



Säkerhetspolisen

En vägledning till Säkerhetsanalys



Råd & Anvisningar
2005

Denna skrift är avsedd som en vägledning i arbetet att ta fram en säkerhetsanalys.

I verksamhet där säkerhetsskyddslagen (1996:627) gäller ska det säkerhetsskydd finnas som behövs med hänsyn till verksamhetens art, omfattning och övriga omständigheter. Säkerhetsskyddet ska utformas med beaktande av enskildas rätt att enligt tryckfrihetsförordningen ta del av allmänna handlingar.

Säkerhetsskydd

Säkerhetsskydd innefattar informationssäkerhet, tillträdesbegränsning och säkerhetsprövning. Informationssäkerhet förebygger att uppgifter som omfattas av sekretess och som rör rikets säkerhet inte röjs, förändras, förstörs eller görs otillgängliga för behöriga. Säkerhetsskyddet ska anpassas så att endast behöriga får tillgång till uppgifter eller verksamhet som har betydelse för rikets säkerhet.



Endast de personer som är pålitliga ur säkerhetssynpunkt får delta i verksamhet som rör rikets säkerhet. Säkerhetsskyddet ska även förebygga terrorism.

Säkerhetsanalys

För att uppnå ett bra säkerhetsskydd ska en säkerhetsanalys genomföras. I säkerhetsskyddsförordningen (1996:633) står det att: ”myndigheter och andra som förordningen gäller för ska undersöka vilka uppgifter i deras verksamhet som ska hållas hemliga med hänsyn till rikets säkerhet och vilka anläggningar som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller skyddet mot terrorism. Resultatet av denna undersökning (säkerhetsanalys) ska dokumenteras.”

En säkerhetsanalys är ett beslutsunderlag för ledningen i dess arbete med verksamhetens säkerhetsskydd. Revidering av säkerhetsanalysen ska göras regelbundet, rekommendation är årligen eller vid behov.

Tre steg

Arbetet med säkerhetsanalysen kan delas in i tre steg:

- inventera skyddsvärda resurser
- identifiera hot mot dessa
- analysera risker och sårbarheter

Resultatet av säkerhetsanalysen bör utmynna i en handlings- och åtgärdsplan för att åtgärda brister i skyddet av de skyddsvärda resurserna.

Steg 1: Inventera resurser

Detta innebär att man gör klart för sig vilka uppgifter och vilka anläggningar inom den egna verksamheten som faller inom ramen för säkerhetsskyddet. Styrdokument som uppdragsbeskrivning, säkerhetspolicy och IT-säkerhetspolicy, kan ge vägledning var skyddsvärd verksamhet finns.

Säkerhetsklassade befattningar

Befattningar som är inplacerade i säkerhetsklass ger en vägledning om var viktig verksamhet finns och vem eller vilka som hanterar dem. Uppgifterna bör stämmas av mot det verkliga behovet som framkommer som ett resultat av säkerhetsanalysen. Eftersom verksamhetens behov är styrande, utgår behovet från aktuell säkerhetsanalys.

Rikets säkerhet eller skydd mot terrorism

Information som är nödvändig att hålla hemlig med hänsyn till rikets säkerhet eller till skydd mot terrorism är särskilt skyddsvärd. Uppgifter som kan skada enskilda eller allmänna intressen måste hanteras restriktivt och med omsorg.

Skyddsvärda uppgifter

Skyddsvärda uppgifter kan exempelvis vara beredskapsplanering eller viktiga delar av infrastruktur som rör rikets säkerhet eller till skydd mot terrorism. Dessa återfinns bland annat inom elförsörjning, transport, livsmedels- och vattenförsörjning samt inom data- och telekommunikation.

Ytterligare exempel kan vara anläggningars kapacitet och de skyddsåtgärder som vidtagits samt exakta lägesangivningar för anläggningar.

Sammanställning av öppna uppgifter

En sammanställning av öppna uppgifter är i normala fall inte hemlig. Om uppgifterna sammanställts på sådant sätt att ny information framkommer eller kan härledas ur den samlade informationen kan sammanställningen bli hemlig.

De uppgifter som inte bedöms vara skyddsvärda med hänsyn till rikets säkerhet eller till skydd mot terrorism kan ändå vara skyddsvärda för den egna verksamheten. Dessa behandlas normalt i verksamhetens riskanalyser.



Steg 2: Identifiera hot

Med säkerhetsshot menas: spioneri, sabotage, terrorism, kriminalitet med säkerhetsanknytning, infiltration samt teknik som hot.

Spioneri

Spioneri är brott mot rikets säkerhet, som består i att någon med uppsåt att gå främmande makt tillhanda obehörigen anskaffar, befordrar, lämnar eller röjer skyddad uppgift rörande sådana förhållanden, vilkas uppenbarande för främmande makt kan medföra men för rikets säkerhet.

Inhämtning av underrättelser kan ske från främmande makt (underrättelseorganisationer), andra intressenter eller konkurrenter. Det kan även vara illojala medarbetare som anser att de har blivit illa behandlade eller känner sig missnöjda på något sätt.

Målet med inhämtningen är att införskaffa information av politisk, militär, ekonomisk, teknisk eller annan art som ska hemlighållas av nationella säkerhetsskäl.

Sabotage

Sabotage är ett allmänfarligt brott och kännetecknas av att någon förstör eller skadar egendom, som har avsevärd betydelse för samhället. Motiv till sabotage kan vara politiskt, ekonomiskt eller militärt.

Terrorism

Terrorism omfattar handlingar som inkluderar våld eller hot om våld som syftar till att:

- ❑ injaga fruktan hos en befolkning eller befolkningsgrupp,
- ❑ påverka offentliga organ eller mellanstatliga organisationer att agera i en viss riktning samt
- ❑ allvarligt destabilisera eller förstöra de grundläggande politiska, konstitutionella, ekonomiska eller sociala strukturerna i en stat eller i en mellanstatlig organisation.

Målen för terrorhandlingar kan vara nyckelpersoner, viktiga samhällsfunktioner eller byggnader. Exempel på gärningar kan vara gisslantagande, mordbrand, bombattentat, sabotage, kapning av transportmedel, spridande av gift eller smitta.

Även sådana gärningar som kan skada ett väsentligt allmänintresse eller orsaka allvarliga störningar i en stats samhällsfunktioner eller försörjningsmöjligheter omfattas av denna definition av terrorism. Med detta avses viktiga infrastruktursystem som allmänhetens kommunikationsnät och kommunikationsmedel, el- och vattenförsörjning, telekommunikationer, hälso- och sjukvård, radio och TV men även viktiga försörjningsgrenar och industrier samt handelsplatser såsom börser.

Kriminalitet med säkerhetsanknytning

Kriminalitet med säkerhetsanknytning har en direkt koppling till övriga säkerhetshot och kan ses som en metod för att utföra undermåttseffektivitet, sabotage eller terrordåd.

Exempel på kriminalitet som ingår kan vara:

- ❑ hot mot de demokratiska fri- och rättigheterna t.ex. hot mot beslutsfattare, politiker, journalister,
- ❑ dataintrång,
- ❑ tillgänglighetsangrepp (s.k. Denial of Service, DoS),
- ❑ ”stöld” av elektronisk identitet,
- ❑ stöld av passhandling, passerbevis och stämplat,
- ❑ inbrott och stöld från förråd,
- ❑ stöld av högteknologikomponenter samt
- ❑ bombhot.

Infiltration

Infiltration kan ske genom att underrättelseorganisationer eller andra intressenter placerar personer på särskilt viktiga positioner i företag, organisationer eller myndigheter. Infiltration kan vara svårt att upptäcka om personen i fråga endast passivt samlar på sekretessbelagd information som sedan vidarebefordras till någon underrättelseorganisation eller annan intressent.

Teknik som hot

Informations- och kommunikationsteknik, IKT, kan användas för att åstadkomma säkerhetshöjande åtgärder, men kan även innebära ett hot. Man bör därför beakta i vilken typ av utrustning sekretessbelagd information lagras eller kommuniceras. Modern teknik kan avsevärt underlätta för en angripare att genomföra det som beskrivs i ovanstående hot.



Steg 3: Analysera

Sannolikhet

Hur sannolikt är det att de hot som identifierats kan genomföras?
Vad är aktörens avsikt och förmåga?

En aktör kan exempelvis vara främmande stat, terrororganisation, våldsbenägna aktivistorganisationer eller enskilda personer. Avsikten kan vara underrättelseverksamhet, terrorism eller personlig vederköllning.

Med förmåga avses kompetens, tid eller ekonomi för att verkställa hotet.

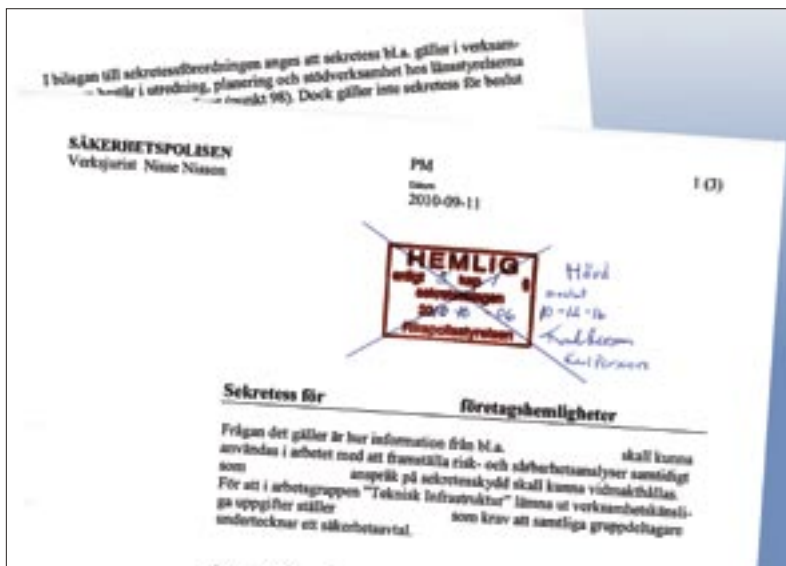
En aktör kan ha en klar och tydlig avsikt men bedömas sakna förmåga att verkställa hot alternativt ha förmåga men sakna avsikt. I båda fallen är sannolikheten för ett fullbordat hot låg. Risken bör bedömas som större i de fall aktören bedöms ha förmåga. Bedöms däremot aktören ha både avsikt och förmåga är sannolikheten för ett fullbordat hot högre.

Kan i verksamheten nyttjad teknik enkelt utnyttjas av en angripare?
Hur skyddas sekretessbelagd information i IT-system och under kommunikation?

Konsekvens

Utifrån den inventering som gjorts av verksamheten fastställs de konsekvenser som ett fullbordat hot kan åstadkomma.

- ❑ Riskeras uppgifter att röjas, ändras eller förstöras?
- ❑ Vilka följdverkningar kan det bli både på kort och lång sikt och då inte enbart ekonomiskt?
- ❑ Klarar verksamheten av sin tilldelade uppgift, ansvar, anseende och förtroende?
- ❑ Vilka men eller vilken skada kan uppstå?
- ❑ Vem eller vilka påverkas av menen eller skadan?
- ❑ Hur lång tid tar det att återskapa eller ersätta uppgiften?



Risk och sårbarhet

Genom att inordna sannolikheterna och konsekvenserna för respektive risk kan en tabell få följande utseende:

Sannolikhet (S)	Konsekvens (K)
Nivå 1 = Osannolikt	Nivå 1 = Betydelselös
Nivå 2 = Mindre sannolikt	Nivå 2 = Låg, viss påverkan på verksamheten eller människors liv eller hälsa
Nivå 3 = Mer sannolikt	Nivå 3 = Hög, stor påverkan på verksamheten eller människors liv eller hälsa
Nivå 4 = Sannolikt	Nivå 4 = Mycket hög, mycket stor påverkan på verksamheten eller människors liv eller hälsa (döda och skadade)

Riskenivå (R) = (S) x (K)

Låg: 1 – 4 kan accepteras

Medel: 6 – 8 åtgärdas snarast

Hög: 9 – 16 åtgärdas omedelbart

Är verksamheten sårbar?

En aktuell dokumentation över vidtagna skyddsåtgärder inom verksamheten är nödvändig. I den bör även framgå vilka säkerhets- skyddsåtgärder som vidtagits mot identifierade hot eller som bedömts som ringa och kan accepteras. I det senaste fallet bör det framgå om det är en risk som är kalkylerad, försumbar eller ekonomiskt försvarbar.

Vilka risker ska åtgärdas?

Finns anledning att revidera eller komplettera åtgärder som ska läggas fram för verksamhetsansvariga för beslut?



Handlings- och åtgärdsplan

När en säkerhetsanalys är genomförd måste en handlings- och åtgärdsplan upprättas.

De risker som säkerhetsanalysen redovisar bör bedömas, prioriteras och åtgärdas i nivåerna omedelbara åtgärder, åtgärder på kort sikt (till exempel ett år) och åtgärder på lång sikt (till exempel tre år). Investeringar för att höja säkerhetsskyddet bör planeras i kommande budgetarbete.

Omedelbara åtgärder

Visar säkerhetsanalysen att risknivån är hög bör åtgärder omedelbart vidtas. Både tillfälliga och varaktiga lösningar bör beaktas.

Åtgärder på kort sikt

Om risknivån är på medelnivå, kan åtgärderna planeras och utföras inom en inte för avlägsen framtid.

Åtgärder på lång sikt

Är risknivån låg kan åtgärderna utföras under en längre tid.

Exempel på åtgärder

Säkerhetsprövning och registerkontroll

Personal som enligt säkerhetsanalysen arbetar med hemliga uppgifter ska genomgå säkerhetsprövning och eventuell registerkontroll.

Säkerhetsprövning görs vid nyanställningar och fortlöpande.

Utbildning

En grundläggande förutsättning för ett effektivt säkerhetsskydd är att all personal får nödvändig utbildning i ämnet. Utbildning i säkerhetsskydd ska främst syfta till att klargöra varför och hur man ska vidta skyddsåtgärder mot hot av olika slag. Varje myndighet och företag som omfattas av säkerhetsskyddslagstiftningen ska anordna utbildning efter eget behov.

Den fortlöpande säkerhetsskyddsutbildningen kan anpassas och riktas mot utvald målgrupp. Exempel på målgrupper är chefer och säkerhetsansvariga samt personal som arbetar inom IT, rekrytering och inköp.

En utbildningsplan bör upprättas och dokumentation ska finnas över den personal som genomgått utbildning.

Redundans och reservfunktioner

En bedömning måste göras av vilka verksamheter som kräver redundans och reservfunktioner.

Skyddsåtgärder

Åtgärder som kan införas med kort varsel kan inkludera följande:

- Revidera den egna säkerhetsorganisationen.
- Höj säkerhetsnivån i passersystem genom att kräva både kort och kod, till exempel vid entréer.
- Byt lösenord för IT-system. Kräv svårare lösenord och kortare giltighetstid. Testa lösenord med programvara.
- Granska och följ upp loggning från IT- och passersystem.
- Inför eller se över bevakningsplan och larmfunktioner.

Säkerhetspolisens fem verksamhetsgrenar

Kontraspionage innebär att förebygga och avslöja spioneri och olovlig underrättelseverksamhet samt flyktingspionage. Inom kontraspionage bedrivs även arbete för att minska risken för spridning av massförstörelsevapen.

Kontraterroism innebär att förhindra att terrorbrott begås i Sverige eller utomlands.

Författningsskydd innebär att förebygga och avslöja brottslig verksamhet som hotar våra demokratiska institutioner eller medborgerliga fri- och rättigheter.

Säkerhetsskydd innebär att genom rådgivning och kontroll bidra till en ökad säkerhetsnivå i samhället i syfte att skydda rikets säkerhet och bekämpa terrorism.

Personskydd innebär bevaknings- och säkerhetsarbete som avser den centrala statsledningen, kungafamiljen och utländsk diplomatisk personal samt vid statsbesök och liknande händelser.

Läs mer på www.sakerhetspolisen.se



Säkerhetspolisen

Rikspolisstyrelsen • Box 8304 • 104 20 Stockholm • 08-401 90 00
e-post: sakerhetspolisen@sakerhetspolisen.se • www.sakerhetspolisen.se