Myndigheten för samhällsskydd och beredskap

UPPDRAGSREDOVISNING

Datum	Diarienr
2011-03-01	2010-4528

Ett nationellt tekniskt IT-intrångsdetekterings- och varningssystem (TDV)

Svar på regeringens uppdrag till Myndigheten för samhällsskydd och beredskap

(Fö2010/702/SSK, Regeringsbeslut 13, 2010-04-14)

Förord

Regeringen gav den 14 april 2010 Myndigheten för samhällsskydd och beredskap (MSB)i uppdrag att senast den 1 mars 2011 lämna förslag beträffande ett tekniskt detekterings- och varningssystem för samhällsviktig verksamhet och kritisk infrastruktur.

MSB redovisar i denna rapport sitt förslag på hos vilka aktörer ett nationellt tekniskt IT-intrångsdetekterings- och varningssystem kan införas. MSB berör även kostnaderna för införandet av systemet.

Arbetet med regeringsuppdraget har bedrivits av en projektgrupp vid MSB. Synpunkter har även inhämtats från myndigheterna i Samverkansgruppen för informationssäkerhet (SAMFI) samt externa aktörer.

MSB har i utredningsarbetet särskilt beaktat regeringens uppdrag till FRA angående hur ett tekniskt detekterings- och varningssystem för samhällsviktig verksamhet och kritisk infrastruktur kan utformas och införas.

Stockholm 1 mars 2011

Helena Lindberg

Generaldirektör

Richard Oehme

Chef för Enheten för samhällets informationssäkerhet

Sammanfattning

Utvecklingen under det senaste årtiondet har lett fram till att IT-incidenter kan hota kritisk infrastruktur, samhällsviktiga verksamheter och Sveriges säkerhet. Det finns därför ett behov av insatser på ett helt annat sätt än tidigare för att förebygga och hantera IT-incidenter.

Ett *nationellt tekniskt IT-intrångsdetekterings- och varningssystem (TDV)* är ett viktigt verktyg i arbetet med att bygga upp en nationell lägesbild över verkliga och potentiella IT-intrång samt avvikelser från normalläget. En sådan *informationssäkerhetsrelaterad lägesbild* är en förutsättning för ett samordnat hanterande av allvarliga IT-incidenter. Ett TDV kan snabbare identifiera samordnade attacker mot svenska intressen, samhällsviktig verksamhet och kritisk infrastruktur. Detta skapar förutsättningar för ett samordnat beslutsfattande på nationell nivå, vilket i sin tur ger möjligheter att avvärja, eller begränsa konsekvenserna av, IT-angrepp.

Det är dock viktigt att påpeka att TDV inte är tänkt att ersätta ordinarie skyddsmekanismer hos någon aktör. Många aktörer använder redan skyddsmekanismer som intrångsdetekteringssystem, brandväggar och antivirussystem. Ändamålet med TDV är att bidra till *ökad informations-säkerhet på nationell nivå*.

MSB föreslår att deltagande i ett nationellt tekniskt IT-intrångsdetekterings- och varningssystem (TDV) inledningsvis ska erbjudas alla statliga myndigheter som särskilt är utpekade i bilagan till förordningen (2006:942) om krisberedskap och höjd beredskap (KBF).

I en senare fas bör även andra myndigheter och offentliga organisationer, såsom landsting och kommuner, erbjudas att få ansluta sig till TDV, och även samhällsviktig verksamhet och kritisk infrastruktur som drivs i privat regi. Målsättningen bör vara ett representativt samhälleligt deltagande i TDV i syfte att skapa en god nationell informationssäkerhetsrelaterad lägesbild.

När det gäller kostnaderna för införandet av TDV bedömer MSB att dessa huvudsakligen rör (i) anskaffning och installation av detekteringsenheter och kommunikationslösningar, samt (ii) en central funktion för analys. Kostnader som hänförs till (i) behandlas i Försvarets radioanstalts uppdragsredovisning. Vad gäller (ii), bedömer MSB att det är kostnadseffektivt att bygga på den verksamhet som redan bedrivs vid CERT-SE. Det är dessutom juridiskt, tekniskt och praktiskt motiverat. Förslaget kan medföra behov av viss förstärkning av personalresursen vid CERT-SE beroende på vilka tjänster som ska ingå i TDV och vilka beredskapskrav som kan komma att ställas.

Innehållsförteckning

1. Inledning

1.1 Uppdraget

Myndigheten för samhällsskydd och beredskap (MSB) fick i april 2010 i uppdrag av regeringen (Regeringsbeslut 13, 2010-04-14, Fö2010/702/SSK), att i samråd med övriga myndigheter inom Samverkansgruppen för informationssäkerhet (SAMFI), ta fram ett förslag på hos vilka aktörer ett tekniskt detekterings- och varningssystem för samhällsviktig verksamhet och kritisk infrastruktur skulle kunna införas (se även Bilaga A).

Uppdraget formulerades enligt följande:

> *Myndigheten för samhällsskydd och beredskap ska lämna förslag på hos vilka aktörer ett tekniskt detekterings- och varningssystem för samhällsviktig verksamhet och kritisk infrastruktur kan införas. Uppdraget ska genomföras i samråd med övriga myndigheter som ingår i samverkansgruppen för informationssäkerhet, SAMFI, (Försvarets radioanstalt, Försvarets materielverk, Post- och telestyrelsen, Försvarsmakten och Säkerhetspolisen). Myndigheten för samhällsskydd och beredskap ska särskilt beakta det uppdrag till Försvarets radioanstalt som regeringen beslutat om denna dag.*
>
> *Myndigheten för samhällsskydd och beredskap ska också bedöma kostnaden för införandet av systemet.*
>
> *Myndigheten för samhällsskydd och beredskap ska hålla Regeringskansliet (Försvarsdepartementet) fortlöpande informerat under uppdragets genomförande.*
>
> *Uppdraget ska redovisas senast 1 mars 2011 till regeringskansliet (Försvarsdepartementet).*

I anslutning till att MSB erhöll ovan uppdrag fick Försvarets radioanstalt (FRA) i uppdrag av regeringen (Regeringsbeslut 14, 2010-04-14, Fö2010/703/SSK) att utreda hur ett tekniskt detekterings- och varningssystem för samhällsviktig verksamhet och kritisk infrastruktur kan utformas och införas.

1.2 Genomförande

MSB:s arbetet med att ta fram ett förslag på hos vilka aktörer ett tekniskt detekterings- och varningssystem skulle kunna införas har i huvudsak bedrivits av en arbetsgrupp vid Enheten för samhällets informationssäkerhet. MSB har samverkat med CERT-SE (tidigare Sitic) kontinuerligt i detta uppdrag, och sedan den 1 januari är CERT-SE en del av MSB. CERT-SE bedriver etablerad verksamhet med intrångsdetekteringssystem, exempelvis ”CERT-SE Honeynet”

samt ett system för insamling och analys av webbloggar (”LISA”). Därutöver bedriver CERT-SE försöksverksamhet med nya former av intrångsdetekterings-system.[1]

MSB har även hämtat erfarenheter från den försöksverksamhet med intrångs-detekteringssystem som Krisberedskapsmyndigheten (KBM), MSB:s före-gångare, bedrev för ett antal år sedan.

För att studera befintliga statliga detekterings- och varningssystem genom-fördes ett besök hos GovCERT i Danmark. MSB har även studerat det norska systemet Varslingssystem för digital infrastruktur (VDI) som NorCERT ansvarar för. Utöver detta har MSB också gjort studiebesök hos privata aktörer, i Sverige, Japan och Singapore, vilka tillhandahåller tjänster för intrångs-detektering och IT-incidenthantering (s.k. Managed Security Services).

För att säkerställa medverkan och delaktighet från samhället i stort har MSB regelbundet konsulterat relevanta externa aktörer, både från det offentliga och från det privata. Se vidare Bilaga B för uppdragets organisation.

I uppdragsbeskrivningen framgår att uppdraget ska genomföras i samråd med Samverkansgruppen för informationssäkerhet (SAMFI). Därför beslöts att låta uppdraget vara en stående punkt vid ordinarie möten, för att säkerställa en kontinuerlig uppdatering av arbetets fortskridande samt en plattform för att lyfta principiella frågor för bedömning.

De tekniska frågorna har hanterats av FRA inom ramen för FRA:s uppdrag. MSB och FRA har samverkat kontinuerligt.

Utformningen av ett tekniskt varnings- och detekteringssystem kräver juridiska, organisatoriska, ekonomiska, tekniska och praktiska överväganden. MSB har analyserat de juridiska aspekterna i en särskild studie för att skapa underlag till denna rapport.

Vidare har MSB analyserat hur det aktuella uppdraget förhåller sig till myndig-hetens övriga regeringsuppdrag på informationssäkerhetsområdet. Här identifierades särskilt starka kopplingar till uppdraget om en säker digital informations- och kommunikationsinfrastruktur för myndigheter, kommuner och landsting, samt uppdraget om obligatorisk IT-incidentrapportering för statliga myndigheter (se vidare Kapitel 7).

[1] ”CERT-SE Honeynet” detekterar och registrerar skadlig kod och intrångsförsök. LISA är ett system för insamling och analys av webbloggar. Deltagarna i ”LISA” skickar regelbundet loggar till CERT-SE och får en detaljerad rapport över potentiella attacker en gång i veckan. Se vidare www.cert.se.

2. Tolkning av uppdraget

MSB ska enligt regeringsuppdraget ta fram ett förslag på hos vilka aktörer ett tekniskt detekterings- och varningssystem skulle kunna införas samt bedöma kostnaden för införandet av systemet. Det framtagna förslaget och bedömningen har begränsats till att endast gälla samhällsviktig verksamhet och kritisk infrastruktur. Begreppen samhällsviktig verksamhet och kritisk infrastruktur är centrala i arbetet med att föreslå vilka verksamheter som ska ingå i systemet. Något uttalat uppdrag att precisera dessa begrepp närmare finns dock inte. Se även Bilaga C för en begreppsdiskussion.

Med hänsyn till komplexiteten hos system av den här typen och de många olika sätt de kan utformas på tolkar MSB regeringsuppdraget i dess första del som att det inte rör sig om att ta fram en statisk lista över vilka aktörer som bör omfattas utan att istället formulera ett mer principiellt förslag på vilken typ av aktörer som kan komma att bli aktuella.

När det gäller kostnaderna för systemet är det inte möjligt att ge några mer detaljerade uppskattningar. Förslaget tar främst sikte på att klargöra vilka kostnadsposter som kan komma att bli aktuella samt att diskutera möjliga principer för finansieringen.

Myndigheten gör tolkningen att uppdragsredovisningen inte ska innehålla några förslag på förändringar i rättsliga förutsättningar eller utpekade ansvar. De förslag som läggs fram ska hålla sig inom den ram som finns i dag.

Uppdragsredovisningen kommer inte heller att närmare behandla den tekniska utformningen av detekterings- och varningssystemet eftersom denna del utreds av FRA tillsammans med frågan om hur ett sådant tekniskt system kan införas.

3. Bakgrund

3.1 Hot mot den digitala informations- och kommunikationsinfrastrukturen

Utvecklingen under det senaste årtiondet har lett fram till att IT-incidenter nu kan hota kritisk infrastruktur, samhällsviktiga verksamheter och Sveriges säkerhet. Det finns därför ett behov av att på ett helt annat sätt än tidigare fokusera resurser på att förebygga och hantera IT-incidenter i alla sektorer och på alla nivåer i samhället.

Den digitala informations- och kommunikationsinfrastrukturens föränderlighet när det gäller teknik, organisation, metoder och kompetens ställer särskilda krav på säkerhet och nationell IT-incidenthanteringsförmåga. Mängden hot, risker och sårbarheter fortsätter att öka medan förmågan att hantera dessa inte tillnärmelsevis ligger på samma nivå.

De flesta IT-incidenter är inte ett resultat av brottsligt uppsåt utan uppstår på grund av bristande kompetens, misstag, felaktig användardokumentation eller liknande. Incidenter kan också orsakas av tekniska sammanbrott och naturhändelser. Men de antagonistiska hoten går inte att bortse från. Informationssystem utsätts regelbundet för angrepp. De flesta incidenter och angreppsförsök leder inte till allvarliga konsekvenser. Många av dem kan avvärjas snabbt genom de tekniska säkerhetsmekanismer som finns i bruk, genom egna åtgärder inom den drabbade organisationen eller genom kontakt med och hjälp från nätoperatörer eller motsvarande.[2]

En växande krets av statliga och icke-statliga aktörer – till exempel främmande underrättelsetjänster, kriminella grupper och terroristgrupper – har dock skaffat sig förmåga att komma över, stjäla, förändra och förstöra information. Aktörerna riktar sitt intresse mot hela skalan av tänkbara mål; från enskilda medborgare och affärsverksamheter till kritisk infrastruktur och samhällsviktig verksamhet.

Hoten mot den globala, digitala informations- och kommunikationsinfrastrukturen är en av de allvarligaste ekonomiska och säkerhetsmässiga utmaningarna som samhället idag står inför.

3.2 Att förebygga och hantera IT-incidenter

IT-incidenter kan drabba hela samhället och har i regel ett mycket snabbt händelseförlopp. På kort tid kan de eskalera från lokal till internationell nivå. Utgångspunkten för att förebygga och hantera *allvarliga IT-incidenter* är *samhällets samlade förmåga* – det krävs både nationell mobilisering av privata och offentliga resurser samt internationellt samarbete.

Hanteringen av allvarliga IT-incidenter kräver ett samfällt agerande och åtgärder för att hantera IT-incidenter kan behöva sättas in mycket snabbt. Det finns dock stora skillnader i samhällets förmåga till åtgärder. Vissa aktörer vidtar nödvändiga åtgärder omedelbart, andra aktörer agerar med stor fördröjning eller i värsta fall inte alls. För att aktörerna ska kunna samordna de åtgärder som behöver vidtas för att akut hantera incidenten och sedan för att återställa drabbade verksamheter är det viktigt att snabbt kunna klarlägga läget.

En krissituation kännetecknas av såväl många informationskällor som många informationsmottagare. *Lägesinformation* utgör en nödvändig förutsättning för att alla inblandade aktörer ska förstå situationen och kunna hantera den. Ska aktörerna samordnat kunna planera åtgärder och fördela resurser måste

[2] MSB:s bedömning baseras på öppna och andra källor, inklusive information från CERT-SE. En IT-incident definieras här som en ”oönskad och oplanerad störning och drabbar eller påverkar ett IT-system” (se även Bilaga C). MSB arbetar med att ta fram en definition av ”IT-incident” för att använda i ett framtida system för obligatorisk IT-incidentrapportering för statliga myndigheter.

lägesinformationen dessutom sammanfattas till en *gemensam lägesbild*. Samordnat handlande kräver med andra ord en gemensam uppfattning om det aktuella läget, det vill säga en sådan lägesbild som gör att aktörerna tillsammans kan gå vidare mot ett *koordinerat beslutsfattande*. Beslutsfattandet kan till exempel gälla hur aktörerna ska lämna samlad information till allmänheten eller vilken handlingslinje de ska välja.

Det är av stor vikt att snabbt kunna detektera och presentera händelseförloppet vid en IT-incident. Visar den *informationssäkerhetsrelaterade lägesbilden* att en rad centrala aktörer i samhället samtidigt drabbats av samordnade intrång, verkliga eller potentiella, ställer det krav på ett annat agerande än om endast någon enstaka aktör är drabbad.

Alla kriser har i dag en IT-dimension och det finns ett behov av att sammanföra den informationssäkerhetsrelaterade lägesbilden med den övergripande och samhällsinriktade *nationella lägesbilden* som MSB enligt instruktionen har ett utpekat ansvar för att upprätthålla och rapportera till regeringen.[3] Den informationssäkerhetsrelaterade lägesbilden tas i huvudsak fram genom samarbetet mellan berörda aktörer inom ramen för den nationella operativa samverkansfunktionen för informationssäkerhet (NOS) vid MSB.

MSB löser genom NOS regeringens inriktning som uttrycks i proposition 2010/11:1, utgiftsområde 6:

> *För att förbättra samhällets förmåga att förebygga och hantera allvarliga IT-incidenter anser regeringen att det krävs en mer sammanhållen struktur på området. Ett viktigt medel för att uppnå detta mål är inrättandet av en nationell samverkansfunktion för informationssäkerhet. Regeringen anser därför att Myndigheten för samhällsskydd och beredskap i samverkan med berörda myndigheter bör verka för en sådan funktion.*[4]

För att praktiskt skapa en informationssäkerhetsrelaterad lägesbild, och för att olika aktörer ska kunna agera samordnat vid allvarliga IT-incidenter, krävs mycket god kunskap om hur *normalbilden* för olika sektor ser ut över tid. En normalbild kan skapas genom att man bygger upp kompetens om de olika verksamheterna. Det är nödvändigt att veta vilken verksamhet som bedrivs inom olika samhällssektorer, vilka krav som finns vid olika tidpunkter, vad som är på gång inom olika verksamheter etc. En välgrundad uppfattning om vad som ingår i normalbilden ger även viktiga förutsättningar för att kunna detektera och studera avvikelser från normalbilden och vilka konsekvenser upptäckta avvikelser kan få ur ett samhällsperspektiv. Olika sektorsansvariga myndigheter eller teleoperatörer samt andra aktörer har idag tillgång till delar

[3] Se vidare 7 § förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

[4] Proposition 2010/11:1 utgiftsområde 6, sid. 83.

av denna lägesbild, men det saknas en samlad bild som belyser situationen ur ett samhällsperspektiv.

En gemensam informationssäkerhetsrelaterad lägesbild och normalbild byggs upp med hjälp av ett antal metoder och instrument för att löpande identifiera allmäntillståndet i den digitala informations- och kommunikationsinfrastrukturen. I detta arbete kan central information erhållas från ett strukturerat tekniskt intrångsdetekterings- och varningssystem för samhällsviktig verksamhet och kritisk infrastruktur. Det gäller såväl det förebyggande arbetet som arbetet med att hantera inträffade incidenter. I ett flertal länder är därför ett nationellt tekniskt intrångsdetekterings- och varningssystem ett viktigt verktyg i arbetet med att öka samhällets informationssäkerhet.

4. Grundförutsättningar för ett TDV

4.1 En principiell beskrivning av ett detekterings- och varningssystem

Ett tekniskt system för att detektera, och varna för, IT-angrepp kan utformas på en rad olika sätt men består i huvudsak av tre generella huvudkomponenter. Dessa huvudkomponenter kan ha olika prestanda och pris, men i sin grundkonstruktion består systemet av följande:

- *Detekteringsenheter* (”*larmklockor*”) som varnar vid intrång eller attacker och som är placerad utanför brandväggen mot Internet hos medverkande organisation.
- En *kommunikationslösning* som möjliggör att information förs över från detekteringsenheten till en central aktör.
- En *central analysfunktion* som kan hantera och sätta samman information från detekteringsenheterna med annan information samt vid behov skicka ut varningar.

Till ovanstående kommer organisation, personal, arbetsprocesser, avtal etc.

Den centrala delen i detekteringsenheten utgörs av ett *tekniskt regelverk* som avgör i vilka situationer enheten ska varna. Regelverket kan exempelvis innehålla signaturer (sökmönster) och varna när känd skadlig kod, eller definierade IT-angrepp, upptäcks, men även innehålla funktioner som gör det möjligt att analysera inkommande data för att upptäcka avvikelser från det normala.

Regelverket har inte bara betydelse för när detekteringsenheten ska varna utan påverkar även utformningen av systemet i sin helhet. I det fall regelverket innehåller signaturer som är framtagna med hjälp av information från under-

rättelseverksamhet begränsas antalet organisationer som får operera systemet och särskilda sekretessregler aktualiseras.

Information från detekteringsenheten hos medverkande organisation, exempelvis om ett intrångsförsök, skickas till en eller flera centrala aktörer. Den centrala aktören analyserar informationen i syfte att skapa en samlad bild av läget. Som tidigare nämnts kan ett tekniskt detekterings- och varnings-system vara uppbyggt av flera olika system. Vad systemet kan leverera är beroende av vilka och hur många aktörer som har detekteringsenheter, samt vilka regelverk som finns i de olika enheterna.

I dag finns ett stort utbud av kommersiella lösningar för intrångsdetektering i IT-miljöer. Se exempelvis NIST:s vägledning till intrångsdetekteringssystem (IDS) och intrångsförhindrande system (IPS).[5]

För förslag på teknisk lösning avseende ett tekniskt detekterings- och varningssystem för samhällsviktig verksamhet och kritisk infrastruktur, se FRA:s uppdragsredovisning.[6]

4.2 Ändamål med och beskrivning av ett TDV

För att kunna föra ett principiellt resonemang kring vilken typ av aktörer som ett tekniskt detekterings- och varningssystem kan införas hos, samt vilka kostnader som är förknippade med införandet av systemet är det nödvändigt att ge en övergripande beskrivning av ändamålet med ett sådant system.

Det system som avses här benämns **nationellt tekniskt IT-intrångs-detekterings- och varningssystem**, vilket förkortas **TDV**.

Ett TDV består av ett eller flera system, som har som syfte att detektera intrång och attacker via Internet genom en eller flera detekteringsenheter (”larm-klockor”) placerade hos de medverkande organisationerna. Information från ett TDV skulle exempelvis kunna klarlägga förekomst, frekvens och typ av attacker som sker mot de medverkande organisationerna via Internet samt möjliggöra att varningar skickas ut till berörda.

Idag finns en rad kommersiella system som uppfyller den beskrivning som ges ovan. Det är inte den tekniska funktionaliteten utan *ändamålet med systemet* som skiljer TDV från dessa. Det huvudsakliga ändamålet med TDV är att öka informationssäkerheten på nationell nivå och följande punkter är särskilt viktiga:

---

[5] *Guide to Intrusion Detection and Prevention Systems*, SP 800-94, National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce, Gaithersburg, MD.

[6] *Utformning av ett tekniskt detekterings- och varningssystem för samhällsviktig verksamhet och kritisk infrastruktur, Redovisning av regeringens uppdrag till Försvarets radioanstalt (2010-04-14 Regeringsbeslut nr 14)*, Försvarets radioanstalt (FRA), Bromma.

- TDV är ett viktigt verktyg i arbetet med att bygga upp en *nationell informationssäkerhetsrelaterad lägesbild* över verkliga och potentiella intrång samt avvikelser från normala trafikflöden. I dag saknas möjligheten att skapa en sådan lägesbild. Informationen från TDV kan även kombineras med information från andra källor för att få en god grund för den gemensamma informationssäkerhetsrelaterade lägesbilden, vilken i sin tur är en förutsättning för en samordnad hantering av allvarliga IT-incidenter.
- TDV kan, beroende på hos vilka aktörer detekteringsenheterna är placerade, snabbare *identifiera samordnade attacker mot svenska intressen*, samhällsviktig verksamhet och kritisk infrastruktur. Detta skapar förutsättningar för ett samordnat beslutsfattande på nationell nivå, vilket i sin tur ger möjligheter att avvärja, eller begränsa konsekvenserna av, IT-angrepp.

TDV som det beskrivs i denna rapport utesluter inte andra tekniska varnings- och detekteringssystemet i samhället. Aktörer kan ha särskilda behov som inte täcks av TDV, exempelvis kan underrättelse- och säkerhetstjänsternas arbete ställa krav på andra system.

4.3 Juridiska frågeställningar rörande ett TDV

Inledningsvis nämndes att MSB har tolkat uppdraget så att de förslag som läggs fram inte ska kräva några författningsförändringar. Införandet av ett nationellt tekniskt IT-intrångsdetekterings- och varningssystem (TDV) aktualiserar dock flera rättsliga överväganden och juridiken är i många fall central för utformningen och utplaceringen av systemet. Myndigheten har därför, som ett led i arbetet med uppdraget, gjort en översiktlig analys av den rättsliga ramen för TDV.

Ändamålet med systemet är i stor utsträckning styrande för vilka rättsliga regelverk som direkt påverkar hur och hos vilka aktörer som detekterings-enheter i TDV kan placeras ut. Som framgår av de två föregående avsnitten, avsnitt 4.1 och 4.2, kan sättet på vilket information hanteras i det TDV som beskrivs här, och som myndigheten utgår från i sin analys, i många delar jämställas med informationshanteringen och informationskanalerna i brandväggar och spamfilter.

Listan över regelverk som bör beaktas i arbetet med ett TDV är omfattande och innehåller exempelvis offentlighets- och sekretesslag (2009:400), person-uppgiftslag (1998:204), olika registerförfattningar, lag (2003:389) om elektronisk kommunikation och brottsbalkens regler om dataintrång 4 kap 9c §. I korthet kan konstateras att det särskilt är *sättet för insamling* och *formerna för samverkan* som aktualiserar juridiska gränsdragningsfrågor. Därför behandlas dessa närmare nedan.

De sätt som väljs för att *samla in information* i detekteringsenheterna får inte strida mot den straffrättsliga regleringen eller mot reglerna om personuppgiftsskydd. Metoderna måste vidare vara utformade så att de inte riskerar att förväxlas med exempelvis polisens brottsutredande eller brottsförebyggande verksamhet, till exempel hemlig teleövervakning, eller med försvarsunderrättelseverksamhet. Informationshanteringen i TDV blir jämförbar med allmänt brukade informationssäkerhetsskydd, som brandväggar, spamfilter eller traditionella intrångsdetekteringssystem genom att

- koppla in systemet i medverkande organisations egen IT-miljö som organisationen själv kontrollerar och har lovlig åtkomst till,
- endast läsa av trafik som är riktad mot den medverkande organisationens egen anslutning till Internet (alltså inte trafik riktad till någon annan eller trafik som initierats av den medverkande organisationen)
- endast granska inkommande data genom ett automatiserat förfarande på transportnivå som syftar till att identifiera ”digitala attacker” (förfarandet kan jämföras med att i traditionell miljö skilja mellan vanliga brev skickade till organisationen respektive att upptäcka och stoppa en brevbomb).

Eftersom syftet är att på ett samordnat sätt upptäcka attacker mot respektive medverkande organisations IT-miljö bör även behandlingen av inkommande data på detta sätt, rätt utformade, anses som en sådan nödvändig teknisk och organisatorisk åtgärd som ska vidtas enligt 31 § PUL för att skydda personuppgifter.

Det är även centralt att utforma *formerna för samverkan och informationsförmedling* mellan den myndighet som tillhandahåller den centrala analysfunktionen och de medverkande organisationerna, så att rutinerna blir förenliga med den centrala myndighetens instruktioner och uppdrag i övrigt. De rättsliga möjligheterna för en central aktör att *självständigt inhämta* och dela information är begränsade och detta måste beaktas, jämför exempelvis med reglerna om hemlig teleövervakning. Det är därför viktigt att det är den medverkande organisationen som i TDV självständigt *lämnar rapporter* till den centrala analysfunktionen samt att den centrala analysfunktionen *lämnar* varningar eller annan information. Systemet får inte utgöra ett verktyg för brottsutredande verksamhet eller försvarsunderrättelseverksamhet. Sättet på vilket informationen lämnas måste dessutom vara sådant sätt att åtgärderna inte strider mot till exempelvis regler om sekretess eller personuppgiftsskydd.

När systemlösning för TDV bestämts i mer detalj kan rättsfrågorna analyseras närmare.

5. Utgångspunkter för förslag om införande av ett TDV

Förslaget avseende vilka aktörer som bör medverka i ett nationellt tekniskt IT-intrångsdetekterings- och varningssystem (TDV) vilar på ett antal principiella resonemang som sammanfattas i detta kapitel.

Begreppen samhällsviktig verksamhet och kritisk infrastruktur är centrala i arbetet med att föreslå vilka verksamheter som ska ingå i TDV (se även Bilaga C). Samhällsviktig verksamhet och kritisk infrastruktur omfattar både offentliga och privata aktörer. Något uttalat uppdrag att operationalisera dessa begrepp i anslutning till arbetet med samhällets informationssäkerhet och hantering av IT-incidenter, finns dock inte. MSB har tolkat regeringsuppdragets första del som att det inte rör sig om att ta fram en statisk lista över vilka aktörer som bör ingå i TDV utan att i stället formulera ett principiellt förslag på vilken typ av aktörer som kan komma att bli aktuella.

Det är nödvändigt att införa ett TDV så att det skapas ett *förtroende* för systemet i hela samhället – hos de aktörer som deltar i TDV och hos Sveriges medborgare. MSB anser därför att *transparens* och *integritet* måste vara ledstjärnor i alla avseenden när det gäller ett TDV. En viktig fråga är att skapa en balans mellan sekretess och transparens så att värdefulla erfarenheter kan förmedlas utan att vare sig sekretess eller personlig integritet äventyras. Verksamheten måste bygga på kompetens, delaktighet och professionell integritet. Den måste också utföras med respekt för de deltagande aktörernas ansvar och uppgifter. Deltagandet bör därför i så hög grad som möjligt bygga på *frivillighet*.

Ytterligare en viktig utgångspunkt när det gäller att ge förslag på vilka aktörer som bör medverka i ett TDV, är att det offentliga bör vara en föregångare i arbetet med att öka informationssäkerheten i samhället. Sverige tillhör de ledande IT-nationerna i världen. Modern infrastruktur och samhällsnyttiga IT-tjänster förenklar vardagen och förbättrar livskvaliteten för Sveriges medborgare i alla delar av landet. Informationssäkerhet är en stödjande verksamhet för att öka kvaliteten hos samhällets alla funktioner. Det är också en förutsättning för att nya företeelser i samhället ska kunna fungera, till exempel e-förvaltning. Sedan slutet av 2009 ställs dessutom krav på statliga myndigheters arbete med informationssäkerhet genom MSB:s föreskrift MSBFS 2009:10.

Ett TDV ska inte konkurrera med kommersiella intrångsdetekteringssystem och det ska inte heller ersätta befintliga säkerhetsmekanismer. Det är i detta avseende också viktigt att betona att *ansvarsprincipen* gäller. Den praktiska hanteringen av IT-incidenter kommer alltid i huvudsak att skötas av de drabbade organisationerna. TDV är tänkt att vara ett komplement till de åtgärder som aktörerna vidtar för att skydda sin IT-miljö, med huvudsakligt

syfte att skapa en nationell informationssäkerhetsrelaterad lägesbild och ge berörda aktörer tidig förvarning. Se även diskussionen om ändmål i avsnitt 4.2.

De tekniska frågorna kring TDV, exempelvis prestanda och säkerhet, lämnas därhän i denna rapport. Det är dock viktigt att betona att ett TDV måste utformas för att uppfylla högt ställda krav på säkerhet och tillförlitlighet i alla avseenden, vad gäller såväl deltagande personal och organisation som teknik. Det kan också konstateras att ett TDV i sig själv kan utgöra ett mål för IT-angrepp. IT-säkerhets- och informationssäkerhetskraven bör därför ställas högt.

Slutligen pekar den juridiska analysen ovan på ett antal viktiga förutsättningar. De flesta organisationer i dag använder redan skyddsverktyg som brandväggar, intrångsdetekteringssystem, antivirussystem, spamfilter etc. Det system som diskuteras här är i ett tekniskt avseende inte något nytt. Ändmålet kompletteras emellertid så att syftet är att skapa en ökad informationssäkerhet på nationell nivå. Systemet får, enligt den översiktliga rättsliga analys som genomförts, inte utgöra ett verktyg för brottsutredande verksamhet eller försvarsunderrättelseverksamhet.

6. Förslag

MSB föreslår att deltagande i ett nationellt tekniskt IT-intrångsdetekterings- och varningssystem (TDV) inledningsvis ska erbjudas alla statliga myndigheter som är särskilt utpekade i bilagan till förordningen (2006:942) om krisberedskap och höjd beredskap (KBF).

I ett senare skede bör andra myndigheter och offentliga organisationer, såsom landsting och kommuner, erbjudas möjlighet att ansluta sig till TDV. Samhällsviktig verksamhet och kritisk infrastruktur som drivs i privat regi bör också erbjudas att ansluta sig till TDV i ett senare skede. Ett TDV är inte tänkt att ersätta ordinarie skyddsmekanismer, inklusive intrångsdetekteringssystem, hos någon aktör. Målsättningen bör vara ett representativt samhälleligt deltagande i TDV i syfte att skapa en god nationell informationssäkerhetsrelaterad lägesbild och ge berördas aktörer en tidig förvarning.

När det gäller kostnaderna för *införandet* av ett nationellt tekniskt IT-intrångsdetekterings- och varningssystem bedömer MSB att dessa huvudsakligen rör (i) anskaffning och installation av detekteringsenheter och kommunikationslösningar, samt (ii) en central funktion för analys. Kostnader som hänförs till (i) behandlas i FRA:s uppdragsredovisning. Vad gäller (ii) bedömer MSB att det är kostnadseffektivt att bygga på den verksamhet som redan bedrivs vid CERT-SE och den nationella operativa samverkansfunktionen (NOS). Det är dessutom juridiskt, tekniskt och praktiskt motiverat. Förslaget kan medföra behov av viss förstärkning av personalresursen vid CERT-SE beroende på vilka tjänster som ingår i TDV och vilka beredskapskrav som ställs.

6.1 Aktörer som bör omfattas av ett TDV

Fullt utbyggt bör ett nationellt tekniskt IT-intrångsdetekterings- och varningssystem (TDV) åtminstone omfatta alla statliga myndigheter som är särskilt utpekade i bilagan till förordningen (2006:942) om krisberedskap och höjd beredskap (KBF). Totalt sett rör det sig om 23 centrala myndigheter och samtliga 21 länsstyrelser. Ett viktigt skäl till att TDV bör omfatta dessa myndigheter är att de har, av regeringen och MSB, ansetts ha en särskilt viktig roll i krishanteringssystemet. Idag har alla former av kriser någon IT-dimension. Genom att systemet, fullt utbyggt, omfattar dessa myndigheter skapas en bra grund för ett skydd av den centrala förvaltningen i Sverige. De myndigheter som anges i KBF har ett säkerhetsmedvetande och flertalet av dem arbetar systematiskt med informationssäkerhet. Det är därför även en praktisk lösning att låta kärnan i TDV utgöras av de myndigheter som pekas ut i bilagan till KBF. Det är MSB:s bedömning att förslaget ger goda förutsättningar för att systemet relativt snabbt kan tas i drift – av ekonomiska, juridiska och tekniska skäl.

Utöver de myndigheter som nämns i KBF, bör andra myndigheter och offentliga organisationer, såsom landsting och kommuner, erbjudas en möjlighet att i ett senare skede på frivillig grund ansluta sig till TDV. MSB bedömer dock att det inte är nödvändigt eller realistiskt att alla myndigheter, landsting och kommuner individuellt ansluter sig till det TDV som avses här. TDV är inte tänkt att ersätta ordinarie skyddsmekanismer, inklusive intrångsdetekteringssystem, hos någon aktör. Enligt ansvarsprincipen ska varje enskild aktör själv ansvara för att vidta tillräckliga åtgärder för att skydda sin verksamhet. Det är dock troligt att många av de myndigheter, landsting och kommuner som inte föreslås ingå i TDV inledningsvis, i allt högre grad kommer att samverka för att skydda sina IT-miljöer. Därvid kan det bli aktuellt att ansluta grupper av aktörer som inte pekas ut i KBF; se de diskussioner som förs i regeringsuppdraget om en säker digital informations- och kommunikationsinfrastruktur för myndigheter, kommuner och landsting (Kapitel 7).

Den privata sektorn ansvarar idag för en mycket stor del av samhällsviktig verksamhet och kritisk infrastruktur i samhället. Idag har många privata aktörer installerat kvalificerade skyddsmekanismer i sina IT-miljöer. En nära samverkan mellan det privata och det offentliga är en grundförutsättning för att öka hela samhällets informationssäkerhet. För att skapa en nationell informationssäkerhetsrelaterad lägesbild krävs information från både privata och offentliga aktörer. Därför bör samhällsviktig verksamhet och kritisk infrastruktur som drivs i privat regi erbjudas att ansluta sig till TDV i ett senare skede.

Sammanfattningsvis bör ett TDV byggas ut successivt för att skapa och upprätthålla ett förtroende hos privata och offentliga aktörer i samhället. Målsättningen bör vara ett representativt samhälleligt deltagande i syfte att skapa en god nationell informationssäkerhetsrelaterad lägesbild och att kunna skapa en tidig förvarning. I en första fas bör en förstudie genomföras. Här bör

ett mindre antal av de myndigheter som är särskilt utpekade i bilagan till KBF erbjudas att delta på frivillig basis. Med ledning av resultaten från förstudien bör en plan för hur TDV ska vidareutvecklas tas fram.

6.2 Kostnad för införande av ett TDV

När det gäller kostnaden för *införandet* av ett nationellt tekniskt IT-intrångs-detekterings- och varningssystem (TDV) gör MSB bedömningen att det i huvudsak rör sig om två kostnadsposter:

- Anskaffning och installation av detekteringsenheter och kommunikationslösningar.
- En central funktion för analys.

För att detaljerade kostnadsuppskattningar ska kunna göras behöver ett antal vägval göras och inriktningsbeslut fattas. Nedan diskuteras de två huvudsakliga kostnadsposterna, samt möjliga finansieringsprinciper.

Frågor om anskaffning av detekteringsenheter och kommunikationslösningar behandlas i FRA:s uppdragsredovisning. Beroende på vilken teknisk system-lösning som väljs rör det sig antingen om att anskaffa kommersiellt tillgängliga produkter och eventuellt anpassa dessa, eller att nyttja av staten utvecklade produkter. I det senare fallet kan det handla om tillkommande utvecklings-kostnader beroende på vilka krav som kan komma att ställas på system-lösningen. Idag finns en utvecklad marknad för intrångsdetekteringssystem och internationellt finns både exempel på statliga aktörer som driver egen-utvecklade system och sådana som använder kommersiella system. Det unika i intrångsdetekterings- och varningssystemen är, som nämnts ovan, i många fall den regelsamling som används.

Till anskaffningskostnaderna kommer installationskostnader, vilka även inbegriper persontid och systemtester.

När det gäller den centrala funktionen för analys finns två alternativ – antingen att etablera en ny organisation eller att nyttja en redan etablerad verksamhet.

Det är förknippat med kostnader och tidsåtgång att etablera en ny organisation. Därför förordar MSB alternativet att nyttja en redan befintlig verksamhet.

Enligt MSB:s bedömning är det en kostnadseffektiv lösning att bygga på den verksamhet som redan bedrivs i form av CERT-SE vid MSB. Det är dessutom juridiskt, tekniskt och praktiskt motiverat. Vid CERT-SE finns redan personal och etablerade processer för nationell IT-incidenthantering samt traditionellt CERT-arbete, inklusive en beredskapsorganisation. Till detta kommer den nationella operativa samverkansfunktion för informationssäkerhet (NOS) som

MSB bygger upp för samverkan med samhällets aktörer kring IT-incident-hantering. MSB:s mandat inom informationssäkerhetsområdet ger stöd för rollen som central analysfunktion.[7]

Förslaget kan medföra behov av viss förstärkning av personalresursen vid CERT-SE beroende på vilka tjänster som ska ingå i TDV och de beredskapskrav som ska ställas på den centrala analysfunktionen.

När TDV väl är infört uppkommer löpande drifts- och vidareutvecklings-kostnader.

När det gäller *finansieringen* av införandet av TDV kan det vara lämpligt att tillämpa principer från näraliggande verksamheter. Exempelvis finansierar MSB i dag kryptoutrustning för civilt bruk till statliga myndigheter via centrala beredskapsmedel. I fallet TDV kan det vara lämpligt med en kombination av centrala medel och egenfinansiering. Centrala medel skulle exempelvis kunna täcka en viss del av införandet av systemet, medan egenfinansiering skulle stå för en viss del av införande av systemet och för huvuddelen av drifts- och förvaltningskostnaderna.

7. Synergier mellan ett TDV och andra uppdrag

Ett nationellt tekniskt IT-intrångsdetekterings- och varningssystem (TDV) som, i ett första steg, vänder sig till de myndigheter som är särskilt utpekade i bilagan till förordningen (2006:942) om krisberedskap och höjd beredskap (KBF), kan underlätta arbetet med *obligatorisk IT-incidentrapportering för statliga myndigheter* (Regeringsbeslut 13, 2010-04-14, Fö2010/701/SSK). För de statliga myndigheter som deltar i TDV kan arbetet med rapportering av IT-incidenter komma att förenklas och det finns därför möjligheter att skapa synergier mellan de två verksamheterna.

Det finns även synergier mellan ett TDV enligt ovan och en *skyddad kommunikationsinfrastruktur för offentlig sektor* som diskuteras i regerings-uppdraget om en säker digital informations- och kommunikationsinfrastruktur för myndigheter, kommuner och landsting (Regeringsbeslut 12, 2010-04-14, Fö2010/701/SSK). Speciellt finns möjliga samordningsvinster mellan ett TDV och det koncept för skyddade internetanslutningar som förs fram i förslaget.

---

[7] Av 11a § i förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap framgår bland annat att myndigheten ”ska stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området”. Vidare gäller att myndigheten ska ”svara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera IT-incidenter”. MSB ”ska i detta arbete agera skyndsamt vid inträffade IT-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och medverka i arbete som krävs för att avhjälpa eller lindra effekter av det inträffade”.

Utöver synergier med ovanstående två uppdrag finns ett antal kopplingar till andra aktuella uppdrag och verksamheter inom informationssäkerhets-området. Exempelvis är ett av huvudsyftena med ett TDV att stödja arbetet med att skapa en god informationssäkerhetsrelaterad lägesbild i samhället. Detta har naturligtvis bäring på de arbetsprocesser som föreslås i den nationella planen för att hantera allvarliga IT-incidenter och även för det arbete som bedrivs inom den nationella operativa samverkansfunktion (NOS) för informationssäkerhet, som MSB för närvarande inrättar. I detta finns även synergier med MSB:s arbete avseende risk och sårbarhetsanalyser, i synnerhet de delar som rör förmågebedömning av informationssäkerhet.[8]

[8] Arbete med förmågebedömning regleras i bilagorna till MSBFS 2010:6 och 2010:7.

Bilaga A: Regeringsuppdraget

REGERINGEN

Regeringsbeslut 13

2010-04-14 Fö2010/702/SSK

Försvarsdepartementet

Myndigheten för samhällsskydd och beredskap
651 81 KARLSTAD

Uppdrag om hur ett tekniskt detekterings- och varningssystem för samhällsviktig verksamhet kan utformas

Regeringens beslut

Myndigheten för samhällsskydd och beredskap ska lämna förslag på hos vilka aktörer ett tekniskt detekterings- och varningssystem för samhällsviktig verksamhet och kritisk infrastruktur kan införas.

Uppdraget ska genomföras i samråd med övriga myndigheter som ingår i samverkansgruppen för informationssäkerhet, SAMFI, (Försvarets radioanstalt, Försvarets materielverk, Post- och telestyrelsen, Försvarsmakten och Säkerhetspolisen). Myndigheten för samhällsskydd och beredskap ska särskilt beakta det uppdrag till Försvarets radioanstalt som regeringen beslutat om denna dag.

Myndigheten för samhällsskydd och beredskap ska också bedöma kostnaden för införandet av systemet.

Myndigheten för samhällsskydd och beredskap ska hålla Regeringskansliet (Försvarsdepartementet) fortlöpande informerat under uppdragets genomförande.

Uppdraget ska redovisas senast 1 mars 2011 till Regeringskansliet (Försvarsdepartementet).

Ärendet

Storskaliga IT-incidenter blir snabbt tvärsektoriella frågor som kräver ett samfällt agerande från många olika aktörer. Vid angrepp som drabbar kritisk infrastruktur och samhällsviktig verksamhet saknas det för närvarande möjlighet att skapa en samlad lägesbild.

Postadress 103 33 Stockholm
Besöksadress Jakobsgatan 9
Telefonväxel 08-405 10 00
Telefax 08-723 11 89
E-post: registrator@defence.ministry.se

2

En sådan lägesbild handlar dels om att detektera verkliga och potentiella intrång, dels om att studera avvikelser från normalbilden. Idag förfogar nätoperatörerna och andra aktörer var och en över sin del av lägesbilden, men ingen av dem kan se helheten.

Den 29 oktober 2009 fick Myndigheten för samhällsskydd och beredskap i uppdrag av regeringen att lämna förslag på samhällets samlade förmåga att förebygga och hantera IT-incidenter. Myndigheten för samhällsskydd och beredskap lämnade sin rapport (Fö2009/2162/SSK) den 15 januari 2010. Enligt rapporten bör myndigheten i samverkan med de övriga myndigheter som ingår i SAMFI, utreda hur ett mer strukturerat tekniskt detekterings- och varningssystem för samhällsviktig verksamhet och kritisk infrastruktur kan införas.

På regeringens vägnar

Sten Tolgfors

Linda Ericson

Kopia till

Statsrådsberedningen/SAM
Justitiedepartementet/PO
Justitiedepartementet/GRANSK
Justitiedepartementet/L4
Utrikesdepartementet/FIM
Finansdepartementet/BA
Finansdepartementet/SF
Finansdepartementet/SKA
Näringsdepartementet/ITP
Försvarets radioanstalt
Rikspolisstyrelsen
Säkerhetspolisen
Försvarsmakten
Försvarets materielverk
Myndigheten för samhällsskydd och beredskap
Totalförsvarets forskningsinstitut
Post och telestyrelsen

Bilaga B: Uppdragets organisation

Styrning

Richard Oehme, Chef för Enheten för samhällets informationssäkerhet, MSB

Projektledare

Dr. Åke J. Holmgren, Enheten för samhällets informationssäkerhet, MSB

Projektgrupp

Helena Andersson, Enheten för samhällets informationssäkerhet, MSB

Kristian Borryd, CERT-SE/Enheten för samhällets informationssäkerhet, MSB

Michael Patrickson, Enheten för samhällets informationssäkerhet, MSB

Per Furberg vid Setterwalls har bistått i juridiska analyser.

Extern samverkan

Projektets status har presenterats regelbundet vid ordinarie möten i Samverkansgruppen för informationssäkerhet (SAMFI).

Ett möte har genomförts i en extern referensgrupp i vilken följande organisationer ingått:

- Borlänge kommun
- Försvarets radioanstalt
- Försvarsmakten
- Post- och telestyrelsen
- Myndigheten för samhällsskydd och beredskap
- Svenska kraftnät
- Stockholms läns landsting
- Säkerhetspolisen
- Trafikverket

Myndigheten för
samhällsskydd och beredskap

UPPDRAGSREDOVISNING

Datum	Diarienr
2011-03-01	2010-4528

Bilaga C: Förkortningar och begrepp

Rapportens terminologi följer där så är möjligt SIS handbok *Terminologi för informationssäkerhet (SIS HB 550)*.[1]

Allvarlig IT-incident
En *IT-incident* är en ”oönskad och oplanerad störning och drabbar eller påverkar ett IT-system. En IT-incident kan resultera i allvarliga negativa konsekvenser för ägaren av systemet”.[2] Enligt SIS HB 550 är en incident en ”händelse som potentiellt kan få eller kunnat få allvarliga konsekvenser för verksamheten”.

En IT-incident behöver inte vara ett resultat av brottsligt uppsåt. Orsaken kan vara bristande kompetens, misstag, felaktig användardokumentation eller liknande. En IT-incident kan också orsakas av tekniska sammanbrott och naturhändelser.

En *allvarlig IT-incident* definieras i ”Nationell hanterandeplan – För allvarliga IT-incidenter” som en IT-relaterad händelse som:

1. avviker från det normala och som
2. innebär en allvarlig störning i samhällsviktig verksamhet samt
3. kräver skyndsamma och
4. samordnade insatser på nationell nivå.

Definitionen anknyter till hur en extraordinär händelse definieras i lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap, samt hur begreppet samhällsviktig verksamhet definieras (se nedan).

En allvarlig IT-incident kan resultera i omfattande negativa konsekvenser för hela samhället. Konsekvenserna kan vara ekonomiska, men kan även involvera skador på miljön eller påverka människors liv och hälsa. Ofta handlar det om en händelse som drabbar flera samhällssektorer, men även händelser som kan få mycket omfattande konsekvenser i en enskild samhällssektor räknas hit.

CERT/CSIRT
CERT (Computer Emergency Response Team) och *CSIRT* (Computer Security Incident Response Team) – Funktion för IT-incidenthantering.

CERT-SE
Den svenska nationella CERT-funktionen. Formellt en del av MSB.

---

[1] *Terminologi för informationssäkerhet,* SIS HB 550 utgåva 3, SIS Förlag, Stockholm, 2007
[2] *Hantering av IT-incidenter – Vem gör vad och hur?* IT-kommissionen, Statskontoret, 2001

IDS
Intrångsdetekteringssystem (Intrusion Detection System) – ”System för upptäckt av försök till eller fullbordat intrång” (SIS HB 550).

Intrång (IT-intrång)
”Oönskad interaktion med system
- i strid med systemets policy
- som kan medföra
  förändring, störning eller skada” (SIS HB 550)

IPS
Intrångsförhindrande system (Intrusion Prevention System) – ”IDS som är särskilt konstruerat för att aktivt kunna reagera på attacker/attackförsök” (SIS HB 550).

IT-angrepp
Begreppet *IT-angrepp* omfattar i denna rapport alla typer av IT-relaterade angreppsformer, från tillgänglighetsattacker och slumpmässiga automatiska intrångsförsök till angrepp med riktad skadlig kod.

IT-incident
Se “Allvarlig IT-incident”.

NOS
Nationell operativ samverkansfunktion för informationssäkerhet är en samverkansform som inrättats av MSB. NOS syftar till att skapa en förbättrad förmåga i samhället att hantera allvarliga IT-incidenter.

Samhällsviktig verksamhet och kritisk infrastruktur
Samhällsviktig verksamhet ur ett krisberedskapsperspektiv är verksamhet som uppfyller det ena eller båda av följande villkor[3]:

- Ett bortfall av eller en svår störning i verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid leda till att en allvarlig kris inträffar i samhället.
- Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad allvarlig kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt.

Exempel på sektorer där det finns verksamheter som alltid måste fungera är: Energiförsörjning, vattenförsörjning, information och kommunikation, finansiella tjänster, socialförsäkringar, hälso- och sjukvård, social omsorg, skydd och säkerhet, transporter, kommunalteknisk försörjning, livsmedel, handel och industri och offentlig förvaltning.

[3] Proposition 2007/98:92 *Stärkt krisberedskap – för säkerhets skull*.

Regeringen har gett MSB i uppdrag att ta fram en samlad nationell strategi för skydd av samhällsviktig verksamhet.[4] I detta ingår att förtydliga begreppet samhällsviktig verksamhet.

Kritisk infrastruktur definieras på följande sätt i direktiv från EU: ”anläggningar, system eller delar av dessa belägna i medlemsstaterna som är nödvändiga för att upprätthålla centrala samhällsfunktioner, hälsa, säkerhet, trygghet och människors ekonomiska eller sociala välfärd och där driftsstörning eller förstörelse av dessa skulle få betydande konsekvenser i en medlemsstat till följd av att man inte lyckas upprätthålla dessa funktioner”.[5]

SAMFI

Samverkansgruppen för informationssäkerhet – Gruppen består av Försvarets materielverk, Försvarets radioanstalt, Försvarsmakten, MSB, Post- och telestyrelsen, Rikspolisstyrelsen samt Säkerhetspolisen.

Skadlig kod (illasinnad kod)

Ett program som syftar till att utföra oönskade åtgärder på ett IT-system. Begreppet omfattar exempelvis virus, trojaner, maskar och rootkits. ”Kod som vid exekvering orsakar avsiktlig störning eller skada” (SIS HB 550).

TDV

Förkortningen används i den här rapporten i betydelsen ett *nationellt tekniskt IT-intrångsdetekterings- och varningssystem*.

[4] Regeringsuppdrag Fö2010/698/SSK

[5] RÅDETS DIREKTIV 2008/114/EG av den 8 december 2008 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna. Artikel 2a.