Hot- och riskrapport 2004

GRÄNSÖVERSKRIDANDE SÅRBARHETER

KBM:S TEMASERIE | 2004:6

KRISBEREDSKAPS MYNDIGHETEN

KBM:S TEMASERIE | 2004:6

Hot- och riskrapport 2004

GRÄNSÖVERSKRIDANDE SÅRBARHETER

Titel: Hot- och riskrapport 2004 – Gränsöverskridande sårbarheter
Utgiven av Krisberedskapsmyndigheten (KBM)
Omslagsfoto: Tangentbord: David Carmack/Pressens bild, Hönsfåglar: Tommy Svensson/ Pressens bild, Terrordåd i Madrid: Kai Pfaffenbach/Reuters/Scanpix, Parkeringsskylt: Göran Gustafsson/Pressens bild, Skyddskläder: Trippett/Sipa/Scanpix

ISSN: 1652-2915
ISBN: 91-85053-64-3
KBM:s dnr: 1286/2004
Grafisk form: AB Typoform

Skriften kan laddas ned från Krisberedskapsmyndighetens webbplats
www.krisberedskapsmyndigheten.se

KBM:s temaserie 2004:6

Innehåll

Förord

Krisberedskapsmyndigheten ger i denna rapport läsaren en övergripande bild av vilka hot och risker som vårt samhälle kan komma att utsättas för. I första hand vänder vi oss till myndigheter som årligen genomför risk- och sårbarhetsanalyser. En förhoppning är att rapporten även kan vara till nytta för säkerhetsarbete inom näringsliv och för organisationer utanför den offentliga sektorn. Medan man säkert har en god bild av vad som utgör hot och risker inom den egna sektorn, har man också ett behov av att se helheten.

I dag föreligger en komplexitet i hotbilder som samhället måste hantera tvärs över sektorsgränserna. Hoten har många dimensioner och berör samtidigt delar av samhället som inte vanligtvis arbetar med dessa frågor. Det är därför nödvändigt att analysera hot och risker ur ett helhetsperspektiv. Endast då kan man förebygga, upptäcka och hantera de hot och risker som kan skapa allvarliga konsekvenser för samhället.

Rapporten har inte som ambition att vara heltäckande. Denna första rapport har ett fördjupat avsnitt om informationssäkerhet. KBM har ett särskilt ansvar för analyser inom detta område. Övriga avsnitt bygger på material från respektive expertmyndighet. KBM har sammanställt och skapat en syntes av detta material. Vilka konsekvenser har hotet för samhället som helhet? Är hotet eller risken av en sådan karaktär att det kräver att olika delar av samhället samarbetar för att förebygga och hantera det? Kan konsekvenserna vara så stora att samverkan mellan flera myndigheter krävs?

Rapporten är den första i en årligen återkommande serie. Ambitionen är att kommande rapporter ska behandla andra typer av hot och gå djupare. Genom publiceringen av denna första rapport inbjuder KBM till en dialog om hot och risker. Kan våra rapporter utvecklas ytterligare?

Bidra med Era synpunkter kring denna första rapport genom att kontakta informationssäkerhets- och analysenheten vid KBM. Vi har ett gemensamt ansvar att utveckla en god förmåga till hot- och riskanalys till stöd för samhällets krisberedskap.

Staffan Karlsson
Enhetschef Informationssäkerhets- och analysenheten,
Krisberedskapsmyndigheten

Sammanfattande slutsatser

En generell risk för samhällets krisberedskap är stuprörstänkande och brist på samverkan över myndighets- och sektorsgränser. Detta kan leda till svårigheter att upptäcka, förebygga och hantera hot och risker som kan få allvarliga konsekvenser för samhället.

Det är viktigt att höja blicken och se Sverige som en del av ett större internationellt sammanhang. Konsekvenser av internationell brottslighet, IT-relaterade hot, aktörsbundna hot, fallerade stater eller smittutbrott påverkar också Sverige. Många av dagens hot är gränslösa till sin karaktär. När Sveriges säkerhet och beredskap byggs upp bör den därför ses i ett internationellt perspektiv.

Det är viktigt att inte bara myndigheter inom smittskyddet har planer för att hantera konsekvenser av en pandemi. Vid en pandemi eller större epidemi kommer hela samhället att drabbas allvarligt. Exempelvis krävs kontinuitetsplanering för hur man hanterar bortfall av nyckelpersoner.

Vid en pandemi kan också viktiga flöden av exempelvis varor att påverkas. I ett läge där en kris har en internationell utbredning kan Sverige endast räkna med begränsat stöd från andra länder. Sannolikt kommer dessa att i ett sånt läge prioritera egna intressen. Detta gäller inte minst tillgången på vaccin, där Sverige i dagsläget saknar en egen kapacitet för tillverkning.

Det ökade ömsesidiga beroendet mellan olika tekniska system i kombination med avreglering har lett till en minskad överblick över den samhällsviktiga infrastrukturen. En bättre överblick gör det möjligt att bättre värdera hot och risker på samhällsnivå. Identifiering av beroendeförhållanden gör det också lättare att förebygga eller mildra effekterna av händelser som kan leda till allvarliga kriser i samhället.

Även om Sverige i dagsläget inte är ett förstahandsmål för internationella terroristnätverk gör det dock inte riskerna för en terrorattack i Sverige försumbara. Dels finns ett hot mot utländska intressen i Sverige, där de direkta konsekvenserna av en attack kan drabba och måste kunna hanteras av svenska aktörer. Dels kan Sverige komma att användas som en bas för terrornätverk och utnyttjas för terrorattacker mot andra länder.

Idag bedöms hotet från terroristattacker med CBRN-medel (kemiska, biologiska, radiologiska och nukleära) som lågt. Konsekvenserna av en sådan händelse bedöms dock vara så allvarliga att hotbilden inte bör ignoreras.

Det är viktigt att uppmärksamma att risken för attacker mot svenska intressen snabbt kan komma att förändras på grund av exempelvis politiska ställningstaganden eller deltagande i en internationell operation.

Organiserad brottslighet kan komma att utvecklas till ett allvarligt hot mot det svenska samhället. Det är viktigt att motverka att Sverige används som en bas för denna typ av verksamhet. Dessutom blir det allt svårare att dra en skarp gräns mellan organiserad brottslighet och terroristnätverk. Utvecklingen går mot att samma personer och resurser används för olika ändamål beroende på när de bäst behövs. Sammansmältningen mellan terrorism och organiserad brottslighet gör att den potentiella faran i dessa hot ökar ytterligare.

Närvaron av andra staters underrättelsetjänster är betydande. Företag och myndigheter som arbetar med strategiskt beslutsfattande, spetsteknologi, medicinsk utveckling, försvarsindustri eller finansiell verksamhet löper större risk att utsättas för denna typ av verksamhet. Förlust av information kan allvarligt skada viktiga nationella intressen. Dessa företag och myndigheter bör ägna sitt säkerhetsarbete extra stor uppmärksamhet.

Skadlig kod används i allt högre utsträckning i kriminella syften och för illegal informationsinhämtning. Kod specialutvecklas för givna syften och sprids i allt större omfattning genom att utnyttja bristande skydd hos slutanvändarna som utgör såväl delmål som slutmål för attacker. Dessutom ökar riskerna att samhällsviktiga system påverkas av sådana attacker på grund av den ökade konvergensen mellan informations-, kommunikations-, styr- och reglersystem. Ett allvarligt hot mot Internet men även för tilliten till informationssamhället är det ökande problemet med spam (massutskick av t ex reklam). Den gränsöverskridande förekomsten av botnets (nätverk av fjärrstyrda datorer) och den kraft ett samlat angrepp kan innebära utgör ett allvarligt hot mot samhället.

De samlade effekterna av den illegala verksamhet som förekommer på Internet påverkar samhället negativt. Det som dagligen sker indikerar vad en resursstark och målmedveten aktör, som en stat eller en terrororganisation, skulle kunna åstadkomma genom en riktad attack.

Till stor del skulle samhällets motståndskraft mot informationssäkerhetsrelaterade hot reduceras om befintliga brandväggar och virusskydd används och uppdaterades, om systemens säkerhetshål regelbundet åtgärdades och grundinställningarna justerades. Ett säkerhetsmedvetet agerande skulle ytterligare reducera riskerna. Idag bidrar i stor utsträckning slutanvändarna själva till att råka illa ut genom ett obetänksamt beteende.

Bakgrund och syfte

Årlig lägesbild av hot och risker

Den årliga sammanställningen har som huvudsakligt syfte att redovisa KBM:s samlade lägesbild över de hot och risker som krishanteringssystemet har att hantera. Rapporten behandlar de hot och risker som KBM bedömer vara de mest angelägna att belysa utifrån ett samlat krishanteringsperspektiv.

Rapporten är baserad KBM:s egna omvärldsanalys och på underlag från flera olika enskilda och sektorsvisa hot- och riskanalyser.[1] Den ger både en samlad helhetsbild och en sammanställning av lägesbilden på hot- och riskområdet.

Målgrupp för rapporten är i första hand de personer i krishanteringssystemet som arbetar med den egna organisationens risk- och sårbarhetsanalys.[2]

De aktörer som KBM vill nå med rapporten känner till situationen inom den egna sektorn, men har också ett behov av en översiktlig bild av helheten.

Rapporten är tänkt att fungera som ett ingångsvärde för myndigheternas årliga risk- och sårbarhetsanalyser. KBM har haft som ambition att se på hoten ur ett tvärsektoriellt perspektiv och genom detta ge en helhetsbild. Det är sedan upp till var och en av de aktörer som läser rapporten att avgöra vilka delar som är tillämpbara för den egna verksamheten. De hot, risker och sårbarheter som beskrivs i rapporten har alla gemensamt att de kan få konsekvenser inom flera samhällssektorer.

KBM har i tidigare utredningar och skrifter gjort genomgångar av de hot och risker som är aktuella för krishanteringssystemet. I KBM:s planeringsinriktning ”Samhällets krisberedskap 2006 – inriktning för myndigheternas planering” och i utredningen ”Nya villkor för samhällets krisberedskap” anges ett antal hot och risker i samhället.

1. En lista över de myndigheter som lämnat underlag finns i slutet av rapporten.
2. Av 3 § förordningen (2002:472) om åtgärder för fredstida krishantering och höjd beredskap framgår att varje statlig myndighet under regeringen, i syfte att stärka sin krishanteringsförmåga, årligen skall analysera om det finns sådan sårbarhet och sådana risker inom myndighetens ansvarsområde som synnerligen allvarligt kan försämra förmågan till verksamhet inom området.

Denna rapport utgår till del från de resonemang som förs i dessa rapporter och ambitionen har varit att i denna rapport fördjupa resonemangen vidare.

I rapporten har området informationssäkerhet tilldelats ett eget avsnitt. Detta är mer detaljerat och djupgående än den övriga rapporten. Orsaken till detta är att KBM har ett särskilt uppdrag, enligt myndighetens instruktion, att ha ett sammanhållande myndighetsansvar för samhällets informationssäkerhet.

Generella utvecklings-tendenser i samhället

De hot och risker som redovisas i rapporten kan inte ses lösryckta ur sitt sammanhang, utan måste ställas i förhållande till det samhälle som vi verkar i. Samhället präglas i högre grad än tidigare av en osäkerhet av vad som kan komma att utvecklas till en svår kris för samhället.[3]

Globalisering är en betydande drivkraft i samhällsutvecklingen. Vi är på många sätt mer internationella än vi någonsin varit. När tidigare ungdomsgenerationer reste på språkresa till Europa, reser dagens unga till platser som tidigare sågs som avlägsna. Det ökade resandet har lett till att idéer och värderingar sprids snabbare, men också till negativa effekter, som att smitta sprids fortare.

Ekonomin har också internationaliserats. Många verksamheter som historiskt drivits av staten är idag avreglerade och drivs av multinationella företag. Som en följd av att ekonomin har blivit mer gränsöverskridande har också brottslighet blivit det.

En viktig aspekt av detta är de konsekvenser ett ökat internationellt ekonomiskt beroende kan komma att få. Ett exempel är när telekommunikationsbolaget Worldcom drabbades av ett konkursföreläggande och de konsekvenser som då riskerade att uppstå. Worldcoms dominerande ställning på Internetmarknaden och inom telekommunikationer gjorde att exempelvis företag i Sverige riskerade att drabbas av avbrott i telefon- och mobiltelefonförbindelser.[4]

Den snabba teknikutvecklingen är en annan betydande drivkraft i samhällsutvecklingen. Teknikutvecklingen har bland annat lett till att information sprids mycket snabbare än tidigare. Teknikutvecklingen har även bidragit till att automatisera moment som tidi-

3. Beskrivningar av den hotbild och de utvecklingstendenser som har betydelse för krisberedskapen finns bl.a. i Försvarsberedningens senaste rapporter *Säkrare grannskap – osäker värld* (Ds 2003:8) och *Försvar för en ny tid* (Ds 2004:30) samt i den av KBM redovisade rapporten *Nya villkor för samhällets krisberedskap* (KBM dnr 0753/2003)
4. Finansinspektionen ”Från elavbrott till 11 september”, 2004

gare var mycket arbetskrävande, vilket i sin tur bidragit till ett ökad beroende av att tekniken fungerar som den ska.

Ytterligare en viktig drivkraft i samhällsutvecklingen är vad som sker på det politiska planet, såväl nationellt som internationellt. Terrorhändelserna i USA den 11 september 2001 och i Madrid den 11 mars 2004 har fått stora efterverkningar i de politiska processerna på bland annat EU-nivå. Inom EU sker för närvarande stora förändringar inom det gemensamma krisberedskapsarbetet. Mycket tyder på att man i många delar håller på att gå ifrån den strikta sektorsindelningen när man behandlar dessa frågor. Istället har en mer sektorsövergripande arbetsprocess börjat växa fram. För första gången kan man inom EU skönja framväxten av ett mer samlat system för krisberedskap. Idag är krisberedskap ett politiskt mycket prioriterat område inom EU-samarbetet.

Ett aktuellt exempel på detta är att flera viktiga sektorsövergripande dokument som rör krisberedskap presenterats. För första gången används krishantering som ett samlat begrepp för att beskriva arbetet med unionens inre säkerhet. Ett övergripande dokument för hantering av terrorfrågor, den så kallade terrorismdeklarationen har tagits fram. Denna hanterar allt terrorismrelaterat arbete och krisberedskapsfrågorna finns med som en del.[5]

Beroendeförhållanden i samhällsviktiga funktioner och tjänster

Ytterligare en viktig generell utvecklingstendens är att beroendeförhållanden mellan olika samhällsviktiga funktioner och tjänster ökar. I rapporter från både Försvarsberedningen och KBM redovisas exempel på hur förändringar av hotbilden i kombination med vissa inslag i samhällsutvecklingen har medfört en ökad risk för att störningar i samhällsviktiga funktioner leder till allvarliga kriser i samhället.[6]

Försvarsberedningen har konstaterat att den verksamhet och de system som omfattas av de samhällsviktiga funktionerna blivit allt svårare att skydda. Detta eftersom infrastruktursystemen generellt sett präglas av tilltagande komplexitet och föränderlighet. Systemen tenderar att bli alltmer storskaliga och komplexa. Ett exempel på detta är att många infrastruktursystem är beroende av IT-stöd och fungerande datakommunikationer för att styrning och övervakning av systemen ska kunna utföras. Dessa styrnings- och övervakningsfunktioner är ofta centraliserade vilket ytterligare ökar risken för att en störning ska sprida sig och få allvarliga konsekvenser för samhället. Den pågående digitaliseringen av radio, TV och telekommunikationer och sammankopp-

5. Helén Jarlsvik, ”Ett europeiskt krisberedskapssystem och dess internationella implikationer”, 2004
6. Försvarsberedningen ”Försvar i en ny tid”, Ds 2004:30; KBM, ”Nya villkor för samhällets beredskap – KBM:s underlag inför 2004 års försvarsbeslut”

lingen med IT-nätverk leder dessutom till nya ännu inte kartlagda risker för angrepp och en ökad sårbarhet.

Marknadsreformer har medfört att fler aktörer har tillkommit inom vissa sektorer. Dubbleringar av system och resurser kan ibland minska sårbarheten. I vissa fall har dock säkerhets- och beredskapsnivåerna sänkts som en konsekvens av att konkurrensförhållanden och lönsamhetskrav minskar företagens möjligheter att ta på sig åtaganden som inte kan motiveras företagsekonomiskt. En liknande utveckling kan skönjas inom kommunsektorn. I detta fall är orsaken dock en kärv ekonomi i kombination med ökade anspråk på service inom vissa områden. Sammantaget medför detta att man på vissa håll i samhället kan se tendenser till en snävare syn på åtaganden som inte direkt och otvetydigt anses tillhöra den egna kärnverksamheten eller det egna ansvarsområdet.

Exemplen ovan visar att beroendeförhållandena mellan olika verksamheter i samhället har en tendens att förstärkas och bli alltmer komplexa och svåröverskådliga. Det är därför inte möjligt att korrekt värdera hot och risker på samhällsnivå utan att ta hänsyn till dessa kritiska beroendeförhållanden. Identifiering av sådana beroendeförhållanden kan också göra det lättare att förebygga eller mildra effekterna av händelser som kan leda till allvarliga kriser i samhället.[7]

7. KBM, ”Förstudie om kritiska beroendeförhållanden mellan samhällsviktiga funktioner och tjänster”

Icke-aktörsbundna hot och risker

Med icke-aktörsbundna hot och risker menas de typer av hot och risker där en illasinnad aktör inte står bakom. Rapporten tar upp tre olika kategorier av icke-aktörsbundna hot: smitta, tekniska kollapser och extrema natur- och väderhändelser.

Smitta

Den senaste stora världsomspännande epidemin (pandemin) var Hongkong-influensan som spred sig under 1968. Exempel på andra kända pandemier är Spanska sjukan 1918 och Asiaten 1957. Dessutom spreds två mindre pandemier under 1948 och 1977.

Pandemier är med andra ord långt ifrån ett nytt fenomen, under de senaste hundra åren har världen drabbats av en pandemi 3-4 gånger. Enligt Smittskyddsinstitutet var det längsta tidsintervallet mellan de olika pandemierna under 1900-talet 30 år. Det har nu gått 27 år sedan den senaste.[8]

Det som är nytt för det samhälle vi lever i är att ett influensavirus med stor sannolikhet skulle kunna spridas mycket snabbare än tidigare. När Hongkong-influensan spreds på 60-talet räknade man med att det tog cirka 4-6 månader. Idag skulle den tiden vara kortare, möjligen halverad, mycket på grund av nya resvanor.

Ett aktuellt exempel på vilka effekter en stor utbredning av ett virus, såsom en influensaepidemi, kan komma att få är SARS (svår akut respiratorisk sjukdom) som spreds under 2002-2003. I april 2003 konstaterade Världshälsoorganisationen (WHO) att SARS hade sin grund i ett hittills okänt smittämne.

Många länder i Sydostasien och även Kanada drabbades både på ett mänskligt och ekonomiskt plan, med exempelvis en ökning av antalet konkurser som indirekt följd.[9] Bland annat drabbades

8. Smittskyddsinstitutet, ”Information om fågelinfluensa”, hämtat från: http://www.smittskyddsinstitutet.se/SMItemplates/Newsarticle____4357.aspx
9. Enligt beräkningar gjorda av Världsbanken minskade Sars BNP i Ostasien med 0,4-0,5 %. Se exempelvis: http://web.worldbank.org/WBSITE/EXTERNAL/NEWS/0,,contentMDK:20114259~menuPK:34459~pagePK:34370~piPK:34424~theSitePK:4607,00.html

flygbranschen hårt, eftersom människor valde att inte resa till Asien på grund av risken för smittspridning. I Sverige blev SARS klassad som samhällsfarlig sjukdom i smittskyddslagen i maj 2003.

I samband med den globala bekämpningen av SARS-viruset etablerade WHO en ny och förstärkt roll som samordnare av internationellt smittskydd. De fick även ett enhälligt mandat från världshälsoförsamlingen att kunna agera utifrån uppgifter om utbrott som ännu inte officiellt bekräftats av enskilda länders regeringar. WHO gick under hösten 2003 ut med rekommendationen att fler människor borde vaccineras mot influensa inför influensasäsongen 2003-2004 för att på så sätt minska antalet ”vanliga” influensafall som kunde förväxlas med SARS.

FÅGELINFLUENSA

Många av de smittor och influensor som människor drabbas av härstammar ifrån djur. SARS, HIV och West Nile fever[10], är samtliga exempel på virussjukdomar som har sitt ursprung i djursjukdomar och som under en lång tid förändrats och så småningom förflyttats till människor. Liknande teorier finns om bland annat mässlingen som släkt med virus som orsakar en hästsjukdom.

Det finns indikationer på att fågelinfluensa, som för närvarande har stor spridning bland tamfåglar i Sydostasien, kan utvecklas till att bli en stor utmaning för världens hälsomyndigheter. Så sent som den 31 oktober 2004 gick amerikanska läkare och företrädare för WHO ut med en varning för att det finns risk för en pandemi av fågelinfluensa.

Det är dock i det här sammanhanget viktigt att hålla isär den aktuella uppkomsten av fågelinfluensa och risken för en eventuell framtida pandemi. Fågelinfluensan *kan* komma att utvecklas till en pandemi. Den risken uppstår om fågelviruset muterar och får förmågan att spridas mellan människor. Det kan ske genom att det kombineras med ett mänskligt influensavirus. Inför den faran vill WHO mobilisera regeringar, läkemedelsföretag och forskarsamhället för att påskynda takten i utvecklingen av ett influensavaccin som skyddar mot fågelinfluensan.

Den fågelinfluensa som för närvarande har stor påverkan på den asiatiska tamfågelindustrin har sitt ursprung bland östra Asiens flyttfåglar. Från dessa har den sedan spritt sig till tamfåglar. Det pågående utbrottet av fågelinfluensa är det största någonsin och har drabbat miljontals fåglar i flera ostasiatiska länder. Fågelinfluensa kan överföras från fågel till människa. I de befolkningstäta delarna av Sydostasien finns det sedan förutsättningar för en snabb spridning av sjukdomen, såväl mellan djur som mellan djur och människa. Viruset har dock svårt att överföras från människa till människa.

10. West Nile fever är en virussjukdom som sprids via myggor. Epidemier har på senare år rapporterats från USA, Rumänien, Ryssland och Israel.

Fågelinfluensa har hittills påvisats i Sydkorea, Vietnam, Japan, Thailand, Kambodja, Laos, Kina, Pakistan och Indonesien. Där har ett hundratal människor smittats av fågelviruset direkt från fåglar, med en dödlighet bland de dokumenterade fallen på mellan 70 och 80 procent.

WHO:s strategi för att begränsa effekterna av pandemier bygger på en aktiv internationell övervakning och att i ett sådant läge när en pandemi har uppkommit snabbt få fram influensavaccin. Men den bygger också på att världens länder har en väl fungerande beredskap med genomtänkta pandemiplaner. Den nu uppkomna situationen i Sydostasien är därför en stark signal även till Sverige att vi behöver få till stånd en bättre beredskap mot en hotande pandemi.[11]

Luftburna influensavirus sprids lättare än exempelvis SARS, delvis eftersom smittade individer hos vilka sjukdomen ännu inte brutit ut kan sprida stora mängder virus. Det är också därför som de restriktioner och åtgärder man genomförde i samband med SARS-smittan troligen inte skulle fungera lika bra vid en pandemi av influensa.[12]

Att ta fram ett nytt vaccin inför en eventuell pandemi av fågelinfluensa beräknas ta sex månader. Bland annat måste vaccinet testas grundligt för att leva upp till kraven för att kunna licensieras. I början av april 2004 tog WHO fram en prototyp för ett vaccin tillgänglig för tillverkare. För närvarande har endast två av de ungefär tolv stora producenterna av influensavaccin i världen gjort framsteg i arbetet. Båda producenterna, som finns i USA, har tagit fram små mängder vaccin för att använda vid kliniska tester.

Konsekvenser för krishanteringssystemet

I Sverige finns i dagsläget ingen kapacitet för att tillverka influensavaccin. Idag regleras tillgången till vaccin av för varje år upprättade skriftliga avtal med de internationella läkemedelsföretag som producerar vaccin. Ett av problemen, enligt Socialstyrelsen, är att det i världen idag finns en produktionskapacitet som endast uppfyller en tiondel av behovet vid en pandemi. Bedömningen som Socialstyrelsen gör är att det vid en pandemisituation skulle vara svårt att tillgå de mängder som skulle behövas. Det skulle ta flera år att bygga upp en svensk förmåga att tillverka influensavaccin.

Samhällets kostnader för en influensapandemi skulle bli mycket stora. Beroende på hur spridningen av viruset ser ut kan stora delar av samhället drabbas och en stor del av den yrkesverksamma befolkningen insjukna. Mycket tyder på att tillgång till vaccin och så kallade antivirala medel (läkemedel som motverkar virus) skulle

11. Läs mer om WHO:s strategi angående SARS på http://www.who.int/csr/disease/influenza/sars/en/
12. Robert Bonte-Friedheim och Karl Ekdahl "A flu threat harder to stop than SARS" International Herald Tribune, 2004-04-12

kunna minska risken för stora ekonomiska kostnader och konsekvenser för samhället i övrigt.

En aspekt av detta är de konsekvenser en pandemi kan få för samhällets funktion och säkerhet. Sannolikt är dagens krympta organisationer mer sårbara för stora personalbortfall än under tidigare pandemier. Ett exempel är att tillgången på läkemedel snabbt skulle minska om stora delar av läkemedelsindustrin drabbades av en influensapandemi. Läkemedelsindustrin är mycket personalberoende och den mesta distributionen sker utan tillgång till större lagerhållning vilket gör att ett produktionsbortfall snabbt skulle få följdverkningar.

Tekniska kollapser

Den tekniska infrastrukturen spelar en alltmer avgörande roll för att vi ska kunna upprätthålla samhällsviktiga funktioner och tjänster. Få verksamheter i samhället fungerar utan tillgång till el, telekommunikationer och IT. Därtill är samhället beroende av väl fungerande transporter samt vatten- och avloppsinfrastrukturer.

Som KBM skriver i sitt inriktningsdokument för samhällets krisberedskap 2006, är de samhällsviktiga infrastrukturerna känsliga för tekniska störningar och naturhändelser. Komplexa inbördes beroendeförhållanden bidrar till denna känslighet. Tekniska kollapser, mänskliga felhandlingar, sabotage eller extrema väderförhållanden kan leda till svåra och långvariga störningar som fortplantar sig i mycket stora delar av exempelvis transport- och elförsörjningssystemen.

Genom att system successivt byggs samman till system av system, blir de oöverskådliga, komplexa och tekniskt heterogena. En mindre störning kan då snabbt fortplanta sig och ge upphov till kaskadeffekter (en omfattande spridning av störningar). Användning av informations- och kommunikationsteknikbaserade styr- och reglersystem för fjärrstyrning och kontroll, bland annat via Internet, gör de tekniska systemen sårbara även för IT-relaterade störningar. Vid störningar kan det vara svårt att avgöra om orsaken till störningen var en terrorhandling, en teknisk kollaps, en mänsklig felhandling eller ett sabotage.

Avreglering av offentliga monopol har inom bland annat elförsörjningsområdet lett till att nödvändiga reserver och resurser för att stoppa kaskadeffekter saknas. System som redan är störningskänsliga i normalläget är särskilt sårbara för fysiska och elektroniska angrepp. Att samhället här och nu är sårbart visar bland annat de omfattande elavbrott som inträffat 2003 och som berört USA, Kanada, Storbritannien, Sverige, Danmark och Italien.

Konsekvenser för krishanteringssystemet

Kartan för den tekniska infrastrukturen är svår att överblicka på grund av exempelvis komplexa ägarförhållanden med flera underleverantörer. Det finns ett stort behov att se över hur denna

infrastrukturkarta ser ut. Ett exempel på vilka konsekvenser som fysisk konvergens kan få, är de två tillfällen i mars 2001 och maj 2002 då tunnelbränder ägde rum i Akalla i nordvästra Stockholm. Där blev 50 000 människor utan el under flera dagar eftersom både den ordinarie kabeln och reservkabeln drabbades av en svårsläckt brand i en tunnel.

Avregleringen inom olika tekniska infrastrukturer har också lett till att överblicken över infrastrukturkartan försvunnit. Där det tidigare fanns en ensam ägare som hade möjlighet till överblick finns idag ett flertal olika aktörer, såväl nationella som internationella.

Extrema natur- och väderhändelser

Samhället är känsligt för extrema natur- och väderfenomen. Vårt geografiska läge gör exempelvis att det finns en risk för isstormar, saltstormar[13], extrem kyla och svåra snöoväder. Årets första snöoväder är ett aktuellt exempel på vilka konsekvenser till och med en mindre allvarlig väderhändelse kan ge för bland annat flygtrafiken och för eldistributionen. Andra typer av naturhändelser som samhället riskerar att exponeras för är stormar, saltstormar och översvämningar på grund av höga vattenflöden. Exempelvis kan el, tele och IT-avbrott uppstå när vägbankar eroderar eller broar förstörs vid översvämningar. En översvämning kan ge svåra konsekvenser för vattenförsörjningen.

I planeringsinriktningen för 2006 skriver KBM just om översvämningar och höga flöden och att långvariga, ihållande regn kan ge sådana nederbördsmängder att de största sjöarna i Sverige blir överfulla och måste tappas av. Det skulle kunna leda till mycket allvarliga konsekvenser i Stockholm eller i Göta älvdalen. Vattenmängderna som måste släppas ut kan orsaka ras, utsläpp och störa infrastruktur och viktiga samhällsfunktioner.[14]

Sverige har historiskt sett drabbats av svåra översvämningar med mellan fem och tjugo års mellanrum. Under sommaren 2004 drabbades Jönköpings och Kronobergs län av svåra översvämningar. Erfarenheterna från dessa är att det finns ett behov av att redan i det förebyggande arbetet samordna både personella och materiella resurser. Vid översvämningarna var behovet av att förstärka de kommunala resurserna med statliga (från Räddningsverket), militära (värnpliktiga och från hemvärnet) och i viss mån med resurser från utlandet stort.

Sedan tidigare har Räddningsverket i uppdrag att verka för att regionala samordningsgrupper för älvsystem (älvar och dess biflöden) och andra

13. En saltstorm uppstår när salt från havet stormar in över land. Vinden för sedan saltet vidare och kan bland annat orsaka elavbrott när den avsätts på elledningarnas isolatorer.
14. KBM, planeringsprocessen 2004:3 ”Samhällets krisberedskap 2006 – inriktning för myndigheternas planering”

större vattendrag bildas. För att framgångsrikt kunna förebygga och hantera översvämningar måste varje älvsystem ses som en helhet. En av de erfarenheter som Räddningsverket redovisar från översvämningarna i somras är att samordningsgrupperna för älvsystemen fyller en viktig funktion och bör aktiveras ytterligare, främst när det gäller det förebyggande arbetet.

Konsekvenser för krishanteringssystemet

Samverkan inför extrema väderhändelser är en förutsättning främst för att kunna minska konsekvenserna av en väderhändelse när den uppstår. De allvarligaste och mest extrema väderhändelserna inträffar sällan, den senaste isstormen som inträffade i Sverige ägde rum på 20-talet, och när det gäller mycket svåra översvämningar talar man om 50- och 100-årsflöden. Trots att översvämningar, stormar och snöoväder drabbar den enskilde hårt är dessa händelser något som vi måste leva med och som varje kommun måste ha förmåga att hantera. Däremot bör krishanteringssystemet koncentreras kring att kunna hantera sådana händelser som är sällsynta, men som får mycket svåra konsekvenser för samhällets funktion när de inträffar.

Då det gäller resonemang kring vilka extrema väderhändelser som krishanteringssystemet kan komma att behöva hantera har bland annat Sveriges meteorologiska och hydrologiska institut (SMHI), Sveriges geologiska undersökningar (SGU), Statens geotekniska institut (SGI), samt Räddningsverket viktiga roller att spela.

Vid olika typer av extrema väderhändelser, såsom isstormar, långvariga snöoväder och svåra översvämningar som inträffar sällan finns ett stort behov av såväl mänskliga som tekniska resurser. Detta är något som den enskilda kommunen sällan kan tillhandahålla. I det här sammanhanget är det bland annat viktigt att se över vilka konsekvenser som nedläggning av militära förband har för tillgången på resursförstärkning och hur man bäst löser den frågan. Detta är något som görs i samband med KBM:s regeringsuppdrag om samhällets säkerhet och beredskap inför svåra påfrestningar på samhället i fred (Fö2004/1795/CIV).

En översvämning i Mälaren skulle sannolikt få stora konsekvenser i Stockholmsområdet. Exempelvis kan man tänka sig att vattnet kommer att forsa ner till försörjningstunnlar med elstationer och ställverk, tunnelbanan och andra utrymmen som finns under stadens gator. Problem i el, tele- och IT-försörjning och hos transportsystemen är att vänta. Även vattenförsörjningen kommer att sättas på prov. Dessutom riskerar regering, riksdag, Riksbanken, ett antal statliga verk och företag att bli drabbade. I Göteborg skulle ett liknande scenario bli aktuellt vid en översvämning av Göta älv. Erfarenheter från de svåra översvämningarna som ägde rum i Prag 2002 kan i detta fall ge värdefulla kunskaper kring hantering av denna typ av sällsynta men svåra översvämningar.

Aktörsrelaterade hot och risker

Det här kapitlet syftar till att ge en översiktlig bild av aktörsrelaterade antagonistiska hot och risker som kan orsaka allvarliga kriser och som kräver insatser av flera myndigheter. Antagonistiska hot och risker används här med innebörden aktör eller aktörer som har avsikt att skada Sverige eller svenska intressen utomlands samt utländska intressen i Sverige.

Risk är en sammanvägning av den bedömda sannolikheten och konsekvensen av en skadehändelse. Värderingar av hot från aktörer innefattar vidare att bedöma avsikt, förmåga och möjlighet. Förmågan kan vidare ses som kombinationen av skicklighet och redskap. Materiel och kunskap är huvudbeståndsdelarna i redskap.

För att en antagonistisk handling skall kunna lyckas fordras att det angripna objektet har en sårbarhet som kan exploateras. De hot och risker som behandlas här är sådana som kan medföra omfattande och svårbemästrade skadesituationer eller störningar i grundläggande samhällsfunktioner.

En gränslös, föränderlig och sammankopplad värld

Utvecklingen av hot och risker är nära kopplad till samhällsutvecklingen i stort. Det gäller både i tid och i rum. Stater, terrorister och enskilda aktörer använder de medel som finns tillgängliga i samhället. Konsekvenserna av avsiktliga angrepp avgörs av samhällets uppbyggnad och motståndskraft.

Stater har varit de viktigaste aktörerna i det internationella systemet sedan den westfaliska freden. Krig och omfattande våldsutövning som tidigare i huvudsak skett mellan stater eller i olika slag av inbördeskrig har kommit att i allt högre grad utövas av terrornätverk och individer och riktas mot civila mål. Internationella nätverk av terrorister utmanar nu nationalstater med terrordåd mot både civila och militära mål. Attacker med syfte att döda oskyldiga civila i stor skala har hittills förekommit regelbundet under början av 2000-talet.

Individer som av olika skäl är beredda att utföra terrorattacker verkar i mer eller mindre löst sammankopplade nätverksorganisationer. Nätverken är ofta

icke-hierarkiska och föränderliga. Det gör det svårare att kartlägga och hindra deras verksamhet.

Icke-hierarkiska nätverk av terrorister som har mycket långsiktiga mål använder okonventionella metoder och är beredda att använda massförstörelsevapen för att orsaka mycket omfattande skador på befolkningen eller samhället. Nätverken är ofta icke-hierarkiska och föränderliga. Det gör det svårare att kartlägga och hindra deras verksamhet.

Befolkningen och funktioner som har särskilt folkrättsligt skydd är nu mål för den internationella terrorismen. Konflikterna utkämpas mitt i de fredstida samhällena här och nu. Samhället och befolkningen är både mål och arena för de nya grupper som hotar samhällen och säkerhet.

Hot- och riskmiljön under 2000-talet

Under det kalla kriget byggdes mycket stora arsenaler av massförstörelsevapen upp i Sovjetunionen. I samband med att de kommunistiska diktaturerna upplöstes och globaliseringen ökade under slutet av 1900-talet, har illegal tekniköverföring och transnationell organiserad brottslighet ökat i omfattning och blivit ett större samhällshot.

Teknik och kunskap om produktion av vapen och vapenbärare finns också tillgängliga. Idag ser många länder med oro på den illegala vapen – och teknikspridning som sker. Organiserad brottslighet underlättas av de nya marknaderna och tillgången till personer med specialistutbildning.

Sönderfallande eller fallerade stater (t.ex. Afghanistan och Somalia) är basområden för internationell terrorism. Internationella nätverk av terrorister utmanar nationalstater med terrordåd mot både civila och militära mål. Attacker med syfte att döda oskyldiga civila i stor skala har förekommit regelbundet under början av 2000-talet.

Den bakomliggande orsaken och incitamentet till krig, konflikter och inbördes strider är ofta ekonomiska. Det finns personer många grupper och enskilda individer som har mycket att vinna ekonomiskt på att hålla konflikter vid liv.

Det går heller inte att dra en skarp gräns mellan terrorism och organiserad brottslighet. Samma personer och resurser används för olika ändamål beroende på när de bäst behövs. Möjligheten till statlig finansiering av terrorism har minskat. Detta har lett till ett ökat behov av egenfinansiering av terrorism genom olika typer av organiserad brottslighet.

Befolkningen och samhällsfunktioner som har särskilt folkrättsligt skydd är nu mål för den internationella terrorismen. Konflikterna utkämpas mitt i de fredstida samhällena här och nu. Samhället och befolkningen är både mål och arena för de nya grupper som hotar samhällen och säkerhet. Icke-hierarkiska nätverk av terrorister som har mycket långsiktiga mål använder okonventionella metoder och är beredda att använda massförstörelsevapen för att orsaka mycket omfattande skador på befolkningen eller samhället. Ett delmål

är att skada allmänhetens förtroende för den verkställande makten och det demokratiska systemet. Även om målen hittills ofta har haft anknytning till USA eller dess allierade, kan angreppen ske i delar av världen där lämpliga tillfällen eller resurser finns.

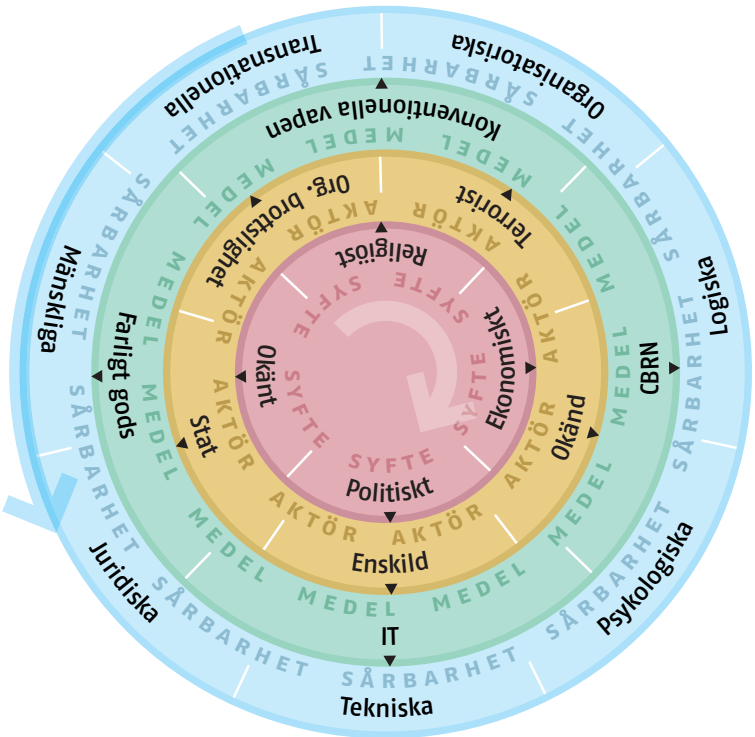

Bild 1: *"Trissan" skall ses som ett stöd för förståelse för hotbildskategorier och skall ses ur ett "utifrån-in-perspektiv". Den gör inget anspråk att ge en helhetsbild utan skall ge en schematisk bild av det som nämns i avsnittet aktörsbundna hot. Trissans olika skikt kan snurras separat och genom detta kan man få olika utfall. Tyngdpunkten i trissan ligger i att få en förståelse för hur komplex hotbilden ser ut idag. Trissan beskriver även de främsta slutsatser KBM har dragit avseende sårbarheter, medel, syfte och aktörer men även konvergensen mellan de olika skikten.*

Olika kategorier av aktörsrelaterade antagonistiska hot

Stater

Staterna är de resursstarkaste aktörerna i det internationella systemet. I kraft av denna styrka utgör de det potentiellt största hotet. Sveriges försvars- och säkerhetspolitiska läge är mycket gott. Det finns inget som tyder på att detta läge skulle komma att ändras under överskådlig tid. Geostrategiskt kommer utvecklingen i Ryssland att ha stor betydelse för Sverige. Att bibehålla och stärka den transatlantiska länken är av stort intresse för Sverige. Samarbetet bör vidgas och fördjupas inom området samhällets säkerhet och beredskap.

Även om Sveriges territoriella integritet inte är hotad kan Sveriges funktionella säkerhet hotas genom till exempel skadlig datakod som sprids av andra stater. Andra stater kan också agera genom internationell terrorism. Fallerade eller kriminella stater kan användas av terrorister i deras verksamhet. Det finns också ett antal stater som ställt sig utanför det internationella samfundet och som har, eller har för avsikt att anskaffa, kärnvapen. Sådana stater är ett hot mot alla stater och därför även en angelägenhet för Sverige.

Andra stater bedriver underrättelseaktiviteter i Sverige. Det är främst inom områdena politik, försvar i vid bemärkelse, vetenskap, teknologi och ekonomi. Förlust av information kan allvarligt skada Sveriges nationella säkerhet. Företag i Sverige kan göra betydande ekonomiska förluster och minska Sveriges resursbas. Förlust av information kan hota Sveriges agerande på den internationella politiska arenan.

I samband med internationella fredsbevarande och fredsframtvingande operationer kan andra stater vara ett hot mot Sverige eller svenska intressen. En förstärkt fredstida förmåga är också basen för en anpassning av den svenska förmågan om hotbilden från andra stater mot Sverige skulle komma att förändras.

Sveriges försvars- och säkerhetspolitiska läge är i grunden förändrat till följd av Sovjetunionens kollaps samt Nato:s och EU:s utvidgningar. Försvarsberedningen gör bedömningen att de för närvarande och under överskådlig tid inte finns något hot mot Sveriges territoriella integritet.[15] Underrättelsehotet är fortsatt omfattande, men har ändrat inriktning. Det riktas främst mot politiska, ekonomiska och högteknologiska förhållanden.

Internationell terrorism

Internationell terrorism med masskade- eller masseffektsyfte har vuxit fram de senaste åren. Exempel på terrordåd som genomförts är attackerna i USA den

15. Försvarsberedningens rapport ”Försvar i en ny tid”, Ds 2004:30

11 september 2004, bombningen av en nattklubb på Bali, attacken mot en synagoga i Tunisien, sprängningen av pendeltåg i Madrid och gisslandramat på en skola i Nordossetien. Internationella terroristnätverk har visat att de kan genomföra terrordåd som kräver lång planering, dolt uppträdande, och använda resurser som finns i samhället. Attackerna har lett till mycket stora förluster i människoliv och har påverkat viktiga politiska beslut.

Den internationella terrorismen består till stor del av icke-hierarkiska nätverk med förgreningar och sympatisörer i många länder. Utöver de islamistiska terrornätverk som har varit i fokus de senaste åren finns ett stort antal aktiva terrornätverk i skilda delar av världen. De har olika mål med sin verksamhet och har skilda förmågor. En oroande trend är att terroristorganisationer i skilda länder och regioner har visat ökade tendenser till att samarbeta. Terroristorganisationer och organiserad brottslig samarbetar eller sammansmälter också i olika kombinationer som delar av internationella nätverk. Genom att kombinera olika förmågor kan oförutsedda och allvarliga former av angrepp möjliggöras.

Kampen förs bland och mot civila mål i samhällena här och nu. Terrorister använder de tillfällen och de medel som enklast och effektivast exploaterar sårbarheterna i samhället. Eldhandvapen, pansarskott, granatgevär, granatkastare och bärbara luftvärnsrobotar är exempel på vapen som kan skaffas på illegalt sätt och som används av terroristgrupper. Konventionella sprängmedel eller användning av andra farliga ämnen som kan användas som sprängmedel är det vanligaste sättet att genomföra terroristattentat.

En del terrornätverk har mycket långsiktiga mål och ser masskade- eller masseffektterrorism som ett mål i sig. De medel som hittills använts ryms inom de ovan nämnda kategorierna. Det är uppenbart att kreativiteten är stor inom den projektliknande terrorism som tillämpas inom terrornätverk som al-Qaida. Vid attentaten den 11 september 2001 i USA utnyttjades till exempel passagerarflygplan som missiler.

Ett av de allvarligaste hoten är terrorism med nukleära, biologiska, kemiska eller radiologiska medel (CBRN). En variant av nukleära vapen är radiologiska vapen, det vill säga spridning av radiologiskt material med till exempel en konventionell bomb. Ett nytt begrepp för hot och risker som får stora konsekvenser oberoende av om det är fysiska eller elektroniska medel som används är masseffektsvapen. Här innefattas massförstörelsevapen men också omfattande angrepp med elektroniska vapen eller psykologiska vapen. Att attacker med masseffektsvapen ännu inte har genomförts av terrorister beror troligen på att de ännu inte har den nödvändiga tekniska och operativa förmågan att genomföra sådana attacker.

Under det kalla kriget var användning av massförstörelsevapen en sista utväg. För den terrorism som syftar till masskadeeffekter kan de vara ett förstahandsalternativ, om och när de får till-

gång till teknisk och operativ förmåga. Ett problem här är spridningen av ny teknologi som kan användas i masseffektssyfte. En särskild utredare har studerat behovet av ett mer samordnat och effektiviserat skydd för farligt gods i Sverige[16].

I Storbritannien anser myndigheterna att det bara är en tidsfråga innan landet utsätts för ett allvarligt terrorangrepp, möjligen med användning av enklare massförstörelsevapen. Med andra ord, att det inte är en fråga *om* ett terrorangrepp kommer att inträffa utan snarare *när*. På mitten av 90-talet avbröts provisoriska Irländska republikanska armén (IRA) innan de lyckades slå ut elförsörjningen i London genom samordnade sabotage mot nyckelpunkter i elförsörjningen. Om attentaten hade lyckats hade London varit utan elförsörjning under en längre tid.

Utgångspunkten för planeringen för samhällets säkerhet och beredskap bör vara att Sverige inte är immunt mot terrorism. Angrepp mot utländska länders intressen i Sverige kan ske på samma sätt som det skedde mot brittiska intressen i Turkiet. Sverige kan i framtiden komma att delta i FN-sanktionerade fredsbevarande eller fredsframtvingande internationella operationer av ett slag som ökar Sveriges exponering för internationell terrorism. Ett svenskt agerande inom ramen för EU:s militära och civila krishantering kan leda till att Sverige uppfattas som en del av en större aktör och därmed ett legitimt mål.

I Sverige finns olika slag av resurser som kan användas inom internationell terrorism. En viktig del i bekämpningen av internationell terrorism är att hindra olika former av stödjande verksamhet. Sverige har åtagit sig att bekämpa internationell terrorism i vilket ingår att förhindra att Sverige utgör ett skyddat basområde för terroristverksamhet (*safe haven*).[17] Inom området samhällets säkerhet och beredskap bör stor uppmärksamhet riktas mot behovet av skydd av resurser som kan användas av terrorister och att Sverige inte ska kunna användas som basområde eller transitland till stöd för terrorism.

Sammanfattningsvis gör KBM bedömningen att terrorattacker kan komma att genomföras i Sverige eller mot svenska intressen utomlands. Hotet är betydande mot amerikanska, brittiska och israeliska intressen i Sverige. Om den potentiella konsekvensen av en terrorattack är stor och sannolikheten är svårbedömbar eller föränderlig, måste planeringen och inriktningen av samhällets säkerhet och beredskap utgå från att fredstida förstärkt förmåga krävs för att möta hotet och de möjliga konsekvenserna av en genomförd attack. Det gäller både pro-aktiva och reaktiva åtgärder.

Sveriges deltagande i internationella civila och militära operationer kräver

16. Näringsdepartementet, ”Ny reglering för transporter av farligt gods”, SOU 2004:87
17. FN, resolution 1269

att det finns en tillräcklig förmåga för att förhindra terrorattacker mot Sverige och svenska intressen utomlands. Det är ett svenskt internationellt åtagande och intresse att Sverige inte är ett basområde för terroristverksamhet.

Konsekvenserna av terrorattacker med masskade- eller masseffektsyfte kan bli så stora att de inte kan hanteras i Sverige utan hjälp från andra länder. KBM bedömer att förmågan ge hjälp till andra länder och att motta hjälp i samband med terrorangrepp är idag otillräcklig.

För att upptäcka och förhindra terroristattacker krävs en förbättrad informationshantering och ett ökat samarbete inom underrättelse- och säkerhetsområdet. Resurserna för att skydda viktiga objekt och för att upptäcka samt avbryta terroristverksamhet bör stärkas.

Organiserad brottslighet

Kombinationen av en allt gränslösare värld och tillgången till instabila stater som basområden för organiserad brottslighet har lett till gynnsammare förutsättningar för transnationella kriminella organisationer. En allvarlig konsekvens av organiserad brottslighet är dess negativa påverkan på rättsstaten och den instabilitet som blir följden.

När väl organiserad brottslighet har etablerats i ett samhälle kräver den stora samhällsresurser för att bekämpas. Det finns vidare ett samband mellan organiserad brottslighet och terrorism. Studier visar att terrororganisationer och gränsöverskridande organiserad brottslighet samarbetar och använder samma resurser. Det finns också betydande likheter i hur organisationerna är uppbyggda. Både terrororganisationer och gränsöverskridande organiserad brottslighet har följande karaktäristika.[18]

- De använder nätverks- och cellbaserade strukturer
- Deras aktiviteter är transnationella
- De behöver fristäder, till exempel fallerade stater
- De drar nytta av folkgrupper i förskingring
- De har liknande mål- och grupperingsprinciper
- De har kapacitet till underrättelse- och kontraunderrättelseverksamhet
- De har program för kontakter med myndigheter och allmänhet
- De är beroende av extern finansiering

Även om den organiserade brottsligheten i Sverige framför allt är en angelägenhet för gränsskyddet och polisen, kräver hanteringen av den ett nära samarbete mellan olika myndigheter. Det svenska samhället har i stort god motståndskraft mot effekterna av organiserad brottslighet. Organiserad brottslighet kan dock hota tilliten till myndigheterna och staten samt utgöra ett särskilt hot mot rättsamhället.

18. Tamara Makarenko, ” Terrorism and Transnational Organised Crime: the emerging nexus”

Sammanfattningsvis gör KBM bedömningen att organiserad brottslighet i dagsläget inte hotar samhällets säkerhet och beredskap men att det är angeläget att den organiserade brottsligheten inte får en ökad successiv utbredning i Sverige. Det är viktigt att samhällets samlade information används effektivt för att bekämpa den organiserade brottsligheten.

Den internationella utvecklingen med en konvergens mellan terrorism och organiserad brottslighet innebär att den transnationella organiserade brottsligheten är ett potentiellt allvarligt hot mot Sverige. Hoten från den transnationella organiserade brottsligheten måste särskilt uppmärksammas i samband med Sveriges deltagande i internationella civila eller militära operationer utomlands.

Extrema grupper

Olika extrema grupper, såsom nynazistiska och andra autonoma grupper som kan hota rikets inre säkerhet följs av Säkerhetspolisens (Säpos) författningsskydd. De senare är grupper som präglas av idéer som frihetlig socialism, anarkism och syndikalism. Det kan också vara olika så kallade djurrättsgrupper. Vilket hot dessa grupper utgör mot samhällets säkerhet och beredskap är enligt KBM:s mening svårbedömt. Internationaliseringen av grupperna kan göra dem resursstarkare. Detsamma är fallet om de lyckas knyta till sig personer som på olika sätt har särskild kunskap.

Utvecklingen i Nederländerna efter mordet på en kulturpersonlighet som kritiserat islamistiska grupper och sedvänjor inom islam är oroande. Efter mordet har våld riktats mot moskéer och andra muslimska centra. Det kan tolkas som ett tecken på att enstaka händelser kan öka stödet för extrema grupper och att benägenheten att använda politiskt motiverat våld kan utlösas av enstaka händelser. Även de planerade attentaten mot viktiga samhällsfunktioner i Västerås under hösten 2004 kan vara ett sånt tecken.

Sammanfattningsvis gör KBM bedömningen att extrema grupper idag inte kan hota samhällets säkerhet och beredskap i så hög grad att de är en angelägenhet för krishanteringssystemet. Åtgärder som genomförs inom krisberedskapen för att möta andra hot och risker gör samhället mer motståndskraftigt mot brottslig verksamhet från extrema grupper.

Enskilda aktörer

Människor styrs av sina känslor och föreställningar. En individ som lider av en psykisk störning eller som av andra skäl har en förvrängd verklighetsuppfattning kan utföra gärningar som är svåra att förutse och förstå.

Även i något vanligare bemärkelse mer rationellt handlande individer kan orsaka allvarlig skada. Det kan handla om personer som känner sig orättvist behandlade eller hyser agg mot samhället. I normalfallet kan inte en enskild individ hota samhällets säkerhet och

beredskap. Myndigheter eller företags verksamheter kan skadas av enskilda individer med särskilda kunskaper. Det kan ske genom fysisk eller informationssystemrelaterade sabotage. Enskilda individer kan också stjäla information från sin arbetsgivare. Personer med särskilda kunskaper eller färdigheter, så kallade insiders, kan allvarligt hota samhällets säkerhet.

Även relativt resurssvaga individer kan, om tillfälle ges, hota statsledningen eller nyckelfunktioner. Ett tragiskt exempel är mordet på utrikesminister Anna Lindh. Den särskilde utredaren med uppdrag att göra en utvärdering av personskyddet för den centrala statsledningen föreslår i sitt betänkande att det är angeläget att skapa en ordning som innebär att inte bara kända hot utan också eventuella eller latenta hot kan motverkas. Utredaren föreslår också att Säpos ska få ökad tillgång till information från hälso- och sjukvården samt kriminalvården. Utredaren pekar också på behovet av ett förbättrat informationsutbyte mellan berörda myndigheter och funktioner.[19]

Sammanfattningsvis gör KBM bedömningen att behovet att skydda viktiga samhällsfunktioner är stort. Vissa samhällsfunktioner är beroende av nyckelpersoner. Det gäller även krishanteringssystemet. Personal- och nyckelpersonsfrågorna bör vara en naturlig del av krisberedskapen och redovisas i risk- och sårbarhetsanalyserna.

Slutsatser

Enligt Säpos bedömning är det är svårt att se att Sverige idag skulle utgöra ett förstahandsmål för internationella terroristnätverk. Detta gör dock inte Sverige immunt mot terrorism eller andra former av antagonistiska hot. Vid de bombattentat som riktades mot bland annat brittiska mål i Turkiet vintern 2003 dog fler turkar än britter. Vid ett terrordåd på Bali oktober 2002 dödades 202 människor, varav sex svenskar. Attentaten riktades mot andra staters intressen utan att ta någon hänsyn till vilka som drabbades eller förolyckades. Antagonistiska hot kan riktas mot utländska mål i Sverige. Terrorism med användning av biologiska medel kan få en okontrollerad spridning som drabbar Sverige. Svenska medborgare, företag, myndigheter och organisationer kan drabbas av terrorism utomlands.

Invånarna i Sverige måste känna tillit till regeringen och myndigheterna att de åtgärder som genomförs är rimliga för att skydda dem mot effekterna av antagonistiska hot. Om smittskyddet stärks, ökar också förmågan att hantera bioterrorism och tvärtom. Är de möjliga konsekvenserna så stora eller allvarliga att de är oacceptabla, bör det räcka med att det finns en sårbarhet och ett relativt litet hot för att relevanta och tillräckliga risk- och krishanteringsåtgärder skall genomföras.

19. Justitiedepartementet, ”Personskyddet för den centrala statsledningen”, SOU 2004:108

Det är viktigt att höja blicken och se Sverige som en del av ett större internationellt sammanhang. Konsekvenser av internationell brottslighet, IT-relaterade hot, antagonistiska hot, fallerade stater eller smittutbrott påverkar också Sverige. Många av dagens hot och risker är gränslösa till sin karaktär.

Utvecklingen inom EU går i riktning mot ett utökat gemensamt skydd mot antagonistiska hot. Sverige har åtagit sig att stärka sin hamnsäkerhet, skyddet av flygplatserna, genomföra åtgärder inom smittskyddsområdet m.m. En solidaritetsklausul i EU:s nya författning skulle innebära solidarisk hjälp till andra medlemsländer i händelse av en terroristattack eller en naturkatastrof. När Sveriges hot-, risk- och krishanteringsförmåga byggs upp bör den ses i ett europeiskt perspektiv.

Informationssäkerhet

Detta avsnitt behandlar aktuella trender i samhällets informationssäkerhet. Under rubriken *Hot* presenteras trender i medel och metoder för spridning av skadlig kod och riktade attacker. Under samma rubrik redogörs för olika antagonistiska aktörer. Vidare presenteras olika mål som är utsatta eller exponerade för olika typer av hot eller som, om de drabbades, skulle kunna orsaka allvarliga konsekvenser i samhället. *Sårbarheter* presenteras ur de tre perspektiven tekniskt, organisatoriskt och relaterat till avsaknad av, eller brister i, befintliga säkerhetssystem.

Under *sammanfattande slutsatser, rekommendationer* sammanfattas avsnittet om Informationssäkerhet och slutsatser presenteras. Rekommendationer lämnas avseende hur myndigheter och andra aktörer kan förbättra sin egen säkerhet. Avslutningsvis lämnas praktiska tips om var ytterligare stöd och hjälp kan fås.

Läsaren av detta avsnitt förutsätts ha en grundläggande förståelse för informationssäkerhet och känna till begrepp såsom datavirus och konfigurering. I en bilaga förklaras hur centrala informationssäkerhetsbegrepp används i denna rapport.

Hot

Medel och metoder

IT-relaterade incidenter, brott och statistik

Nyligen genomförda undersökningar från (CSI/FBI) Computer Security Institute/Federal Bureau of Investigations[20] och företaget Symantec[21] pekar på att det totala antalet icke-auktoriserat användandet av datorer respektive mängden av attacker mot dem har avtagit under det senaste året. Andra rapporter, exempelvis från Verisign, indikerar däremot en ökning i attackmönstret.

20. Tillgänglig på http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf
21. Symantec Internet Security Threat Report, Trends for January 1, 2004 - June 30, 2004.

I Norge har en omfattande mörkertalsundersökning nyligen genomförts bland norska företag.[22] I rapporten konstateras bland annat att endast ett av drygt hundra fullbordade dataintrång anmäldes. I kombination med datavirusangrepp uppskattas företagens extra kostnader till 5 miljarder norska kronor.

Det finns flera svårigheter med att skapa en samlad bild över förekomsten av skadlig kod, IT-incidenter och IT-relaterad brottslighet i Sverige och undersökningar motsvarande de som nämnts ovan saknas. Rapporteringsbenägenheten är låg avseende såväl brott som incidenter. Ett annat problem är att den statistik som finns är svår att finna, måste sökas från olika källor och är svår att sammanställa och jämföra. Dessutom finns ingen gemensam och vedertagen begreppsapparat. Innebörden av begrepp som attack, mask, trojan och spionprogramvara skiftar.

Utifrån inrapporterade incidenter, befintlig officiell och inofficiell statistisk, utländska förhållanden samt svensk expertis kvalitativa bedömningar av situationen är det dock möjligt att peka på vissa trender och dra generella slutsatser. En sådan slutsats är att mörkertalet för antalet inrapporterade brott och incidenter också i Sverige är stort och att kostnaden för dessa är höga.

Skadlig kod

Skadlig kod såsom datavirus, datamaskar eller trojaner är program som orsakar avsiktliga störningar eller skador för en verksamhet.

Antalet datavirusattacker tenderar att minska i omfattning. Idag är mindre än tio procent av den skadliga koden som sprids på Internet datavirus eller makrodatavirus. Även antalet nyskrivna datamaskar tenderar att minska. Däremot modifieras gammal kod i högre utsträckning på sådant sätt att skyddssystem inte känner igen kodens signatur.

Gränserna mellan olika typer av skadlig kod suddas ut, till exempel sprider datamaskar allt oftare sådan funktionalitet som tidigare förknippades med trojaner. Skadlig kod tenderar i allt högre utsträckning att utvecklas för specifika syften, till exempel för att stjäla bank- och kreditkortsinformation.

Den centrala funktionen i spionprogramvara är att den i smyg samlar någon typ av information från den infekterade datorn och förmedlar den vidare. En nyligen genomförd undersökning pekar på att i genomsnitt var tredje dator är infekterad av någon typ av spionprogramvara och spridningen kan ske försåtligt. Det finns till exempel tjänster på Internet som utger sig för att rensa bort spionprogramvara men som i själva verket är trojaner och själva sprider spionprogramvara.

Den största delen av skadlig kod sprids via e-post men allt mer sprids via webbtrafik. Ett vanligt infektionssätt är att slutanvändare besöker webbsidor som utnyttjar sårbarheter i användarens

22. Rapporten kan beställas från http://www.nsr-org.no/materiell.htm

applikationer varigenom spionprogramvara eller bakdörrar installeras eller skadlig kod sprids. Ett annat är nedladdning av filer som, förutom det önskade innehållet, också innehåller dold funktionalitet.

Attacker mot slutanvändares datorer

En ökande trend är att attacker och skadlig kod riktas direkt mot den programvara som finns i slutanvändarnas datorer.[23] Slutanvändare är alla som använder personliga datorer oavsett om detta sker i hemmet, på arbetsplatsen eller någon annanstans.

Genom att en slutanvändare till exempel besöker en webbsida som innehåller skadlig kod laddas den skadliga koden direkt till slutanvändarens dator. I detta fall sker det genom att utnyttja kända sårbarheter i slutanvändarens webbläsare. Också sårbarheter i andra program hos en slutanvändare kan utnyttjas. Detta är fallet med till exempel e-postklienter, P2P (peer-to-peer)-nätverk, mediaspelare och personliga brandväggar.[24]

Problemets omfattning bedöms av säkerhetsexperter som stort och allvarligt. I Svenska Dagbladet varnade till exempel Försvarets Radioanstalt (FRA) den 22 september för de sårbarheter som finns och har funnits i Microsofts webbläsare Internet Explorer under lång tid.[25] Företaget Symantec bedömer att attacker riktade mot slutanvändare kommer att fortsätta att öka.[26] Om de program vars sårbarheter utnyttjas dessutom är vitt spridda och använda, som är fallet med till exempel Internet Explorer, ökar problemets omfattning ur ett samhällsperspektiv.

Botnets

Bot (förkortning för robot) är en dator som infekterats med skadlig kod vilken möjliggör för någon annan att fjärrstyra datorn i olika syften. En dator kan vara infekterad utan att ägaren märker det. Den stora faran utgörs av att infekterade datorer finns på olika ställen i världen men kan fjärrstyras synkroniserat och kraftsamlas mot olika mål och i olika syften. Dessa nätverk av robotar kallas botnets.

Botnets kan användas för att tjäna pengar och det finns en illegal marknad för botnets. De kan köpas eller hyras enligt olika modeller, exempelvis kan ett visst antal datorer eller en bandbredd hyras under en viss tid. Förekomsten och användandet av botnets indikerar att utvecklarna och användarna av skadlig kod, som inte behöver vara samma personer, allt mer professionaliseras och att kopplingar till organiserad brottslighet förekommer.

Användningsområden för botnets är till exempel massspridning av oönskad

23. Slutanvändarnas datorer är de så kallade klienterna som skiljer sig från servrarna.
24. Symantec Internet Security Threat Report, Trends for January 1, 2004 - June 30, 2004.
25. Artikeln tillgänglig på http://www.svd.se/dynamiskt/inrikes/did_8193752.asp
26. Symantec Internet Security Threat Report, Trends for January 1, 2004 - June 30, 2004.

e-post, så kallad spam och utförande av DDoS-attacker (Distributed Denial of Service) vilket har kombineras med utpressning. Spelföretag och bookmakers med verksamhet på Internet har hittills varit särskilt utsatta för denna typ av hot.

Den 10 oktober 2004 utsattes flera holländska myndigheter för DDoS-attacker från botnets runt om i världen vilket gjorde att myndigheternas webbsidor inte var tillgängliga på flera dygn. Sveriges IT-incident centrum, SITIC, bistod sin holländska motsvarighet i att avbryta attackerna genom att kontakta de svenska Internettjänsteleverantörer vars nät utnyttjades. Internettjänsteleverantörerna stängde sedan i sin tur de adresser varifrån attackerna riktades. Bakgrunden till attackerna i Nederländerna var missnöje med aviserade sociala reformer.

Flera ministrar i landet tvingades också byta mobiltelefonnummer eftersom deras telefonnummer hade publicerats på Internet med en uppmaning om att skicka sms till dem, vilket också skedde. Exemplet är intressant eftersom det visar att också andra tekniska system än Internet kan utsättas för DDoS-attacker.

Förekomsten av botnets är ett allvarligt och ökande problem som också förekommer i Sverige. Det förekommer under hösten 2004 minst en svensk polisiär förundersökning där svenskar misstänks ha styrt botnets. Enligt företaget Symantec ökar antalet infekterade datorer och antalet botnets kraftigt. Fenomenet har av brottsbekämpande myndigheter i USA och Storbritannien givits mycket hög prioritet.

Spam

Med spam avses massutskick av oönskad och obeställd elektronisk post utan mottagarens samtycke. Enligt uppgifter från bland annat EU och OECD har mängden spam ökat dramatiskt under de senaste tre åren och utgör idag cirka två tredjedelar av all e-posttrafik i världen. Detta motsvarar hundratals miljoner meddelanden varje dag.[27] Hanteringen av spam tar dels stor dator- och nätverkskapacitet i anspråk. Dessutom innebär problemet att resurser måste avsättas för att administrera problematiken, filtrera inkommande e-post och rensa systemen. Problemet gör också att användarnas förtroende för elektroniska kommunikationer undergrävs.

Det är svårt att beräkna kostnaden för spam men den svenska föreningen *antispam.nu*[28] uppskattar den samlade svenska kostnaden till flera miljarder kronor per år.

Problemet med spam avser i första hand massutskick av obeställd elektronisk direktreklam. I skuggan av detta är det viktigt att påpeka att det också finns en seriös, kostnadseffektiv och efterfrågad marknad för elektronisk direktreklam.

27. Enligt uppgifter från Konsumentverket.
28. www.antispam.nu

Enligt Marknadsföringslagen (1995:450) är det förbjudet att utan föregående samtycke skicka reklam via elektronisk post till konsumenter och andra fysiska personer. Brott mot Marknadsföringslagen är inte en polisiär fråga utan hanteras av Konsumentverket. Anmälningar om spam kan göras på Konsumentverkets hemsida.[29] Under de första 7 månader som Konsumentverket erbjudit denna tjänst har 15 000 anmälningar gjorts. Knappt 20 % av dessa avser spam skrivna på svenska. Antalet anmälningar är nästan dubbelt så många som normalt görs per år inom Konsumentverkets alla övriga ansvarsområden.

Konvergensen mellan Internet och olika nya mobila terminaler och teknik, såsom till exempel 3G-systemet, gör att problematiken med spam riskerar att sprida sig till nya tjänster. Följden blir densamma när IP används för till exempel telefoni eller TV.

Phishing

Phishing är en form av bedrägeri som innebär att e-post, som ger sken av att komma från en legitim avsändare, skickas till mottagaren från en falsk avsändaradress. Härigenom skadar phishing såväl den enskilda konsumenten som det företag som får sitt namn utnyttjat. Genom att utge sig för att vara någon som mottagaren litar på, till exempel en bank, försöker avsändaren förmå mottagaren att svara på e-postmeddelandet och lämna ifrån sig konfidentiell information. Denna information används sedan för att till exempel stjäla pengar eller beställa varor. Ett mer kvalificerat tillvägagångssätt är att mottagaren via en länk i e-postmeddelandet går till en hackad server och lämnar ifrån sig efterfrågad information på en falsk webbsida.

Phishing är ett relativt nytt fenomen och trenden är kraftigt ökande. Företaget MessageLabs uppger att antalet phishing e-postmeddelanden ökat från några hundra i september 2003 till över två miljoner ett år senare.[30] Organisationen Anti-Phishing Working Groups[31] statistik visar att antalet falska webbsidor ökat med 25 % mellan juli och oktober 2004.[32]

Phishing har hittills i första hand drabbat engelskspråkiga finansiella institutioner och deras kunder. Fenomenet har dock börjat sprida sig till andra länder, exempelvis har tyska och brasilianska banker drabbats och i slutet av november 2004 dök den första kvalificerade attacken riktad mot svenskar upp. E-post formulerad på svenska uppmanade Eurocardkunder att logga in och lämna uppgifter på en falsk Eurocardhemsida. I USA uppskattas

29. www.epostreklam.konsumentverket.se
30. MessageLabs Intelligence Annual Email Security Report 2004. Tillgänglig på http://www.messagelabs.com/binaries/LAB480_endofyear_UK_v3.pdf
31. http://www.antiphishing.org
32. Tillgänglig på http://www.antiphishing.org/APWG_Phishing_Activity_Report-Oct2004.pdf

phishing under första halvåret 2004 ha kostat banker och kreditkortsföretag 1,2 miljarder dollar och över 1,5 miljoner människor uppskattas ha drabbats.[33]

Att phishing hittills inte riktats mot svenska kunder och finansiella institut i större omfattning kan bero på att språket i sig utgör en barriär. I jämförelse med den engelskspråkiga marknaden för denna typ av brottslighet är dessutom den svenska förhållandevis liten. En annan anledning är att de flesta svenska banker använder tokens eller i sämsta fall mjuka certifikat för att kunder ska kunna autentisera sig. I andra länder är det vanligare att endast användarnamn och lösenord krävs och det är denna typ av låga säkerhet som phishingattacker hittills utnyttjat.

Ingen samlad bild finns av i vilken omfattning svenskar som är kunder i utländska banker eller till utländska kreditkortsföretag drabbas. Detsamma gäller svenskar som nyttjar auktionssajter som eBay eller betal- och transaktionstjänster som PayPal eller e-gold. I maj 2003 hade företaget Symantec identifierat 20 verktyg som specialiserat sig på att stjäla bank- och kreditkortsinformation. I november 2004 hade antalet ökat till 840. Åtminstone 4 av dessa förekommer i Sverige.

Såväl phishing som utnyttjandet av svagheter i slutanvändarnas datorer innebär att offret genom sitt aktiva agerande många gånger själv bidragit till att råka illa ut. Detta innefattar att lämna konfidentiell information eller att möjliggöra en installation av skadlig kod på den egna datorn. Det främsta skyddet för såväl företag som enskilda utgörs av den enskildas säkerhetsmedvetna agerande på Internet. En diskussion förekommer också kring användandet av så kallad vit-listning istället för svartlistning, det vill säga att ett företag endast tillåter sin personal att besöka i förväg preciserade hemsidor eller att exekvera i förväg godkända filer. Allt som inte är tillåtet är alltså förbjudet.

Social engineering

Även om en organisations tekniska IT-säkerhet är god kan intrång i ett företag eller brott riktat mot det genomföras genom social engineering. Detta innebär att människor manipuleras snarare än datorer. Personer som har värdefull information kan kontaktas personligen och värvas eller luras att avslöja exempelvis personnummer, lösenord, telefonnummer eller annan känslig information. Fenomenet att lura eller värva mänskliga källor har alltid förekommit och används även idag i stor omfattning av till exempel utländska länders underrättelsetjänster. Social engineering är en metod som kan användas för att värva insiders.

Phishing är i sammanhanget intressant. Metoden har främst uppmärksammats i samband med ekonomiska bedrägerier. Företeelsen som sådan, det vill säga att någon luras att lämna ifrån sig

33. Symantec Internet Security Threat Report, Trends for January 1, 2004 - June 30, 2004.

information genom att svara på e-post eller att besöka en falsk hemsida, kan användas också i andra syften. Till exempel kan en stat eller ett konkurrerande företag använda metoden för att lura till sig information i syfta att spionera.

Aktörer

Stater

Begreppet stater innefattar också statsunderstödda aktörer. Ett antal stater har eller utvecklar en kvalificerad förmåga att genomföra informationsoperationer. Med informationsoperationer avses utnyttjande av motståndarens information och informationssystem till stöd för egna politiska eller militära mål.[34] Stater är också den typ av aktör som har störst förmåga att genomföra riktade attacker i specifika syften. Förutom en kvalificerad teknisk kompetens har stater förmågan att genomföra komplexa, samordnade och riktade operationer. De kan avsätta resurser för att identifiera och utnyttja nya sårbarheter och koordinera detta med till exempel social engineering eller signalspaning.

Vissa länder är överrepresenterade som utgångsländer för IT-relaterade brott och incidenter. Även om de flesta attacker bara består av ett led kan det vara vanskligt att med säkerhet avgöra varifrån attacker utgår, inte minst när det gäller kvalificerade angripare.

Organiserad brottslighet

Det finns indikationer på att organiserade brottslingar i allt högre utsträckning börjat intressera sig för de möjligheter som informationstekniken erbjuder. Rikskriminalpolisens IT-brottsrotel uppger emellertid att de renodlade IT-brotten är få men att IT i allt högre grad förekommer i all annan sorts brottslighet. Det förefaller som om möjligheten att tjäna pengar genom IT-relaterad brottslighet stimulerar utvecklingen av densamma. Phishing och botnets är två exempel där informationsteknik utnyttjas för att tjäna pengar genom brott.

Cyberterrorism

Den svenska straffrättsliga definitionen av terroristbrott finns i Lag (2003:148) om straff för terroristbrott. I svensk lag förekommer inte begreppet cyberterror. Centrum för Informationsoperationsstudier (CIOS) vid Försvarshögskolan definierar cyberterrorism som en handling som uppfyller terroristbrottslagens rekvisit och genomförs med hjälp av infologiska medel och metoder. Det finns exempel på att sådana handlingar planerats men inte på att de ännu har genomförts.

Idag använder terroristorganisationer IT, inklusive Internet, för att kommunicera och skaffa pengar. Internet används också för att sprida propaganda och rekrytera folk.

34. För hela definitionen, se Proposition "Ett informationssamhälle för alla", proposition 1999/2000:86. Definitionen finns tillgänglig på http://www.fhs.mil.se/templates/Page____2186.aspx

Enskilda aktörer, hackare

Det är svårt att avgöra hur många enskilda individer som har förmåga att utveckla skadlig kod eller genomföra attacker som hotar samhällsviktig infrastruktur. Dels är de exploits[35] och verktyg som finns tillgängliga över Internet så pass avancerade att också okvalificerade, enskilda individer kan åstadkomma stor skada eller vara framgångsrika i attacker. Dels är många myndigheters säkerhet så bristfällig att det inte krävs särskilt kvalificerade angrepp för att ta sig in i en myndighets nätverk. . Flera datavirus som under senare år drabbat stora delar av världen på bred front har utvecklats av enskilda tonåringar.

Även om enskilda skickliga hackare saknar avsikten att orsaka skada eller begå brott kan denna kompetens, om den säljs eller på annat sätt kommer i orätta händer, utnyttjas i sådana syften. Diskussioner i chattrum visar att hackare och kodare blivit allt mer sofistikerade och målinriktade och att de delger varandra information. Detta indikerar att det finns möjlighet att tjäna pengar genom att till exempel sälja nya skadlig kod såsom trojaner eller genom att hyra ut botnets.

Målgrupper för riktade attacker

En attack mot en slutanvändares dator har, för angriparen, fördelen att den ofta är dåligt patchad och att skyddsmekanismer som brandväggar och virusskydd är dåligt uppdaterade. Karaktären av och syftet med den skadliga kod som installeras eller den sårbarhet som utnyttjas skiftar.

- Slutanvändarens dator eller slutanvändaren själv kan i sig utgöra slutmålet. Syftet kan vara att förstöra datorn med datavirus, att genomföra en phishingattack eller att nå mottagaren med spam.
- Slutanvändarens dator kan utgöra ett delmål för att ta sig vidare in i till exempel ett företags nätverk. På detta sätt behöver angriparen eller den skadliga koden inte passera ett företags relativt sett höga säkerhetsarrangemang.[36]
- Huvudmålet kan vara att kunna fjärrstyra och utnyttja slutanvändarens dator mer allmänt, till exempel som ingående i botnets.

Svenska företag som bedriver forskning och utveckling inom teknik, medicin och andra områden där man har spetskompetens, tilldrar sig stort intresse från både utländska stater och andra företag. Angrepp från kvalificerade och resursstarka aktörer är svåra att upptäcka vilket inte innebär att de inte förekommer. Chanserna för upptäckt försämras dessutom ytterligare om det utsatta företaget är litet och saknar resurser att bedriva eget informationssäkerhetsarbete. Dessa angrepp sker in-

35. Program som utnyttjar specifika sårbarheter.
36. Symantec Internet Security Threat Report, Trends for January 1, 2004 - June 30, 2004.

te bara genom traditionella dataintrång utan även genom utnyttjande av insiders eller en kombination av de båda.

Svensk försvarsindustri tilldrar sig fortsatt stort intresse men det gör också verksamheter som inte faller inom kategorinkategorin rikets säkerhet.

Det finns ett fortsatt stort intresse för information som kan tjäna ett utländskt politiskt eller ekonomiskt syfte. Målet är inte bara att lära känna Sveriges potentiella agerande och ställningstagande i olika frågor utan också att via olika kanaler kunna påverka det genom fredstida informationsoperationer. Sammantaget anses underrättelsetrycket mot Sverige idag vara på en nivå motsvarande det kalla krigets men med delvis annorlunda fokus.

Sårbarheter

Tekniska sårbarheter

SCADA[37] och samhällsviktiga system

Styr och kontrollsystem, så kallade SCADA-system (Supervisory Control And Data Acquisition System) är system som stödjer produktion eller distribution av samhällsviktiga tjänster eller produkter såsom till exempel el eller dricksvatten. SCADA-system är centrala för funktionaliteten i samhällsviktig infrastruktur.

Systemen har ofta utgjort separata nätverk vilket är en orsak till att säkerheten generellt sett är dålig i dem. Säkerheten i SCADA-systemen har inte behövt beakta till exempel skadlig kod och riktade angrepp av den karaktär som förekommer kopplat till Internet. I takt med att SCADA-system i allt högre utsträckning kopplas samman med företags övriga system och Internet ökar riskerna inom infrastrukturer som kontrolleras med SCADA-system.

Idag är säkerheten och de potentiella konsekvenser som ett eventuellt angrepp skulle kunna få bristfälligt kartlagda. Av olika skäl kopplas SCADA-systemen i allt högre omfattning samman med och anpassas till verksamheters övriga system. I och med detta exponeras de också för de hot som finns i och mot andra företagsnät som i princip alltid har kopplingar till Internet på något sätt. SCADA-systemen är komplexa och deras beroendeförhållanden är svåra att överblicka, säkerheten är dålig och systemen har ofta en funktion som är tidskritisk och processer som inte är dimensionerade för brandväggar och virusskydd. Allt detta medför att SCADA-system exponeras för hot och risker som tidigare inte behövde beaktas. De potentiella konsekvenserna av SCADA-system vars funktionalitet försämras eller slås ut kan bli mycket allvarliga, inte bara för den enskilda verksamhet som drabbas utan för stora delar av samhället.

Ett exempel utgörs av masken *Slammer* som den 25 januari 2003 slog ut

37. Christiansson, Henrik. (2004) Värdering av IT-säkerhetsanalysmetoder inom samhällsviktig infrastruktur. Totalförsvarets Forskningsinstitut. FOI-R—1350--SE

ett viktigt övervakningssystem i kärnkraftverket Davis-Besse i Ohio USA. Orsaken till incidenten var att en dator, utan virusskydd, kopplades in i kärnkraftverkets datornät. Kärnkraftverket var vid tillfället avställt och även om exemplet inte är direkt överförbart till svenska förhållanden så indikerar incidenten tydligt den potentiella konsekvensen av att SCADA-system helt eller delvis sätts ur funktion.

Masken Sasser drabbade i maj 2004 bland annat den svenska försäkringskassan till följd av bristande patch-hanteringning. Försäkringskassans förmåga att genomföra normal verksamhet drabbades allvarligt. Effekterna på samhället i övrigt blev begränsade då de utbetalningar som försäkringskassan ansvarar för hade gjorts några dagar tidigare.

Då Sasser drabbat Sverige genomförde KBM en begränsad kartläggning och bedömning av konsekvenserna i samhället. KBM konstaterar att de direkta konsekvenserna för organisationer blev dels att datorer slogs ut till följd av ständiga omstarter, dels att prestandan i nätverken sjönk påtagligt under olika lång tid. De indirekta följderna var främst att den normala arbetsgången störtes. Erfarenheterna visar vidare tydligt vårdsektorns stora beroende av ett fungerande IT-stöd. Erfarenheter från de organisationer som klarade sig bra visar att det finns behov av en väl fungerande organisation som hanterar IT-säkerhetsfrågor och att en kombination av förebyggande (patch-hantering) och skadebegränsande (incidenthantering) åtgärder gav det bästa resultatet.[38]

Dessa system kan inte kategoriseras som SCADA men pekar på de potentiella konsekvenserna av skadlig kod som drabbar samhällsviktiga system eller funktioner.

Trådlösa nät, okända nät

Trådlösa nätverk har under senare år blivit allt mer populära. Tydliga fördelar är att användarens rörlighet ökar till följd av att behovet av sladdar och kablar minskar, vilket också är kostnadsbesparande.

Säkerhetsinställningar som tillhandahålls vid köp ger endast ett begränsat skydd och de ger inget skydd alls om de inte används, något som ofta är fallet. Konsekvensen blir att vem som helst på ett enkelt sätt kan koppla upp sig på ett sådant nätverk och utnyttja det för att till exempel skicka spam, genomföra DDoS-attacker eller installera eller sprida olika typer av skadlig kod. Rikskriminalens IT-brottsrotels samordningsfunktion, S-BIT, uppger att ett vanligt förekommande brott i dessa sammanhang är bedrägerier och att de är mycket svåra att utreda eftersom brottet bara kan spåras tillbaka det trådlösa nätverkets legitima accesspunkt.

Myndigheter, företag och andra organisationer är ofta inte medvetna om

38. Kartläggning och bedömning av konsekvenser av Sasser-masken i samhället, KBM, 2004-06-23 (dnr 0562/2004). Tillgänglig på http://www.krisberedskapsmyndigheten.se/EPiBrowser/Publikationer/Övriga%20publikationer/KBM/slutrapport_sasser_2004.pdf

att det kan finnas okända eller kända men okrypterade accesspunkter inkopplade på deras nätverk. Sådana kan tillkomma till exempel när teknikkunnig personal för att underlätta för sig själva kopplar sin bärbara dator till nätverket för att kunna installera diverse program.

IP-telefoni

Det finns flera varianter av IP-telefoni beroende på hur terminalerna i respektive ände ser ur och över vilket nät informationen skickas. Någon gång går telefonin över ett paketförmedlat nät, till exempel Internet. Terminalerna kan vara vanliga telefoner eller ett mjukvaruprogram i en dator. Överföringen kan också göras över ett privat intranät eller ett Wide Area Network (WAN).

Ett problem med IP-telefoni är att de brandväggar som används är konstruerade för trafik som initieras från det privata nätet, inte för trafik som initierats utifrån. Vissa företag som använder sig av IP-telefoni löser problemet genom att låta trafiken gå genom telefonledningarna istället för att öppna brandväggen vilket gör att funktionen med IP-telefoni delvis går förlorad. Det finns också nyare brandväggar som kan öppna portar dynamiskt för behörig inkommande trafik.

Om IP-telefoni förmedlas över autonoma nätverk och om trafiken krypteras kan det ur avlyssningssynpunkt vara säkrare än vanlig telefoni. Risken för att servrarna kan angripas måste dock beaktas. Det är inte svårare att identifiera och utnyttja svagheter i olika programvara för IP-telefoni än för andra program. Detta gör att avlyssningsrisken, generellt sett, är avsevärt större för IP-telefoni än för vanlig telefoni.

Att ha såväl telefoni som vanlig datortrafik på samma nätverk, som är fallet med IP-telefoni, innebär ur redundanssynpunkt en risk. Ett strömbortfall påverkar inte vanlig telefoni och fax på kort sikt eftersom såväl lokalstationerna som stomnätet är försedda med reservkraft. Motsvarande reservkraftsutbyggnad för de nät som förmedlar IP-trafik finns inte. Detta innebär att ett strömbortfall resulterar i att IP-trafiken upphör att fungera, oavsett om den förmedlar webbtrafik, telefoni eller något annat.[39]

Mobilitet

Mobilitet medför en möjlighet att föra med sig mycket information, att kommunicera trådlöst mellan olika enheter eller överföra information mellan olika tekniska plattformar genom till exempel mobiltelefoner och trådlösa nätverk. Detta innebär även en säkerhetsrisk i enlighet med det som beskrivits ovan. Dessutom kan till exempel bärbara datorer, personal digital assistants (PDA:er) och mobiltelefoner innehålla mycket stora mängder känslig information och bärbara tekniska plattformar kan lätt försvinna. Det kan vara svårt eller omöjligt att avgöra om en förlust

39. IP-telefoni ur ett sårbarhetsperspektiv, Totalförsvarets Forskningsinstitut, FOI- Memo 1035, Oktober 2004.

av en mobil enhet beror på slarv, att någon vill åt hårdvara, mjukvara eller information eller den access mobila enheter med möjlighet till fjärrinloggning erbjuder.

Organisatoriska sårbarheter

Försvarets radioanstalt (FRA) genomför så kallade penetrationstester på uppdrag av myndigheter eller statligt ägda företag som hanterar information som bedöms vara känslig för samhällets sårbarhet eller ur ett försvars- eller säkerhetspolitiskt perspektiv. Erfarenheter från detta arbete visar att många myndigheter har en dålig informationssäkerhet.

Avsaknad av existerande nätverkskartor utgör en vanligt förekommande brist på myndigheter och företag. Om de finns har de ofta gjorts inför någonting, i ett specifikt syfte, varefter de ställts undan och sällan är uppdaterade. Detta gör att nyttan med dem till stor del går förlorad, inte minst i ett akut läge.

Krav och förväntningar finns på myndigheter att vara tillgängliga 24 timmar om dygnet och att erbjuda olika typer av interaktiva tjänster. I strävan att leva upp till dessa krav beaktas ofta säkerheten på ett otillfredsställande sätt.

Många organisationer lägger till synes utan kritisk granskning ut information om sin personal, sina byggnaders konstruktion, kalendarier, rapporter med mera på sina hemsidor. Också resurssvaga aktörer kan härigenom få tillgång till information som kan utnyttjas på icke avsett sätt. Resursstarka konkurrenter eller nationalstater har naturligtvis helt andra förutsättningar att samla in och använda informationen. Information som är tillgänglig över Internet kan dessutom kombineras med information som är tillgänglig med stöd av offentlighetsprincipen eller från andra öppna eller mer svåråtkomliga källor.

Ytterligare en risk utgörs av att myndigheter ofta erbjuder olika interaktiva gränssnitt som i sin tur ofta har en koppling till de interna näten och databaserna. Dessa kopplingar innebär också en potentiell väg in i myndigheternas interna nät.

I många företag och myndigheter upplever IT-säkerhetspersonal fortfarande att det är svårt att motivera att IT-säkerhetsfrågor behandlas på ledningsnivå och att managementnivån brister i kunskap och medvetande inom detta område.

Fysisk säkerhet och informationssäkerhet är till stor del fortfarande uppdelade i olika ansvarsområden. Trenden är emellertid att de långsamt närmar sig varandra vilket är viktigt för att få en helhetlig säkerhet. Det är vidare viktigt att policydokument dels utvecklas, dels implementeras. Många gånger finns policydokument framtagna men de är sällan kända och implementerade i organisationen.

Outsourcing

Outsourcing av sådant som inte utgör kärnverksamheten ökar inom såväl myndigheter som företag. Idag lägger cirka hälften av Sveriges organisationer ut driften av stödverksamheter, till exempel löneadministration, bokföring

och inköp, på externa företag. Inom det amerikanska näringslivet förväntas outsourcingen öka med sju procent årligen.

Ur ett samhälleligt säkerhetsperspektiv utgör outsourcing en risk. Om en samhällsviktig myndighet eller företag outsourcar verksamhet förlorar de kontrollen över åtminstone en del av sin verksamhet. Om fler företag eller myndigheter outsourcar verksamhet till samma ställe finns en risk att viktiga delar hos olika myndigheter eller företag, till och med konkurrerande företag, samlas på en plats och i ett företag. Detta medför en oönskad och icke avsedd koncentration av viss verksamhet. Många gånger görs inte heller någon extern revidering eller granskning av säkerheten i det företag till vilken verksamhet outsourcats.

I sammanhanget skall påpekas att outsourcing, för företag som inte har egen kompetens inom IT eller IT-säkerhet, naturligtvis kan innebära en förbättring av säkerheten.

Avsaknad av eller brister i befintliga säkerhetssystem

Insiders

Insiders är individer som har möjlighet att från insidan utnyttja sin position till att utföra eller planera otillåtna handlingar. Problemet med insiders bedöms av svenska informationssäkerhetsexperter som stort. En orsak till detta är att insidern har legitima skäl att befinna sig i företaget och därigenom har möjlighet att sopa igen spår och dölja sin verksamhet. Trots att insiderproblemet är stort är det ofta svårt att få gehör för det i den egna organisationen.

Outsourcing, liksom olika typer av business-to-business-lösningar och utnyttjande av konsulter innebär ett slags överförd och utökad insiderrisk som också den måste beaktas. Extern servicepersonal eller konsulter kan röra sig i företagets egna lokaler och ha tillgång till det som finns där. Teknik med kopplingar till företagets egna nät finns på annan plats och kontrolleras av ett annat företags personal.

Tekniska

Brandväggar övervakar och begränsar datatrafik till eller från ett nät i enlighet med i förväg gjorda inställningar. Brandväggar förhindrar inte att tidigare okända sårbarheter utnyttjas.

Enligt Australiens Computer Crime and Security Survey för 2004 använder 100% av den undersökta företagen i offentlig och privat sektor virusskydd. Detta till trots uppger 88% av de tillfrågade att de drabbats av datavirus, datamaskar och trojaner.[40] Orsaken till att så många drabbas trots att de har skydd har delvis sin grund i att skydd inte hinner utvecklas och distribueras. En annan bidragande orsak är att användarna inte uppdaterar virusskydden tillräckligt ofta, att systemen är dåligt

40. Rapporten finns tillgänglig på http://www.auscert.org.au/render.html?it=2001

konfigurerade eller att användarnas egna agerande möjliggör infektion. Vissa delar i företag skyddas många gånger, till exempel Internetanslutningarna men inte slutanvändarnas datorer, de enskilda klienter. Skadlig kod som specialanpassas för ett visst ändamål är dessutom mycket svår att upptäcka.

Snittiden från upptäckten av en sårbarhet i en programvara till dess att sårbarheten utnyttjas för en attack är kort och har under senare år minskat drastiskt. Företaget Symantec uppskattar idag siffran till 5,8 dagar.[41] Företag och slutanvändare är generellt sett dåliga på att patcha sina datorer eller system. Då patch-hantering sker är det många gånger med allt för stora intervaller. Jämfört med patch-hanteringning av system är företag relativt duktiga på att använda sig av brandväggar och antivirusprogram. Att inte uppdatera virusskydd och system genom patch-hantering innebär att myndigheter och företag inte utnyttjar det skydd som finns tillgängligt och som de dessutom betalar för.

Många gånger är system konfigurerade med grundinställningar. Detta utgör ett stort problem eftersom det underlättar för en angripare eller skadlig kod att utnyttja systemet. Många gånger beror detta helt enkelt på att IT-personalen inte hinner göra lämpliga justeringar.

Sammanfattande slutsatser

Hot

Utvecklingen av skadlig kod och dess användning indikerar en specialisering och professionalisering av den IT-relaterade brottsligheten. Phishing är en form av bedrägeri som utgör ett exempel på att ekonomisk vinning är en stark drivkraft i detta sammanhang. Detsamma gäller de fjärrstyrda nätverk av datorer som kallas botnets. Dessa kan emellertid användas också i andra syften, allt från att skicka spam till att utföra överbelastningsattacker (DDoS). Den gränsöverskridande förekomsten av botnets och den kraft ett samlat angrepp från botnets kan innebära utgör ett allvarligt hot mot samhället.

Skadlig kod sprids i allt högre utsträckning via webbtrafik men fortfarande i första hand via e-post. Många gånger bidrar slutanvändaren själv aktivt till att råka illa ut genom att svara på e-post, klicka på pop-ups eller besöka okända hemsidor.

Målet för attacker är i allt högre omfattning slutanvändares datorer, oavsett om dessa finns i hemmet, på företag eller myndigheter. Slutanvändares datorer är ofta dåligt skyddade och utgör därför ett lättare mål än en organisations relativt väl skyddade accesspunkter. Slutanvändaren kan utgöra attackens slutgiltiga mål eller ett delmål för att angriparen antingen ska kunna ta sig vidare in

41. Symantec Internet Security Threat Report, Trends for January 1, 2004 - June 30, 2004.

i till exempel ett företag, eller för att ta över datorn för att sedan kunna fjärrstyra den i ett botnet.

Spam, alltså obeställd och oönskad e-post, bedöms utgöra cirka 60 procent av all e-post på Internet och utgör ett enormt problem som påverkar hela Internets funktionalitet på ett ogynnsamt sätt. Att skicka spam står i strid med marknadsföringslagen och hanteras av konsumentverket, inte polisen.

Det är svårt att avgöra vem som ligger bakom en attack och vilket det egentliga syftet är. Spam, datavirus och andra typer av skadlig kod är många gånger inte heller riktade mot en viss målgrupp utan sprids på bred front och får fotfäste där säkerheten är som sämst. Alla som har en Internetuppkoppling utgör ett potentiellt mål. För att skapa en god grundsäkerhetsnivå är det inte nödvändigt att känna till vilket syftet är eller vem den bakomliggande aktören är. Säkerhet åstadkoms dels genom ett säkert agerande, dels med hjälp av tekniska lösningar.

I detta dokument presenteras aktörsbundna hot och medel som dagligen och till stor skada realiseras över Internet. Detta indikerar vilken skada en målinriktad och resursstark aktör med förmåga till koordinering och ledning, såsom en stat, skulle kunna åsamka det svenska samhället. Detsamma gäller för terroristorganisationer eller andra aktörer. Även om de idag saknar förmågan kan detta snabbt förändras, till exempel genom att olika aktörer går samman till ömsesidig nytta för dem själva och till skada för samhället.

Företag och myndigheter som arbetar med spetsteknologi, medicinsk utveckling, försvarsindustri eller finansiell verksamhet löper större risk att utsättas för angrepp från kvalificerade aktörer. Dessa företag och myndigheter bör ägna sin säkerhet extra stor uppmärksamhet.

Säkerhetspolisens förebyggande och granskande verksamhet är inriktad mot sådant som avser rikets säkerhet eller skydd mot terrorism inom den offentliga sektorn. Den offentliga verksamhetens hantering av hemliga uppgifter regleras i Säkerhetsskyddslagen (SFS 1996:627) och Säkerhetsskyddsförordningen (SFS 1996:633). Den vanliga polisen hanterar övrig brottslig verksamhet som kommer till deras kännedom.

Det finns ingen statlig instans som ansvarar för att hantera informationsinsamling eller operationer om de inte är olagliga eller faller inom Säkerhetspolisens ansvarsområde. Sådan verksamhet kan även om den inte bedrivs med olagliga medel snedvrida konkurrensförhållanden. Omfattningen av denna typ av verksamhet är svår att uppskatta men det finns ingen anledning att anta att denna verksamhet inte förekommer i Sverige och det finns all anledning för företag och myndigheter att vara uppmärksamma på detta.

Sårbarheter

Trenden att utnyttja datateknik och standarder för tjänster som tidigare utgjorde separata tekniska lösningar innebär att också sådana tjänster riskerar att fallera i samband med att datornätverken gör det. Exempel på sådant är IP-

telefoni, trådlösa telefoner samt brand- och inbrottslarm.

Styr och kontrollsystem, så kallade SCADA-system, och deras sårbarheter och konsekvenser för samhället får allt större uppmärksamhet. För företag som producerar eller distribuerar samhällsviktiga tjänster eller produkter är det viktigt att kartlägga sina SCADA-system samt vidta skyddsåtgärder.

Risken för avlyssning av trådlösa nät kan till viss del reduceras men inte helt tas bort. Åtgärder som förbättrar skyddet kan vara att kryptera hårddisken och att ändra den funktion som har till uppgift att skilja olika trådlösa nätverk från varandra, det så kallade ESSID. Det sistnämnda utgör ett svagt skydd men är bättre än inget alls. Det främsta skyddet är dock att helt undvika trådlösa accesspunkter på nät som innehåller känslig information, vare sig det handlar om företag eller myndigheter.

24-timmarsmyndigheten ställer allt högre tillgänglighetskrav på myndigheter. Hur denna tillgänglighet utformas måste ställas i relation till de sårbarheter som exponeras. Det är inte tillräckligt att beakta risken med att göra viss information tillgänglig utan att då även beakta annan tillgänglig information.

Genom outsourcing förlorar företaget eller myndigheten såväl delar av säkerhetsarrangemangen som möjligheten till kontroll. För att kompensera detta ställs stora krav på beställarkompetensen och att avtalet noggrant beaktar säkerheten, såväl när det gäller uppsåtliga angrepp som drift.

Rekommendationer

Antivirusprogram och brandväggar liksom spamfilter är säkerhetsverktyg vars användning rekommenderas. De utgör inte kompletta säkerhetslösningar i sig och om de inte kontinuerligt och med täta intervaller uppdateras ger de ett än mer begränsat skydd och fyller inte sitt syfte. Det är vidare nödvändigt att kontinuerligt och med täta intervaller patcha system för att täppa till sårbarheter. Ytterligare ett sätt att tekniskt förbättra säkerheten är att ändra systemens grundkonfigureringar och att begränsa det som är tillåtet att göra så mycket som möjligt utan att det menligt inverkar på företagets verksamhet. Att grundkonfigurering används gör att system är sårbarare än de behöver vara.

Tekniska lösningar bör kombineras med traditionellt säkerhetsarbete. Detta är till exempel säkerhetssamtal med personalen, säkerhetskontroller av personal när det är möjligt, säkerhetsrevisioner och granskningar, skalskydd, klassning av information, policyarbete samt implementering av en säkerhetspolicy.

Klassiska råd som att välja lösenord som är svåra att knäcka och att inte skriva ner dem eller åtminstone förvara dem säkert samt att surfa säkert äger fortfarande relevans. Andra enkla råd är att inte lämna ut konfidentiell information till okända, oavsett om det sker över Internet eller genom direkta samtal. I sin enklaste form kan företag höja säkerhetsmedvetandet genom att nyanställda i samband med introduktionen ges en genomgång av företagets säker-

hetspolicy samt vilka hot företaget kan tänkas vara utsatta för.

Ett tänkbart sätt för företag och myndigheter att skydda sig mot attacker via anställda som har hemarbetsplatser eller kan koppla upp sig mot företagets nät är att erbjuda dem personliga brandväggar på samma sätt som företag subventionerar anställdas friskvård. Detta skulle bidra till att skydda företagets eller myndighetens egna system.

En grund för att skaffa ett tillräckligt skydd utgörs av risk- och sårbarhetsanalyser. Sådana analyser kan inte göras enbart avseende informationssäkerhet utan måste göras utifrån ett helhetsperspektiv som beaktar både fysisk säkerhet och IT-säkerhet. Utifrån en sådan risk- och sårbarhetsanalys bör en kontinuitetsplan utvecklas och implementeras. Utgångspunkten bör vara förmågan att utföra verksamhetens huvuduppgifter. Externa beroenden, skyldigheter och förväntningar måste beaktas och hanteras. Detta är inte minst viktigt avseende samhällsviktig infrastruktur och styr- och kontrollsystem (SCADA). Det som främst berörts på informationssäkerhetsområdet avser:

- Utnyttjande av IP för nya tjänster såsom telefoni eller SCADA
- Sammankoppling av SCADA med företagets övriga nät
- Införande av trådlösa nät och andra accesspunkter
- Införande av mobila terminaler
- Outsourcing
- Vilken information om företaget och dess anställda som ska göras tillgänglig över Internet.

Vid införande av ett nytt informationssystem eller vid en förändring i befintliga system eller nätverk, eller de verksamheter som informationssystemen stödjer, måste förnyade och anpassade risk- och sårbarhetsanalyser genomföras.

Avslutningsvis är det av avgörande vikt att den högsta ledningen är medveten om problematiken och ger sitt fulla stöd till de säkerhetsansvariga.

BILAGA 1

Ordlista för informationssäkerhet

I rapporten används följande begrepp enligt nedanstående definitioner.

Autentisering Att verifiera en uppgiven identitet eller ett meddelandes riktighet.

Botnet Nätverk av datorer som infekterats med skadlig kod som gör det möjligt för en tredje part att kontrollera och fjärrstyra datorerna samtidigt.

Certifikat En unik elektronisk signatur som används för identifiering. Mjuka certifikat finns i datorers mjukvara och är möjliga att stjäla elektroniskt, till exempel genom dataintrång. Hårda certifikat finns till exempel på så kallade smarta kort och kan inte stjälas elektroniskt.

DDos-attacker (Distributed Denial of Service) En DoS (Denial of Service) attack innebär att ett nätverk slås ut genom att mättas med ändlös och ovidkommande datatrafik. DDoS innebär att denna trafik skickas från ett stort antal datorer.

Exploit Program som utnyttjar specifika sårbarheter.

Hacker Idag används begreppet vanligtvis för att beskriva någon som olovligen på elektronisk väg, genom att hacka, tar sig in i en dator eller ett nätverk. Benämns också cracker. Ursprungligen användes begreppet hacker för att beteckna en datorentusiast i största allmänhet.

Informationsoperationer (IO) Enligt Prop 1999/2000:86: Informationsoperationer är samlade och samordnade åtgärder i fred, kris och krig till stöd för politiska eller militära mål genom att påverka eller utnyttja motståndares eller annan utländsk aktörs information och informationssystem. Det kan ske genom att utnyttja egen information och egna informationssystem samtidigt som dessa också måste skyddas. Ett viktigt inslag är att påverka beslutsprocesser och beslutsfattande.

Det finns både offensiva och defensiva informationsoperationer. De genomförs i politiska, ekonomiska och militära sammanhang. Exempel på informa-

tionsoperationer är t.ex. informationskrigföring, massmediemanipulation, psykologisk krigföring och underrättelseverksamhet.

Defensiva informationsoperationer är samordnade och samlade åtgärder i fred, kris och krig avseende policy, operationer, personal och teknik för att skydda och försvara information, informationssystem och förmåga till rationellt beslutsfattande.

IP Internet Protocol. Standard för hur datatrafik skickas mellan datorer.

Klient En dator där slutanvändaren har tillgång till ett nätverk och kör olika typer av program såsom Word, Excel eller Internet Explorer.

Konfigurering De systeminställningar som används på en dator eller i ett nätverk. System levereras med vissa grundinställningar.

Makrodatavirus Ett datavirus som sprids med ett vanligt dokument, till skillnad från ett vanligt datavirus som färdas med hjälp av programfiler.

Mask Program som sprider sig själv från dator till dator.

Patch-hantering Att täppa till upptäckta sårbarheter i befintlig programvara som redan används. Detta sker vanligtvis genom att programvaruleverantören distribuerar då kallade patchar.

P2P (peer to peer) Nätverksarkitektur som gör att användarna kan dela filer över nätet. Filerna kan innehålla t.ex. musik, bilder eller datorprogram. Arkitekturen skiljer sig från den så kallade klient – server arkitekturen.

Phishing Phishing är en metod att lura mottagaren att lämna ifrån sig konfidentiell finansiell information genom att antingen svara på ett falskt e-postmeddelande eller genom att besöka en falsk webbsida och där lämna ifrån sig samma information.

Server En dator eller enhet som styr eller hanterar resurser på ett nätverk.

Klient En personlig dator där slutanvändaren kör olika typer av program såsom Word, Excel eller Internet Explorer.

SCADA-system Styr och kontrollsystem, så kallade SCADA-system (Supervisory Control And Data Acquisition System) är system som stödjer produktion eller distribution av samhällsviktiga tjänster eller produkter såsom till exempel el eller dricksvatten. SCADA-system är centrala för funktionaliteten i samhällsviktig infrastruktur.

Skadlig kod Skadlig kod används i denna rapport som ett samlingsbegrepp för ett program som orsakar avsiktlig direkt eller indirekt störning eller skada eller gör något annat i strid med den drabbades vilja. Är till exempel datavirus, datamaskar eller trojaner.

SMS Short Message Service. Tjänst för att skicka korta textmeddelanden mellan mobiltelefoner.

Spam Massutskick av oönskad, obeställd e-post utan mottagarens samtycke. Företrädesvis reklam.

Spionprogram Program som installeras användarens dator och där samlar och rapporterar information i olika syften och rapporterar det till någon annan. Allt sker i smyg och utan användarens vetskap.

Token En teknisk enhet som kontinuerligt skapar nya lösenord som kan användas för att logga in på till exempel det egna kontot i en bank

Trojan Program som förutom att göra det som uppges också utför oönskade operationer.

Datavirus Program som i smyg installeras på en dator och därefter utför någon oönskad funktion på datorn. Kan kopiera sig själva tills all kapacitet i datorn åtgår till detta. Kan också sprida sig vidare till andra datorer.

Wide Area Network (WAN)
Ett datornätverk som omfattar stora geografiska områden. Det främsta exemplet är Internet.

BILAGA 2

Praktiska tips för informationssäkerhet

Samlad svensk statistik för IT-relaterade brott och incidenter saknas, och mörkertalet bedöms vara mycket stort. För att kunna skapa en tydligare bild av problemet och kunna fördela samhällets resurser på ett så bra sätt som möjligt är det därför viktigt att brott och incidenter anmäls.

IT-relaterad brottslighet anmäls lämpligen genom Rikskriminalpolisens IT-brottsrotels samordningsfunktion, S-BIT. Mer information om IT-brottsroteln finns på http://www.polisen.se/inter/nodeid=30903&pageversion=1.html På hemsidan finns också information om olika typer av IT-relaterad brottslighet. Undvik att röra den dator som utsatts för brott innan samråd skett med polisen. Mer information om åtgärder i samband med brottsanmälan finns på http://www.polisen.se/inter/nodeid=30907&pageversion=1.html Övriga *IT-relaterade incidenter* anmäls till Sveriges IT-incidentcentrum, SITIC, som tillhör Post och Telestyrelsen (PTS). Mer information om detta finns på http://www.sitic.se. På hemsidan får du även tillgång till aktuella hotbilder och råd om åtgärder i det förebyggande arbetet mot IT-incidenter.

På PTS hemsida http://www.pts.se/internetsakerhet/Sidor/startsida.asp finns vidare:

- *Råd och tips för hemanvändaren* som använder Internet.
- Grundläggande information samt *råd och tips om hur arbetsplatsens anslutning till och användning av Internet görs säker.* Målgruppen är småföretagare eller ansvarig för Internetsäkerheten på arbetsplatsen.

Spam anmäls till Konsumentverket på http://www.epostreklam.konsumentverket.se. På hemsidan finns också information och råd om bland annat modemkapningar, e-handel och e-post.

KBM tillhandahåller Basnivå för IT-säkerhet (BITS). BITS är en rekommendation i vilken KBM *definierar den lägsta säkerhetsnivå som organisationernas IT-system måste uppnå.* Denna säkerhetsnivå kallas basnivå. Rekommendationerna gäller alla IT-system som samhället behöver för att kunna upprätthålla en organisations normala

verksamhet. BITS kan laddas ned från http://www.krisberedskapsmyndigheten.se/templates/EntryPage____677.aspx

KBM:s IT-säkerhetsguide är ett hjälpmedel för att kunna *kontrollera om IT-systemen i en verksamhet uppfyller ställda säkerhetskrav*. Guiden innehåller vidare stöd för att styrande dokument enligt BITS skall kunna skapas. KBM:s IT-säkerhetsguide kan hämtas på http://www.krisberedskapsmyndigheten.se/templates/DocumentList____3464.aspx.

Under första kvartalet 2005 kommer Försvarets Radioanstalts (FRA) enhet för Teknisk Informationssäkerhet att publicera så kallade *systemsäkringslistor* som kontinuerligt kommer att uppdateras. Med hjälp av dessa checklistor kan operativsystem installeras och konfigureras till en rimlig säkerhetsnivå med bibehållen användbarheten. De föreslagna konfigurationsändringarna är testade och verifierade av FRA. Syftet är att öka operativsystems motståndskraft mot intrångsförsök och skadlig kod. De första listor som publiceras avser Microsoft och Unix.

Listorna kommer gratis att finnas tillgängliga för myndigheter och statligt ägda företag. Formerna för distribution är ännu inte beslutad. Ytterligare information kan fås via FRA:s enhet för Teknisk Informationssäkerhets hemsida: http://www.fra.se/omfra_infosakerhet.shtml

BILAGA 3

Omvärldsanalys på Krisberedskapsmyndigheten

Enligt förordning (2002:518) med instruktion för Krisberedskapsmyndigheten (KBM) har myndigheten till uppgift att bedriva omvärldsbevakning och genomföra omvärldsanalyser på områden som berör samhällets säkerhet när det gäller krishantering och civilt försvar.

Inom området samhällets informationssäkerhet ska Krisberedskapsmyndigheten ha ett sammanhållande myndighetsansvar genom att sammanställa en helhetsbild av informationssäkerheten. Myndigheten skall i detta arbete analysera omvärldsutvecklingen inom området mot bakgrund av erhållet underrättelseunderlag och årligen lämna en samlad bedömning till regeringen,

Det övergripande målet med KBM:s omvärldsbevakning och omvärldsanalys är att identifiera och förstå förhållanden, händelser och trender som påverkar utvecklingen av svensk krisberedskap.

KBM:s omvärldsbevakning och omvärldsanalys ska bidra till att minska sårbarheten i det svenska samhället och förbättra förmågan att förebygga och hantera kriser. Verksamheten inriktas mot sådana hot, risker och sårbarheter som kan äventyra den nationella säkerheten och ge upphov till allvarliga kriser i fred och krigssituationer.

Myndighetens omvärldsbevakning- och analysarbete har till uppgift att skapa en helhetssyn på samhällets krisberedskap och en ökad förståelse för dess villkor och förutsättningar på både lång och kort sikt. Det finns ett viktigt samband mellan långsiktig kunskap inom områden av central betydelse för krishanteringssystemet och möjligheten att utföra goda analyser av skeenden på kort sikt.

Resultatet av analysarbetet utgör även en viktig grund för formuleringen av målbilder inom krisberedskapen. KBM:s omvärldsanalys ska kunna fungera som underlag för beslut om inriktning och planering samt kunna bidra till utvecklingen av den operativa verksamheten på alla nivåer där det krävs krishanteringsförmåga.

BILAGA 4

Information till rapporten har inhämtats från följande aktörer

Banverket, www.banverket.se
Europol, www.europol.eu.int
Förenta Nationerna, www.un.org
Försvarsmakten, www.mil.se
Försvarets materielverk, www.fmv.se
Försvarets radioanstalt, www.fra.se
Försvarets radioanstalts enhet för teknisk informationssäkerhet, www.fra.se
Försvarshögskolan, www.fhs.mil.se
Interpol, www.interpol.int
Kustbevakningen, www.kustbevakningen.se
Konsumentverket, www.konsumentverket.se
Lantmäteriet, www.lantmateriet.se
Livsmedelsverket, www.slv.se
Luftfartsverket, www.lfv.se
Messagelabs, www.messagelabs.com
Portal för samhällsinformation, www.sverige.se
Post och Telestyrelsen, www.pts.se
Rikskriminalpolisen, www.polisen.se
Rikskriminalpolisens IT-brottsrotels samordningsfunktion, S-BIT www.polisen.se
Statens räddningsverk, www.srv.se
Utrikesdepartementet, www.ud.se
SMHI, www.smhi.se
Smittskyddsinstitutet, www.smittskyddsinstitutet.se
Socialstyrelsen, www.sos.se
Sveriges IT-incidentcentrum, www.sitic.se
Symantec, www.symantec.se
Statens strålskyddsinstitut, www.ssi.se
Styrelsen för psykologiskt förvar, www.psycdef.se
Svenska kraftnät, www.svk.se
Säkerhetspolisen, www.sakerhetspolisen.se
Totalförsvarets forskningsinstitut, www.foi.se
Tullverket, www.tullverket.se

BILAGA 5

Urval av förslag till fördjupad läsning

Icke-aktörsbundna hot

Comprehensive Risk Analysis and Management Network (CRN) http://www.isn.ethz.ch/crn/index.cfm

Critical infrastructure protection in the Netherlands http://www.minbzk.nl/contents/pages/8486/critical_infrastructure_protection.pdf

Dammsäkerhet, CEA Technologies Inc (CEATI), http://www.ceatech.ca

Finansinspektionen, (2004) *Från elavbrott till 11 september*, Trosa tryckeri AB. ISBN 91-631-55265. www.fi.se Angående erfarenheter från kriser i den finansiella sektorn.

Energimyndigheten http://www.stem.se

International Atomic Energy Agency http://www.iaea.org/OurWork/SS/index.html

Nationellt Centrum för Krishanteringsstudier, Crismart http://www.crismart.org/index.htm

Public Safety and Emergency Preparedness Canada http://www.psepc-sppcc.gc.ca

Strategic trends, Joint Doctrine and concept centre (JDCC), UK ministry of defence http://www.jdcc-strategictrends.org/

The World Meteorological Organization (WMO http://www.wmo.ch

The Worldwatch Institute http://www.worldwatch.org

UNICEF http://www.unicef.org

World Health Organization (WHO) http://www.who.int

Aktörsbundna hot

Uppsala Universitet www.silkroadstudies.org

Information om terrorism och relaterade ämnen http://www.tacia.org/documents/Links/TLR011.html#TerrorismLinks

Riskkollegiet http:///www.riskkollegiet.nu

The National Memorial Institute for the Prevention of Terrorism (MIPT) http:///www.tkb.org

The Terrorism Research Center, Inc. (TRC) http://www.terrorism.com

Centre for the Study of Terrorism and Political Violence University of St Andrews http://www.st-andrews.ac.uk/intrel/research/cstpv/

Mobilisering mot narkotika, rapporten ”Organiserad kriminalitet, grov narkotikabrottslighet” http://www.mobilisera.nu

Informationssäkerhet

Christiansson, Henrik (2004) *Värdering av IT-säkerhetsanalysmetoder inom samhällsviktig infrastruktur*, Stockholm, (FOI-R--1350--SE) Totalförsvarets Forskningsinstitut. www.foi.se Angående SCADA-system

Kartläggning och bedömning av konsekvenser av Sasser-masken i samhället, KBM, 2004-06-23 (dnr 0562/2004). Tillgänglig på http://www.krisberedskapsmyndigheten.se/EPiBrowser/Publikationer/Övriga%20publikationer/KBM/slutrapport_sasser_2004.pdf

IT-brottsroteln, http://www.polisen.se/inter/nodeid=30903&pageversion=1.html

Sveriges IT-incidentcentrum (SITIC), http://www.sitic.se

Post och Telestyrelsen (PTS), http:///www.pts.se/internetsakerhet/Sidor/startsidor.asp

Konsumentverket http://www.epostreklam.kunsumentverket.se

IT Sirnet är ett informellt nätverk som syftar till att diskutera betydelsen och nyttan av att hantera den ”mjuka” infrastrukturen”, dvs data-, informations- och kunskapsresurser samt tjänster. http://www.sirnet.info

Symantec Internet Security Threat Report. Trends for January 1, 2004 – June 30, 2004.

Barck-Holst, Svante m. fl. I*P-telefoni ur ett sårbarhetsperspektiv* (2004). Förslag till fortsatt inriktning. Totalförsvarets Forskningsinstitut. FOI Memo 1035. Tillgänglig på www.pts.se/Archive/Documents/SE/IP-telefoni_%20Forslag_till_fortsatt_inriktning.pdf

I slutet av januari 2005 kommer KBM att publicera resultatet av en pågående studie som undersöker vilken påverkan skadlig kod haft på samhällsviktig infrastruktur, vilka konsekvenser detta medfört samt hur samhällsviktig infrastruktur hade kunnat skyddas bättre. Publikationen kommer att finnas tillgänglig via KBM:s hemsida.

Bergström, Mats (2004). *Informationsoperationer mot näringslivet*, Stockholm, Försvarshögskolan ISBN: 91-89683-82-X

Nicander, Lars, Ranstorp, Magnus, (2004) *Terrorism in the Information Age – New Frontiers?*, Stockholm, Försvarshögskolan ISBN: 1-89683-52-8

KBM:S TEMASERIE

2004:6 Hot- och riskrapport 2004
Gränsöverskridande sårbarheter

2004:5 "We're a peaceful nation"
Krigsretorik efter 11 september

2004:4 Ministermordet
En studie om myndigheternas kommunikation vid attentatet mot Anna Lindh

2004:3 Säkerhet och beredskap i Europeiska unionen

2004:2 Stereotyper i vardagen
Bilder av "de främmande"

2004:1 Krisjournalistik eller journalistik i kris?
En forskningsöversikt om medier, risker och kriser

2003:6 Demokratin och mordet på Anna Lindh

2003:5 IT och sårbarhet
Kritiska beroendeförhållanden i den nationella IT-infrastrukturen

2003:4 Från osäker källa
Bevakningen av Irakkriget i svenska medier

2003:3 Krisberedskap i omvärlden
Samordningsstrukturer i fem länder

2003:2 Irakkrigets andra dag
En jämförelse mellan SVT och tidningspressen den 21 mars 2003

2003:1 Bagdad-Bob, menige Jessica Lynch och Cirkus Saddam
Irakkriget iscensatt i svenska medier

SPECIAL FEATURE

2004:5 "We're a peaceful nation"
War Rhetoric after September 11

ISSN 1652-2915
ISBN 91-85053-64-3

Krisberedskapsmyndigheten

Box 599
101 31 Stockholm

Tel 08-593 710 00
Fax 08-593 710 01

kbm@krisberedskaps
myndigheten.se

www.krisberedskaps
myndigheten.se