Olika moduler kan användas för olika typer av detekteringsmetoder.

Då den inkommande trafiken analyserats och ett IT-angrepp har identifierats skickas resultatet till en larmprocess. Denna ansvarar för att sända ett larm, som kan skickas både till den verksamhet som ska skyddas och till funktionen för central analys.

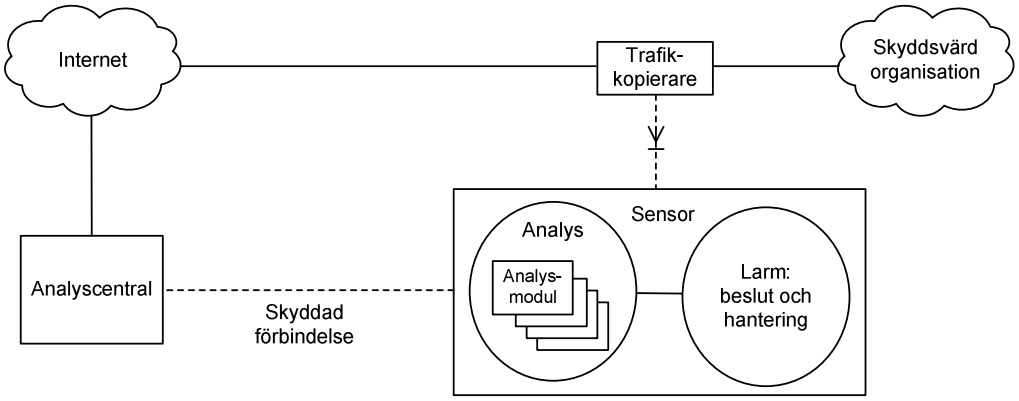

Bild 4: En sensor mer i detalj

3.3.2 Placering

Sensorn bör placeras mellan Internet och den verksamhet som ska skyddas vilket innebär att den bör placeras utanför verksamhetens egen skyddsbarriär (till exempel brandvägg). Placeringen av sensorn är viktig för att

- kunna ge en oförvanskad trafikbild[6]
- kunna upptäcka IT-angrepp som sker samordnat mot flera organisationer
- kunna urskilja angreppstrender
- undvika att sensorn får tillgång till organisationens interna trafik.

Då det gäller anslutningen av en sensor till ett nätverk kan det göras på flera olika sätt. Antingen kan placeringen göras så att all trafik passerar rakt igenom sensorn eller så används en nätverksprodukt, en så kallad trafikkopierare, som kopierar trafiken till sensorn. Det tillvägagångssätt som rekommenderas är det sistnämnda. Överföringen från trafikkopieraren bör vara enkelriktad, vilket innebär att sensorn blir helt passiv och ingen påverkan kan göras på trafikflödet och dess innehåll. En passiv lösning innebär även ett extra säkerhetsskydd för sensorn, vilket är en fördel då denna kategori av system ofta är utsatta för angrepp.

[6] Skyddsbarriärer filtrerar bort trafik och för att fylla sitt syfte bör en sensor kunna se all trafik.

3.3.3 Kommunikation

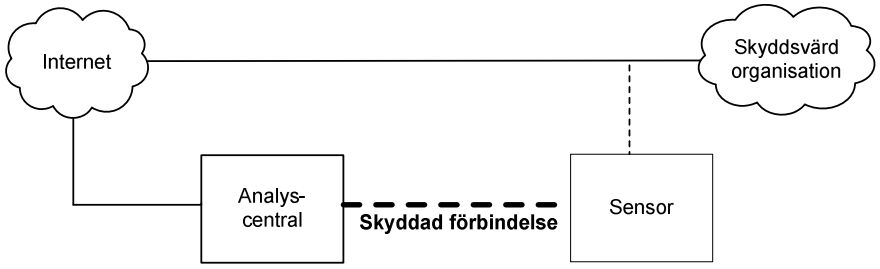

Bild 5: Kommunikationen i ett TDV

Kommunikationen mellan en sensor och den centrala funktionen för analys måste gå via en skyddad förbindelse. En sådan förbindelse kan utformas på olika sätt, en vanligt förekommande metod är att använda en VPN-lösning[7] för att skapa en krypterad kommunikation över Internet. En annan metod, vilket ökar säkerheten ytterligare, är att installera separata nätverksförbindelser över vilken trafiken kan skickas krypterad. Sensorerna i ett TDV kommunicerar aldrig med varandra, all kommunikation är av integritets- och säkerhetsskäl[8] begränsad till att enbart ske mellan analyscentralen och sensorerna. Kommunikationen består av larm från sensorerna till analyscentralen och nya eller förbättrade detekteringsverktyg från analyscentralen till sensorerna.

3.3.4 Central funktion för analys

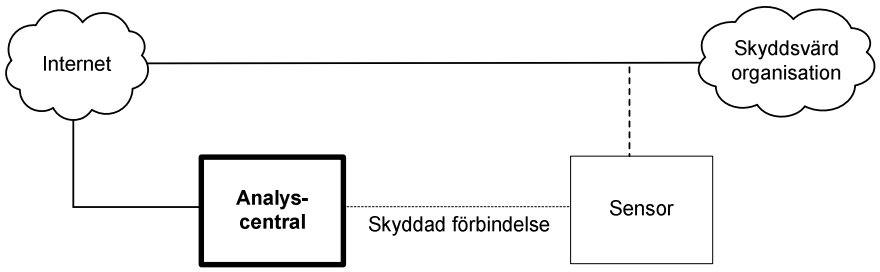

Bild 6: Den centrala analysfunktionens roll i ett TDV

I en central funktion för analys bör personer med olika kompetensprofiler, bedriva det löpande arbetet med analys och skapande av detekteringsverktyg. Den centrala funktionen bör ansvara för att genomföra analyser av skadlig kod, skapa nya och

[7] VPN är en engelsk förkortning av Virtual Private Network, vilket är ett sätt att skapa ett säkert virtuellt nätverk över ett existerande osäkert nätverk (oftast Internet). Denna lösning är dock känslig mot tillgänglighetsattacker.
[8] För att motverka spridningseffekter mellan sensorer om en sensor skulle bli utsatt för ett IT-angrepp.

förbättra befintliga detekteringsverktyg samt skyndsamt distribuera detekteringsverktyg till sensorerna.

Analysarbetet syftar till att skapa kunskap om olika former av angrepp och på så sätt möjliggöra utveckling av detekteringsverktyg. Analys kan ske på ett enskilt IT-angrepp men även på mer komplexa och koordinerade IT-angrepp, vilket möjliggörs med ett TDV där flera sensorer kopplats samman mot en analyscentral. Då innovationstakten inom IT-angreppsområdet är snabb krävs en ständig utveckling av nya och förbättrade detekteringsverktyg och en snabb distribution av verktyg till samtliga anslutna sensorer via den skyddade förbindelsen.

Fördelarna med ett TDV, bestående av en central funktion och många sensorer, är möjligheten att utifrån ett stort underlag av trafikdata kunna

- upptäcka koordinerade IT-angrepp
- skapa effektiva detekteringsverktyg
- skapa en bra förståelse för aktuella angreppstrender
- ge en samlad lägesbild.

Vidare innebär det att då en ny form av IT-angrepp identifieras kan hela den stora träffytan, som många anslutna sensorer utgör, snabbt uppdateras med nya verktyg.

3.4 Detektering

3.4.1 Detekteringsstrategi

En viktig framgångsfaktor, för att åstadkomma ett verkningsfullt TDV, är utveckling av effektiva detekteringsverktyg. Skickliga angripare bedriver sin verksamhet utifrån förutsättningen att skyddet hela tiden förbättras och förändrar därför kontinuerligt sina egna metoder i syfte att hela tiden ligga steget före. Detekteringsverktyg som enbart fokuserar på redan kända företeelser räcker inte till för att skydda mot sofistikerade angripare. För ett effektivt och väl fungerande detekteringsarbete behövs

- analys av IT-angrepp
- analys av program i syfte att hitta okända sårbarheter
- utveckling av detekteringsverktyg
- stort informationsunderlag om IT-angrepp, sårbarheter, hotbilder och omvärldsanalyser
- möjligheter till bred informationsinhämtning via bland annat underrättelsearbete och internationellt kunskapsutbyte.

Den analys av IT-angrepp som görs i sensorerna sker helt automatiserat, medan analys av IT-angrepp i den centrala analysfunktionen till största delen sker manuellt. Manuell analys är en tidskrävande och komplex aktivitet men helt nödvändig för att skapa verksamma detekteringsverktyg. För att ligga steget före en angripare behövs också analys av program för att hitta okända sårbarheter.

Detekteringsverktyg kan fungera på olika sätt, men gemensamt är att de arbetar antingen med signatur[9]- eller avvikelseanalys[10]. Nyckeln till verkningsfulla detekteringsverktyg är analysalgoritmer som är kapabla att sortera ut ett pågående IT-angrepp ur dagens stora trafikmängder, i realtid och med ett korrekt resultat.

Utveckling av detekteringsverktyg underlättas av ett stort informationsutbud från olika källor. Information som har ett mervärde är bland annat information om faktiska IT-angrepp, kända och publikt okända sårbarheter samt aktörsspecifika detaljer. Tillgången till användbar information kan påverkas på flera sätt; genom att flera sensorer används, omvärldsbevakning, resultat från IT-säkerhetsrevisioner, egen forskning och underrättelsearbete.

3.4.2 Underrättelseinformation

IT-angrepp är globala och ständigt pågående aktiviteter som även är riktade mot svenska intressen. Aktionsradien för IT-angrepp spänner över hela Internet och angrepp sänds allt som oftast via en komplicerad kedja av sammankopplade datorer spridda över stora delar av Internet.

Underrättelsearbete kan ge tillgång till information om globala initieringspunkter och kommunikationskanaler för IT-angrepp. Särskilt signalspaning om angriparens identitet, kapacitet, motivation, operationsområden, metoder och verktyg är viktiga ingångsvärden vid framtagning av effektiva detekteringsverktyg. Samarbetet med andra länder i signalspaningsfrågor och i frågor om informationssäkerhet kan ge unik och kompletterande information som kan användas i detta sammanhang.

Utmaningen att skydda mot IT-angrepp är mångfacetterad och för att skapa ett kvalificerat och dynamiskt TDV bör skyddsarbetet fortgå på flera olika plan. En helhetssyn som kombinerar analyserad information från traditionellt informationssäkerhetsarbete och signalunderrättelseverksamhet ger unika möjligheter att skapa ett effektivt TDV. Underrättelseinformation är särskilt viktig när det gäller att upptäcka förberedelser av IT-angrepp.

3.4.3 Skyddsvärde

Alla detekteringsverktyg som används i ett TDV är skyddsvärda och har olika känslighetsgrad. Verktyg som kommer från öppna källor är allmänt kända medan andra verktyg kan vara känsliga i olika grad. Även om de använda verktygen är allmänt kända så kan det sammansatta urvalet vara skyddsvärt. Forskningsresultat om tidigare okända sårbarheter är skyddsvärda, liksom verktyg för att upptäcka aktörsspecifika avancerade IT-angrepp mot svenska intressen.

Exponering av implementerade detekteringsverktyg avslöjar TDV:s inriktning och kapacitet, vilket kan ge en angripare möjlighet att undvika detektering. Kunskap om detekteringsverktygen kan utnyttjas för att skapa nätverkstrafik som medvetet genererar falska larm. Detta kan göras i syfte att skapa förvirring, iscensätta ett

---

[9] Ett trivialt exempel är den textbaserade signaturen *”cat ’+ +’ > /.rhosts”*, vilken har potential att göra UNIX-baserade operativsystem sårbara för nätverksbaserade angrepp. Givet att ”rlogin”-tjänsten är aktiverad så tillåter kommandot valfri användare från valfri maskin att logga in utan att använda lösenord. Notera att just denna sårbarhet är gammal, allmänt känd och att det avrådes från att använda tjänsten.
[10] Ett exempel är analys av välkända nätverksprotokoll för att finna avvikelser som ger indikationer om dolda kommunikationskanaler.

tillgänglighetsangrepp eller för att försöka dölja ett verkligt intrångsförsök i en mängd irrelevanta larm.

Alla verktyg som har sitt ursprung i underrättelseinformation är mycket känsliga till sin natur då de kan avslöja hur underrättelsearbetet bedrivs och dess kapacitet.

3.5 Olika typer av system

Med en anpassningsbar teknisk lösning är det lätt att, utifrån ett och samma grundsystem, tillhandahålla flera systemvarianter för att tillfredställa olika behov. Användningen av olika systemlösningar kan ha varierande orsaker som till exempel ekonomiska och kundspecifika skäl, storleken på trafikmängden, verksamhetens skyddsvärde och möjlighet att uppfylla ställda säkerhetskrav.

Med anpassningsbar åsyftas att den tekniska lösningen skall kunna användas på olika datorer med olika prestanda samt att det bör vara möjligt att distribuera ut analysmoduler till flera datorer och välja vilka detekteringsverktyg som ska installeras. En avancerad sensor kan bestå av flera datorer och använda resurskrävande detekteringsverktyg, medan en enklare sensor kan producera goda resultat på en normal dator.

3.5.1 Exempel på två system

Nedan ges exempel på två TDV som är av olika karaktär och fyller olika syften.

En systemlösning skulle kunna utgöras av ett nationellt nätverk av TDV innehållande allmänt kända och mindre känsliga detekteringsverktyg. Valda verktyg möjliggör detektering av ett urval av vanligt förekommande IT-angrepp i syfte att skapa en nationell och sektorbaserad IT-angreppsbild. Denna typ av system baseras i hög grad på öppenhet och tillit mellan anslutna organisationer eftersom valda detekteringsverktyg är kända av alla inblandade parter.

En annan systemlösning skulle kunna agera grundstomme i ett framtida cyberförsvar. Ett sådant system kräver en mer avancerad lösning som kan analysera datatrafik i syfte att upptäcka ett större spektrum av IT-angrepp. Detekteringen kan utföras av en kombination av verktyg, baserade på både signatur- och avvikelseanalys, varav vissa kan utformas för att upptäcka mer sofistikerade aktörer. Det sistnämnda innebär att verktygen blir mycket känsliga för exponering, då kännedom om dem avslöjar systemets kapacitet och inriktning.

Gemensamt för organisationer anslutna till ett TDV, oavsett typ, är att de löpande ska informeras om pågående IT-angrepp samt motta nya och förbättrade detekteringsverktyg.

3.6 Krav på systemet

3.6.1 Prestandakrav

Teknikutvecklingen driver ständigt fram allt högre trafikhastigheter vilket ställer stora krav på den tekniska lösningen. Ett TDV måste redan från början stödja stora datamängder och det måste finnas utvecklingspotential för att öka den maximala kapaciteten.

Den trafikmängd som en viss specifik implementation av ett TDV bör klara att hantera är beroende av vilka detekteringsverktyg som ska användas, mängden signaturer samt det trafikflöde som ska undersökas. En viktig parameter är val av detekteringsverktyg eftersom vissa verktyg är mer resurskrävande än andra. Valet av ett TDV som är anpassat till den aktuella verksamhetens trafikmängder är viktigt för att undvika att larm fördröjs.

Erfarenheten av denna typ av system visar att det i dagsläget är fullt möjligt att klara av stora trafikmängder (Gb/s) med hjälp av kraftfulla datorer. Denna kapacitet är i dagsläget helt tillräcklig för att skydda en enskild organisation. En vidareutveckling av systemet och parallellisering mellan ytterligare datorer kan möjliggöra en ökning av dagens kapacitet.

3.6.2 Säkerhetskrav

Rigorösa säkerhetskrav krävs för att säkerställa integriteten av ett TDV. Säkerhetskrav bör ställas inom följande områden:

- fysisk säkerhet
- säkerhet för detekteringsverktyg
- kommunikationssäkerhet
- övriga säkerhetskrav.

Då ett TDV innehåller skyddsvärda detekteringsverktyg måste den tekniska utrustningen placeras i en fysiskt skyddad miljö. Datorerna bör även innehålla fysiska manipuleringsskydd. Om placering i en fysiskt skyddad miljö inte är möjlig kan särskilt känsliga detekteringsmoduler inte användas. Vidare bör det finnas särskilda skyddsmekanismer för enskilda detekteringsverktyg, till exempel för signaturer.

Den förbindelse som knyter samman alla sensorer med analyscentralen kräver en hög säkerhet för att garantera integriteten, antingen används separata nätverkskopplingar eller en VPN-lösning över Internet. Oavsett lösning så bör en kryptografisk metod, som är anpassad för ändamålet, användas för att skydda trafiken.

I övrigt krävs att sensorer uppfyller normala säkerhetskrav för känsliga system som till exempel genomtänkta mekanismer och rutiner för autentisering, logghantering och redundans. Det är av stor vikt att skydda hela TDV-lösningen och speciellt sensorerna, då dessa ofta utsätts för IT-angrepp.

3.7 Övrigt

Ett TDV i enlighet med regeringens uppdrag som beskrivs i denna rapport är en passiv lösning. Det innebär att systemet detekterar och varnar för IT-angrepp, men utan att vidta ytterligare åtgärder för att skydda den verksamhet som är utsatt. Således detekteras ett angrepp och ett larm skickas men inga åtgärder vidtas automatiskt för att avbryta ett pågående angrepp.

Ett TDV kan utökas med funktionalitet att automatiskt vidta lämpliga skyddsåtgärder utifrån genererade larm och följaktligen bli mer effektivt mot IT-angrepp. Åtgärder som kan automatiseras är bland annat blockering av trafik, såväl mot intrång utifrån som mot otillåten utförsel av information inifrån.

4 Kostnader

I uppdraget ingår att bedöma kostnaden för skapandet av ett TDV. För att kunna ange mer exakta kostnadsuppskattningar förutsätts ett antal vägval och beslut. Det är i nuläget för många osäkra variabler för att en kostnadsuppskattning skulle ge en rättvisande bild. En av de mest avgörande parametrarna är huruvida man utnyttjar befintliga kunskaper, erfarenheter och tekniska system[11], vilket leder till lägre kostnader. Här redovisas dock en mycket grov kostnadsuppskattning vid en nyutveckling. Vidare redovisas översiktligt kostnadsdrivande aktiviteter för drift och vidareutveckling.

4.1 Utveckling av ett TDV

De aktiviteter som initialt krävs är:

- systemutveckling
- etablering av en central analysfunktion
- anskaffning av ingående mjukvarubaserade komponenter
- utveckling av en säker kommunikationslösning
- systemintegration
- anskaffning av hårdvara.

Om arbetet startas från grunden är de största kostnaderna kopplade till systemutveckling samt etablering av en central analysfunktion, vilket bland annat inkluderar att finna rätt kompetenser samt utveckla arbetsmetoder och processer. Då det gäller anskaffning av hårdvara är det inte unika lösningar som krävs; lämpliga lösningar finns att köpa på den kommersiella marknaden.
En mycket grov uppskattning är att de aktiviteter som presenteras ovan bedöms kosta mellan 10–25 Mkr, om man inte utnyttjar tekniska system som staten redan har tillgång till. Hårdvara för enskild sensor bedöms kosta 30tkr–200tkr. De lägre beloppen i kostnadsuppskattningarna avser ett enklare TDV, en systemlösning som innehåller allmänt kända och mindre känsliga detekteringsverktyg. De högre beloppen avser en mer avancerad systemlösning som kan utgöra en grundstomme i ett svenskt cyberförsvar. Vidare kan val av kommunikationslösning påverka kostnadsbilden.

4.2 Drift och vidareutveckling

Då ett system utvecklats och driftsatts tillkommer kostnader relaterade till löpande drift, till exempel följande:

- Teknisk drift
- Drift av analysfunktionen
- Installation av enskilda sensorer
- Vidareutveckling av systemet

Ett antal beslut vid såväl skapandet av ett TDV som vid drift och vidareutveckling kommer att behöva tas. Vart och ett av besluten kommer att påverka kostnadsbilden.

[11] Av staten utvecklade eller som staten på annat sätt har tillgång till.